Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

Introducción a la teoría de Galois diferencial

Autor: Miguel Valderrama de las Heras

Tutor: Manuel Mariano Carnicer Arribas

Curso 2022-2023

Índice

0. Resumen e introducción

0.1. Resumen y abstract

RESUMEN. En este trabajo intentamos entender la *teoría de Galois diferencial* y su analogía con la teoría de Galois clásica. En el primer capítulo, introducimos la idea de *derivación* y ampliamos los conceptos algebraicos al caso diferencial (ideales diferenciales, morfismos diferenciales, etc.). En el segundo estudiamos los *isomorfismos admisibles* y vemos varios resultados relacionados con estos, que serán necesarios más adelante. En el tercer capítulo, se introduce la teoría de Galois diferencial y las *extensiones de Picard-Vessiot*, con un papel similar al de los cuerpos de descomposición de la teoría clásica, y se dan los resultados habituales en términos diferenciales. En el cuarto capítulo se hace un repaso de la idea de conjunto algebraico y la topología de Zariski y se introducen los *grupos algebraicos*, que relacionaremos con el *grupo de Galois diferencial* de las extensiones de Picard-Vessiot en el capítulo cinco. En este último capítulo, se dan los pasos finales hasta llegar al objetivo del trabajo: el *teorema fundamental de la teoría de Galois diferencial*, análogo al teorema fundamental de la teoría de Galois clásica.

ABSTRACT. In this project we aim to understand the *differential Galois theory* and its analogy to classic Galois theory. In the first chapter, we introduce the idea of *derivation* and extend algebraic concepts to the differential case (differential ideals, differential morphisms, etc.). In the second chapter, we study *admissible isomorphisms* and explore various related results that will be necessary later on. The third chapter introduces differential Galois theory and *Picard-Vessiot extensions*, which play a similar role to splitting fields in classical theory, and presents the usual results in differential terms. The fourth chapter provides an overview of the notion of algebraic set and Zariski topology, and introduces *algebraic groups*, which we will relate to the *differential Galois group* of Picard-Vessiot extensions in the fifth chapter. In this last chapter, we present the final steps to reach the project's goal: the *fundamental theorem of differential Galois theory*, analogous to the fundamental theorem of classical Galois theory.

0.2. Introducción

Desde la antigüedad se ha planteado el problema de la resolución de ecuaciones algebraicas. La solución de la ecuación de segundo grado y, más adelante, la de tercer y cuarto grado, ya se había encontrado mediante métodos geométricos antes del siglo XVII. El desarrollo del análisis matemático durante estos años permitió refinar estas soluciones, pero la ecuación de quinto grado parecía escaparse de su alcance. No fue hasta el año 1822 que Niels Henrik Abel (1802-1829) consigue demostrar el resultado que hoy todos conocemos: no es posible encontrar una fórmula general para resolver la ecuación de quinto grado por radicales, es decir, con un número finito de operaciones algebraicas.

En este contexto, Evariste Galois (1811-1831), en su efímera pero prolífera labor investigadora, consiguió relacionar este hecho con el comportamiento de ciertos grupos de permutaciones. Es entonces cuando nace la *teoría de Galois* que, tras ser estudiada y refinada a lo largo de los años, es de gran importancia hoy en día y permite abordar el problema de la resolución de ecuaciones algebraicas mediante métodos algebraicos.

Durante los siglos XIX y XX, la atención pasa a las ecuaciones diferenciales. Emile Picard (1856-1941) y su alumno de tesis Ernest Vessiot (1865-1952) intentan abordar este problema desde la teoría de Galois, adaptando sus resultados a este nuevo caso y desarrollando así la *teoría de Galois diferencial* que intentamos introducir en este trabajo. El objetivo va a ser dar los primeros pasos para comprender esta tería que permite buscar la existencia de soluciones a las ecuaciones diferenciales por técnicas algebraicas análogas a las empleadas por la teoría de Galois clásica con las ecuaciones algebraicas.

Para el desarrollo del trabajo hemos seguido principalmente la introducción al álgebra diferencial que hace Irving Kaplansky en [3], aunque también hemos consultado habitualmente y utilizado alguna idea de [7] y, para lo referente a conjuntos algebraicos y topología de Zariski, nos hemos apoyado en [2]. Empezaremos añadiendo una noción de *derivación* a nuestras estructuras algebraicas y extendiendo ciertos conceptos algebraicos, como el de *ideal* o *morfismo*, al caso diferencial. Luego iremos desarrollando la teoría de Galois en estos nuevos términos diferenciales y, tras relacionar estos resultados con el concepto de *grupo algebraico* introducido en el cuarto capítulo del trabajo, veremos un último capítulo en el que se alcanza el *teorema fundamental de la teoría de Galois diferencial*, que es el objetivo de este trabajo.

1. Anillos e ideales diferenciales

Durante todo el trabajo, los anillos que manejaremos serán siempre anillos conmutativos con unidad.

1.1. Derivaciones

Definición. Una *derivación* en un anillo A es una aplicación $D : A \longrightarrow A$ tal que:

(D1) $D(a+b) = D(a) + D(b)$

(D2) $D(ab) = D(a)b + aD(b) \qquad \forall a, b \in A.$

Escribiremos $D(a) = a'$, $D(a') = a''$ y, en general, $D(a^{(n-1)}) = a^{(n)}$ (por convenio, $a = a^{(0)}$). A un anillo con una derivación definida en él lo llamaremos *anillo diferencial*.

***Nota* 1.1.** $0' = (0+0)' = 0' + 0' \implies 0' = 0$

$1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1' = 1' + 1' \implies 1' = 0$

En general, $(n \cdot 1)' = n \cdot 1' = 0 \ \forall n \in \mathbb{Z}$, donde si $a \in A$ y $n \in \mathbb{Z}$, "$n \cdot a$" representa:

$$n \cdot a = \begin{cases} 0 & \text{si } n = 0 \\ a + \cdots + a \ (n \text{ veces}) & \text{si } n > 0 \\ -(a + \cdots + a) \ (-n \text{ veces}) & \text{si } n < 0 \end{cases}$$

Como consecuencia, la única derivación posible en $\mathbb{Z}$ es la derivación trivial ($n' = 0$ $\forall n \in \mathbb{Z}$).

Si $a \in A$ es una unidad, entonces, derivando en $1 = aa^{-1}$, deducimos que:

$$0 = (aa^{-1})' = a'a^{-1} + a(a^{-1})' \implies (a^{-1})' = -a^{-1}a'a^{-1} = -a'a^{-2}.$$

Por inducción en n, podemos ver que si $a \in A$, $(a^n)' = n \cdot a^{n-1} \cdot a' \ \forall\, n \in \mathbb{N}$. El caso $n = 1$ es inmediato y, si lo suponemos cierto para $n-1$, tenemos que:

$$(a^n)' = (a \cdot a^{n-1})' = a' \cdot a^{n-1} + a \cdot (a^{n-1})' = a' \cdot a^{n-1} + a\dot{(}n-1) \cdot a^{n-2} \cdot a' =$$

$$= a^{n-1} \cdot a' + (n-1) \cdot a^{n-1} \cdot a' = n \cdot a^{n-1} \cdot a'.$$

Teorema 1.2. *Una derivación definida en un dominio de integridad A se extiende de forma única a su cuerpo de fracciones $Fr(A)$.*

Demostración. Sean $a, b \in A$, entonces definimos

$$\left(\frac{a}{b}\right)' = \frac{a'b - ab'}{b^2}$$

y la unicidad de la expresión es evidente ya que se deduce de las propiedades de la derivación de A:

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

Veamos ahora que esta expresión no depende del representante elegido para un elemento de $Fr(A)$. Si $a, b, c, d \in A$ son tales que $ad = cb$, derivando en esta expresión deducimos que

$$(ad)' = (cb)' \implies a'd + ad' = c'b + cb' \implies a'd - cb' = c'b - ad' \implies \frac{a'd - cb'}{bd} = \frac{c'b - ad'}{bd}$$

$$\implies \frac{a'd - cb'}{bd} \cdot \left(\frac{b}{b}\right) = \frac{c'b - ad'}{bd} \cdot \left(\frac{d}{d}\right) \implies \frac{a'b - ab'}{b^2} = \frac{c'd - cd'}{d^2}.$$

Finalmente comprobamos que esta expresión define efectivamente una derivación en $Fr(A)$.

(D1)

$$\left(\frac{a}{b} + \frac{c}{d}\right)' = \left(\frac{ad + cb}{bd}\right)' = \frac{(ad + cb)'(bd) - (ad + cb)(bd)'}{(bd)^2} =$$

$$= \frac{(a'd + ad' + c'b + cb')bd - (ad + cb)(b'd + bd')}{b^2d^2} = \frac{(a'b - ab')d^2 + (c'd - cd')b^2}{b^2d^2} =$$

$$= \frac{a'b - ab'}{b^2} + \frac{c'd - cd'}{d^2} = \left(\frac{a}{b}\right)' + \left(\frac{c}{d}\right)'$$

(D2)

$$\left(\frac{ac}{bd}\right)' = \frac{(ac)'(bd) - (ac)(bd)'}{(bd)^2} = \frac{(a'c + ac')bd - ac(b'd + bd')}{b^2d^2} =$$

$$= \frac{a'bcd - ab'cd + abc'd - abcd'}{b^2d^2}$$

$$\left(\frac{a}{b}\right)'\left(\frac{c}{d}\right) + \left(\frac{a}{b}\right)\left(\frac{c}{d}\right)' = \frac{a'b - ab'}{b^2} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{c'd - cd'}{d^2} = \frac{a'bcd - ab'cd + abc'd - abcd'}{b^2d^2}.$$

□

***Nota* 1.3.** Se deduce, siguiendo la Nota 1.1, que la única derivación posible en $\mathbb{Q} = Fr(\mathbb{Z})$ es también la trivial.

***Ejemplos* 1.4.** 1) Cualquier anillo puede considerarse diferencial definiendo en él la derivación trivial.

2) El anillo $\mathscr{C}^\infty(\mathbb{R})$ de las funciones infinitamente derivables con la derivada usual es evidentemente un anillo diferencial, pero no es un dominio, ya que dos funciones no idénticamente nulas pueden dar la función nula al multiplicarlas. Sin embargo, el anillo de las funciones complejas enteras, debido al carácter aislado de sus ceros, sí es un dominio y esta derivada puede por tanto extenderse a su cuerpo de fracciones (el de las funciones meromorfas).

3) Dado un anillo diferencial A, podemos definir una derivada en el anillo de polinomios con coeficientes en A, $A[X]$, asignando un valor cualquiera a X' en $A[X]$, respetando siempre que $(X^n)' = nX^{n-1}X'$ y extendiendo la derivada a un polinomio cualquiera $a_0+a_1X+\cdots+a_nX^n$ siguiendo las reglas (D1) y (D2) para la derivada de las sumas y productos. Si A es un dominio, esta derivada podrá por tanto extenderse a una en el cuerpo de fracciones de polinomios $A(X) = Fr(A[X])$. Observamos que si definimos $X' = 1$, obtenemos la derivada usual en un anillo de polinomios $A[X]$ (por ejemplo, en $\mathbb{Z}[X]$). Sin embargo, podemos definir $X' = a$ para cualquier $a \in A$ y se obtiene una derivación válida, si se extiende de forma adecuada a un polinomio cualquiera. Si en $\mathbb{Z}[X]$ consideramos la derivada usual y tomamos $Y = nX$ con $n \in \mathbb{Z}$, entonces $Y' = nX' = n$ y la derivada que se induce en $\mathbb{Z}[Y]$ es la determinada por $Y' = n$. Más aún, podemos definir $X' = P$ siendo P un polinomio cualquiera en $A[X]$. Consideramos $Y = e^t$ con la derivada usual. Dado que e es trascendente sobre $\mathbb{Z}$, se tiene que $\mathbb{Z}[Y]$ es isomorfo a $\mathbb{Z}[e^t]$ y dado que $(e^t)' = e^t$, obtenemos un anillo de polinomios isomorfo a $Z[Y]$ en el que $Y' = Y$.

4) De la misma forma, podemos dotar a $A[X_1, X_2, \ldots, X_n]$ de una estructura diferencial asignando valores arbitrarios a la derivada de cada indeterminada. Por ejemplo, si en $\mathbb{Z}[\cosh(t), \sinh(t)]$ consideramos la derivada usual, obtenemos un anillo diferencial en el que $X' = Y$ e $Y' = X$. Sin embargo, este anillo no es isomorfo al anillo de polinomios en dos variables habitual ya que si $X = \cosh(t)$, $Y = \sinh(t)$, entonces se tiene la identidad $X^2 - Y^2 = 1$ (el conjunto $\{\cosh(t), \sinh(t)\}$ no es trascendente sobre $\mathbb{Z}$).

5) Dado un anillo diferencial A, consideramos el anillo de polinomios con infinitas indeterminadas, $A[X_0, X_1, X_2, \ldots] = A[X_i]$. Definimos en él una derivación considerando $X_i' = X_{i+1}$ para cada $i = 0, 1, 2, \ldots$ Denotamos $X_0 = X$, $X_n = X^{(n)}, n \geq 1$. A este proceso lo llamamos *adjunción de una indeterminada diferencial*, denotamos por $A\{X\}$ al anillo diferencial obtenido y a sus elementos los llamamos *polinomios*

diferenciales. Si A es un cuerpo diferencial (es suficiente con que sea dominio diferencial), $A\{X\}$ es un dominio diferencial y por tanto podemos extender de forma única esta estructura diferencial a su cuerpo de fracciones $Fr(A\{X\})$ que denotaremos $A\langle X\rangle$.

Sabemos que dada una extensión (clásica) de cuerpos $L|K$ (es decir, $K \subset L$ son dos cuerpos tales que la estructura de cuerpo de K se obtiene por restricción de la de L) y un elemento $\alpha \in L$, el cuerpo $K(\alpha) = Fr(K[\alpha])$ era la menor extensión de K que contenía a α. Sin embargo, si $L|K$ es una extensión diferencial de cuerpos ($L|K$ es una extensión de cuerpos diferenciales y la derivación de K se obtiene por restricción de la de L) y $\alpha \in L$, $K(\alpha)$ no tiene por qué ser una extensión diferencial. Por ejemplo, si consideramos $\mathbb{R}(sin(X), cos(X))|\mathbb{R}$ con la derivada usual, es decir, $sin(X)' = cos(X)$, $cos(X)' = -sin(X)$, entonces es una extensión diferencial y $\mathbb{R}(sin(X))$ es un cuerpo intermedio de la extensión, pero no es diferencial. El método para construir la menor extensión diferencial que contiene a K y a un elemento α es el explicado en este último apartado de los ejemplos, considerando $K\langle\alpha\rangle = K(\alpha, \alpha', \alpha'', \dots)$.

Proposición 1.5. *Sea A un anillo diferencial y $C = \{a \in A : a' = 0\}$. Entonces C es un subanillo de A. Si A es un cuerpo, entonces C es un cuerpo. Llamaremos a C el anillo (o cuerpo) de constantes.*

Demostración. Basta ver que $1 \in C$, y que $\forall a, b \in C$, $a - b \in C$ y $ab \in C$. Ya vimos antes que $1' = 0$. Ahora, si $a' = b' = 0$, entonces,

$$(a - b)' = a' - b' = 0 \quad \text{y} \quad (ab)' = a'b + ab' = 0 + 0 = 0.$$

Para ver que si A es cuerpo, también lo es C, solo falta ver que en este caso, si $a \in C$, $a \neq 0$, su inverso para el producto, $a^{-1} \in A$, también está en C, y esto es inmediato ya que si $a' = 0$, entonces $(a^{-1})' = -a'a^{-2} = 0$. □

1.2. Ideales y morfismos diferenciales

Definición. Sea I un ideal en un anillo diferencial A. Diremos que I es un *ideal diferencial* si $I' \subset I$, es decir, $a' \in I \ \ \forall a \in I$.

Podemos definir trivialmente una derivada en el cociente A/I dada por $(a+I)' = a'+I$. Para empezar, esta aplicación, que después veremos que es una derivación, está bien definida ya que $a + I = b + I \iff a - b \in I \implies (a - b)' = a' - b' \in I \iff a' + I = b' + I$.

Además en esta cadena de implicaciones se observa por qué es necesario que el ideal I sea diferencial para asegurar que la derivada de A induce en el cociente una aplicación bien definida.

Finalmente, esta aplicación es de hecho una derivada:

(D1) $\big((a+I)+(b+I)\big)' = \big((a+b)+I\big)' = (a+b)'+I = (a'+b')+I = (a'+I)+(b'+I)$
$= (a+I)'+(b+I)'$

(D2) $\big((a+I)(b+I)\big)' = (ab+I)' = (ab)'+I = (a'b+ab')+I = (a'+I)(b+I)+(a+I)(b'+I)$

Definición. Decimos que un homomorfismo entre dos anillos diferenciales $f : A \longrightarrow B$ es un *homomorfismo diferencial* si cumple que $f(a') = f(a)' \ \ \forall a \in A$. Se define de igual modo un *automorfismo diferencial* o un *isomorfismo diferencial*.

De forma similar al caso clásico en el que un morfismo de $K(\alpha)$ sobre K (es decir, que deja fijos los elementos de K) viene determinado por la imagen de α, en el caso diferencial, un morfismo diferencial de $K\langle\alpha\rangle$ sobre K queda unívocamente determinado por la imagen de α, ya que la imagen de sus derivadas queda fijado por el carácter diferencial de dicho morfismo. Concretamente, dar un morfismo de $K\langle\alpha\rangle$ sobre K dando la imagen de α y pidiendo que dicho morfismo sea diferencial equivale a dar un morfismo de $K(\alpha, \alpha', \dots)$ sobre K dando la imagen de α y cada una de sus derivadas, lo cual lo determina unívocamente.

***Nota* 1.6.** El morfismo identidad definido en un anillo diferencial es siempre diferencial: $id(a') = a' = id(a)'$.

La composición de morfismos diferenciales es nuevamente un morfismo diferencial, puesto que $f(g(a')) = f(g(a)') = f(g(a))'$.

El inverso de un isomorfismo diferencial f es también diferencial ya que derivando en $f(f^{-1}(a)) = a$, obtenemos $f(f^{-1}(a))' = f(f^{-1}(a)') = a'$ y aplicando f^{-1} concluimos que $f^{-1}(a)' = f^{-1}(a')$.

Teorema 1.7. *Sea A un anillo diferencial y sea I el núcleo de un homomorfismo diferencial f definido en A. Entonces I es un ideal diferencial en A y A/I es diferencialmente isomorfo a la imagen de A, $f(A)$.*

Demostración. Sabemos por resultados conocidos de álgebra clásica que I es un ideal y que la aplicación $\varphi : A/I \longrightarrow f(A)$ dada por $\varphi(a+I) = f(a)$ define un ismomorfismo entre

A/I y $f(A)$. Basta por tanto demostrar que el ideal I y el isomorfismo φ son diferenciales.

Para empezar, si $a \in I$, es decir, $f(a) = 0$, entonces al ser f un homomorfismo diferencial se tiene que $f(a') = f(a)' = 0' = 0$, luego $a' \in I$. Por otro lado, si $a \in A$, entonces $\varphi\big((a+I)'\big) = \varphi(a'+I) = f(a') = f(a)' = \varphi(a+I)'$. □

Lema 1.8. *Sea I un ideal radical y diferencial y $a, b \in A$ con $ab \in I$. Entonces $a'b \in I$ y $ab' \in I$ (un ideal I es radical si $x^n \in I$ para algún $n \in \mathbb{N} \implies x \in I$).*

Demostración. Como I es diferencial, $ab \in I \implies (ab)' = a'b + ab' \in I$. Multiplicando por ab' tenemos que $(a'b + ab')ab' = (ab)a'b' + (ab')^2 \in I$. Puesto que $(ab)a'b' \in I$, se tiene que $(ab')^2 \in I$ y por ser I radical, esto implica que $ab' \in I$ como queríamos ver. Para probar que $a'b \in I$, multiplicamos por $a'b$ en vez de por ab' y repetimos el razonamiento. □

Lema 1.9. *Sea A un anillo diferencial, I un ideal radical diferencial de A y $S \subset A$ un subconjunto cualquiera. Sea $J = \{x \in A : xS \subset I\}$. Entonces J es un ideal radical diferencial de A (recordemos que si $x \in A$, entonces $xS = \{xs : s \in S\}$).*

Demostración. Empecemos probando que J es un ideal. Sean $a, b \in J$ y $\lambda, \mu \in A$. Sea $s \in S$, entonces $(\lambda a + \mu b)s = \lambda(as) + \mu(bs) \in I$, luego $\lambda a + \mu b \in J$.

Veamos que es diferencial. Sea $a \in J$, $\forall s \in S$, por ser I radical y diferencial, como $as \in I$, el Lema anterior nos asegura que $a's \in I$, luego $a' \in J$.

Finalmente, veamos que J es radical. Sea $a \in A$ y $n \in \mathbb{N}$ tal que $a^n \in J$. Entonces, $\forall s \in S$, $a^n s \in I \implies (a^n s)s^{n-1} = (as)^n \in I$ y por ser I radical, se tiene que $as \in I$, luego $a \in J$. □

Es un resultado conocido que la intersección cualquiera de ideales es un ideal, y que, si estos son radicales, también lo es su intersección. Por otra parte, si $\{I_i\}_{i\in\Lambda}$ es una familia de ideales diferenciales y $a \in \cap_{i\in\Lambda} I_i$, para cada $i \in \Lambda$, por ser I_i diferencial, se tiene que $a \in I_i \implies a' \in I_i$, luego $a' \in I_i$, $\forall i \in \Lambda \implies a' \in \cap_{i\in\Lambda} I_i$ y observamos que la propiedad diferencial también se mantiene al intersecar ideales. Por tanto, dado un subconjunto cualquiera S de A, existe un único ideal radical diferencial que contiene a S, minimal para la contención, dado por la intersección de todos los ideales radicales diferenciales que contienen a S, y que denotamos $\{S\}$.

Lema 1.10. *Sea A un anillo diferencial:*

i) Sean $a \in A$, $S \subset A$. Entonces $\{S\}a \subset \{Sa\}$.

ii) Sean $S, T \subset A$. Entonces $\{S\}\{T\} \subset \{ST\}$.

Demostración. *i)* El *Lema 1.9* garantiza que $\{x \in A : xa \in \{Sa\}\}$ es un ideal radical diferencial y contiene a S ya que, evidentemente, $sa \in Sa \subset \{Sa\}\, \forall s \in S$. Entonces contiene también a $\{S\}$ por ser este el menor ideal radical diferencial que contiene a S.

ii) Nuevamente, por el *Lema 1.9*, $\{x \in A : x\{T\} \in \{ST\}\}$ es un ideal radical diferencial y por el apartado *i)*, para todo $s \in S$, $s\{T\} \subset \{sT\} \subset \{ST\}$, luego contiene a S y por tanto a $\{S\}$.

□

Dado un ideal diferencial I, podríamos pensar que, al ser I diferencial, su radical $\sqrt{I}$ (el menor ideal radical que lo contiene) coincide con $\{I\}$, pero eso no es necesariamente cierto. El radical de un ideal I dado se obtiene considerando todos los elementos $x \in A$ con $x^n \in I$ para algún $n \in \mathbb{N}$. Al añadir estos elementos al ideal de partida, puede ocurrir que el resultado no sea un ideal diferencial.

***Ejemplo* 1.11.** Consideramos el anillo de polinomios sobre el cuerpo de dos elementos, $\mathbb{F}_2$, con la relación $x^2 = 0$ y definimos en él una derivada fijando $x' = 1$. Entonces el ideal (0) es evidentemente diferencial, pero su radical (que llamamos el nilradical del anillo) es el ideal generado por x y no es diferencial, pues $x' = 1$ no es nilpotente ($1^n \neq 0 \forall n \in \mathbb{N}$).

1.3. Álgebras de Ritt

Definición. Un *álgebra de Ritt* es un anillo diferencial que contiene al cuerpo de los números racionales, $\mathbb{Q}$. Concretamente, un álgebra de Ritt es un álgebra sobre $\mathbb{Q}$.

***Nota* 1.12.** Cualquier cuerpo K de característica 0 es un álgebra de Ritt. Si consideramos $n_K = n \cdot 1_K$ (como en la Nota 1.1) para cada $n \in \mathbb{Z}$, como la característica de K es 0, $n_K \neq 0\ \forall n \in \mathbb{Z} \setminus \{0\}$, y como K es un cuerpo, esto implica que n_K es unidad y, por tanto, $1/n_K \in K\ \forall n \in \mathbb{Z} \setminus \{0\}$. Dado que $(n+m)_K = n_K + m_K$ y $(nm)_K = n_K m_K$, se deduce que $nq = pm \implies n_K q_K = p_K m_K$, luego $\frac{n}{m} = \frac{p}{q} \implies \frac{n_K}{m_K} = \frac{p_K}{q_K}$. Se deduce fácilmente que, efectivamente, el conjunto $\{\frac{n_K}{m_K} : n, m \in \mathbb{Z}, m \neq 0\}$ es un subcuerpo de K isomorfo a $\mathbb{Q}$.

***Nota* 1.13.** Como vimos anteriormente, $\mathbb{Q}$ estará contenido en el subanillo de constantes de cualquier álgebra de Ritt.

Lema 1.14. *En un álgebra de Ritt A, sea I un ideal diferencial y sea $a \in A$. Si para algún $n \in \mathbb{N}$, $a^n \in I$, entonces $(a')^{2n-1} \in I$.*

Demostración. Veamos por inducción sobre $1 \leq k \leq n$ que $a^{n-k}(a')^{2k-1} \in I$. Para $k = 1$, $(a^n)' = na^{n-1}a' \implies na^{n-1}a' \in I$ porque I es diferencial. Al ser A un álgebra de Ritt, $1/n \in A$, luego $(1/n) \cdot (na^{n-1}a') = a^{n-1}a' \in I$. Supongamos ahora el resultado cierto para k, es decir, $a^{n-k}(a')^{2k-1} \in I$, con $1 \leq k \leq n-1$. Entonces:

$$(a^{n-k}(a')^{2k-1})' = (n-k)a^{n-k-1}(a')^{2k} + (2k-1)a^{n-k}(a')^{2k-2}a'' \in I$$

Multiplicando esta expresión por a', obtenemos que

$$(n-k)a^{n-k-1}(a')^{2k+1} + (2k-1)a^{n-k}(a')^{2k-1}a'' \in I$$

Como el segundo sumando está en I por hipótesis de inducción, el primero también lo está, y multiplicando por $1/(n-k) \in A$, obtenemos la expresión buscada para el caso $k+1$. En el último caso, $k = n$, tenemos $(a')^{2n-1} \in I$ como buscábamos. □

Corolario 1.15. *Como consecuencia, en un álgebra de Ritt, el radical de un ideal diferencial es diferencial.*

Demostración. Si $a \in \sqrt{I}$ con I diferencial, es decir, $a^n \in I$ para algún $n \in \mathbb{N}$, entonces hemos visto que $(a')^{2n-1} \in I$, es decir, $a' \in \sqrt{I}$. □

2. Extensión de isomorfismos

2.1. Extensión de ideales

Vamos a ver varios resultados sobre extensión de ideales e isomorfismos e introduciremos el concepto de isomorfismo admisible.

Sabemos que un ideal radical es la intersección de todos los ideales primos que lo contienen. Veamos que un ideal radical diferencial es, a su vez, la intersección de todos los ideales primos diferenciales que lo contienen.

Lema 2.1. *Sea A un anillo diferencial y $T \subset A$ un subconjunto multiplicativamente cerrado. Sea Q un ideal radical diferencial maximal para la exclusión de T, es decir, $Q \cap T = \emptyset$ y, si $I \supset Q$, es otro ideal radical diferencial, entonces $I \cap T \neq \emptyset$. Entonces Q es primo.*

Demostración. Supongamos que, por el contrario, $a, b \in A$ son tales que $a, b \notin Q$ pero $ab \in Q$. Entonces $\{Q, a\}$ y $\{Q, b\}$ son dos ideales radicales diferenciales que contienen estrictamente a Q luego existen $t_a, t_b \in T$ con $t_a \in \{Q, a\}$ y $t_b \in \{Q, b\}$ por la definición de Q. Entonces, $t_a t_b \in T$ por ser T multiplicativamente cerrado y $t_a t_b \in \{Q, a\}\{Q, b\}$. Vamos a denotar por $Q_a = Q \cup \{a\}$ y $Q_b = Q \cup \{b\}$ para facilitar la notación. Observemos que, por el Lema 1.10, $\{Q, a\}\{Q, b\} = \{Q_a\}\{Q_b\} \subset \{Q_a Q_b\}$. Además, observemos que $Q_a Q_b = \{xy : x \in Q_a, y \in Q_b\}$, luego si $x \in Q_a$ e $y \in Q_b$, hay dos opciones: si x o $y \in Q$, entonces $xy \in Q$, si no, $x = a$ e $y = b$, luego $xy = ab \in Q$, así que $Q_a Q_b \subset Q$. Entonces, $\{Q_a\}\{Q_b\} \subset \{Q_a Q_b\} \subset \{Q\} = Q$, luego $t_a t_b \in Q \cap T = \emptyset$, absurdo. □

Teorema 2.2. *Todo ideal radical diferencial I de un anillo diferencial A es la intersección de los ideales primos diferenciales que lo contienen.*

Demostración. Solo hay que ver que esta intersección de ideales está contenida en I, ya que la contención contraria es obvia. En otras palabras, hay que ver que si un elemento $x \in A$ no está en I, existe un ideal primo diferencial Q que contiene a I y que no contiene a x.

Sea entonces $x \in A \setminus I$ (asumimos $I \neq A$ ya que, en tal caso, el resultado es trivial) y sea $T = \{x^n : n \in \mathbb{N}\}$, que es un subconjunto multiplicativamente cerrado de A. Sea Γ el conjunto de los ideales radicales diferenciales de A que contienen a I y no cortan a T ($\Gamma \neq \emptyset$ porque $I \in \Gamma$). Sea $S \subset \Gamma$ una cadena de ideales de Γ, es decir, un subconjunto de Γ totalmente ordenado. Entonces $J_0 = \cup_{J \in S} J$ es una cota superior de la cadena en Γ. Efectivamente, sabemos que J_0 es un ideal que contiene a cada uno de los ideales de S y, por tanto, es una cota superior de la cadena y contiene a I. Además,

$J_0 \cap T = (\cup_{J \in S} J) \cap T = \cup_{J \in S}(J \cap T) = \emptyset$. Falta comprobar que J es también un ideal radical diferencial. Si $a \in A$ y $a^n \in J_0$ para algún $n \in \mathbb{N}$, existe $J \in S$ tal que $a^n \in J$ y, como J es radical, $a \in J$, luego $a \in J_0$, es decir, J_0 es un ideal radical. Además, si $b \in J_0$, existe $J \in S$ tal que $b \in J$, luego $b' \in J$ por ser este un ideal diferencial, así que $b' \in J_0$, luego J_0 es también un ideal diferencial, es decir, $J_0 \in \Gamma$ es una cota superior de la cadena en Γ. Como toda cadena de Γ admite una cota superior en Γ, podemos aplicar el Lema de Zorn y concluir que existe un elemento maximal Q en Γ, es decir, Q es un ideal radical diferencial que contiene a I y es maximal para la exclusión de T. Por el Lema 2.1, Q es un ideal primo y, además, como $Q \in \Gamma$, es un ideal primo diferencial que contiene a I y no a x. □

Teorema 2.3. *Sea $A \subset B$ una extensión de anillos diferenciales, es decir, A y B son dos anillos diferenciales con $A \subset B$ tales que, tanto la estructura de anillo de A, como su derivación, son exactamente la restricción de las de B a los elementos de A. Sea $I \subset B$ un ideal radical diferencial de B.*

i) Si $P = I \cap A$ es un ideal primo diferencial de A, entones existe un ideal primo diferencial Q de B con $I \subset Q$ y $Q \cap A = P$, es decir, I se puede extender a un ideal primo diferencial de B que también se contrae en P al intersecar con A.

ii) Si I cumple que, para todos $a \in A$ y $b \in B$ tales que $ab \in I$ se tiene que $a \in I$ o $b \in I$ (y por tanto, $P = I \cap A$ es un ideal primo diferencial de A), entonces I es la intersección de todos los ideales primos diferenciales de B que lo contienen y que se contraen en P al intesecarlos con A.

Demostración. Observemos primero que, por ser I un ideal radical diferencial de B y A un subanillo diferencial de B, $P = I \cap A$ es inmediatamente un ideal radical diferencial de A, ya que, además de ser un ideal (resultado conocido), si $a \in P$ y $b^n \in P$ para ciertos $a, b \in A$ y $n \in \mathbb{N}$, por ser I un ideal radical diferencial, $a', b \in I$ y, por ser A un anillo diferencial, $a', b \in A$, luego $a', b \in P$.

i) Sea $T = A \setminus P \subset B$. Por ser P primo, T es multiplicativamente cerrado. De la misma forma que en la demostración anterior, existe un ideal radical diferencial Q en B que contiene a I y es maximal para la exclusión de T. Esta última propiedad implica que $Q \cap A \subset P$, ya que $Q \cap T = \emptyset$ y, como $P \subset I \subset Q$, se tiene que $Q \cap A = P$. Además, por el Lema 2.1, Q es un ideal primo diferencial.

ii) Primero vamos a probar la afirmación que aparece entre paréntesis, es decir, que $P = I \cap A$ es un ideal primo diferencial. Ya sabemos que es un ideal radical diferencial.

Además, si $a, b \in A$ son tales que $ab \in P \subset I$, como $b \in A \subset B$, por hipótesis, $a \in I$ (luego $a \in I \cap A = P$) o $b \in I$ (luego $b \in I \cap A = P$), es decir, P es primo.

Ahora, al igual que en el teorema anterior, solo nos hace falta probar que la intersección de todos los ideales primos diferenciales de B que contienen a I y cuya intersección con A es P, está contenida en I, ya que la contención contraria es obvia. Sea $x \in B$ con $x \notin I$ (nuevamente, asumimos que $I \neq B$ ya que, en tal caso, el resultado es trivial), veamos que existe un ideal primo diferencial Q de B que contiene a I pero no a x y tal que $Q \cap A = P$. Sea $T = \{ax^n : a \in A \setminus P, n \in \mathbb{N}\}$, que es multiplicativamente cerrado por serlo $A \setminus P$ al ser P primo y contiene a x ya que, por ser $I \neq B$, se tiene que $1 \in B \setminus I$, luego $1 \in A \setminus P$. Además, $T \cap I = \emptyset$, ya que si se tuviera $ax^n \in I$ con $a \in A \setminus P$ ($a \notin I$), entonces, por hipótesis, $x^n \in I$, luego se tendría $x \in I$ por ser I radical. Nuevamente, por un razonamiento análogo al del teorema anterior, existe un ideal primo diferencial Q que contiene a I y con $Q \cap T = \emptyset$ y, en particular, $x \notin Q$. Se tiene que $Q \cap A \subset P$, ya que si existiera $a \in A \setminus P$ con $a \in Q$, entonces $ax \in Q \cap T$, lo cual no puede darse. Como además $P \subset I \subset Q$, se tiene que $Q \cap A = P$ y Q es el ideal primo diferencial que buscábamos. □

Veamos un último resultado, que no tiene que ver con la característica diferencial que estamos estudiando, pero que necesitaremos para los dos últimos resultados del capítulo.

Lema 2.4. *Sea $L|K$ una extensión de cuerpos (la estructura de cuerpo de $K \subset L$ es la misma que la de L, restringida a K). Sean $A \subset B$ los anillos obtenidos al adjuntar un mismo conjunto (no necesariamente finito) de indeterminadas a K y a L respectivamente ($A \subset B$ es una extensión de anillos). Sean P un ideal de A, J el ideal generado por P en B e $I = \sqrt{J}$ el radical de J en B.*

i) Si P es radical, entonces $P = I \cap A$.

ii) Si P es primo, entoncees I cumple que para todos $a \in A$ y $b \in B$ tales que $ab \in I$, se tiene que $a \in I$ o $b \in I$.

iii) Si K y L son de característica 0 (siempre son de la misma característica) y P es un ideal propio de A (no necesariamente radical ni primo), si X es una de las indeterminadas y $\alpha \in L \setminus K$, entonces $X - \alpha \notin I$.

Demostración. Sabemos que, como $L|K$ es una extensión de cuerpos, L puede verse como un espacio vectorial sobre K. Sea $\{u_\lambda\}_{\lambda \in \Lambda}$ una base (no necesariamente finita ni numerable) de dicho espacio vectorial. Entonces, todo elemento de L tiene una única expresión del tipo $\sum_{\lambda \in \Lambda} k_\lambda u_\lambda$, donde $k_\lambda \in K$ $\forall \lambda \in \Lambda$ y k_λ es no nulo a lo sumo para un número finito de valores de λ. Además, en esta situación, la base $\{u_\lambda\}_{\lambda \in \Lambda}$ genera a su vez a B como A-módulo, ya que en todo polinomio sobre L, se pueden sustituir sus coeficientes por sus

expresiones como combinación lineal de los u_λ. Es decir, todo elemento de B admite una expresión de la forma $\sum_{\lambda\in\Lambda} a_\lambda u_\lambda$, donde $a_\lambda \in A\ \forall\lambda\in\Lambda$ y a_λ es no nulo a lo sumo para un número finito de valores de λ. Esta expresión es además única, ya que si se tuviera que $\sum_{\lambda\in\Lambda} a_\lambda u_\lambda = \sum_{\lambda\in\Lambda} b_\lambda u_\lambda$, siendo estas dos expresiones como se acaba de describir, entonces sería $\sum_{\lambda\in\Lambda}(a_\lambda - b_\lambda)u_\lambda = 0$, luego el coeficiente (en L) de cada monomio de esta última expresión es nulo. Si nos fijamos en uno de estos monomios (cualquiera) y su coeficiente (en L) en cada una de las dos expresiones iniciales viene dado por $\sum_{\lambda\in\Lambda} \tilde{a}_\lambda u_\lambda$ y $\sum_{\lambda\in\Lambda} \tilde{b}_\lambda u_\lambda$ respectivamente, con $\tilde{a}_\lambda, \tilde{b}_\lambda \in K$ para cada $\lambda\in\Lambda$, entonces, su coeficiente en la última expresión que, como hemos dicho, ha de ser nulo, viene dado por $0 = \sum_{\lambda\in\Lambda}(\tilde{a}_\lambda - \tilde{b}_\lambda)u_\lambda \in L$, luego $\tilde{a}_\lambda = \tilde{b}_\lambda$ para todo $\lambda\in\Lambda$ al ser los u_λ linealmente independientes sobre K. Al darse para cualquier monomio, se tiene que las dos expresiones iniciales son idénticas, es decir, $a_\lambda = b_\lambda$ para todo $\lambda\in\Lambda$. Podemos suponer que $u_1 = 1$ es uno de los elementos de esta base (estamos suponiendo que $1\in\Lambda$, el cual es un conjunto de índices arbitrario, pero basta con fijar uno de los elementos de este conjunto de índices y suponer que el elemento de la base correspondiente a ese índice es el 1, sin perder generalidad). En esta situación, por la unicidad de estas expresiones, un elemento k de L está en K si, y solo si, todos sus coeficientes en dicha expresión son nulos salvo $k_1 = k$ y un elemento a de B está en A si, y solo si, todos sus coeficientes en dicha expresión son nulos salvo $a_1 = a$.

Como $J\subset B$ es el ideal generado en B por $P\subset A$, los elementos de J son las combinaciones lineales sobre B de elementos de P. Si los coeficientes (en B) de estas combinaciones lineales los expresamos a su vez como combinación lineal de los u_λ, obtenemos para cada elemento de J una expresión (única) del tipo $\sum_{\lambda\in\Lambda} a_\lambda u_\lambda$, cuyos coeficientes a_λ son elementos de P. Recíprocamente, una expresión de este tipo cuyos coeficientes están todos en P da lugar a un elemento de J. Deducimos que una expresión de este tipo corresponde a un elemento de J exactamente cuando todos los coeficientes a_λ están en P. En particular, $J\cap A$ son los elementos cuyas expresiones de este tipo tienen todos sus coeficientes nulos salvo $a_1\in P$, es decir, $J\cap A\subset P$. Además, $P\subset J \implies P\subset J\cap A$, luego $P = J\cap A$.

i) Sabemos que $P\subset J\subset I$, luego $P\subset I\cap A$. Supongamos ahora que $b\in I\cap A$. Como $b\in I = \sqrt{J}$, existe $n\in\mathbb{N}$ tal que $b^n\in J$ y, además, $b^n\in A$, luego $b^n\in J\cap A = P$. Como P es radical, $b\in P$, luego $P\supset I\cap A$. Juntando ambas contenciones, se concluye que $P = I\cap A$.

ii) Supongamos que P es primo y sean $a\in A$, $b\in B$ con $ab\in I$. De nuevo, como $I = \sqrt{J}$, existe $n\in\mathbb{N}$ tal que $a^n b^n\in J$. Si $b^n\in B$ se expresa como $b^n = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$, entonces $a^n b^n = a^n\sum_{\lambda\in\Lambda} a_\lambda u_\lambda = \sum_{\lambda\in\Lambda}(a^n a_\lambda)u_\lambda \in J$, luego $a^n a_\lambda\in P$ para todo índice

$\lambda \in \Lambda$. Como P es primo, se tiene que, o bien $a^n \in P$, luego $a \in P$, o bien $a_\lambda \in P$ para todo $\lambda \in \Lambda$, luego $b^n \in J$ y, por tanto $b \in I$.

iii) Sea X una de las indeterminadas de A y B y sea $\alpha \in L$ con $\alpha \notin K$. Supongamos que $X - \alpha \in I$. Entonces, existe $n \in \mathbb{N}$ tal que $(X-\alpha)^n \in J$. Sea $J_X = J \cap L[X]$ el conjunto de los polinomios de J que únicamente tienen a X como indeterminada. Entonces J_X es un ideal propio y no vacío de $L[X]$. En efecto, si $F(X), G(X) \in J_X$ y $R(X), S(X) \in L$, entonces $F, G \in J$, luego $RF + SG \in J$ y, como F, G, R y S solo dependen de la indeterminada X, $RF + SG$ también depende solo de esta indeterminada, luego $RF+SG \in J_X$, y J_X es un ideal de $L[X]$. Es un ideal propio porque lo es P, ya que, si $1 \in J_X$, entonces $1 \in J$, luego $J = B$ y $P = J \cap A = A$, y es no vacío porque $(X-\alpha)^n \in J_X$. Como $L[X]$ es un dominio de ideales principales, J_X está generado por algún elemento de $L[X]$, no constante (porque $J_X \neq L[X]$) y que divide a $(X-\alpha)^n$. Entonces este generador tiene que ser de la forma $(X-\alpha)^r$ para algún r con $1 \leq r \leq n$, ya que $X - \alpha$ es una expresión irreducible en $L[X]$. Observemos que, como $\alpha \notin K$, 1 y α son linealmente independientes sobre K, luego podemos partir del conjunto $\{1, \alpha\}$ y completarlo hasta formar una base $\{u_\lambda\}_{\lambda \in \Lambda}$ de L como K-espacio vectorial, es decir, elegimos la base de forma que $u_2 = \alpha$ sea otro de sus elementos. Recordemos que, para encontrar la expresión de un polinomio en $L[X]$ como combinación lineal de los u_λ, sustituimos cada coeficiente del polinomio por su expresión en la base $\{u_\lambda\}_{\lambda \in \Lambda}$ y agrupamos los monomios que acompañan a un mismo elemento u_λ de la base, para obtener así el coeficiente $a_\lambda(X) \in K[X]$ que le corresponde. En consecuencia, cuando expresamos un polinomio $Q(X) \in L[X]$ de esta forma, ninguno de los coeficientes $a_\lambda(X) \in K[X]$ de dicha expresión puede tener mayor grado que Q. Entonces, como $(X-\alpha)^r = X^r - rX^{r-1}\alpha + Q(X)$ con $Q(X) \in L[X]$ de grado $\leq r-2$, si $Q(X) = \sum_{\lambda \in \Lambda} \tilde{a}_\lambda(X) u_\lambda$ ($\tilde{a}_\lambda$ de grado $\leq r-2$) y $(X-\alpha)^r = \sum_{\lambda \in \Lambda} a_\lambda(X) u_\lambda$, se tiene que $(X-\alpha)^r = X^r u_1 - rX^{r-1}u_2 + \sum_{\lambda \in \Lambda} \tilde{a}_\lambda(X) u_\lambda$, luego $a_1(X) = X^r + \tilde{a}_1(X)$ no tiene términos en X^{r-1}. Sin embargo, como $(X-\alpha)^r \in J$, cada uno de los a_λ está en P y, en particular, $a_1(X) \in P \subset J$, así que $a_1 \in J_X$. Como J_X está generado por $(X-\alpha)^r$, $a_1(X) = X^r + \tilde{a}_1(X)$ es múltiplo de $(X-\alpha)^r$ y,por ser ambos mónicos y del mismo grado, tiene que ser $a_1(X) = (X-\alpha)^r$, pero el término en X^{r-1} de $(X-\alpha)^r$ es $(-r\alpha)X^{r-1} \neq 0$ ya que $\alpha \notin K$, luego $\alpha \neq 0$ y $r \neq 0$ ya que la característica es 0. $\square$

2.2. Isomorfismos admisibles

Definición. Un isomorfismo entre dos cuerpos K y F se dice que es un *isomorfismo admisible* si existe un cuerpo L que contiene a K y a F.

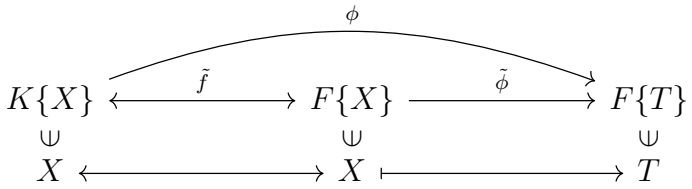
Observemos que, si K y F son subcuerpos de L, entonces $\sigma : K \to F$ es un isomorfismo admisible si, y solo si, $\sigma : K \to L$ es un homomorfismo de cuerpos y $F = \sigma(K)$, ya que todo homomorfismo de cuerpos es inyectivo, luego es un isomorfismo entre el cuerpo en el que se define y su imagen.

Teorema 2.5. *Sea L un cuerpo diferencial de característica 0, K y F dos subcuerpos diferenciales de L y $f : K \to F$, un isomorfismo diferencial definido entre ellos. Entonces existe un isomorfismo admisible $g : L \to M$ para algún cuerpo M, que extiende a f.*

Demostración. Como el propio isomorfismo diferenciable $g = f : K \to F$ es admisible, ya que L contiene a ambos cuerpos, vamos a ver que si $\alpha \in L \setminus K$, existe un isomorfismo diferencial admisible definido en $K\langle\alpha\rangle$ que extiende a f. El resultado se sigue inmediatamente mediante inducción transfinita ($L = K\langle\{\alpha_\lambda\}_{\lambda\in\Lambda}\rangle$ para cierto conjunto $\{\alpha_\lambda\}_{\lambda\in\Lambda}$ de elementos de L).

Sea $\alpha \in L \setminus K$, vamos a ver que existe un isomorfismo diferencial $g : K\langle\alpha\rangle \to M$ siendo M una extensión de F. Este isomorfismo será admisible puesto que, si $M = F\langle\{\alpha_\lambda\}_{\lambda\in\Lambda}\rangle$ con $\alpha_\lambda \in L$ para todo $\lambda \in \Lambda$, entonces L y M son subcuerpos de $L\langle\{\alpha_\lambda\}_{\lambda\in\Lambda}\rangle$. Sea $\varphi : K\{X\} \to K\{\alpha\}$ el morfismo sobre K (es decir, con $\varphi(x) = x\ \forall x \in K$) dado por $\varphi(X) = \alpha$, siendo X una indeterminada diferencial y sea $P = ker(\varphi)$. Notemos que el morfismo φ es el morfismo de evaluación en α, es decir, si $R(X) \in K\{X\}$ es un polinomio diferencial, entonces $\varphi(R) = R(\alpha)$. Por el Teorema 1.7, P es un ideal diferencial y, además, si $R, S \in K\{X\}$ y $RS \in P$, entonces $\varphi(RS) = \varphi(R)\varphi(S) = R(\alpha)S(\alpha) = 0$, por lo que $R(\alpha) = 0$ o $S(\alpha) = 0$, luego P es primo. Sea $\tilde{f} : K\{X\} \to F\{X\}$ la extensión diferencial de f con $\tilde{f}(X) = X$. Nótese que en $K\{X\} = K[X, X', \dots]$ hay un número infinito de indeterminadas adjuntadas a K y al decir que f se extiende diferencialmente con $\tilde{f}(X) = X$, no se da la imagen de una sola indeterminada, sino de todas ellas, entendiéndose que $\tilde{f}(X') = \tilde{f}(X)' = X'$. Por ser f un isomorfismo de cuerpos, es evidente que $\tilde{f}$ es un isomorfismo de anillos, luego $\tilde{P} = \tilde{f}(P)$ es un ideal primo diferencial de $F\{X\}$. Sea J el ideal generado por $\tilde{P}$ en $L\{X\}$, $J = \{\sum_{i=1}^{n} a_i p_i : n \in \mathbb{N}, a_i \in L\{X\}, p_i \in \tilde{P}\}$. Se tiene que J es un ideal diferencial, ya que, para cada $\sum_{i=1}^{n} a_i p_i \in J$, se cumple que $\left(\sum_{i=1}^{n} a_i p_i\right)' = \sum_{i=1}^{n} (a_i p_i)' = \sum_{i=1}^{n} a_i' p_i + \sum_{i=1}^{n} a_i p_i' \in J$, porque $a_i, a_i' \in L\{X\}$ y $p_i, p_i' \in \tilde{P}$ por ser $\tilde{P}$ diferencial. Sea $I = \sqrt{J}$. Por la Nota 1.13, al ser L de característica 0, $L\{X\}$ es un álgebra de Ritt y, por el Corolario 1.15, I es un ideal radical diferencial. Nótese que $F\{X\}$ se obtiene adjuntando una cantidad numerable de indeterminadas a F, así que, por

el primer apartado del Lema 2.4, $I \cap F\{X\} = \tilde{P}$ y, por el primer apartado del Teorema 2.3, existe un ideal primo diferencial Q de $L\{X\}$ con $I \subset Q$ y $Q \cap F\{X\} = \tilde{P}$. Vamos a denotar por T a la clase de X en el cociente $L\{X\}/Q$. Este cociente es un nuevo anillo diferencial como se explica tras la definición de ideal diferencial en el capítulo 1, siendo T' la clase de X' en el cociente. Vamos a considerar la siguiente composición de morfismos diferenciales de anillos:



El núcleo de $\tilde{\phi}$ es $Q \cap F\{X\} = \tilde{P}$, luego el núcleo de ϕ es $\tilde{f}^{-1}(\tilde{P}) = P$. Como ϕ es sobreyectiva al serlo evidentemente $\tilde{\phi}$ y ser $\tilde{f}$ un isomorfismo, ϕ induce un isomorfismo diferencial entre $\frac{K\{X\}}{P}$ y $F\{T\}$. De igual forma, al ser φ claramente sobreyectivo y ser P su núcleo, induce a su vez un isomorfismo diferencial entre $\frac{K\{X\}}{P}$ y $K\{\alpha\}$. Componiendo el inverso de este último con el isomorfismo diferencial anterior, obtenemos un isomorfismo diferencial $\tilde{g} : K\{\alpha\} \to F\{T\}$, que nos permite definir un isomorfismo diferencial de cuerpos $g : K\langle\alpha\rangle \to F\langle T\rangle$ donde si $a/b \in K\langle\alpha\rangle$, es decir, $a, b \in K\{\alpha\}$ y $b \neq 0$, se define $g(a/b) = \tilde{g}(a)/\tilde{g}(b) \in F\langle T\rangle$ ya que $\tilde{g}(a), \tilde{g}(b) \in F\{T\}$ y $\tilde{g}(b) \neq 0$. Este isomorfismo diferencial es admisible gracias a la construcción de T, ya que $K\langle\alpha\rangle$ y $F\langle T\rangle$ son subcuerpos del cuerpo diferencial $L\langle T\rangle = Fr(L\{T\}) \cong Fr(L\{X\}/Q)$. □

Teorema 2.6. *Sea $L|K$ una extensión diferencial de cuerpos (la estructura de cuerpo y la derivación de K son la restricción de las de L a los elementos de K) de característica 0 y sea $\alpha \in L \setminus K$. Existe un isomorfismo admisible definido en L sobre K (es decir, que deja fijos los elementos de K) que no deja α fijo.*

Demostración. Sea $F = K\langle\alpha\rangle \subset L$ y sea nuevamente $\varphi : K\{X\} \to K\{\alpha\}$ el morfismo de evaluación en α. Sea $P = ker(\varphi)$, que, de nuevo, es un ideal primo diferencial de $K\{X\}$. Sea J el ideal generado por P en $F\{X\}$. Por un razonamiento análogo al dado en la demostración del teorema anterior, J es un ideal diferencial e $I = \sqrt{J}$ es un ideal radical diferencial de $F\{X\}$. Nuevamente, por el primer apartado del Lema 2.4, $I \cap K\{X\} = P$ y, por el primer apartado del Teorema 2.3, existe un ideal primo diferencial Q de $F\{X\}$ con $I \subset Q$ y $Q \cap K\{X\} = P$. Sea T la clase de X en el cociente $F\{X\}/Q$. El núcleo del morfismo diferencial natural $\phi : K\{X\} \to K\{T\}$, que es sobreyectivo, es $Q \cap K\{X\} = P$, luego induce un isomorfismo diferencial $K\{X\}/P \cong K\{T\}$. A su vez, como $P = ker(\varphi)$, φ induce un isomorfismo diferencial $K\{\alpha\} \cong K\{X\}/P$. Componiendo ambos obtenemos nuevamente un isomorfismo diferencial $\tilde{g} : K\{\alpha\} \to K\{T\}$, que nos permite definir un

isomorfismo diferencial de cuerpos $K\langle\alpha\rangle \to K\langle T\rangle$, el cual deja fijos los elementos de K y envía α en T. Ahora buscamos extender este isomorfismo a todo L para terminar, pero necesitamos que α no quede fijo (que α y T sean distintos), es decir, que la clase de α en $F\{X\}/Q$ no sea la misma que la de X o, equivalentemente, que $X - \alpha \in F\{X\}$ no esté en Q. Observemos que, por el segundo apartado del Lema 2.4, I cumple las hipótesis del segundo apartado del Teorema 2.3 y, por tanto, I es la intersección de todos los ideales primos diferenciales Q de $F\{X\}$ tales que $I \subset Q$ y $Q \cap K\{X\} = P$. Por el tercer apartado del Lema 2.4, $X - \alpha \notin I$, luego existe un ideal Q como los que se acaban de describir con $X - \alpha \notin Q$, es decir, al elegir Q, siempre se puede encontrar uno tal que α y X no son el mismo elemento en el cociente $F\{X\}/Q$ y $\alpha \neq T$. Entonces, conseguimos un isomorfismo diferencial entre $K\langle\alpha\rangle$ y $K\langle T\rangle$ que deja fijos los elementos de K pero no deja fijo α. Como $K\langle\alpha\rangle$ y $K\langle T\rangle$ son ambos subcuerpos diferenciales de $L\langle T\rangle$, por el Teorema 2.5, este isomorfismo puede ampliarse a un isomorfismo diferencial admisible definido en $L\langle T\rangle$. Si nos restringimos a L, obtenemos un isomorfismo diferencial admisible entre L y su imagen, que deja fijos los elementos de K, pero que no deja fijo α.

□

3. Teoría de Galois diferencial

Vamos a recordar las bases de la teoría de Galois clásica antes de ver cómo la podemos combinar con la estructura diferencial que estamos estudiando.

3.1. Teoría de Galois clásica

Dados dos cuerpos K y L tal que $K \subset L$ y tal que la estructura de cuerpo de K se obtiene por restricción de la de L (las operaciones entre elementos de K son equivalentes vistos como elementos de K o como elementos de L), decimos que L es una *extensión* de K y lo escribimos $L|K$. En este caso, L puede verse como un espacio vectorial sobre K cuya dimensión llamamos *grado de la extensión* $L|K$ y lo denotamos por $[L : K]$. Si el grado de la extensión es finito, diremos que es una *extensión finita*. Esta notación es la misma que la que representa al índice de un subgrupo H en un grupo G, $[G : H]$, y hay que interpretarlo como indique el contexto según sean cuerpos o grupos lo que aparezca entre los corchetes. Si $L|F$ y $F|K$ son dos extensiones de cuerpos, entonces $L|K$ es una extensión de cuerpos y F es un *cuerpo intermedio* de la extensión. En este caso, $[L : K] = [L : F] \cdot [F : K]$.

Dado $L|K$, y $\alpha_1, \ldots, \alpha_n \in L$, $K[\alpha_1, \ldots, \alpha_n] = \{P(\alpha_1, \ldots, \alpha_n) : P \in K[X_1, \ldots, X_n]\}$ es un dominio y denotamos por $K(\alpha_1, \ldots, \alpha_n) = \{\frac{p}{q} : p, q \in K[\alpha_1, \ldots, \alpha_n], q \neq 0\}$ a su cuerpo de fracciones, que es la menor extensión de K que contiene a $\alpha_1, \ldots, \alpha_n$ y es un cuerpo intermedio de la extensión $L|K$. Si $\alpha \in L$, decimos que α es algebraico sobre K si $\exists P(X) \in K[X]$ tal que $P(\alpha) = 0$, y decimos que es trascendente sobre K en caso contrario. Si $\alpha \in L$ es algebraico sobre K, definimos el *polinomio mínimo* de α en K, $m_\alpha^K(X)$, como el (único) polinomio mónico de menor grado en $K[X]$ que se anula en α y definimos el grado de α sobre K, $\deg_K(\alpha) = \deg(m_\alpha^K(X))$. Si no hay ambigüedad, escribiremos $m_\alpha^K(X) = m_\alpha(X)$. Decimos que $K(\alpha)|K$ es una extensión simple y se cumple que $[K(\alpha) : K] = \deg_K(\alpha)$. Una extensión $L|K$ es *finitamente generada* si existen $\alpha_1, \ldots, \alpha_n \in L$ tal que $L = K(\alpha_1, \ldots, \alpha_n)$ y, en particular, toda extensión finita es finitamente generada y una extensión finitamente generada $K(\alpha_1, \ldots, \alpha_n)|K$ es finita si, y solo si, $\alpha_1, \ldots, \alpha_n$ son algebraicos sobre K.

Dada una extensión $L|K$, definimos el *grupo de Galois* de la extensión, $Gal(L|K)$, como el grupo de los automorfismos de L sobre K, es decir, que dejan fijos a los elementos de K. La operación entre morfismos que dota a este conjunto de estructura de grupo es la dada por $\sigma\tau := \sigma \circ \tau$ para $\sigma, \tau \in Gal(L|K)$. Se tienen las *correspondencias de Galois* entre

los subgrupos de $G = Gal(L|K)$ y los cuerpos intermedios de la extensión $L|K$ dadas de la siguiente forma:

- Si F es un cuerpo intermedio de $L|K$, consideramos el subgrupo $F^* \subset G$ de los automorfismos de L que dejan fijos a los elementos de F ($F^* = Gal(L|F)$).
- Si $H \subset G$ es un subgrupo de G, consideramos H^* como el conjunto de elementos de L que quedan fijos por cada automorfismo de H, que es un cuerpo intermedio de $L|K$.

Estas correspondencias tienen las siguientes propiedades: si F, F_1 y F_2 son cuerpos intermedios de $L|K$, y H, H_1 y H_2 son subgrupos de $G = Gal(L|K)$,

i) $F \subset F^{**}$; $H \subset H^{**}$.

ii) $F_1 \subset F_2 \implies F_1^* \supset F_2^*$; $H_1 \subset H_2 \implies H_1^* \supset H_2^*$.

iii) $F^{***} = F^*$; $H^{***} = H^*$.

Decimos que un cuerpo F o un subgrupo H es cerrado si $F = F^{**}$ o, respectivamente, $H = H^{**}$. Los cuerpos F de la forma $F = H^*$ para algún subgrupo H de G y los subgrupos H con $H = F^*$ para algún cuerpo intermedio F de $L|K$ son cuerpos y subgrupos cerrados como consecuencia de la propiedad (iii).

Una extensión diferencial $L|K$ se dice que es *normal* en el sentido clásico si todo polinomio en $K[X]$ que tiene una raíz en L descompone totalmente en L, es decir, tiene en L todas sus raíces. Por otra parte, dado un polinomio $P(X) \in K[X]$, decimos que P es *separable* sobre K si tiene todas sus raíces distintas (en alguna extensión de K). Dada una extensión $L|K$ y dado un elemento algebraico $\alpha \in L$ sobre K, decimos que α es separable sobre K si su polinomio mínimo $m_\alpha^K(X)$ es separable sobre K. Decimos que la extensión $L|K$ es separable si todo $\alpha \in L$ es separable sobre K. Finalmente, decimos que una extensión $L|K$ es *de Galois* si es finita, normal y separable. El *teorema fundamental de la teoría de Galois* afirma que en una extensión de Galois, las correspondencias de Galois antes definidas son biyectivas e inversas la una de la otra, es decir, todo cuerpo intermedio de una extensión de Galois es cerrado para la extensión y todo subgrupo del grupo de Galois de dicha extensión es, a su vez, cerrado.

Vamos entonces a enlazar estos conceptos con las estructuras diferenciales que hemos introducido en el capítulo anterior.

3.2. Extensiones diferenciales y grupo de Galois diferencial

Definición. Una *extensión diferencial* $L|K$ es una extensión de cuerpos diferenciales donde la derivada de L es una extensión de la de K. Definimos el *grupo de Galois diferencial* de dicha extensión diferencial como el conjunto de automorfismos diferenciales de L que dejan fijos los elementos de K y lo representaremos sin distinguir del caso clásico como $Gal(L|K)$; el contexto será el que indique si se trata del caso clásico o diferencial. La Nota 1.6 garantiza que este conjunto es de hecho un subgrupo del grupo de Galois en el sentido clásico. Más aún, como consecuencia de esta nota, siempre que consideremos un grupo de morfismos, el subconjunto de dicho grupo formado por los morfismos que además son diferenciales será un subgrupo. Si $L|F$ y $F|K$ son dos extensiones diferenciales, decimos que F es un cuerpo diferencial intermedio de la extensión diferencial $L|K$. Para definir las correspondencias de Galois en el caso diferencial, veamos antes el siguiente resultado:

Lema 3.1. *Sea $L|K$ una extensión diferencial.*

a) Sea F un cuerpo diferencial intermedio de la extensión, entonces el conjunto F^* de los automorfismos de L sobre F, es decir, que dejan fijos los elementos de F, es un subgrupo de $G = Gal(L|K)$.

b) Sea H un subgrupo de G, entonces el conjunto de los elementos de L que quedan fijos por los morfismos de H es un cuerpo diferencial intermedio de $L|K$.

Demostración. a) Es consecuencia nuevamente del resultado correspondiente para la teoría de Galois clásica junto con la Nota 1.6, que permite extender este resultado al caso de morfismos diferenciales.

b) La única novedad respecto al resultado conocido es el hecho de que el cuerpo H^* sea diferencial. Efectivamente, si $x \in H^*$, es decir, si $\sigma(x) = x \ \forall \sigma \in H$, entonces $\sigma(x') = \sigma(x)' = x' \ \forall \sigma \in H$, luego $x' \in H^*$.

□

Comprobado este resultado, definimos las correspondencias entre el conjunto de cuerpos diferenciales intermedios de $L|K$ y el conjunto de los subgrupos de $G = Gal(L|K)$ de la siguiente forma:

- Si F es un cuerpo diferencial intermedio de $L|K$, consideramos el subgrupo $F^* \subset G$ de los automorfismos diferenciales de L que dejan fijos a los elementos de F ($F^* = Gal(L|F)$).

- Si $H \subset G$ es un subgrupo de G, consideramos H^* como el conjunto de elementos de L que quedan fijos por cada automorfismo de H, que es un cuerpo diferencial intermedio de $L|K$.

Dada la analogía con el caso clásico, estas correspondencias tienen todas las propiedades antes mencionadas. Decimos nuevamente que un cuerpo diferencial intermedio F de $L|K$ o un subgrupo H del grupo del grupo de Galois diferencial de dicha extensión es cerrado si $F = F^{**}$ o, respectivamente, $H = H^{**}$. Los cuerpos intermedios (o subgrupos) que son correspondencia de algún subgrupo (o cuerpo intermedio) son cerrados. Además, estas correspondencias son biyectivas e inversas la una de la otra cuando se consideran solo los cuerpos y subgrupos cerrados de la extensión.

Observemos que en una extensión diferencial $L|K$, L es siempre cerrado como cuerpo intermedio y $\{Id_L\}$ es siempre cerrado como subgrupo del grupo de Galois de la extensión, siendo ambos correspondientes el uno del otro. Sin embargo, no podemos en general decir lo mismo de K como cuerpo intermedio de la extensión. Se tiene que $K^* = G$ y por tanto, G sí es cerrado visto como subgrupo de sí mismo, sin embargo, no podemos asegurar más que $G^* \supset K$.

Lema 3.2. *Sea $M|K$ una extensión diferencial y $G = Gal(M|K)$. Sean $F \subset L$ dos cuerpos diferenciales intermedios de la extensión y sean $J \subset H$ dos subgrupos de G. Entonces:*

a) si $[L : F] = n$, entonces $[F^* : L^*] \leq n$ y, si además F es cerrado, también lo es L y se da la igualdad.

b) si $[H : J] = n$, entonces $[J^* : H^*] \leq n$ y, si además J es cerrado, también lo es H y se da la igualdad.

Demostración. Empecemos probando las desigualdades:
a) Al ser $L|F$ finita, es finitamente generada y, dado que $F(\alpha)(\beta) = F(\alpha, \beta)$, podemos limitarnos al caso de extensiones finitas $F(\alpha)|F$ y el caso general se sigue como consecuencia. Sea entonces $L = F(\alpha)$ y sea $\sigma \in F^*$. Los morfismos de L^* son los morfismos de $Gal(M|K)$ que dejan fijos los elementos de $L = F(\alpha)$ o, equivalentemente, los que dejan fijos los elementos de F y también dejan fijo α, es decir, son exactamente los morfismos de F^* que dejan fijo a su vez a α. Observamos que las clases por la izquierda de F^* mod L^* vienen dadas por la imagen que cada morfismo de F^* asocia a α ya que, puesto que tanto los morfismos de F^* como los de L^* son la identidad al restringirlos a F, si $\sigma, \tau \in F^*$, se tiene que $\sigma L^* = \tau L^* \iff \sigma\tau^{-1} \in L^* \iff \sigma\tau^{-1}(\alpha) = \alpha \iff \sigma(\alpha) = \tau(\alpha)$. Sabemos que las posibles imágenes de α por un morfismo $\sigma \in F^*$ son las distintas raíces de $m_\alpha^F(X)$ en L y, como $\deg(m_\alpha^F(X)) = [F(\alpha) : F] = [L : F] = n$, hay a lo sumo n posibles valores distintos y, por tanto, $[F^* : L^*] \leq n$.

b) Razonemos por reducción al absurdo. Supongamos que $[J^* : H^*] > n$ y, por tanto, existen $a_1, \ldots, a_{n+1} \in J^*$ linealmente independientes sobre H^*. Sean $\sigma_1, \ldots, \sigma_n$ representantes de las n distintas clases por la izquierda de H/J, siendo $\sigma_1 = Id$. Consideramos las ecuaciones:

$$(E_j): \quad \sum_{i=1}^{n+1} x_i \sigma_j(a_i) = 0 \quad , \quad j = 1, 2, \ldots, n.$$

Al tratarse de un sistema homogéneo de n ecuaciones con $n+1$ incógnitas $x_1, \ldots, x_{n+1}$, admite soluciones no triviales en M. Consideramos una solución $z_1, \ldots, z_{n+1}$ no trivial pero con un número máximo de ceros y, salvo reordenación de los elementos $a_1, \ldots, a_{n+1}$, supongamos que $z_1, \ldots, z_r$ son sus elementos no nulos ($r \leq n$). Como además $\lambda z_1, \ldots, \lambda z_{n+1}$ es otra solución no trivial del sistema homogéneo con los mismos ceros que la original para cualquier $\lambda \in M$, podemos suponer $z_1 = 1$. Como $\sigma_1 = Id$, la ecuación (E_1) se traduce en $z_1 a_1 + \cdots + z_{n+1} a_{n+1} = 0$ y la independencia lineal de los a_i sobre H^* implica que no todos los z_i pueden estar en H^*, ya que no son todos ellos nulos. Podemos suponer entonces que $z_r \notin H^*$, luego algún morfismo de H no deja z_r fijo. Dicho morfismo estará en la clase $\sigma_k J$ para algún $2 \leq k \leq n$ y, sin pérdida de generalidad, suponemos que dicho morfismo es el que elegimos como representante de la clase, es decir, $\sigma_k(z_r) \neq z_r$. Si aplicamos σ_k a las ecuaciones (E_j) evaluadas en $z_1, \ldots, z_{n+1}$, tenemos

$$\sum_{i=1}^{n+1} \sigma_k(z_i)\, \sigma_k\big(\sigma_j(a_i)\big) = \sigma_k\Big(\sum_{i=1}^{n+1} z_i \sigma_j(a_i)\Big) = \sigma_k(0) = 0 \quad , \quad j = 1, 2, \ldots, n.$$

Observemos que $\{\sigma_k\sigma_1 J, \ldots, \sigma_k\sigma_n J\} = \{\sigma_1 J, \ldots, \sigma_n J\}$, puesto que, evidentemente, $\sigma_k\sigma_i J = \sigma_k\sigma_j J \iff \sigma_i J = \sigma_j J$. No estamos afirmando que $\sigma_k\sigma_i J = \sigma_i J$ para cada $i \in \{1, \ldots, n\}$, sino que $\{\sigma_k\sigma_1 J, \ldots, \sigma_k\sigma_n J\}$ son n clases por la izquierda distintas de H/J, luego son las n clases distintas que hay. Entonces,

$$\sum_{i=1}^{n+1} \sigma_k(z_i)\, \sigma_k\big(\sigma_j(a_i)\big) = \sum_{i=1}^{n+1} \sigma_k(z_i)\sigma_l(a_i) = 0 \quad , \quad l = 1, 2, \ldots, n.$$

Observemos que, salvo un cambio de índice, lo que afirmamos es que $\sigma_k(z_1), \ldots, \sigma_k(z_{n+1})$ es una nueva solución del sistema original. Si restamos ambas soluciones, obtenemos otra solución del sistema dada por $z_1 - \sigma_k(z_1), \ldots, z_{n+1} - \sigma_k(z_{n+1})$, que tiene ceros al menos en las posiciones en las que los tenía $z_1, \ldots, z_{n+1}$. Puesto que $\sigma_k(z_r) \neq z_r$, esta solución es no trivial y dado que $z_1 = 1 = \sigma_k(1) = \sigma_k(z_1)$, esta nueva solución tiene estrictamente más ceros que $z_1, \ldots, z_{n+1}$, lo cual va en contra de la definición que habíamos dado para dicha solución, llegando así a un absurdo.

Veamos ahora que si F es cerrado, es decir, si $F = F^{**}$, entonces $[F^* : L^*] = n$. Tenemos que $[L^{**} : F] = [L^{**} : F^{**}] \leq [F^* : L^*] \leq [L : F] = n$. Por otro lado, sabemos que

$L^{**} \supset L \implies [L^{**} : F] \geq [L : F] = n$. Por tanto, todas las desigualdades anteriores son, de hecho, igualdades y, en particular, $[F^* : L^*] = n$.

Además, $n = [L^{**} : F] = [L^{**} : L] \cdot [L : F] = [L^{**} : L] \cdot n \implies [L^{**} : L] = 1 \implies L^{**} = L$, luego L también es cerrado.

Siguiendo el mismo razonamiento, llegamos a que, si J es un subgrupo cerrado de G, entonces $[J^* : H^*] = n$ y H también es cerrado. □

Teorema 3.3. *Sea $L|K$ una extensión diferencial y $G = Gal(L|K)$ su grupo de Galois.*

a) Si H es un subgrupo normal de G, entonces $\sigma(H^*) = H^*$ para todo $\sigma \in G$.

b) Si F es un cuerpo diferencial intermedio de la extensión tal que $\sigma(F) = F$ para todo $\sigma \in G$, entonces F^* es un subgrupo normal de G y $G/F^* = \{\sigma|_F \ : \ \sigma \in G\}$, donde $\sigma|_F$ representa la restricción de σ a F tanto en su dominio como en su imagen.

Demostración. *a*) Sea $\sigma \in G$ y $x \in H^*$, veamos que entonces $\sigma(x) \in H^*$, es decir, $\tau(\sigma(x)) = \sigma(x)\ \forall \tau \in H$, lo cual equivale a decir que $\sigma^{-1}(\tau(\sigma(x))) = x; \forall \tau \in H$. Como H es normal, $\sigma^{-1}H\sigma = H$, luego $\sigma^{-1}\tau\sigma \in H$ y como $x \in H^*$, se tiene la igualdad buscada. Esto prueba que $\sigma(H^*) \subset H^*$. Siguiendo el mismo razonamiento con σ^{-1}, concluimos que $\sigma^{-1}(H^*) \subset H^* \implies H^* \subset \sigma(H^*)$ y se tiene la igualdad.

b) Sea $\sigma \in G$, veamos que $\sigma^{-1}F^*\sigma = F^*$, es decir, $\sigma^{-1}\tau\sigma \in F^*\ \forall \tau \in F^*$. Sea $\tau \in F^*$ y sea $x \in F$, queremos ver que $\sigma^{-1}(\tau(\sigma(x))) = x$ o, equivalentemente, que $\tau(\sigma(x)) = \sigma(x)$. Esto se da porque $\tau \in F^*$ y, como $x \in F$, por hipótesis, $\sigma(x) \in F$. Finalmente, observemos que dado $\sigma \in G$, si restringimos su dominio de definición a F, podemos restringir a F la imagen también ya que $\sigma(F) = F$ y obtener un morfismo de $Gal(F|K)$, que vamos a denotar, con cierto abuso de notación, $\sigma|_F$. Este proceso nos define una aplicación entre G y $Gal(F|K)$ que resulta trivialmente ser un homomorfismo entre ambos grupos. Decir que al restringir un automorfismo de G a F obtenemos la identidad en F es exactamente lo mismo que decir que dicho automorfismo está en F^*, es decir, F^* es el núcleo de este homomorfismo y su imagen es obviamente $\{\sigma|_F \ : \ \sigma \in G\}$, de donde se sigue el resultado buscado. □

3.3. Extensiones normales

Definición. Dada una extensión diferencial $L|K$, decimos que L *es normal sobre* K o que dicha extensión es *normal* si para todo elemento de $L \setminus K$ hay un morfismo diferencial en $Gal(L|K)$ que no lo deja fijo.

Esta definición dada para extensiones diferenciales normales difiere de la que se maneja para las extensiones en el sentido clásico. Veremos más adelante que esta propiedad juega un papel en la teoría de Galois diferencial similar al que jugaban las extensiones normales en el sentido clásico dentro de la teoría de Galois clásica. De aquí en adelante, salvo que se indique lo contrario, cuando hablemos de extensiones normales nos referiremos a esta nueva noción de normalidad que acabamos de introducir.

***Nota* 3.4.** Decir que L es normal sobre K es equivalente a decir que K es un cuerpo cerrado de la extensión diferencial $L|K$. $K \subset K^{**}$ siempre y se da la igualdad si, y solo si, no hay elementos fuera de K que queden fijos por todos los morfismos de $K^* = Gal(L|K)$, es decir, que ningún elemento de $L \setminus K$ queda fijo por todos los morfismos del grupo de Galois.

Lema 3.5. *Sea $L|K$ una extensión diferencial normal y sea $G = Gal(L|K)$. Si $H \subset G$ es un subgrupo normal, entonces H^* es normal sobre K.*

Demostración. Sea $x \in H^* \setminus K \subset L \setminus K$. Como L es normal sobre K, existe $\sigma \in G$ tal que $\sigma(x) \neq x$. Como H es un subgrupo normal de G, por el Teorema 3.3, $\sigma(H^*) = H^*$, luego $\sigma|_{H^*} \in Gal(H^*|K)$ donde $\sigma|_{H^*}$ representa, como anteriormente, la restricción de σ a H tanto en su dominio como en su imagen. Se tiene que $\sigma|_{H^*}(x) = \sigma(x) \neq x$, luego x no queda fijo por todos los morfismos de $Gal(H^*|K)$ y concluimos que H^* es normal sobre K. □

Veamos que, bajo ciertas hipótesis adicionales, podemos también afirmar el resultado recíproco.

***Nota* 3.6.** Recordamos que dado un grupo G y un subgrupo $H \subset G$, definimos el *normalizador de H en G* como $N(H) = \{g \in G : g^{-1}Hg = H\}$, que es otro subgrupo de G, que contiene a H y en el cual H es normal (es el mayor subgrupo de G que contiene a H con esta propiedad) y, además, H es normal si, y solo si, $N(H) = G$.

Lema 3.7. *Sea F un cuerpo diferencial intermedio cerrado de una extensión diferencial $L|K$, $H = F^*$ y sea $N(H)$ el normalizador de H en $G = Gal(L|K)$, entonces $N(H) = \{\sigma \in G : \sigma(F) = F\}$.*

Demostración. Sea $\sigma \in N(H)$, veamos que $\sigma(F) \subset F$. Sea $x \in F,\ \forall \tau \in H$,

$$\sigma^{-1}\tau\sigma \in H = F^* \implies \sigma^{-1}\tau\sigma(x) = x \implies \tau\sigma(x) = \sigma(x)$$

y, como esto se da $\forall \tau \in H$, $\sigma(x) \in H^* = F^{**} = F\ \ \forall x \in F \implies \sigma(F) \subset F$. Repitiendo el razonamiento con σ^{-1} que también está en el normalizador de H al ser este un grupo,

obtenemos que $\sigma^{-1}(F) \subset F \implies F \subset \sigma(F)$ y, juntando ambas contenciones, concluimos que $\sigma(F) = F$.

Recíprocamente, supongamos que $\sigma \in G$ cumple que $\sigma(F) = F$ y veamos que $\sigma \in N(H)$, es decir, sea $\tau \in H$, veamos que $\sigma^{-1}\tau\sigma \in H$. Sea $x \in F$, $\sigma(x) \in F$ y, como $\tau \in H = F^*$, $\tau\sigma(x) = \sigma(x)$, es decir, $\sigma^{-1}\tau\sigma(x) = x \ \ \forall x \in F \implies \sigma^{-1}\tau\sigma \in F^* = H$ como queríamos ver. Así, tenemos que $\sigma^{-1}H\sigma \subset H$. Como $\sigma(F) = F$, se tiene que $F = \sigma^{-1}\sigma(F) = \sigma^{-1}(F)$ y podemos repetir el razonamiento anterior con σ^{-1} y concluir análogamente que $\sigma H\sigma^{-1} \subset H \implies H \subset \sigma^{-1}H\sigma$ y, por tanto, $\sigma^{-1}H\sigma = H$, luego $\sigma \in N(H)$. □

Lema 3.8. *Sea F un cuerpo diferencial intermedio cerrado de una extensión diferencial $L|K$, F normal sobre K, $H = F^*$ y $N(H)$ el normalizador de H en $G = Gal(L|K)$. Supongamos que $N(H)$ es cerrado y que todo morfismo de $Gal(F|K)$ puede extenderse a uno de G, es decir, $Gal(F|K) = \{\sigma|_F \ : \ \sigma \in G\}$. Entonces H es un subgrupo normal de G y $G/H = Gal(F|K)$.*

Demostración. Cada $\sigma \in Gal(F|K)$ admite por hipótesis una extensión $\tilde{\sigma} \in G$, es decir, existe $\tilde{\sigma} \in G$ tal que $\tilde{\sigma}|_F = \sigma$ donde por $\tilde{\sigma}|_F$ entendemos la restricción a F de $\tilde{\sigma}$, tanto en su dominio como en su imagen, igual que anteriormente. En particular, $\tilde{\sigma}(F) = \sigma(F) = F$. Por el lema anterior, sabemos que $N(H) = \{\tau \in G : \tau(F) = F\}$, luego si $\sigma \in Gal(F|K)$, entonces $\tilde{\sigma} \in N(H)$ por la última observación. F es normal sobre K, luego $\forall x \in F \setminus K$ existe $\sigma \in Gal(F|K)$ tal que $\sigma(x) \neq x \implies \tilde{\sigma}(x) = \sigma(x) \neq x$, es decir, todo elemento de $F \setminus K$ puede moverse por algún morfismo de $N(H)$, es decir, $(F \setminus K) \cap N(H)^* = \emptyset$. Como $N(H) \supset H \implies N(H)^* \subset H^* = F$ y como $(F \setminus K) \cap N(H)^* = \emptyset$, se tiene que $N(H)^* \subset K$, luego $N(H)^* = K$ y, por tanto, $N(H) = N(H)^{**} = K^* = G$, es decir, H es normal en G. Además, el apartado b del Teorema 3.3 nos permite concluir que $G/H = G/F^* = \{\sigma|_F \ : \ \sigma \in G\} = Gal(F|K)$. □

Nótese que, puesto que $G = Gal(L|K)$ y $H = F^* = Gal(L|F)$, la última afirmación del enunciado del lema puede escribirse como $Gal(F|K) = \frac{Gal(L|K)}{Gal(L|F)}$.

3.4. Wronskiano

Definición. Dado un anillo diferencial A y $y_1, y_2, \ldots, y_n \in A$, se define la *matriz fundamental* de $y_1, y_2, \ldots, y_n$, como:

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

El *Wronskiano* de $y_1, y_2, \ldots, y_n$, $W(y_1, y_2, \ldots, y_n)$, es el determinante de su matriz fundamental.

Teorema 3.9. *Sea K un cuerpo diferencial y sean $y_1, \ldots, y_n \in K$, entonces $y_1, \ldots, y_n$ son linealmente dependientes sobre el cuerpo de constantes C de K si, y solo si, $W(y_1, \ldots, y_n) = 0$.*

Demostración. Consideremos el sistema de ecuaciones $\sum_{k=1}^{n} x_k y_k^{(i)} = 0,\ i = 0, 1, \ldots, n-1$, donde $x_1, \ldots, x_n \in C$. Al tratarse de un sistema homogéneo de n ecuaciones y n incógnitas, admitirá soluciones no triviales si, y solo si, la matriz del sistema (la matriz fundamental) tiene determinante nulo, es decir, $W(y_1, \ldots, y_n) = 0$.

Si $y_1, \ldots, y_n$ son linealmente dependientes sobre C, existen $c_1, \ldots, c_n \in C$ no todos nulos tales que $\sum_{k=1}^{n} c_k y_k = 0$. Derivando $n-1$ en este sumatorio, obtenemos las expresiones: $\sum_{k=1}^{n} c_k y_k^{(i)} = 0$ para $i = 1, \ldots, n-1$. Observemos que si $c \in C$ e $y \in K$, entonces $(cy)' = c'y + cy' = cy'$. Entonces $\{c_1, \ldots, c_n\}$ es una solución no nula del sistema de ecuaciones antes mencionado, luego $W(y_1, \ldots, y_n) = 0$.

Recíprocamente, razonemos por inducción sobre n. Si $W(y_1) = 0$, entonces $y_1 = 0$ y el resultado es inmediato. Supongamos que el resultado es cierto para $n-1$ y que $W(y_1, \ldots, y_n) = 0$, luego el sistema considerado admite soluciones no triviales en K. Si $W(y_2, \ldots, y_n) = 0$, por hipótesis de inducción, $y_2, \ldots, y_n$ son linealmente dependientes sobre C, luego también lo son $y_1, \ldots, y_n$, así que podemos suponer que $W(y_2, \ldots, y_n) \neq 0$. Si $\{c_1, \ldots, c_n\}$ es una solución no nula del sistema, dado que $\{\lambda c_1, \ldots, \lambda c_n\}$ también lo es para cualquier $\lambda \in K$ al tratarse de un sistema homogéneo, podemos asumir que $c_1 = 1 \in C$. El sistema queda entonces de la forma:

$$y_1^{(i)} + \sum_{k=2}^{n} c_k y_k^{(i)} = 0,\ \ i = 0, 1, \ldots, n-1.$$

Derivando en las primeras $n-1$ ecuaciones, obtenemos el sistema:

$$y_1^{(i+1)} + \sum_{k=2}^{n}(c_k' y_k^{(i)} + c_k y_k^{(i+1)}) = \sum_{k=1}^{n} c_k y_k^{(i+1)} + \sum_{k=2}^{n} c_k' y_k^{(i)}, \quad i = 0, 1, \ldots, n-2.$$

Como el primer sumando es nulo al ser $\{c_1, c_2, \ldots, c_n\}$ solución del sistema original, observamos finalmente que $\{c_2', \ldots, c_n'\}$ es una solución del sistema homogéneo de ecuaciones: $\sum_{k=2}^{n} x_k y_k^{(i)}$ $i = 0, 1, \ldots, n-2$. Como $W(y_2, \ldots, y_n) \neq 0$, este sistema no admite soluciones no triviales, luego $c_2' = \cdots = c_n' = 0$, es decir, $c_2, \ldots, c_n \in C$ y concluimos que $y_1, \ldots, y_n$ son linealmente dependientes sobre C. □

***Nota* 3.10.** Nótese que una vez fijados los elementos $y_1, \ldots, y_n$ en un cierto cuerpo diferencial, la condición de tener wronskiano nulo es independiente del cuerpo en el que se consideren dichos elementos, luego estos serán linealmente dependientes (o independientes) sobre el cuerpo de constantes de cualquier cuerpo al que pertenezcan y por tanto podemos decir sin ambigüedad que estos elementos son linealmente dependientes (o independientes) sobre las constantes.

Dada una ecuación diferencial lineal homogénea: $\mathcal{L}(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0 y = 0$, con coeficientes en cierto cuerpo diferencial K, si $\alpha_1, \ldots, \alpha_{n+1}$ son soluciones de dicho sistema en alguna extensión de K, entonces son linealmente dependientes sobre las constantes, ya que, si denotamos por $\boldsymbol{\alpha}_i$ a la i-ésima fila de su matriz fundamental, se tiene que $\boldsymbol{\alpha}_n = -a_{n-1}\boldsymbol{\alpha}_{n-1} - \cdots - a_0\boldsymbol{\alpha}_0$, es decir, la última fila de su matriz fundamental es combinación lineal de las anteriores, luego su wronskiano es nulo. Deducimos que para esta ecuación diferencial existen, a lo sumo, n soluciones linealmente independientes sobre las constantes en cualquier extensión diferencial de K.

3.5. Extensiones de Picard-Vessiot

Definición. Sea $\mathcal{L}(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0$ una ecuación diferencial lineal homogénea con coeficientes en un cuerpo diferencial K, decimos que una extensión diferencial $L|K$ es *de Picard-Vessiot* para dicha ecuación si $L = K\langle \alpha_1, \ldots, \alpha_n \rangle$ donde $\alpha_1, \ldots, \alpha_n$ son soluciones del sistema, linealmente independientes sobre las constantes y L y K tienen el mismo cuerpo de constantes.

Las extensiones por *adjunción de una integral* o por *adjunción de la exponencial de una integral* que veremos más adelante son ejemplos de extensiones de Picard-Vessiot.

Lema 3.11. *Sea $L|K$ una extensión diferencial y sean $\alpha_1, \ldots, \alpha_n \in L$ n soluciones linealmente independientes sobre las constantes de una ecuación diferencial lineal homogénea con coeficientes en K, $\mathcal{L}(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y' + a_0y = 0$. Entonces, si σ es un isomorfismo diferencial admisible definido en L (en particular, si $\sigma \in Gal(L|K)$), $\sigma(\alpha_j)$ es combinación lineal de $\alpha_1, \ldots, \alpha_n$ sobre las constantes (del cuerpo que contiene a L y su imagen) $\forall j \in 1, \ldots, n$.*

Demostración. Veamos que $\mathcal{L}(\sigma(\alpha_i)) = 0$, luego $\alpha_1, \ldots, \alpha_n, \sigma(\alpha_j)$ son $n+1$ soluciones de la ecuación diferencial lineal homogénea $\mathcal{L}(y) = 0$ y, por tanto, son linealmente dependientes sobre las constantes, o equivalentemente, $\sigma(\alpha_j)$ es combinación lineal de $\alpha_1, \ldots, \alpha_n$ sobre las constantes.

$$\begin{aligned}\mathcal{L}(\sigma(\alpha_j)) &= (\sigma(\alpha_j))^{(n)} + a_{n-1}(\sigma(\alpha_j))^{(n-1)} + \cdots + a_1(\sigma(\alpha_j))' + a_0\sigma(\alpha_j) \\ &= \sigma(\alpha_j^{(n)} + a_{n-1}\alpha_j^{(n-1)} + \cdots + a_1\alpha_j' + a_0\alpha_j) = \sigma(0) = 0.\end{aligned}$$

□

Dada una extensión $L|K$ de Picard-Vessiot y un morfismo diferencial $\sigma : L \to N$ sobre K, siendo N una extensión diferencial de L (σ es un isomorfismo diferencial admisible entre L y su imagen), escribimos $\sigma(\alpha_j) = \sum_{i=1}^{n} c_{ij}\alpha_i$ para cada $i = 1, \ldots, n$, siendo $\{c_{ij}\}_{i,j=1}^{n}$ constantes de N. En esta situación, podemos asociar a cada isomorfismo diferencial admisible de L sobre K la matriz de dichos coeficientes: $M(\sigma) = (c_{ij})_{i,j=1}^{n}$. Recordemos que en esta situación ($L = K\langle\alpha_1, \ldots, \alpha_n\rangle$), el morfismo diferencial σ está determinado unívocamente por la imagen de $\alpha_1, \ldots, \alpha_n$.

En el caso de que se tenga $\sigma(L) \subset L$, el propio cuerpo diferencial L puede jugar el papel de N (el cuerpo que contiene tanto a L como a su imagen). En este caso, la matriz asociada a σ está formada por constantes de L, luego de K. Obviamente, los automorfismos de $Gal(L|K)$ son un caso particular de estos.

Lema 3.12. *Sea $L|K$ una extensión diferencial y F un cuerpo diferencial intermedio de la extensión. Supongamos que $F|K$ es una extensión de Picard-Vessiot y que L tiene el mismo cuerpo de constantes que K, entonces $\sigma(F) = F$ $\forall\sigma \in Gal(L|K)$.*

Demostración. Supongamos que $F = K\langle\alpha_1, \ldots, \alpha_n\rangle$ y sea $\sigma \in Gal(L|K)$, veamos que $\sigma(\alpha_j) \in F$ $\forall j \in 1, \ldots, n$. Como $F \subset L$, por el lema anterior, $\sigma(\alpha_j)$ es combinación lineal de $\alpha_1, \ldots, \alpha_n$ sobre las constantes. Recordemos que esto quiere decir que $\sigma(\alpha_j)$ es combinación lineal de $\alpha_1, \ldots, \alpha_n$ sobre el cuerpo de constantes de cualquier cuerpo al que pertenezcan tanto $\alpha_1, \ldots, \alpha_n$, como $\sigma(\alpha_j)$, en particular, L. Como su cuerpo de constantes es el mismo que el de K y el de F, deducimos que $\sigma(\alpha_j)$ es combinación lineal

de elementos de F, luego está en F. Concluimos que $\sigma(F) \subset F$ y nuevamente, razonando con σ^{-1}, obtenemos la desigualdad contraria y, por tanto, la igualdad. □

Vamos a ver ahora dos ejemplos de cómo construir extensiones de Picard-Vessiot de un cuerpo diferencial dado.

Sea K un cuerpo diferencial y sean $a, \alpha \in K$, decimos que α es una integral de a si a es una derivada de α, es decir, $\alpha' = a$.

Lema 3.13. *Sea K un cuerpo diferencial de característica 0 y sea $a \in K$ un elemento sin integrales en K. Si α es una integral de a en alguna extensión diferencial de K, entonces α es trascendente sobre K, $K\langle\alpha\rangle$ es una extensión de Picard-Vessiot y su grupo de Galois es isomorfo al grupo aditivo de las constantes de K.*

A este proceso se le llama adjunción de una integral.

Demostración. Razonemos por reducción al absurdo. Supongamos que α es algebraico sobre K. Entonces podemos considerar $m_\alpha(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$ el polinomio mínimo de α sobre K. Recordemos que este polinomio genera el ideal en $K[X]$ de los polinomios que se anulan en α y que, por tanto, ningún polinomio no nulo de menor grado de $K[X]$ se anula en α. Nótese que $n \geq 2$ puesto que $\alpha \notin K$.

Derivando en la expresión $m_\alpha(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$, obtenemos la siguiente : $b_0 + b_1\alpha + \cdots + b_{n-2}\alpha^{n-2} + b_{n-1}\alpha^{n-1} = 0$, donde $b_i = a_i' + a(i+1)a_{i+1} \in K$ para $i = 0, 1, \ldots, n-1$. Recordemos que $\alpha' = a$ y que los coeficientes a_i no tienen por qué ser constantes, salvo $1 \in K$, cuya derivada siempre es nula. Observamos que el polinomio $P(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} \in K[X]$ es de grado a lo sumo $n-1$ y se anula en α, luego tiene que ser nulo. En otras palabras, cada uno de los b_i es nulo y, en particular, $b_{n-1} = a_{n-1}' + na = 0 \implies a = -\frac{a_{n-1}'}{n} = (-\frac{a_{n-1}}{n})'$, luego $-\frac{a_{n-1}}{n} \in K$ es una integral de a en K, absurdo. Observemos que, como se indica en la Nota 1.12, al ser K un cuerpo de característica 0, es un álgebra de Ritt y se justifica la división por n.

Para ver que $K\langle\alpha\rangle|K$ es una extensión de Picard-Vessiot, veamos que las constantes de $K\langle\alpha\rangle$ son exactamente las de K. Empecemos viendo que no hay constantes nuevas en $K[\alpha]$ y luego pasaremos a estudiar el cuerpo de fracciones. Observemos que, dado que $\alpha' = a \in K$, en este caso, $K\langle\alpha\rangle = K(\alpha)$.

Supongamos que existe una constante en $K[\alpha] \setminus K$, es decir, que existe una constante $P(\alpha) \in K[\alpha]$ de la forma $P(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + a_n\alpha^n$ con $n \geq 1$ y $a_n \neq 0$.

Derivando, $P(\alpha)' = b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0$, donde $b_i = a_i' + a(i+1)a_{i+1} \in K$ para $i = 0, 1, \ldots, n-1$ y $b_n = a_n' \in K$. Hemos encontrado un polinomio en $K[X]$ que se anula en α. Sabemos entonces que este polinomio ha de ser el polinomio nulo por ser α trascendente sobre K, es decir, $b_i = 0\ \forall i = 0, 1, \ldots, n$. En particular, $b_n = a_n' = 0$, luego a_n es una constante y $b_{n-1} = a_{n-1}' + ana_n = 0 \implies a = -\frac{a_{n-1}'}{na_n} = (-\frac{a_{n-1}}{na_n})'$, luego $-\frac{a_{n-1}}{na_n} \in K$ es una integral de a en K, lo cual es nuevamente absurdo.

Supongamos finalmente que existe una constante en $K(\alpha) \setminus K[\alpha]$, es decir, que existe una constante de la forma $P(\alpha)/Q(\alpha)$ donde $P, Q \in K[X]$, $Q(\alpha) \neq 0$ (se tiene siempre al ser α trascendente sobre K). Podemos suponer que esta expresión es irreducible, es decir, que P y Q no tienen factores comunes (son del menor grado posible) y que Q es mónico. Como además hemos visto que no puede haber constantes en $K[\alpha] \setminus K$, el grado de Q es necesariamente positivo y, además, $P(\alpha)' \neq 0 \neq Q(\alpha)'$. Derivando, observamos que:

$$\left(\frac{P(\alpha)}{Q(\alpha)}\right)' = \frac{P(\alpha)'Q(\alpha) - P(\alpha)Q(\alpha)'}{Q(\alpha)^2} = 0 \implies \frac{P(\alpha)'}{Q(\alpha)} = \frac{P(\alpha)Q(\alpha)'}{Q(\alpha)^2}$$

$$\implies P(\alpha)' = \frac{P(\alpha)Q(\alpha)'}{Q(\alpha)} \implies \frac{P(\alpha)'}{Q(\alpha)'} = \frac{P(\alpha)}{Q(\alpha)}.$$

Observemos que, por ser Q mónico y de grado positivo, $Q(\alpha)'$ es un polinomio en α de grado estrictamente menor que el de Q, lo cual va en contra de la irreducibilidad de la expresión $P(\alpha)/Q(\alpha)$.

Finalmente, observemos que 1 y α son dos soluciones de la ecuación diferencial lineal homogénea $y'' - (\frac{a'}{a})y' = 0$ y son linealmente independientes sobre las constantes, puesto que $\alpha \notin K$ y las constantes de $K\langle\alpha\rangle$ están en K.

Para terminar, veamos que el grupo de Galois de la extensión diferencial $K\langle\alpha\rangle|K$ es isomorfo al grupo aditivo $(C, +)$, donde C son las constantes de K. Sea $\sigma \in Gal(K\langle\alpha\rangle|K)$. Sabemos que σ viene unívocamente determinado por la imagen de α, que tiene que ser otra integral de a ya que, por ser σ un automorfismo diferencial, $\sigma(\alpha)' = \sigma(\alpha') = \sigma(a) = a$. Se tiene que

$$\sigma(\alpha)' = \alpha' \iff \sigma(\alpha)' - \alpha' = (\sigma(\alpha) - \alpha)' = 0 \iff (\sigma(\alpha) - \alpha) = c \iff \sigma(\alpha) = \alpha + c$$

para alguna constante c. En resumen, cada morfismo diferencial de $Gal(K\langle\alpha\rangle|K)$ es uno de los morfismos del grupo de Galois clásico que envía α en $\alpha + c$ para alguna constante $c \in C$, el cual denotaremos por σ_c (son todos ellos morfismos sobre K por ser α trascendental sobre K). Veamos que todos estos morfismos son diferenciales.

Sea $P(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in K[\alpha]$ un polinomio en α con coeficientes en K cualquiera. Entonces

$$\begin{aligned}\sigma_c(P(\alpha))' = P(\sigma_c(\alpha))' = P(\alpha + c)' &= (a_0 + a_1(\alpha + c) + \cdots + a_n(\alpha + c)^n)' \\ &= b_0 + b_1(\alpha + c) + \cdots + b_n(\alpha + c)^n,\end{aligned}$$

donde $b_i = a_i' + a(i+1)a_{i+1} \in K$ para $i = 0, 1, \ldots, n-1$, $b_n = a_n'$. Por otro lado, $P(\alpha)' = b_0 + b_1\alpha + \cdots + b_n\alpha^n$ para los mismos b_i que acabamos de definir, luego

$$\sigma_c(P(\alpha)') = b_0 + b_1(\alpha + c) + \cdots + b_n(\alpha + c)^n = \sigma_c(P(\alpha))'.$$

Ahora, para un elemento $\beta \in K\langle\alpha\rangle = K(\alpha)$ cualquiera, si escribimos $\beta = P(\alpha)/Q(\alpha)$ con $P, Q \in K[X]$, $Q(\alpha) \neq 0$, tenemos que:

$$\begin{aligned}\sigma_c(\beta)' &= \left(\sigma_c\left(\frac{P(\alpha)}{Q(\alpha)}\right)\right)' = \left(\frac{\sigma_c(P(\alpha))}{\sigma_c(Q(\alpha))}\right)' = \frac{\sigma_c(P(\alpha))'\sigma_c(Q(\alpha)) - \sigma_c(P(\alpha))\sigma_c(Q(\alpha))'}{\sigma_c(Q(\alpha))^2} \\ &= \sigma_c\left(\frac{P(\alpha)'Q(\alpha) - P(\alpha)Q(\alpha)'}{Q(\alpha)^2}\right) = \sigma_c\left(\left(\frac{P(\alpha)}{Q(\alpha)}\right)'\right) = \sigma_c(\beta')\end{aligned}$$

Tenemos entonces una correspondencia biyectiva $C \longleftrightarrow Gal(K\langle\alpha\rangle|K)$ que a cada constante $c \in C$ le hace corresponder el morfismo diferencial σ_c y a cada $\sigma \in Gal(K\langle\alpha\rangle|K$ le hace corresponder la constante $c \in C$ tal que $\sigma(\alpha) = \alpha + c$ (es decir, tal que $\sigma = \sigma_c$). Estas asignaciones son evidentemente inversas la una de la otra y, además, es claro que $\sigma_c\sigma_d = \sigma_{c+d}$, luego esta correspondencia es un isomorfismo entre el grupo $Gal(K\langle\alpha\rangle|K)$ y el grupo aditivo $(C, +)$. □

Lema 3.14. *Sea K un cuerpo diferencial, $a \in K$, $a \neq 0$ y $\alpha \neq 0$ un elemento de alguna extensión diferencial de K tal que $a = \alpha'/\alpha$. Supongamos que el cuerpo de constantes de K y el de $K\langle\alpha\rangle$ son el mismo, C. Entonces $K\langle\alpha\rangle$ es una extensión de Picard-Vessiot de K y su grupo de Galois es isomorfo al grupo multiplicativo de constantes no nulas si α es trascendental sobre K, o es un grupo cíclico finito si α es algebraico sobre K.*

A este proceso se le llama adjunción de la exponencial de una integral.

Demostración. Como α es una solución no nula de la ecuación diferencial lineal homogénea $y' - ay = 0$, $K\langle\alpha\rangle|K$ es una extensión de Picard-Vessiot. Observemos también que, como $\alpha' = a\alpha \in K$, nuevamente $K\langle\alpha\rangle = K(\alpha)$.

Sea $\sigma \in Gal(K\langle\alpha\rangle|K)$, se tiene que $\sigma(\alpha)' = \sigma(\alpha') = \sigma(a\alpha) = a\sigma(\alpha)$, de donde deducimos que $\sigma(\alpha)$ es una nueva solución de la ecuación diferencial lineal homogénea antes mencionada y, además,

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)' = \frac{\sigma(\alpha)'\alpha - \sigma(\alpha)\alpha'}{\alpha^2} = \frac{a\sigma(\alpha)\alpha - \sigma(\alpha)a\alpha}{\alpha^2} = 0 \implies \frac{\sigma(\alpha)}{\alpha} = c \implies \sigma(\alpha) = c\alpha$$

para alguna constante $c \in C$ no nula (ya que $\alpha \neq 0 \implies \sigma(\alpha) \neq 0$).

Si α es trascendente sobre K, tenemos un morfismo τ_c de $K(\alpha) = K\langle\alpha\rangle$ sobre K para cada $c \in C$, $c \neq 0$, dado por $\tau_c(\alpha) = c\alpha$, $\tau_c(b) = b\ \forall b \in K$. Veamos que estos morfismos son diferenciales. Sea $P(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in K[\alpha]$, entonces:

$$\tau_c(P(\alpha))' = P(\tau_c(\alpha))' = P(c\alpha)' = (a_0 + a_1c\alpha + \cdots + a_nc^n\alpha^n)' = b_0 + b_1c\alpha + \cdots + b_nc^n\alpha^n,$$

donde $b_i = a_i' + aia_i$, $i = 0, 1, \ldots, n$. Por otro lado, $P(\alpha)' = b_0 + b_1\alpha + \cdots + b_n\alpha^n$ para los mismos coeficientes b_i que acabamos de definir, luego

$$\tau_c(P(\alpha)') = b_0 + b_1c\alpha + \cdots + b_nc^n\alpha^n = \tau_c(P(\alpha))'.$$

Al igual que en el ejemplo anterior, lo que tenemos es una correspondencia biyectiva $C \setminus \{0\} \longleftrightarrow Gal(K\langle\alpha\rangle|K)$ que a cada $c \in C$, $c \neq 0$ le hace corresponder el morfismo diferencial τ_c y, de manera inversa, a cada $\sigma \in Gal(K\langle\alpha\rangle|K$ le hace corresponder la constante $c \in C \setminus \{0\}$ tal que $\sigma(\alpha) = c\alpha$ (es decir, tal que $\sigma = \tau_c$). Como en este caso se tiene que $\tau_c\tau_d = \tau_{cd}$ para cada $c, d \in C \setminus \{0\}$, esta correspondencia define un isomorfismo entre el grupo multiplicativo $(C \setminus \{0\},\ .\ )$ y $Gal(K\langle\alpha\rangle|K)$.

Si α es algebraico sobre K, entonces consideramos su polinomio mínimo sobre K, $m_\alpha(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in K[X]$. Derivando, la expresión $m_\alpha(\alpha) = 0$, obtenemos $m_\alpha(\alpha)' = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} + b_n\alpha^n = 0$, donde $b_i = a_i' + aia_i$ si $i = 0, 1, \ldots, n-1$ y $b_n = an$. Observamos que $anm_\alpha(\alpha) - m_\alpha(\alpha)' = 0$, luego el polinomio $P(X) = anm_\alpha(X) - m_\alpha(X)' = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, donde para cada $i = 0, 1, \ldots, n-1$, $c_i = ana_i - b_i = a(n-i)a_i - a_i'$, es un polinomio de grado estrictamente menor que n que se anula en α y, por tanto, es nulo. Entonces, para $i = 0, 1, \ldots, n-1$, $a(n-i)a_i - a_i' = 0$ y, como sabemos que $a_0 \neq 0$ al ser $m_\alpha(X)$ irreducible, se tiene que

$$\left(\frac{\alpha^n}{a_0}\right)' = \frac{ana_0\alpha^n - a_0'\alpha^n}{a_0^2} = \frac{(ana_0 - a_0)'\alpha^n}{a_0^2} = 0,$$

luego $\alpha^n/a_0 = d \implies \alpha^n = a_0d \in K$ para alguna constante $d \neq 0$ y, en particular, $X^n - a_0d$ divide a $m_\alpha(X)$, luego $m_\alpha(X) = X^n - a_0d$.

En este caso, al igual que en el trascendente, si $\sigma \in Gal(K\langle\alpha\rangle|K)$, $\sigma(\alpha) = c\alpha$ para alguna constante $c \neq 0$. Además, como $\alpha^n \in K$, $c^n\alpha^n = \sigma(\alpha)^n = \sigma(\alpha^n) = \alpha^n \implies c^n = 1$, luego el grupo $Gal(K\langle\alpha\rangle|K)$ es en este caso isomorfo al subgrupo del grupo cíclico finito de raíces n-ésimas de la unidad en K engendrado por c (que no es necesariamente una raíz primitiva). □

Vamos a ver el interés especial que tienen estos dos tipos de extensiones de Picard-Vessiot. Para ello, primero veremos el concepto de *grupo resoluble* y cómo caracterizarlos.

3.6. Grupos resolubles y extensiones de Liouville

Definición. Dados un grupo G y $x, y \in G$, denotamos por $[x, y] = xyx^{-1}y^{-1}$ al *conmutador* de x e y. Denotamos por $[G, G]$ al subgrupo de G engendrado por todos los conmutadores de elementos de G, al cual llamaremos *grupo derivado de G*. Si $x, y, z \in G$, entonces $z^{-1}[x, y]z = [z^{-1}xz, z^{-1}yz] \in [G, G]$, luego $[G, G]$ es un subgrupo normal de G. Este subgrupo cumple que $G/[G, G]$ es abeliano y es el menor subgrupo con esta propiedad ya que, si H es un subgrupo normal de G tal que G/H es abeliano, claramente todos los conmutadores $[x, y]$ de G tienen que estar en H, luego $[G, G] \subset H$.

Escribimos $D^0G = G$, $D^1G = [G, G]$ y, de manera inductiva, $D^iG = [D^{i-1}G, D^{i-1}G]$ para $i \geq 0$. Dados dos grupos A, B, la notación $A \triangleleft B$ (o $B \triangleright A$) indica que A es un subgrupo normal de B. Entonces, llamamos la *serie derivada de G* a la cadena $G = D^0G \triangleright D^1G \triangleright D^2G \triangleright \dots$

Decimos que G es *resoluble* si su serie derivada termina en el grupo trivial, es decir, si existe $n \in \mathbb{N}$ tal que $D^nG = \{1\}$.

Proposición 3.15. *Un grupo G es resoluble si, y solo si, existe una cadena finita de subgrupos $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$ tal que G_{i-1}/G_i es abeliano para cada $i = 1, \dots, n$.*

Demostración. Si G es resoluble, la serie derivada de G cumple esta condición, así que solo hay que ver el recíproco. Supongamos que existe una tal cadena de subgrupos $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$ tal que G_{i-1}/G_i es abeliano para cada $i = 1, \dots, n$. Como hemos visto antes como $G_1 \triangleleft G$ y G/G_1 es abeliano, $D^1G \subset G_1$. Evidentemente, si A y B son dos grupos con $A \subset B$, entonces se tiene $D^1A \subset D^1B$, luego en este caso, $D^1G \subset G_1 \implies D^2G \subset D^1G_1$. De igual forma, como $G_2 \triangleleft G_1$ y G_1/G_2 es abeliano, $D^1G_1 \subset G_2$ y por tanto, $D^2G \subset D^1G_1 \subset G_2$. Siguiendo este razonamiento, de manera recursiva, deducimos que $D^iG \subset G_i$ para cada $i = 1, \dots, n$. Por tanto, e n particular, $D^nG \subset G_n = \{1\} \implies D^nG = \{1\}$, luego G es resoluble. □

Definición. Decimos que una extensión diferencial $L|K$ es *de Liouville* si existe una cadena de cuerpos intermedios $K = F_0 \subset F_1 \subset \cdots \subset F_n = L$ tales que para cada $i = 1, \dots, n$, F_i es una extensión de F_{i-1} obtenida por adjunción de una integral o de la exponencial de una integral.

Teorema 3.16. *Sea L una extensión de Liouville de un cuerpo diferencial K con el mismo cuerpo de constantes, entonces $Gal(L|K)$ es un grupo resoluble.*

Demostración. Si $K = F_0 \subset F_1 \subset \cdots \subset F_n = L$ es una cadena de extensiones como la descrita en la definición anterior, vamos a ver que se tiene la cadena de subgrupos

$$Gal(L|K) \triangleright Gal(L|F_1) \triangleright Gal(L|F_2) \triangleright \cdots \triangleright Gal(L|F_{n-1}) \triangleright Gal(L|L) = \{1\}$$

y que $Gal(L|F_{i-1})/Gal(L|F_i)$ es abeliano para cada $i = 1, \ldots, n$. Empecemos viendo que $Gal(L|F_i)$ es un subgrupo normal de $Gal(L|F_{i-1})$. Que es subgrupo ya lo sabemos ($F_{i-1} \subset F_i \implies F_{i-1}^* \supset F_i^*$). Además, como hemos visto antes, F_i es una extensión de Picard-Vessiot de F_{i-1} y ambos tienen el mismo cuerpo de constantes que K, luego por el Lema 3.12, $\sigma(F_i) = F_i \ \forall \sigma \in Gal(L|F_{i-1})$ y, por el Teorema 3.3 b), $F_i^* = Gal(L|F_i)$ es un subgrupo normal de $Gal(L|F_{i-1})$. Además, este teorema asegura también que $Gal(L|F_{i-1})/Gal(L|F_i)$ es isomorfo a un subgrupo de $Gal(F_i|F_{i-1})$, luego es abeliano. □

Teorema 3.17. *Sea $L|K$ una extensión diferencial normal de cuerpos y $\alpha_1, \ldots, \alpha_n \in L$ tales que para todo $\sigma \in Gal(L|K)$, $\sigma(\alpha_j) = a_{1j}\alpha_1 + \cdots + a_{jj}\alpha_j$, $j = 1, \ldots, n$ para ciertas constantes $a_{ij} \in L$, $1 \leq i \leq j \leq n$, que dependen de σ. Entonces $K\langle \alpha_1, \ldots \alpha_n \rangle$ es una extensión de Liouville de K.*

Demostración. Hagamos inducción sobre n. Para cualquier $\sigma \in Gal(L|K)$, se tiene que $\sigma(\alpha_1) = a_{11}\alpha_1$ y, derivando, $\sigma(\alpha_1') = a_{11}\alpha_1'$, luego $\sigma(\alpha_1'/\alpha_1) = \alpha_1'/\alpha_1$, es decir, α_1'/α_1 queda fijo por todos los morfismos de $Gal(L|K)$ y, como L es normal sobre K, esto implica que $\alpha_1'/\alpha_1 \in K$. Por tanto, la extensión $K\langle \alpha_1 \rangle | K$ se obtiene adjuntando una integral, luego $K\langle \alpha_1 \rangle$ es una extensión de Liouville de K.

Supongamos ahora el resultado cierto para $n-1$ y veámoslo para n. Repitiendo el razonamiento anterior, deducimos que nuevamente $K\langle \alpha_1 \rangle$ se obtiene adjuntando una integral a K. Sea $\sigma \in Gal(L|K)$, si a la ecuación j-ésima le restamos la primera, obtenemos:

$$\sigma\left(\frac{\alpha_j}{\alpha_1}\right) = \frac{a_{1j}}{a_{11}} + \frac{a_{2j}}{a_{11}}\left(\frac{\alpha_2}{\alpha_1}\right) + \cdots + \frac{a_{jj}}{a_{11}}\left(\frac{\alpha_j}{\alpha_1}\right),$$

y ahora, derivando:

$$\sigma\left(\frac{\alpha_j}{\alpha_1}\right)' = \frac{a_{2j}}{a_{11}}\left(\frac{\alpha_2}{\alpha_1}\right)' + \cdots + \frac{a_{jj}}{a_{11}}\left(\frac{\alpha_j}{\alpha_1}\right)'.$$

Observamos que hemos obtenido para cada $\sigma \in Gal(L|K)$ una condición análoga a la del enunciado sobre los elementos $(\alpha_2/\alpha_1)', \ldots, (\alpha_n/\alpha_1)'$. Por hipótesis de inducción,

$K\langle\alpha_1, (\alpha_2/\alpha_1)', \ldots, (\alpha_n/\alpha_1)'\rangle$ es una extensión de Liouville y, por tanto, concluimos que $K\langle\alpha_1, (\alpha_2/\alpha_1), \ldots, (\alpha_n/\alpha_1)\rangle = K\langle\alpha_1, \ldots \alpha_n\rangle$ también lo es, ya que se obtiene de la anterior adjuntando $(\alpha_2/\alpha_1), \ldots, (\alpha_n/\alpha_1)$, es decir, adjuntando integrales.

□

4. Grupos algebraicos

Antes de ver el concepto de grupo algebraico y de entender su relevancia en la teoría de extensiones diferenciales, vamos a repasar varios resultados relacionados con ideales de polinomios y variedades afines.

4.1. Conjuntos algebraicos afines y topología de Zariski

Dado un cuerpo K, denotaremos por $\mathbb{A}^n_K$ o, simplemente $\mathbb{A}^n$ si no hay ambigüedad, al espacio afín n-dimensional sobre K, o en otras palabras, a $K^n = K \times \cdots \times K$ dotado de estructura afín.

Dado $f \in K[X_1, \ldots, X_n]$, denotamos por $\mathcal{V}(f)$ al conjunto de ceros de f en $\mathbb{A}^n$, es decir, $\mathcal{V}(f) = \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n : f(\mathbf{x}) = 0\} \subset \mathbb{A}^n$. En general, dado $S \subset K[X_1, \ldots, X_n]$ un conjunto de polinomios cualquiera, definimos $\mathcal{V}(S) = \{\mathbf{x} \in \mathbb{A}^n : f(\mathbf{x}) = 0 \ \forall f \in S\}$. Decimos que un subconjunto V de $\mathbb{A}^n$ es un *conjunto algebraico afín* si es de la forma $V = \mathcal{V}(S)$ para algún $S \subset K[X_1, \ldots, X_n]$. Si I es el ideal generado por S en $K[X_1, \ldots, X_n]$, se tiene que $\mathcal{V}(S) = \mathcal{V}(I) = \mathcal{V}(\sqrt{I})$, luego todo conjunto algebraico puede expresarse como imagen de un ideal, que puede además considerarse radical. Los conjuntos algebraicos de la forma $V = \mathcal{V}(f)$ para algún $f \in K[X_1, \ldots, X_n]$ se denominan *hipersuperficies* de $\mathbb{A}^n$. Análogamente, para cualquier subconjunto $V \subset \mathbb{A}^n$, vamos a definir $\mathcal{I}(V) = \{f \in K[X_1, \ldots, X_n] : f(\mathbf{x}) = 0 \ \forall \mathbf{x} \in V\}$, que resulta ser un ideal radical de $K[X_1, \ldots, X_n]$.

Si I, I_1 e I_2 son ideales de $K[X_1, \ldots, X_n]$ y V, V_1 y V_2 son subconjuntos de $\mathbb{A}^n$, se verifican las siguientes propiedades:

i) $I \subset \mathcal{I}(\mathcal{V}(I)) \quad ; \quad V \subset \mathcal{V}(\mathcal{I}(V))$.

ii) $I_1 \subset I_2 \implies \mathcal{V}(I_1) \supset \mathcal{V}(I_2) \quad ; \quad V_1 \subset V_2 \implies \mathcal{I}(V_1) \supset \mathcal{I}(V_2)$.

iii) $\mathcal{V}(I) = \mathcal{V}(\mathcal{I}(\mathcal{V}(I))) \quad ; \quad \mathcal{I}(V) = \mathcal{I}(\mathcal{V}(\mathcal{I}(V)))$.

A mayores, los conjuntos algebraicos cumplen las siguientes propiedades, de gran interés:

i) $\mathcal{V}(\cup_{i\in\Lambda} I_i) = \cap_{i\in\Lambda} \mathcal{V}(I_i)$.

ii) $\mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$, donde si I y J son ideales, $IJ = \langle\{fg : f \in I, g \in J\}\rangle$.

iii) $\mathcal{V}(K[X_1, \ldots, X_n]) = \emptyset$.

iv) $\mathcal{V}(0) = \mathbb{A}^n$

En otras palabras: los conjuntos algebraicos de $\mathbb{A}^n$ son cerrados para intersecciones arbitrarias y uniones finitas y tanto el conjunto vacío como el total son algebraicos. Los conjuntos algebraicos cumplen por tanto los axiomas de conjuntos cerrados y definen una topología en $\mathbb{A}^n$, la *topología de Zariski*. En $\mathbb{A}^n_{\mathbb{R}}$ y $\mathbb{A}^n_{\mathbb{C}}$, esta topología es menos fina que la usual, ya que los conjuntos algebraicos son también cerradas para esta, al ser los conjuntos de ceros de ciertas aplicaciones continuas (los polinomios). Esta topología va a ser de gran importancia e interés cuando hablemos de grupos algebraicos y los relacionemos con la teoría de Galois diferencial que venimos desarrollando.

El *teorema de la base de Hilbert* afirma que si A es un *anillo noetheriano*, entonces también lo es $A[X_1, \ldots, X_n]$. Entonces, por ser K un cuerpo (que siempre son noetherianos como anillos), $K[X_1, \ldots, X_n]$ es un anillo noetheriano y, por tanto, todo ideal en $K[X_1, \ldots, X_n]$ es finitamente generado. En consecuencia, todo conjunto algebraico puede expresarse como intersección finita de hipersuperficies: si $V = \mathcal{V}(I)$ con $I = \langle f_1, \ldots, f_r \rangle$, entonces $V = \mathcal{V}(I) = \mathcal{V}(\langle f_1, \ldots, f_r \rangle) = \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r)$.

Un conjunto algebraico $V \subset \mathbb{A}^n$ es *reducible* si existen dos conjuntos algebraicos V_1 y V_2 distintos de V tales que $V = V_1 \cup V_2$; en caso contrario diremos que V es *irreducible*. Una caracterización importante es la siguiente: un conjunto algebraico V es irreducible si, y solo si, $\mathcal{I}(V)$ es un ideal primo de $K[X_1, \ldots, X_n]$. A los conjuntos algebraicos irreducibles de $\mathbb{A}^n$ se les denomina también *variedades afines*. Todo conjunto algebraico V se expresa de manera única como unión finita de conjuntos algebraicos irreducibles, $V = V_1 \cup \cdots \cup V_n$. Los V_i se llaman *componentes irreducibles de* V y esta igualdad es la *descomposición* de V en componentes irreducibles.

Uno de los resultados principales sobre conjuntos algebraicos es el *teorema de los ceros de Hilbert*. Como resultado previo, se tiene el *teorema débil de los ceros de Hilbert*, que afirma que si K es algebraicamente cerrado e $I \subset K[X_1, \ldots, X_n]$ es un ideal propio, entonces $\mathcal{V}(I) \neq \emptyset$. El resultado para una sola variable es trivial: todo ideal propio de $K[X]$ está engendrado por un único polinomio (no constante) al ser $K[X]$ un dominio de ideales principales. Este polinomio tiene al menos una raíz en K (un cero, de ahí el nombre), y dicha raíz es cero de todo polinomio del ideal. Este teorema sería una generalización de este resultado a un numero finito cualquiera de variables y un número finito cualquiera de polinomios.

El *teorema de los ceros de Hilbert* se apoya en este resultado y va más allá. Si K es algebraicamente cerrado, entonces $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ para cualquier ideal I de $K[X_1, \ldots, X_n]$.

La condición de que K sea algebraicamente cerrado es necesaria para ambos teoremas. Si consideramos $f(X) = X^2 + 1 \in \mathbb{R}[X]$, observamos que $V(f) = V(\langle f \rangle) = \emptyset \subset \mathbb{A}^n_{\mathbb{R}}$ pese a que, evidentemente, $\langle f \rangle \subsetneq \mathbb{R}[X]$, luego no se cumple el teorema débil. Además, $\mathcal{I}(\mathcal{V}(\langle f \rangle)) = \mathcal{I}(\emptyset) = K[X_1, \ldots, X_n]$ mientras que $\sqrt{\langle f \rangle} = \langle f \rangle$ puesto que f es irreducible en $\mathbb{R}[X]$, luego tampoco se cumple el teorema de ceros.

Como resultado de este teorema, si K es algebraicamente cerrado y $V = \mathcal{V}(I)$ es un conjunto algebraico, se tiene que $\mathcal{I}(V) = \mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\mathcal{V}(\sqrt{I})) = \sqrt{I}$ y, además, $\mathcal{V}(\mathcal{I}(V)) = \mathcal{V}(\mathcal{I}(\mathcal{V}(I))) = \mathcal{V}(I) = V$, luego estas correspondencias son biyectivas e inversas la una de la otra entre los conjuntos algebraicos de $\mathbb{A}^n$ y los ideales radicales de $K[X_1, \ldots, X_n]$. Además, si I es un ideal radical, entonces $V = \mathcal{V}(I)$ es irreducible si, y solo si, $\mathcal{I}(V) = \mathcal{I}(\mathcal{V}(I)) = I$ es primo, luego las variedades se corresponden con ideales primos y viceversa. Si $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ es un punto de $\mathbb{A}^n$, entonces $\{P\} = \mathcal{V}(\langle X_1 - a_1, \ldots, X_n - a_n \rangle)$, siendo $m_P = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ un ideal maximal (luego primo) de $K[X_1, \ldots, X_n]$. Además, si $m \subset K[X_1, .., X_n]$ es un ideal maximal, entonces la variedad que define (que es no vacía por el teorema débil) es unipuntual. En resumen, si K es algebraicamente cerrado, se tienen las siguientes correspondencias biyectivas entre subconjuntos de $\mathbb{A}^n$ e ideales de $K[X_1, \ldots, X_n]$:

$$\begin{aligned} \{\text{Conjuntos algebraicos de } \mathbb{A}^n\} &\longleftrightarrow \{\text{Ideales radicales de } K[X_1, \ldots, X_n]\} \\ \{\text{Variedades de } \mathbb{A}^n\} &\longleftrightarrow \{\text{Ideales primos de } K[X_1, \ldots, X_n]\} \\ \{\text{Puntos de } \mathbb{A}^n\} &\longleftrightarrow \{\text{Ideales maximales de } K[X_1, \ldots, X_n]\} \end{aligned}$$

Volviendo a la topología de Zariski, recordamos que esta es la topología en $\mathbb{A}^n$ cuyos cerrados son los conjuntos algebraicos. Como mencionamos previamente, cada conjunto algebraico puede expresarse como intersección finita de hipersuperficies, luego basta con tomar estas como base de cerrados para generar la misma topología. Los conjuntos de la forma $V_f = \{\mathbf{x} \in \mathbb{A}^n : f(\mathbf{x}) \neq 0\} \subset \mathbb{A}^n$ donde $f \in K[X_1, \ldots, X_n]$, es decir, los complementarios de las hipersuperficies ($V_f = \mathbb{A}^n \setminus \mathcal{V}(f)$), son abiertos de esta topología y se denominan *conjuntos abiertos básicos*, ya que forman, de hecho, una base de la topología de Zariski.

Dado un conjunto cualquiera $V \subset \mathbb{A}^n$, se tiene que $\mathcal{V}(\mathcal{I}(V)) \subset \mathbb{A}^n$ es su clausura topológica en $\mathbb{A}^n$ para esta topología, ya que es un conjunto algebraico con $V \subset \mathcal{V}(\mathcal{I}(V))$ y, si $W \subset \mathbb{A}^n$ es otro conjunto algebraico con $V \subset W$, entonces $\mathcal{I}(V) \supset \mathcal{I}(W)$ y, por

tanto, $\mathcal{V}(\mathcal{I}(V)) \subset \mathcal{V}(\mathcal{I}(W)) = W$. En consecuencia, $V \subset \mathbb{A}^n$ es cerrado si, y solo si, $V = \mathcal{V}(\mathcal{I}(V))$, es decir, si, y solo si, $\forall\, \mathbf{x} \notin V$, existe $f \in \mathcal{I}(V)$, es decir, con $f|_V = 0$, tal que $f(\mathbf{x}) \neq 0$.

Si en $\mathbb{A}^n$ se considera la topología de Zariski, en un subconjunto $V \subset \mathbb{A}^n$ se induce una topología de subespacio, que llamaremos la topología de Zariski de V. Si $V = \mathcal{V}(I_1) \subset \mathbb{A}^n$ es un conjunto algebraico, sus cerrados para esta topología son de la forma $V \cap \mathcal{V}(I_2) = \mathcal{V}(I_1) \cap \mathcal{V}(I_2) = \mathcal{V}(I_1 \cup I_2) = \mathcal{V}(I_1 + I_2)$ con $I_2 \subset K[X_1, \ldots, X_n]$, ya que $I_1 + I_2 = \langle I_1 \cup I_2 \rangle$. Equivalentemente, los cerrados de $V = \mathcal{V}(I)$ son los cerrados de $\mathbb{A}^n$ de la forma $\mathcal{V}(J)$ con $I \subset J \subset K[X_1, \ldots, X_n]$ (siendo I y J ideales o no).

Dados dos conjuntos algebraicos afines $V_1 = \mathcal{V}(I_1) \subset \mathbb{A}^n$ y $V_2 = \mathcal{V}(I_2) \subset \mathbb{A}^m$, donde $I_1 \subset K[X_1, \ldots, X_n]$ e $I_2 \subset K[Y_1, \ldots, Y_m]$, su producto cartesiano $V_1 \times V_2$ es un conjunto algebraico de $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$ ya que dado $\mathbf{z} = (\mathbf{x}, \mathbf{y}) = (x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{A}^{n+m}$, entonces $\mathbf{z} \in V_1 \times V_2 \iff \mathbf{x} \in V_1$ e $\mathbf{y} \in V_2 \iff f(\mathbf{x}) = 0\ \forall f \in I_1$ y $g(\mathbf{y}) = 0\ \forall g \in I_2$. Vamos a considerar el conjunto (no ideal):

$$S = \{f(X_1, \ldots, X_n) : f \in I_1\} \cup \{g(Y_1, \ldots, Y_m) : g \in I_2\} \subset K[X_1, \ldots, X_n, Y_1, \ldots, Y_m].$$

Entonces se observa que $\mathbf{z} \in V_1 \times V_2 \iff \mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathcal{V}(S)$, es decir, $V_1 \times V_2 = \mathcal{V}(S)$.

Como con cualquier producto de espacios topológicos, en $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$ se induce una topología, producto de las topologías de Zariski en $\mathbb{A}^n$ y $\mathbb{A}^m$. Esta topología resulta ser menos fina que la topología de Zariski de $\mathbb{A}^{n+m}$.

Lema 4.1. *La topología de Zariski de $\mathbb{A}^{n+m}$ es más fina que la topología que se induce como producto de los espacios $\mathbb{A}^n$ y $\mathbb{A}^m$ con sus respectivas topologías de Zariski.*

Demostración. Por un lado, la topología producto está generada por el producto de los abiertos de las bases de las respectivas topologías. En este caso, si $f \in K[X_1, \ldots, X_n]$ y $g \in K[Y_1, \ldots, Y_n]$, entonces

$$\begin{aligned} \mathbf{z} = (\mathbf{x}, \mathbf{y}) \in V_f \times V_g &\iff \mathbf{x} \in V_f \text{ e } \mathbf{y} \in V_g \\ &\iff f(\mathbf{x}) \neq 0 \text{ y } g(\mathbf{y}) \neq 0 \\ &\iff \mathbf{z} \notin \mathcal{V}(\tilde{f}) \subset \mathbb{A}^{n+m} \text{ y } \mathbf{z} \notin \mathcal{V}(\tilde{g}) \subset \mathbb{A}^{n+m}, \end{aligned}$$

donde $\tilde{f}(X_1, \ldots, X_n, Y_1, \ldots, Y_m) = f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ y, análogamente, $\tilde{g}(X_1, \ldots, X_n, Y_1, \ldots, Y_m) = g(Y_1, \ldots, Y_m) \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$. En otras palabras, $V_f \times V_g = (\mathbb{A}^{n+m} \setminus \mathcal{V}(\tilde{f})) \cap (\mathbb{A}^{n+m} \setminus \mathcal{V}(\tilde{g})) = \mathbb{A}^{n+m} \setminus (\mathcal{V}(\tilde{f}) \cup \mathcal{V}(\tilde{g})) = \mathbb{A}^{n+m} \setminus \mathcal{V}(\tilde{f}\tilde{g})$,

que es un abierto para la topología de Zariski de $\mathbb{A}^{n+m}$, es decir, todo abierto de una base de la topología producto (y por tanto, toda la topología producto) es abierto para la topología de Zariski de $\mathbb{A}^{n+m}$.

Sin embargo, no todo subconjunto de $\mathbb{A}^{n+m}$ cerrado para la topología de Zariski, es cerrado en la topología producto de las respectivas topologías de Zariski en $\mathbb{A}^n$ y $\mathbb{A}^m$. Por ejemplo, consideramos $\Delta = \{(x, x) : x \in \mathbb{C}\} \subset \mathbb{A}^2_{\mathbb{C}} = A^1_{\mathbb{C}} \times \mathbb{A}^1_{\mathbb{C}}$. Este conjunto es cerrado para la topología de Zariski de $A^2_{\mathbb{C}}$ ya que $\Delta = \mathcal{V}(x - y)$. Sin embargo, decir que $\Delta \subset \mathbb{A}^1_{\mathbb{C}} \times \mathbb{A}^1_{\mathbb{C}}$ es cerrado para la topología producto equivale a decir que $\mathbb{A}^1_{\mathbb{C}}$ con la topología de Zariski es un espacio de Hausdorff, y no lo es. Esto se debe a que dos abiertos no vacíos cualesquiera de $A^1_{\mathbb{C}}$ con esta topología tienen intersección no vacía: si $I_1, I_2 \in \mathbb{C}[X]$, al ser $\mathbb{C}[X]$ un dominio de ideales principales, existen $f_1, f_2 \in \mathbb{C}[X]$ tales que $I_1 = \langle f_1 \rangle$ e $I_2 = \langle f_2 \rangle$ y $(\mathbb{A}^1_{\mathbb{C}} \setminus \mathcal{V}(f_1)) \cap (\mathbb{A}^1_{\mathbb{C}} \setminus \mathcal{V}(f_2)) = \mathbb{A}^1_{\mathbb{C}} \setminus (\mathcal{V}(f_1) \cup \mathcal{V}(f_2)) = \mathbb{A}^1_{\mathbb{C}} \setminus \mathcal{V}(f_1 f_2)$. Si ambos abiertos eran no vacíos, es decir, $\mathcal{V}(I_i) \neq \mathbb{A}^1_{\mathbb{C}}$, $i = 1, 2$, entonces $f_i \neq 0$, $i = 1, 2$, luego $f_1 f_2 \neq 0$ y por tanto, $\mathcal{V}(f_1 f_2) \neq \mathbb{A}^1_{\mathbb{C}}$ ya que al ser $f_1 f_2$ un polinomio no nulo, tiene un número finito de raíces, luego la intesección de los abiertos es $\mathbb{A}^1_{\mathbb{C}} \setminus \mathcal{V}(f_1 f_2) \neq \emptyset$.

Este razonamiento sobre $\mathbb{C}$ sirve para cualquier cuerpo infinito (un polinomio no nulo sobre un cuerpo finito puede anularse en todo el cuerpo, por ejemplo, $X^q - X \in \mathbb{F}_q[X]$ con $q = p^r$, p primo), luego si K es un cuerpo infinito (en particular, si es algebraicamente cerrado), la topología de Zariski de $\mathbb{A}^2_K$ es estrictamente más fina que el producto de las topología de Zariski de $\mathbb{A}^1_K$ consigo mismo. □

Nos interesará especialmente, para enlazar con la teoría de Galois diferencial, estudiar el conjunto de matrices invertibles como un conjunto algebraico (y más adelante, como un grupo algebraico). Es sencillo identificar el conjunto de las matrices de tamaño $n \times n$ con $\mathbb{A}^{n^2}$, escribiendo las n filas de una matriz seguidas, con n coeficientes cada una, en forma de vector; y viceversa, reordenando los n^2 coeficientes de un vector como una matriz $n \times n$ por filas. Si por $GL(n, K)$ denotamos al conjunto de las matrices invertibles de tamaño $n \times n$ sobre K, habitualmente denominado el *grupo lineal general*, lo podríamos identificar con un cierto subconjunto de $\mathbb{A}^{n^2}$. La cuestión es que la propiedad que define a los elementos de dicho subconjunto, es decir, la de tener determinante no nulo como matriz, es precisamente una condición de no anulación de un polinomio (recordemos que el determinante de una matriz cuadrada se puede expresar como un polinomio en sus coeficientes). En otras palabras, si consideramos $GL(n, K)$ como subconjunto de $\mathbb{A}^{n^2}$, este es un abierto básico de su topología de Zariski y no un conjunto algebraico, como nos gustaría.

Lema 4.2. *Un abierto básico de $\mathbb{A}^n$, es decir, un subconjunto $V_f \subset \mathbb{A}^n$ de la forma $V_f = \{\boldsymbol{x} \in \mathbb{A}^n : f(\boldsymbol{x}) \neq 0\}$ con $f \in K[X_1, \ldots, X_n]$, es homeomorfo al conjunto algebraico $\mathcal{V}(g) \subset \mathbb{A}^{n+1}$ donde $g(X_1, \ldots, X_{n+1}) = f(X_1, \ldots, X_n)X_{n+1} - 1 \in K[X_1, \ldots, X_{n+1}]$, cuando en ambos conjuntos se considera la topología de Zariski como subespacios de $\mathbb{A}^n$ y $\mathbb{A}^{n+1}$ respectivamente.*

Demostración. Vamos a ver que la aplicación

$$\begin{aligned} \varphi\colon V_f &\longrightarrow \mathcal{V}(g) \\ \mathbf{x} &\longmapsto \Big(\mathbf{x}, \frac{1}{f(\mathbf{x})}\Big), \end{aligned}$$

está bien definida y es un homeomorfismo entre V_f y $\mathcal{V}(g)$. Para empezar, está bien definida porque si $\mathbf{x} = (x_1, \ldots, x_n) \in V_f$, entonces $f(\mathbf{x}) \neq 0$, luego $1/f(\mathbf{x}) \in K$ tiene sentido y $g(\mathbf{x}, 1/f(\mathbf{x})) = f(\mathbf{x}) \cdot (1/f(\mathbf{x})) - 1 = 0 \implies (\mathbf{x}, 1/f(\mathbf{x})) \in \mathcal{V}(g)$. Además,

$$(x_1, \ldots, x_n, x_{n+1}) = (\mathbf{x}, x_{n+1}) \in \mathcal{V}(g) \iff f(\mathbf{x}) \cdot x_{n+1} = 1 \iff \begin{cases} f(\mathbf{x}) \neq 0 \ \ (\mathbf{x} \in V_f) \\ \quad \text{y} \\ x_{n+1} = 1/f(\mathbf{x}) \end{cases},$$

luego φ es biyectiva y la proyección desde $\mathcal{V}(g) \subset \mathbb{A}^{n+1}$ en las primeras n coordenadas, que tiene llegada en V_f, es su inversa.

Veamos que es abierta y continua, luego es un homeomorfismo. Sea $h \in K[X_1, \ldots, X_n]$ y consideramos $\tilde{h}(X_1, \ldots, X_{n+1}) = h(X_1, \ldots, X_n) \in K[X_1, \ldots, X_{n+1}]$. Entonces,

$$\begin{aligned} \varphi\big(V_f \cap V_h\big) &= \varphi\big(\{\mathbf{x} \in V_f : h(\mathbf{x}) \neq 0\}\big) \\ &= \{(\mathbf{x}, x_{n+1}) \in \mathcal{V}(g) : h(\mathbf{x}) \neq 0\} \\ &= \{(\mathbf{x}, x_{n+1}) \in \mathcal{V}(g) : \tilde{h}(\mathbf{x}, x_{n+1}) \neq 0\} = \mathcal{V}(g) \cap V_{\tilde{h}}\ , \end{aligned}$$

es decir, todo abierto básico de V_f (que es la intersección de un abierto básico de $\mathbb{A}^n$ con V_f), se envía por φ en un abierto básico de $\mathcal{V}(g)$, luego φ es abierta.

Finalmente, si $p \in K[X_1, \ldots, X_{n+1}]$, entonces es de la forma

$$p(X_1, \ldots, X_{n+1}) = \sum_{\boldsymbol{\lambda} \in \mathbb{N}^{n+1}} a_{\boldsymbol{\lambda}} X^{\boldsymbol{\lambda}} = \sum_{\boldsymbol{\lambda} \in \mathbb{N}^{n+1}} a_{\boldsymbol{\lambda}} X_1^{\lambda_1} \ldots X_{n+1}^{\lambda_{n+1}}$$

donde $a_{\boldsymbol{\lambda}} = 0$ salvo para un número finito de valores de $\boldsymbol{\lambda} \in \mathbb{N}^{n+1}$. Sea r el máximo valor de λ_{n+1} que aparece en los $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_{n+1})$ que definen p con $a_{\boldsymbol{\lambda}} \neq 0$, entonces

$$\tilde{p}(X_1, \ldots, X_n) = \sum_{\boldsymbol{\lambda} \in \mathbb{N}^{n+1}} a_{\boldsymbol{\lambda}} X_1^{\lambda_1} \ldots X_n^{\lambda_n} \cdot f(X_1, \ldots, X_n)^{r - \lambda_{n+1}}$$

es un polinomio en $K[X_1, \ldots, X_n]$ ya que $r - \lambda_{n+1} \geq 0 \ \forall \boldsymbol{\lambda} \in \mathbb{N}^{n+1}$ con $a_{\boldsymbol{\lambda}} \neq 0$. Observemos que, si $(x_1, \ldots, x_n, x_{n+1}) = (\mathbf{x}, x_{n+1}) \in \mathcal{V}(g)$, entonces, como vimos antes, necesariamente $f(\mathbf{x}) \neq 0$ y $x_{n+1} = 1/f(\mathbf{x})$, luego p adquiere la expresión

$$p(\mathbf{x}, x_{n+1}) = p\Big(\mathbf{x}, \frac{1}{f(\mathbf{x})}\Big) = \sum_{\boldsymbol{\lambda} \in \mathbb{N}^{n+1}} a_{\boldsymbol{\lambda}} x_1^{\lambda_1} \ldots x_n^{\lambda_n} \cdot \Big(\frac{1}{f(x_1, \ldots, x_n)}\Big)^{\lambda_{n+1}}$$

y, dado que $f(\mathbf{x}) \neq 0$, se tiene que

$$p(\mathbf{x}, x_{n+1}) = p\Big(\mathbf{x}, \frac{1}{f(\mathbf{x})}\Big) \neq 0 \iff p\Big(\mathbf{x}, \frac{1}{f(\mathbf{x})}\Big) \cdot f(\mathbf{x})^r = \tilde{p}(\mathbf{x}) \neq 0$$

y entonces,

$$\begin{aligned} \varphi^{-1}\big(\mathcal{V}(g) \cap V_p\big) &= \varphi^{-1}\big(\{(\mathbf{x}, x_{n+1}) \in \mathcal{V}(g) : p(\mathbf{x}, x_{n+1}) \neq 0\}\big) \\ &= \{\mathbf{x} \in V_f : p(\varphi(\mathbf{x})) = p(\mathbf{x}, 1/f(\mathbf{x})) \neq 0\} \\ &= \{\mathbf{x} \in V_f : \tilde{p}(\mathbf{x}) \neq 0\} = V_f \cap V_{\tilde{p}}, \end{aligned}$$

es decir, la contraimagen por φ de un abierto básico de $\mathcal{V}(g)$ es un abierto básico de V_f, luego φ es continua.

□

Como consecuencia, podemos considerar $GL(n, K) \subset \mathbb{A}^{n^2}$ y, en general, cualquier abierto básico, como un conjunto algebraico para toda cuestión topológica.

4.2. Grupos algebraicos

Vamos a introducir el concepto de *grupo algebraico* y a ver el rol que juega en la teoría de Galois diferencial.

Definición. Un *grupo algebraico* $(G, \ . \ )$ sobre K es un conjunto algebraico $G \subset \mathbb{A}_K^n$ dotado de una estructura de grupo de forma que, al considerar en G la topología de Zariski como subespacio de $\mathbb{A}_K^n$, la aplicación $\iota : G \to G$, con $\iota(x) = x^{-1}$ es continua y la aplicación $\mu : G \times G \to G$, donde $\mu(x, y) = xy$ es separadamente continua en sus dos variables, es decir, para cada $x_0 \in G$ fijo, las aplicaciones $x \mapsto \mu(x, x_0) = x \cdot x_0$ y $x \mapsto \mu(x_0, x) = x_0 \cdot x$ son ambas continuas.

Normalmente, en un abuso de notación, diremos que G es un grupo algebraico, sin especificar la operación que aporta la estructura de grupo.

Es importante notar que la condición de continuidad que se pide para el producto en G es más débil que pedir su continuidad global en $G \times G$ como función de dos variables. Toda función continua es separadamente continua en sus variables, pero no recíprocamente. Un ejemplo de función separadamente continua en sus variables pero no globalmente continua se ve en [6, pág 31, ej 1.20].

Vamos a hablar ahora de funciones polinómicas y racionales. Conviene notar la diferencia entre un polinomio sobre K, que es una expresión formal, y la función polinómica que define, que es una aplicación de $\mathbb{A}^n_K$ en K.

Definición. Decimos que una función $f : \mathbb{A}^n \to K$ es una *polinómica* si existe un polinomio $P \in K[X_1, \ldots, X_n]$ tal que $f(\mathbf{x}) = P(\mathbf{x})$ para todo $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n$. Generalmente, confundiremos la función polinómica con el polinomio que la define (lo hemos estado haciendo hasta ahora cuando hablábamos de conjuntos algebraicos como ceros de polinomios, cuando son técnicamente los ceros de la función racional asociada), pero conviene hacer la distinción a la hora de hablar de funciones racionales.

Decimos que una función $r : S \to K$ con $S \subset \mathbb{A}^n$ es *racional* si existen polinomios $P, Q \in K[X_1, \ldots, X_n]$ tales que $Q(\mathbf{x}) \neq 0$ en S ($S \subset V_Q$) y $r(\mathbf{x}) = P(\mathbf{x})/Q(\mathbf{x})$ para todo $\mathbf{x} = (x_1, \ldots, x_n) \in S$. Equivalentemente, r es racional si existen dos funciones polinómicas $p, q : S \to \mathbb{A}^n$ tales que q no se anula en S y $r(\mathbf{x}) = p(\mathbf{x})/q(\mathbf{x})$ para todo $\mathbf{x} \in S$.

Es importante hacer aquí la distinción entre polinomio y función polinomial ya que, las expresiones del tipo $P(X_1, \ldots, X_n)/Q(X_1, \ldots, X_n)$ con $P, Q \in K[X_1, \ldots, X_n]$ y $Q \neq 0$ forman $K(X_1, \ldots, X_n)$, que se suele llamar el *cuerpo de funciones racionales*, pero cuyos elementos no definen una función en todo $\mathbb{A}^n$. Aunque Q sea no nulo, la función polinomial que define puede anularse en algunos puntos de $\mathbb{A}^n$, y esta expresión que, como expresión formal, está perfectamente definida, no da lugar a una función definida en dichos puntos.

Lema 4.3. *Sea $r : S \to \mathbb{A}^m$ una aplicación cuyas m componentes $r_1, \ldots, r_m$ son funciones racionales en las variables $X_1, \ldots, X_n$, es decir, $r_i = p_i/q_i$ con p_i, q_i funciones polinómicas y $q_i(\boldsymbol{x}) \neq 0$ si $\boldsymbol{x} \in S$ para cada $i = 1, \ldots, m$ ($S \subset V_{q_1} \cap \cdots \cap V_{q_m}$). Entonces, la función $r : S \to \mathbb{A}^m$ es continua al considerar en ambos espacios la topología de Zariski.*

Demostración. Para probar la continuidad de r, es decir, que la imagen inversa por r de un abierto de $\mathbb{A}^m$ es un abierto de S, veremos equivalentemente que la imagen inversa por r de un cerrado de $\mathbb{A}^m$ es un cerrado de S.

Sea $V \subset A^m$ un cerrado para la topología de Zariski, es decir, $V = \mathcal{V}(f_1, \ldots, f_s)$ con $f_1, \ldots, f_s \in K[Y_1, \ldots, Y_m]$. Sea $g_i = f_i \circ r = f_i(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}) \in K(X_1, \ldots, X_n)$ para $i = 1, \ldots, s$. Entonces,

$$\begin{aligned} r^{-1}(V) &= \{\mathbf{x} \in S : r(\mathbf{x}) =\in \mathcal{V}(f_1, \ldots, f_s)\} \\ &= \{\mathbf{x} \in S : f_i(r(\mathbf{x})) = 0 \ \forall i = 1, \ldots, s\} \\ &= \{\mathbf{x} \in S : g_i(\mathbf{x}) = 0 \ \forall i = 1, \ldots, s\} \end{aligned}$$

Las funciones g_i son funciones racionales cuyos denominadores son productos y potencias de los q_j. Entonces, si se toma $N \in \mathbb{N}$ como el mayor exponente al que aparece elevada cada una de las incógnitas $Y_1, \ldots, Y_m$ en las expresiones de $f_1, \ldots, f_s$, se tiene que $(q_1 \ldots q_m)^N g_i \in K[X_1, \ldots, X_n]$ para cada $i = 1, \ldots, s$. Como las funciones $q_1, \ldots, q_m$ no se anulan en S, $r^{-1}(V)$, que como hemos visto, es el subconjunto de S donde se anulan las g_i, coincide con el subconjunto de S donde se anula $(q_1 \ldots q_m)^N g_i \in K[X_1, \ldots, X_n]$, luego es cerrado en S para la topología de Zariski.

□

Corolario 4.4. *Toda función $f : \mathbb{A}^n \to \mathbb{A}^m$ cuyas funciones componentes son polinómicas, es continua para las respectivas topologías de Zariski.*

A partir de ahora, el cuerpo sobre el que trabajaremos será $K = C$ un cuerpo algebraicamente cerrado de característica 0. El ejemplo de grupo algebraico que nos interesa y con el cual vamos a trabajar de ahora en adelante es el del grupo lineal general, $GL(n, C)$.

Corolario 4.5. *El grupo lineal general $GL(n, C)$ de las matrices invertibles o regulares de tamaño $n \times n$ sobre C es un grupo algebraico sobre C.*

Demostración. Sabemos que el conjunto $GL(n, C)$ tiene una estructura de grupo para el producto de matrices y ya vimos anteriormente que puede considerarse como un conjunto algebraico. Para cualquier matriz $X = (X_{ij})_{i,j=1}^n \in GL(n, C)$, el producto por una matriz fija $A = (A_{ij})_{i,j=1}^n \in GL(n, C)$ se expresa componente a componente como:

$$X \longmapsto AX; \ \ (AX)_{ij} = \sum_{k=1}^{n} A_{ik} X_{kj}$$

$$X \longmapsto XA; \ \ (XA)_{ij} = \sum_{k=1}^{n} X_{ik} A_{kj}$$

que son expresiones polinómicas en las variables $\{X_{ij}\}_{i,j=1}^n$. Por otro lado, la inversa de X tiene la expresión, componente a componente:

$$X \longmapsto X^{-1} = \frac{1}{det(X)} Adj(X)^T; \ \ (X^{-1})_{ij} = \frac{(-1)^{i+j} det(\hat{X}_{ji})}{det(X)},$$

donde $\hat{X}_{ij}$ es la matriz que se obtiene al eliminar la i-ésima fila y la j-ésima columna de X. Esta es claramente una expresión racional en las variables $\{X_{ij}\}_{i,j=1}^{n}$, al ser el determinante una función polinómica en dichas variables y por ser no nulo para las matrices de este grupo. En virtud del Lema, todas estas funciones son continuas y, por tanto, $GL(n, C)$ es un grupo algebraico para la operación del producto de matrices. □

5. Teorema fundamental de la teoría de Galois

Vamos finalmente a enlazar estos conceptos con la teoría de Galois diferencial. Ya vimos que el grupo de Galois de una extensión diferencial es isomorfo a cierto grupo de matrices invertibles. Veremos que dicho subconjunto viene dado por el conjunto de ceros de una serie de polinomios y esto permite dotar al grupo de Galois de dicha extensión de una estructura de grupo algebraico.

5.1. El grupo algebraico de Galois

En todos los resultados posteriores, el cuerpo diferencial K tiene característica 0 y cuerpo de constantes $C \subset K$, algebraicamente cerrado.

Proposición 5.1. *Si $L = K\langle \alpha_1, \dots, \alpha_n \rangle$ es una extensión de Picard-Vessiot de K y σ es un isomorfismo diferencial admisible de L sobre K, entonces $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ son linealmente independientes sobre las constantes (de cualquier cuerpo que los contenga).*

Demostración. Observemos que, dadas n indeterminadas diferenciales $Z_1, \dots, Z_n$ sobre K, el Wronskiano de dichas inderminadas, $W(Z_1, \dots, Z_n)$ dado por el determinante de su matriz fundamental, es un polinomio diferencial en dichas indeterminadas con coeficientes en $\mathbb{Z} \subset \mathbb{Q} \subset K$, es decir, $W(Z_1, \dots, Z_n) \in \mathbb{Z}\{Z_1, \dots, Z_n\} \subset K\{Z_1, \dots, Z_n\}$. Como σ es un morfismo diferencial sobre K, $W(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) = \sigma(W(\alpha_1, \dots, \alpha_n)) \neq 0$ ya que σ es inyectivo por ser un morfismo de cuerpos y $W(\alpha_1, \dots, \alpha_n) \neq 0$ por el Teorema 3.9, al ser $\alpha_1, \dots, \alpha_n$ linealmente independientes sobre las constantes, luego también $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ son linealmente independientes sobre las constantes.

□

***Nota* 5.2.** Recordemos que en el Lema 3.11 vimos cómo a cada isomorfismo diferencial admisible de L sobre K, siendo $L|K$ una extensión de Picard-Vessiot, se le puede asociar una matriz de constantes de alguna extensión diferencial de L que contiene tanto a L como a su imagen. Sea N dicha extensión de L ($\sigma(L) \subset N$) y sean C y D los cuerpos de constantes de K y N respectivamente (C es también el cuerpo de constantes de L). Veamos que $M(\sigma) = (c_{ij})_{i,j=1}^n$ siendo cada c_{ij} una constante de D, es una matriz invertible. Supongamos que no lo fuera, entonces existen constantes $d, \dots, d_n \in D$ no todas nulas tales que $M(\sigma)(d_1, \dots, d_n)^T = (0, \dots, 0)^T$, es decir, tales que $\sum_{j=1}^n c_{ij} d_j = 0$ para cada $i = 1, \dots, n$. Entonces,

$$\sum_{j=1}^{n} d_j \sigma(\alpha_j) = \sum_{j=1}^{n} d_j \Big(\sum_{i=1}^{n} c_{ij} \alpha_i \Big) = \sum_{i=1}^{n} \Big(\sum_{j=1}^{n} c_{ij} d_j \Big) \alpha_i = \sum_{i=1}^{n} 0 \cdot \alpha_i = 0,$$

lo cual es absurdo ya que, en virtud de la Proposición 5.1, $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ son linealmente independientes sobre las constantes.

Vimos también en el Lema 3.11 el caso particular en el que $\sigma(L) \subset L$ y las constantes $\{c_{ij}\}_{i,j=1}^n$ se toman en C. Dijimos que el caso de los automorfismos diferenciales del grupo $Gal(L|K)$ eran un caso particular de este, pero, de hecho, no es tan particular, ya que podemos comprobar que si σ es un homomorfismo diferencial de L en L sobre K siendo $L = K\langle\alpha_1, \ldots, \alpha_n\rangle$ una extensión de Picard-Vessiot de K, entonces es un isomorfismo, es decir, todos los isomorfismos diferenciales σ de L sobre K con $\sigma(L) \subset L$ cumplen, de hecho, que $\sigma(L) = L$ y son, por tanto, automorfismos del grupo $Gal(L|K)$. Como todo homomorfismo de cuerpos es inyectivo, dado un homomorfismo diferencial $\sigma : L \to L$ sobre K, falta comprobar que es también sobreyectivo. Como $L = K\langle\alpha_1, \ldots, \alpha_n\rangle$, solo hace falta ver que $\alpha_j \in \mathrm{Im}(\sigma)\ \forall j = 1, \ldots, n$. Como la matriz $M(\sigma) = (c_{ij})_{i,j=1}^n$ es invertible, si consideramos $((c_{ij})_{i,j=1}^n)^{-1} = (d_{ij})_{i,j=1}^n \in GL(n, C)$ y tomamos $\beta_j = \sum_{i=1}^n d_{ij}\alpha_i \in L$ para cada $j = 1, \ldots, n$, entonces,

$$\begin{aligned}\sigma(\beta_j) &= \sum_{k=1}^n d_{kj}\sigma(\alpha_k) = \sigma\Big(\sum_{k=1}^n d_{kj}\alpha_k\Big) = \sum_{k=1}^n d_{kj}\Big(\sum_{i=1}^n c_{ik}\alpha_i\Big) \\ &= \sum_{i=1}^n \Big(\sum_{k=1}^n c_{ik}d_{kj}\alpha_i\Big) = \sum_{i=1}^n \Big(\sum_{k=1}^n c_{ik}d_{kj}\Big)\alpha_i = \alpha_j.\end{aligned}$$

Si $\sigma, \tau \in Gal(L|K)$, se comprueba fácilmente que $M(\sigma\tau) = M(\sigma)M(\tau)$ y dado que evidentemente $M(id_L) = Id$, será $M(\sigma)^{-1} = M(\sigma^{-1})$. Se define así un homomorfismo $M : Gal(L|K) \longrightarrow GL(n, C)$ (grupo de matrices invertibles de tamaño $n \times n$ sobre C). Deducimos entonces que el grupo de Galois de una extensión de Picard-Vessiot es isomorfo a cierto subgrupo del grupo de matrices invertibles sobre C, $M(Gal(L|K))$ (nótese que $M(\sigma) = Id \iff \sigma = id_L$ porque $L = K\langle\alpha_1, \ldots, \alpha_n\rangle$). Vamos a encontrar este subgrupo.

Proposición 5.3. *Sea $L|K$ una extensión diferencial de Picard-Vessiot, $L = K\langle\alpha_1, \ldots, \alpha_n\rangle$, con cuerpo de constantes C. Entonces existe un conjunto de polinomios S sobre C en las variables $\{X_{ij}\}_{i,j=1}^n$ tales que:*

i) Si σ es un isomorfismo diferencial admisible sobre K definido en L, con L y $\sigma(L)$ subcurpos diferenciales de M para cierta extensión diferencial M de L con cuerpo de constantes $D \subset M$ y $\sigma(\alpha_j) = \sum_{i=1}^n c_{ij}\alpha_i$, $j = 1, \ldots, n$, siendo $\{c_{ij}\}_{i,j=1}^n \subset D$ constantes de M, entonces $F((c_{ij})_{i,j=1}^n) = 0$ para todo polinomio $F \in S$.

ii) Dada una extensión diferencial M de L con cuerpo de constantes D y dada una matriz $(c_{ij})_{i,j=1}^n \in GL(n, D)$ tal que $F((c_{ij})_{i,j=1}^n) = 0\ \forall F \in S$, existe un isomorfismo

diferencial admisible σ entre $L = K\langle\alpha_1, \ldots, \alpha_n\rangle$ y otro subcuerpo diferencial F de M dado por $\sigma(\alpha_j) = \sum_{i=1}^{n} c_{ij}\alpha_i \; \forall j = 1, \ldots, n$.

Demostración. Sea $K\{Z_1, \ldots, Z_n\}$ el anillo de polinomios diferenciales sobre K en n indeterminadas diferenciales. Recordemos no confundir este anillo con su cuerpo de fracciones, $K\langle Z_1, \ldots, Z_n\rangle$. Consideramos el morfismo diferencial sobre K, $\varphi : K\{Z_1, \ldots, Z_n\} \to L$, dado por $\varphi(Z_j) = \alpha_j$ y sea $\Gamma = \mathrm{Ker}(\varphi)$, que es un ideal de $K\{Z_1, \ldots, Z_n\}$, evidentemente primo y, como sabemos (Teorema 1.7), diferencial. Sea $L[\{X_{ij}\}_{i,j=1}^{n}]$ el anillo de polinomios sobre L en las indeterminadas $\{X_{ij}\}_{i,j=1}^{n}$, donde consideramos la derivación definida por $X'_{ij} = 0 \;\; \forall\, i, j = 1, \ldots, n$. Definimos ahora el morfismo diferencial ψ sobre K, $\psi : K\{Z_1, \ldots, Z_n\} \to L[\{X_{ij}\}_{i,j=1}^{n}]$, con $\psi(Z_j) = \sum_{i=1}^{n} X_{ij}\alpha_i$ y sea $\Delta = \psi(\Gamma) \subset L[\{X_{ij}\}_{i,j=1}^{n}]$. Dado que $C \subset K \subset L$, podemos considerar una base $\{w_k\}_{k\in\Lambda}$ de L como espacio vectorial sobre C. Cada elemento de Δ es un polinomio con coeficientes en L, los cuales son, a su vez, combinación lineal de los w_k sobre C. Entonces, podemos escribir todos los elementos de Δ como combinaciones lineales de los w_k sobre el anillo de polinomios $C[\{X_{ij}\}_{i,j=1}^{n}]$. Sea $S \subset C[\{X_{ij}\}_{i,j=1}^{n}]$ el conjunto de los coeficientes de dichas combinaciones lineales. Veamos que este conjunto de polinomios cumple todo lo pedido.

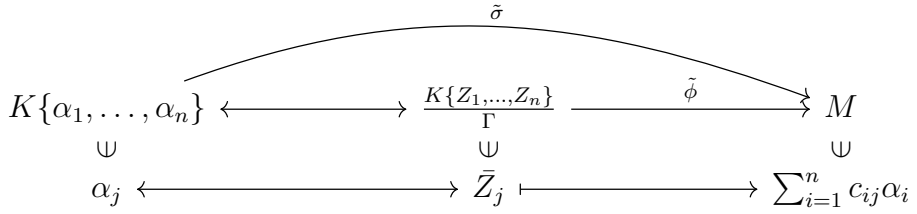
i) Sea $\sigma : L \to M$ un homomorfismo diferencial de cuerpos sobre K, siendo M una extensión diferencial de L ($\sigma : L \to \sigma(L) = F$ es un isomorfismo diferencial admisible), y sea $D \subset M$ el cuerpo de constantes de M. Por el Lema 3.11, existen n^2 constantes $\{c_{ij}\}_{i,j=1}^{n} \subset D$ tales que $\sigma(\alpha_j) = \sum_{i=1}^{n} c_{ij}\alpha_i \; \forall j = 1, \ldots, n$. Definimos el morfismo diferencial $\nu : L[\{X_{ij}\}_{i,j=1}^{n}] \to M$ sobre L, con $\nu(X_{ij}) = c_{ij}$. Tenemos el siguiente diagrama, claramente conmutativo:

$$\begin{array}{ccc}
K\{Z_1, \ldots, Z_n\} & \xrightarrow{\qquad\varphi\qquad} & L \\
\Big\downarrow{\scriptstyle \psi} & Z_j \longmapsto \alpha_j & \Big\downarrow{\scriptstyle \sigma} \\
\sum_{i=1}^{n} X_{ij}\alpha_i & \longmapsto & \sum_{i=1}^{n} c_{ij}\alpha_i \\
L[\{X_{ij}\}_{i,j=1}^{n}] & \xrightarrow[\qquad\nu\qquad]{} & M
\end{array}$$

Si nos fijamos en $\Gamma = \mathrm{Ker}(\varphi)$, por un lado, tenemos que $(\sigma\circ\varphi)(\Gamma) = \sigma(\varphi(\Gamma)) = \sigma(0) = 0$. Por otro lado, $(\nu \circ \psi)(\Gamma) = \nu(\psi(\Gamma)) = \nu(\Delta)$ y, dado que el diagrama es conmutativo, $\nu(\Delta) = 0$, es decir, los polinomios de Δ se anulan al evaluarlos en los c_{ij}. Como $\{w_k\}_{k\in\Lambda}$ es una base de L como C-espacio vectorial, como vimos en el Lema 2.4, cada polinomio de $L[\{X_{ij}\}_{i,j=1}^{n}]$ puede expresarse de forma única como combinación lineal de los w_k

sobre $C[\{X_{ij}\}_{i,j=1}^n]$. Una combinación lineal de los w_k con polinomios de $C[\{X_{ij}\}_{i,j=1}^n]$ puede ser nula solo si todos estos polinomios son nulos. Por tanto, que se anulen todos los polinomios en Δ al evaluarlos en c_{ij}, equivale a que se anulen cada uno de sus coeficientes (en $C[\{X_{ij}\}_{i,j=1}^n]$) al escribir estos polinomios como combinación lineal de los w_k sobre $C[\{X_{ij}\}_{i,j=1}^n]$, es decir, todos los polinomios de S se anulan al evaluarlos en $(c_{ij})_{i,j=1}^n$.

ii) Sea M una extensión diferencial de L con cuerpo de constantes D y sea una matriz $(c_{ij})_{i,j=1}^n \in GL(n,D)$ tal que $F((c_{ij})_{i,j=1}^n) = 0\ \forall F \in S$. Consideramos el morfismo diferencial sobre K, $\phi : K\{Z_1,\dots,Z_n\} \to M$, dado por $\phi(Z_j) = \sum_{i=1}^n c_{ij}\alpha_i$. Observamos que $\phi = \nu \circ \psi$. Entonces, $\phi(\Gamma) = (\nu\circ\psi)(\Gamma) = \nu(\Delta)$ y, como por hipótesis, todos los polinomios de S (que son los coeficientes en la base $\{w_k\}_{k\in\Lambda}$ de los polinomios de Δ) se anulan al evaluarlos en $(c_{ij})_{i,j=1}^n$, $\phi(\Gamma) = \nu(\Delta) = 0$, luego $\Gamma \subset \mathrm{Ker}(\phi)$ y, por tanto, ϕ induce un nuevo morfismo diferencial $\tilde{\phi} : \frac{K\{Z_1,\dots,Z_n\}}{\Gamma} \to M$. Como $\Gamma = \mathrm{Ker}(\varphi)$ y $\varphi(K\{Z_1,\dots,Z_n\}) = K\{\alpha_1,\dots,\alpha_n\}$, $\frac{K\{Z_1,\dots,Z_n\}}{\Gamma} \cong K\{\alpha_1,\dots,\alpha_n\}$, luego obtenemos un morfismo diferencial sobre K, $\tilde{\sigma} : K\{\alpha_1,\dots,\alpha_n\} \to K\{\alpha_1,\dots,\alpha_n\}$, dado por:



Cada elemento de $K\{\alpha_1,\dots,\alpha_n\}$ es de la forma $P(\alpha_1,\dots,\alpha_n)$ con $P \in K\{X_1,\dots,X_n\}$ y se tiene que $\tilde{\sigma}(P(\alpha_1,\dots,\alpha_n)) = P(\tilde{\sigma}(\alpha_1),\dots,\tilde{\sigma}(\alpha_n))$, al ser $\tilde{\sigma}$ un morfismo diferencial sobre K. Entonces, $\mathrm{Im}(\tilde{\sigma}) = \tilde{\sigma}(K\{\alpha_1,\dots,\alpha_n\}) \subset K\{\tilde{\sigma}(\alpha_1),\dots,\tilde{\sigma}(\alpha_n)\}$. Como obviamente $K\{\tilde{\sigma}(\alpha_1),\dots,\tilde{\sigma}(\alpha_n)\} \subset \mathrm{Im}(\tilde{\sigma})$, si restringimos la imagen y consideramos entonces $\tilde{\sigma} : K\{\alpha_1,\dots,\alpha_n\} \to K\{\tilde{\sigma}(\alpha_1),\dots,\tilde{\sigma}(\alpha_n)\}$, tenemos un morfismo diferencial de anillos sobreyectivo. Vamos a ver que, así definido, $\tilde{\sigma}$ es biyectivo.

Veamos que $\tilde{\sigma}$ es inyectivo. Supongamos que existe $z \in K\{\alpha_1,\dots,\alpha_n\}$ no nulo con $z \in ker(\tilde{\sigma})$. En particular, $z \notin K$ ya que si $z \in K$, por ser $\tilde{\sigma}$ un morfismo sobre K, $\tilde{\sigma}(z) = z \neq 0$. Más aún, z no puede ser algebraico sobre K, porque en ese caso, si $m_z^K(X) = a_0 + a_1X + \cdots + a_{m-1}X^{m-1} + X^m \in K[X]$ fuera su polinomio mínimo, se tendría que $0 = m_z^K(z)$, luego

$$0 = \tilde{\sigma}(m_z^K(z)) = \tilde{\sigma}(a_0 + a_1z + \cdots + z^m) = a_0 + a_1\tilde{\sigma}(z) + \cdots + \tilde{\sigma}(z)^m = a_0,$$

luego $m_z^K(X) = X(a_1 + a_2X + \cdots + X^{m-1})$ y, como $m > 1$ porque $z \notin K$, $m_z^K(X)$ no sería irreducible.

Sabemos entonces que z tiene que ser trascendente sobre K. Veamos primero que el grado de trascendencia de $K\langle\alpha_1,\dots,\alpha_n\rangle$ sobre K es finito. Equivalentemente, vamos a ver que si β es una solución de una ecuación diferencial lineal homogénea con coeficientes en K, $\mathcal{L}(y)=y^{(n)}+a_{n-1}y^{(n-1)}+\cdots+a_1y'+a_0y=0$, entonces $K\langle\beta\rangle=K(\beta,\beta',\dots,\beta^{(n-1)})$. Entonces, sabremos que $\operatorname{trdeg}(K\langle\beta\rangle|K)=\operatorname{trdeg}(K(\beta,\beta',\dots,\beta^{(n-1)})|K)\leq n$ y, en nuestro caso, el grado de trascendencia de $K\langle\alpha_1,\dots,\alpha_n\rangle$ sobre K será finito al haberse adjuntado una cantidad finita de soluciones de una ecuación diferencial lineal homogénea. Sabemos que, evidentemente, $K\langle\beta\rangle=K(\beta,\beta',\dots)\supset K(\beta,\beta',\dots,\beta^{(n-1)})$, veamos por inducción en $k\in\mathbb{N}$ que $\beta^{(k)}\in K[\beta,\beta',\dots,\beta^{(n-1)}]\subset K(\beta,\beta',\dots,\beta^{(n-1)})$ para todo $k\geq n$. En el caso $k=n$, tenemos que

$$\mathcal{L}(\beta)=\beta^{(n)}+a_{n-1}\beta^{(n-1)}+\cdots+a_1\beta'+a_0\beta=0\implies$$
$$\implies\beta^{(n)}=-(a_{n-1}\beta^{(n-1)}+\cdots+a_1\beta'+a_0\beta)=P(\beta,\beta',\dots,\beta^{(n-1)})\in K[\beta,\beta',\dots,\beta^{(n-1)}],$$

donde $P\in K[X_0,\dots,X_{n-1}]$. Ahora, supongamos que $\beta^{(k)}\in K[\beta,\beta',\dots,\beta^{(n-1)}]$ para cierto $k\geq n$, es decir, que existe $Q\in K[X_0,\dots,X_{n-1}]$ tal que $\beta^{(k)}=Q(\beta,\beta',\dots,\beta^{(n-1)})$, veamos que entonces $\beta^{(k+1)}\in K[\beta,\beta',\dots,\beta^{(n-1)}]$ también. Debido a que, si se deriva un polinomio en las variables $\beta,\beta',\dots,\beta^{(n-1)}$ lo que se obtiene es un polinomio en las variables $\beta,\beta',\dots,\beta^{(n)}$ de grado a lo sumo 1 en $\beta^{(n)}$, se tiene que

$$\begin{aligned}\beta^{(k+1)}&=(\beta^{(k)})'=(Q(\beta,\dots,\beta^{(n-1)}))'=Q_1((\beta,\dots,\beta^{(n-1)}))\beta^{(n)}+Q_2(\beta,\dots,\beta^{(n-1)})\\&=Q_1((\beta,\dots,\beta^{(n-1)}))\cdot P(\beta,\beta',\dots,\beta^{(n-1)})+Q_2(\beta,\dots,\beta^{(n-1)})\\&=\tilde{Q}(\beta,\dots,\beta^{(n-1)})\in K[\beta,\beta',\dots,\beta^{(n-1)}].\end{aligned}$$

Observemos que podemos encontrar una base de trascendencia de $K\langle\alpha_1,\dots,\alpha_n\rangle$ sobre K de la forma $\{z_1,\dots,z_r\}$ formada únicamente por elementos de $K\{\alpha_1,\dots,\alpha_n\}$ y con $z_1=z$, ya que z es trascendente sobre K y podemos ir añadiendo elementos de $K\{\alpha_1,\dots,\alpha_n\}$ hasta conseguir un conjunto con el mayor número de elementos algebraicamente independientes sobre K posible, es decir, $\{z_1,\dots,z_r\}$ es algebraicamente independiente y $\{z_1,\dots,z_r,z_{r+1}\}$ es algebraicamente dependiente sobre K para cualquier elemento $z_{r+1}\in K\{\alpha_1,\dots,\alpha_n\}$. Entonces todo elemento de $K\{\alpha_1,\dots,\alpha_n\}$ es algebraico sobre $K(z_1,\dots,z_n)$ y, por tanto, todo elemento de $K\langle\alpha_1,\dots,\alpha_n\rangle$ es a su vez algebraico sobre $K(z_1,\dots,z_n)$, ya que este elemento será de la forma a/b con $a,b\in K\{\alpha_1,\dots,\alpha_n\}$ y $b\neq0$ y, al ser a y b algebraicos sobre $K(z_1,\dots,z_n)$, el cuerpo $K(z_1,\dots,z_n,a,b)$ es una extensión algebraica de $K(z_1,\dots,z_n)$, luego $a/b\in K(z_1,\dots,z_n,a,b)$ es algebraico sobre $K(z_1,\dots,z_n)$. Entonces, $\{z_1,\dots,z_r\}$ es una base de trascendencia de $K\langle\alpha_1,\dots,\alpha_n\rangle$ sobre K y contiene a z.

Veamos finalmente que si $\{z_1,\dots,z_r\}\subset K\{\alpha_1,\dots,\alpha_n\}$, con $z_1=z$ es una base de trascendencia de $K\langle\alpha_1,\dots,\alpha_n\rangle$ sobre K, entonces $K\langle\tilde\sigma(\alpha_1),\dots,\tilde\sigma(\alpha_n)\rangle$ es algebraico sobre la extensión diferencial $K(\tilde\sigma(z_1),\tilde\sigma(z_2),\dots,\tilde\sigma(z_r))=K(\tilde\sigma(z_2),\dots,\tilde\sigma(z_r))$ y, en particular, $\operatorname{trdeg}(K\langle\alpha_1,\dots,\alpha_n\rangle|K)=r>r-1\geq\operatorname{trdeg}(K\langle\tilde\sigma(\alpha_1),\dots,\tilde\sigma(\alpha_n)\rangle|K)$. Sea u un elemento cualquiera de $K\{\tilde\sigma(\alpha_1),\dots,\tilde\sigma(\alpha_n)\}$, entonces existe algún polinomio diferencial $P\in K\{X_1,\dots,X_n\}$ tal que $u=P(\tilde\sigma(\alpha_1),\dots,\tilde\sigma(\alpha_n))=\tilde\sigma(P(\alpha_1,\dots,\alpha_n))$. En otras palabras, $u=\tilde\sigma(t)$ donde $t=P(\alpha_1,\dots,\alpha_n)\in K\{\alpha_1,\dots,\alpha_n\}\subset K\langle\alpha_1,\dots,\alpha_n\rangle$. Como $\{z_1,\dots,z_r\}$ es una base de trascendencia de $K\langle\alpha_1,\dots,\alpha_n\rangle$ sobre K, $\{z_1,\dots,z_r,t\}$ es un conjunto algebraicamente dependiente sobre K, es decir, existe un polinomio $f\in K[X_1,\dots,X_{r+1}]$ tal que $f(z_1,\dots,z_r,t)=0$. Equivalentemente, existe un polinomio $f\in K[z_1,\dots,z_r][X]$ con $f(t)=0$. Sea f un polinomio en $K[z_1,\dots,z_r][X]$ con $f(t)=0$, de menor grado posible (en X). Entonces, si

$$f(X)=f_0(z_1,\dots,z_r)+f_1(z_1,\dots,z_r)X+\cdots+f_k(z_1,\dots,z_r)X^k$$

con $f_j\in K[X_1,\dots,X_r]\ \forall j=1,\dots,k$, se tiene que

$$\begin{aligned}0=\tilde\sigma(0)=\tilde\sigma(f(t))&=\tilde\sigma(f_0(z_1,\dots,z_r)+f_1(z_1,\dots,z_r)t+\cdots+f_k(z_1,\dots,z_r)t^k)\\&=\tilde\sigma(f_0(z_1,\dots,z_r))+\tilde\sigma(f_1(z_1,\dots,z_r))u+\cdots+\tilde\sigma(f_k(z_1,\dots,z_r))u^k\\&=f_0(\tilde\sigma(z_1),\dots,\tilde\sigma(z_r))+f_1(\tilde\sigma(z_1),\dots,\tilde\sigma(z_r))u+\cdots+f_k(\tilde\sigma(z_1),\dots,\tilde\sigma(z_r))u^k\\&=\tilde f_0(\tilde\sigma(z_2),\dots,\tilde\sigma(z_r))+\tilde f_1(\tilde\sigma(z_2),\dots,\tilde\sigma(z_r))u+\cdots+\tilde f_k(\tilde\sigma(z_2),\dots,\tilde\sigma(z_r))u^k\\&=g(\tilde\sigma(z_2),\dots,\tilde\sigma(z_r),u),\quad g\in K[X_2,\dots,X_{r+1}],\end{aligned}$$

siendo $\tilde f_j(X_2,\dots,X_r)=f_j(0,X_2,\dots,X_r)\in K[X_2,\dots,X_r]$ para cada $j=0,\dots,k$. Concluimos que $\{\tilde\sigma(z_2),\dots,\tilde\sigma(z_r),u\}$ es un conjunto algebraicamente dependiente sobre K, salvo que se tenga que el polinomio g es nulo, es decir, cada uno de los $\tilde f_j$ es nulo. Pero en este caso,

$$\begin{aligned}&0=\tilde f_0(\tilde\sigma(z_2),\dots,\tilde\sigma(z_r))=f_0(\tilde\sigma(z_1),\dots,\tilde\sigma(z_r))=\tilde\sigma(f_0(z_1,\dots,z_r))\implies\\&\implies\tilde\sigma(f(t)-f_0(z_1,\dots,z_r))=\tilde\sigma(t(f_1(z_1,\dots,z_r)+\cdots+f_k(z_1,\dots,z_r)t^{k-1}))=0.\end{aligned}$$

Como $\tilde\sigma(t)=u\neq0$, se tiene que $\tilde\sigma(f_1(z_1,\dots,z_r)+\cdots+f_k(z_1,\dots,z_r)t^{k-1})=0$, siendo $f_1(z_1,\dots,z_r)+\cdots+f_k(z_1,\dots,z_r)X^{k-1}$ un polinomio en $K[z_1,\dots,z_r][X]$ de menor grado que f, lo cual es absurdo. Concluimos que todo elemento de $K\{\tilde\sigma(\alpha_1),\dots,\tilde\sigma(\alpha_n)\}$ es algebraico sobre $K(\tilde\sigma(z_2),\dots,\tilde\sigma(z_r))$. Entonces, también lo es todo elemento del cuerpo diferencial $K\langle\tilde\sigma(\alpha_1),\dots,\tilde\sigma(\alpha_n)\rangle$ como vimos anteriormente, es decir, $K\langle\tilde\sigma(\alpha_1),\dots,\tilde\sigma(\alpha_n)\rangle$ es una extensión algebraica de $K(\tilde\sigma(z_2),\dots,\tilde\sigma(z_r))$.

Recordemos que, si K_2 es un cuerpo intermedio de una extensión $K_1|K_3$, se tiene que $\operatorname{trdeg}(K_3|K_1)=\operatorname{trdeg}(K_3|K_2)+\operatorname{trdeg}(K_2|K_1)$. Hemos demostrado (simplificando la notación) que $\operatorname{trdeg}(K\langle\boldsymbol\alpha\rangle|K)>\operatorname{trdeg}(K\langle\tilde\sigma(\boldsymbol\alpha)\rangle|K)$, luego, como acabamos de observar,

$\mathrm{trdeg}(K\langle\boldsymbol{\alpha},\tilde{\sigma}(\boldsymbol{\alpha})\rangle|K\langle\boldsymbol{\alpha}\rangle) < \mathrm{trdeg}(K\langle\boldsymbol{\alpha},\tilde{\sigma}(\boldsymbol{\alpha})\rangle|K\langle\tilde{\sigma}(\boldsymbol{\alpha})\rangle)$ y todos estos grados de trascendencia son finitos al ser los α_j y los $\tilde{\sigma}(\alpha_j)$ soluciones de una ecuación diferencial lineal homogénea sobre K. Observemos que, dado que $\alpha_j = \sum_{i=1}^{n} c_{ij}\alpha_i \ \forall j = 1,\ldots,n$, $\mathrm{trdeg}(K\langle\boldsymbol{\alpha},\tilde{\sigma}(\boldsymbol{\alpha})\rangle|K\langle\boldsymbol{\alpha}\rangle) = \mathrm{trdeg}(K\langle\boldsymbol{\alpha},\boldsymbol{c}\rangle|K\langle\boldsymbol{\alpha}\rangle) = \mathrm{trdeg}(C(\boldsymbol{c})|C)$, siendo $\boldsymbol{c} = \{c_{ij}\}_{i,j=1}^{n}$. Vamos a demostrar esta última igualdad.

Para empezar, observemos que, como las $c_{ij} \in D$ son constantes, $K\langle\boldsymbol{\alpha},\boldsymbol{c}\rangle = K\langle\boldsymbol{\alpha}\rangle(\boldsymbol{c})$, luego, si $\mathrm{trdeg}(K\langle\boldsymbol{\alpha},\boldsymbol{c}\rangle|K\langle\boldsymbol{\alpha}\rangle) = \mathrm{trdeg}(K\langle\boldsymbol{\alpha}\rangle(\boldsymbol{c})|K\langle\boldsymbol{\alpha}\rangle) = l$, entonces existe una base de trascendencia $\{\tilde{c}_1,\ldots,\tilde{c}_l\}$ de $K\langle\boldsymbol{\alpha}\rangle(\boldsymbol{c})$ sobre $K\langle\boldsymbol{\alpha}\rangle$ con $\{\tilde{c}_1,\ldots,\tilde{c}_l\} \subset \{c_{ij}\}_{i,j=1}^{n}$, es decir, cada $\tilde{c}_k$ es alguna de las c_{ij}. En particular, $\tilde{c}_1,\ldots,\tilde{c}_l$ son elementos de $C(\boldsymbol{c})$ algebraicamente independientes sobre $K\langle\boldsymbol{\alpha}\rangle \supset C$, luego son algebraicamente independientes sobre C y, por tanto, $l = \mathrm{trdeg}(K\langle\boldsymbol{\alpha},\boldsymbol{c}\rangle|K\langle\boldsymbol{\alpha}\rangle) \leq \mathrm{trdeg}(C(\boldsymbol{c})|C)$.

Por otro lado, si $m = \mathrm{trdeg}(C(\boldsymbol{c})|C)$ y $\{\tilde{c}_1,\ldots,\tilde{c}_m\}$ es una base de trascendencia de $C(\boldsymbol{c})$ sobre C, siendo nuevamente cada $\tilde{c}_k$ una de las c_{ij}, entonces $\tilde{c}_1,\ldots,\tilde{c}_m$ son elementos de $K\langle\boldsymbol{\alpha},\boldsymbol{c}\rangle = K\langle\boldsymbol{\alpha}\rangle(\boldsymbol{c})$ algebraicamente independientes sobre $K\langle\boldsymbol{\alpha}\rangle$ ya que, si no lo fueran, existiría un polinomio $P \in K\langle\boldsymbol{\alpha}\rangle[X_1,\ldots,X_m]$ con $P(\tilde{c}_1,\ldots,\tilde{c}_m) = 0$. Pero en este caso, tomando una base de $K\langle\boldsymbol{\alpha}\rangle$ como espacio vectorial sobre C y expresando P (de forma única) como una combinación lineal de polinomios de $C[X_1,\ldots,X_m]$ con los elementos de esta base, tenemos que P se anula en $\tilde{c}_1,\ldots,\tilde{c}_m$ si, y solo si, lo hacen cada uno de estos polinomios de $C[X_1,\ldots,X_m]$, siendo además alguno de ellos no nulo por serlo P, lo cual es absurdo, ya que $\tilde{c}_1,\ldots,\tilde{c}_m$ son algebraicamente independientes sobre C al formar una base de trascendencia de $C(\boldsymbol{c})$ sobre C. Entonces, como $\tilde{c}_1,\ldots,\tilde{c}_m$ son algebraicamente independientes sobre $K\langle\boldsymbol{\alpha}\rangle$, $\mathrm{trdeg}(K\langle\boldsymbol{\alpha},\boldsymbol{c}\rangle|K\langle\boldsymbol{\alpha}\rangle) \geq \mathrm{trdeg}(C(\boldsymbol{c})|C) = m$.

Tenemos entonces que $\mathrm{trdeg}(K\langle\boldsymbol{\alpha},\tilde{\sigma}(\boldsymbol{\alpha})\rangle|K\langle\boldsymbol{\alpha}\rangle) = \mathrm{trdeg}(C(\boldsymbol{c})|C)$ y, de forma similar, $\mathrm{trdeg}(K\langle\boldsymbol{\alpha},\tilde{\sigma}(\boldsymbol{\alpha})\rangle|K\langle\tilde{\sigma}(\boldsymbol{\alpha}\rangle)) = \mathrm{trdeg}(\tilde{C}(\boldsymbol{c})|\tilde{C})$, siendo $\tilde{C}$ el cuerpo de constantes de $K\langle\boldsymbol{\alpha}\rangle$. Como $\mathrm{trdeg}(K\langle\boldsymbol{\alpha},\tilde{\sigma}(\boldsymbol{\alpha})\rangle|K\langle\boldsymbol{\alpha}\rangle) < \mathrm{trdeg}(K\langle\boldsymbol{\alpha},\tilde{\sigma}(\boldsymbol{\alpha})\rangle|K\langle\tilde{\sigma}(\boldsymbol{\alpha})\rangle)$, se debería tener $\mathrm{trdeg}(C(\boldsymbol{c})|C) < \mathrm{trdeg}(\tilde{C}(\boldsymbol{c})|\tilde{C})$, pero esto es absurdo, ya que C el cuerpo de constantes de K y $\tilde{C}$ el de $K\langle\boldsymbol{\alpha}\rangle \supset K$, luego $C \subset \tilde{C}$ y, por tanto, como vimos al demostrar que $\mathrm{trdeg}(K\langle\boldsymbol{\alpha},\boldsymbol{c}\rangle|K\langle\boldsymbol{\alpha}\rangle) \leq \mathrm{trdeg}(C(\boldsymbol{c})|C)$, debería tenerse $\mathrm{trdeg}(\tilde{C}(\boldsymbol{c})|\tilde{C}) \leq \mathrm{trdeg}(C(\boldsymbol{c})|C)$. Llegamos a un absurdo asumiendo que existe un elemento $z \in K\{\alpha_1,\ldots,\alpha_n\}$ no nulo en el núcleo de $\tilde{\sigma}$, tanto si es algebraico como si es trascendente, es decir, $\tilde{\sigma}$ tiene que ser inyectivo.

En conclusión, $\tilde{\sigma}$ es biyectivo, luego puede extenderse a un automorfismo de extensiones diferenciales sobre K, $\sigma : L = K\langle\alpha_1,\ldots,\alpha_n\rangle \to K\langle\tilde{\sigma}(\alpha_1),\ldots,\tilde{\sigma}(\alpha_n)\rangle$. Concretamente, si

$x \in K\langle\alpha_1, \ldots, \alpha_n\rangle$, entonces $x = a/b$, con $a, b \in K\{\alpha_1, \ldots, \alpha_n\}$ y $b \neq 0$ y podemos definir $\sigma(x) = \sigma(a/b) = \tilde{\sigma}(a)/\tilde{\sigma}(b)$. Esta expresión da una aplicación bien definida por ser $\tilde{\sigma}$ inyectiva, ya que $\tilde{\sigma}(b) \neq 0$. Además, σ es un morfismo diferencial biyectivo (isomorfismo) sobre K por serlo $\tilde{\sigma}$ y es admisible por ser $L = K\langle\alpha_1, \ldots, \alpha_n\rangle$ y $K\langle\tilde{\sigma}(\alpha_1) \ldots, \tilde{\sigma}(\alpha_n)\rangle$ subcuerpos de M. □

Corolario 5.4. *Sea $L|K$ una extensión diferencial de Picard-Vessiot, $L = K\langle\alpha_1, \ldots, \alpha_n\rangle$, con cuerpo de constantes C. Entonces existe un conjunto de polinomios S sobre C en las variables $\{X_{ij}\}_{i,j=1}^n$ tales que:*

i) Si $\sigma \in Gal(L|K)$ y $\sigma(\alpha_j) = \sum_{i=1}^n c_{ij}\alpha_i$, $j = 1, \ldots, n$, entonces $F((c_{ij})_{i,j=1}^n) = 0$ para todo polinomio $F \in S$.

ii) Dada una matriz $(c_{ij})_{i,j=1}^n \in GL(n, C)$ tal que $F((c_{ij})_{i,j=1}^n) = 0\ \forall F \in S$, existe un automorfismo $\sigma \in Gal(L|K)$ tal que $\sigma(\alpha_j) = \sum_{i=1}^n c_{ij}\alpha_i\ \forall j = 1, \ldots, n$.

Demostración. Se aplica la proposición, siendo L la extensión diferencial de L que contiene también a su imagen y siendo C el cuerpo de constantes de dicha extensión. El primer apartado es inmediato. En el segundo, las matrices de $GL(n, C)$ que anulan a los polinomios que obtenemos no dan lugar, a priori, a un automorfismo de $Gal(L|K)$, sino a un isomorfismo admisible definido en L sobre K con imagen contenida en L pero, gracias a la Nota 5.2, sabemos que todos estos son automorfismos de $Gal(L|K)$. □

Este resultado tiene una consecuencia importante.

Corolario 5.5. *Si $L|K$ es una extensión de Picard-Vessiot, entonces su grupo de Galois, $Gal(L|K)$, es un grupo algebraico.*

Demostración. Vamos a denotar por $G \subset GL(n, C)$ al conjunto de las matrices invertibles cuyos coeficientes anulan a los polinomios del conjunto S dado por la el Corolario 5.4. Ya habíamos mencionado en la Nota 5.2 que la asignación de la matriz correspondiente a cada automorfismo de $Gal(L|K)$ era un morfismo de grupos. Vamos a comprobarlo. Si $L = K\langle\alpha_1, \ldots, \alpha_n\rangle$ y $\sigma, \tau \in Gal(L|K)$, con $M(\sigma) = (c_{ij})_{i,j=1}^n$ y $M(\tau) = (d_{ij})_{i,j=1}^n$, entonces, para cada $j = 1, \ldots, n$,

$$\sigma\tau(\alpha_j) = \sigma\Big(\sum_{k=1}^n d_{kj}\alpha_k\Big) = \sum_{k=1}^n d_{kj}\sigma(\alpha_k) = \sum_{k=1}^n d_{kj}\Big(\sum_{i=1}^n c_{ik}\alpha_i\Big) = \sum_{i=1}^n\Big(\sum_{k=1}^n c_{ik}d_{kj}\alpha_i\Big) =$$

$$= \sum_{i=1}^n\Big(\sum_{k=1}^n c_{ik}d_{kj}\Big)\alpha_i = \sum_{i=1}^n e_{ij}\alpha_i,$$

donde $(e_{ij})_{i,j=1}^n = M(\sigma)M(\tau)$, es decir, $M(\sigma\tau) = M(\sigma)M(\tau)$. Además, como se mencionaba antes, $M(\sigma) = Id \iff \sigma = id_L$, luego es un morfismo de grupos inyectivo, cuya

imagen está contenida en $GL(n, C)$. Esta última proposición asegura que la imagen de esta correspondencia es G y es, por tanto, un isomorfismo de grupos entre $Gal(L|K)$ y G y, en particular, G es un subgrupo de $GL(n, C)$. Además, G es un subconjunto cerrado (para la topología de Zariski) del conjunto algebraico $GL(n, C)$, luego es a su vez un subconjunto algebraico de $GL(n, C)$, es decir, G (y por tanto $Gal(L|K)$) es un subgrupo algebraico de $GL(n, C)$. □

Vamos a terminar viendo un par de resultados que nos permiten alcanzar el teorema principal de esta teoría, el *teorema fundamental de la teoría de Galois diferencial*, muy similar al resultado existente para la teoría de Galois clásica, en el que las extensiones de Picard-Vessiot jugarán un papel análogo al de las extensiones de Galois en el caso clásico.

5.2. Teorema fundamental de la teoría de Galois diferencial

Lema 5.6. *Dada una extensión de Picard-Vessiot $L|K$, si F es un cuerpo diferencial intermedio, entonces $L|F$ también es una extensión de Picard-Vessiot*

Demostración. Si $L|K$ es una extensión de Picard-Vessiot, entonces $L = K\langle \alpha_1, \dots, \alpha_n \rangle$ donde $\alpha_1, \dots, \alpha_n$ son soluciones linealmente independientes sobre las constantes de una ecuación diferencial lineal homogénea $\mathcal{L}(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0$, con coeficientes en K y, además, L y K tienen el mismo cuerpo de constantes. Si C_K, C_F y C_L son los cuerpos de constantes de K, F y L respectivamente, como $K \subset F \subset L$, es evidente que $C_K \subset C_F \subset C_L = C_K$, luego $C_K = C_F = C_L$ y, por tanto, L y F tienen el mismo cuerpo de constantes. Además, como $K \subset F$, la ecuación diferencial $\mathcal{L}(y) = 0$ es a su vez una ecuación diferencial lineal homogénea con coeficientes en F y $L = K\langle \alpha_1, \dots, \alpha_n \rangle \subset F\langle \alpha_1, \dots, \alpha_n \rangle \subset L$, luego $L = F\langle \alpha_1, \dots, \alpha_n \rangle$, donde $\alpha_1, \dots, \alpha_n$ son soluciones de dicha ecuación, linealmente independientes sobre las constantes, luego efectivamente, $L|F$ es una extensión de Picard-Vessiot. □

Lema 5.7. *Sea $L|K$ una extensión diferencial y sean C y D los cuerpos de constantes de K y L respectivamente, C algebraicamente cerrado. Sean $\{f_\lambda\}_{\lambda \in \Lambda}$ y g polinomios en $K[X_1, \dots, X_n]$, siendo Λ un conjunto de índices arbitrario. Si el sistema $f_\lambda = 0\ \forall \lambda \in \Lambda$, $g \neq 0$ tiene solución en D, entonces también tiene solución en C.*

Demostración. Como $K|C$ es una extensión de cuerpos, K tiene estructura de espacio vectorial sobre C. Sea $\{w_\gamma\}_{\gamma \in \Gamma}$ una base de dicho espacio vectorial. En particular, los w_γ son linealmente independientes sobre C, es decir, sobre las constantes de K y, por tanto, como se indica en la Nota 3.10, lo son sobre las constantes de cualquier extensión de K, concretamente, son linealmente independientes sobre D. Al ser esta una base de K como C-espacio vectorial, lo es también de $K[X_1, \dots, X_n]$ como módulo sobre $C[X_1, \dots, X_n]$ (visto en el

Lema 2.4), es decir, existen polinomios $h_{\lambda\gamma} \in C[X_1, \ldots, X_n]$ tales que $f_\lambda = \sum_{\gamma\in\Gamma} h_{\lambda\gamma} w_\gamma$ para cada $\lambda \in \Lambda$.

Sean $d_1, \ldots, d_n \in D$ tal que $\boldsymbol{d} = (d_1, \ldots, d_n)$ es una solución del sistema. Para cada $\lambda \in \Lambda$, $f_\lambda(\boldsymbol{d}) = \sum_{\gamma\in\Gamma} h_{\lambda\gamma}(\boldsymbol{d}) w_\gamma = 0$ y, como $h_{\lambda\gamma}(\boldsymbol{d}) \in D$ al tenerse $C \subset D$, y al ser los w_γ linealmente independientes sobre D, se tiene que $h_{\lambda\gamma}(\boldsymbol{d}) = 0$ para todo $\lambda \in \Lambda$ y $\gamma \in \Gamma$. Si $I \subset C[X_1, \ldots, X_n]$ es el ideal generado en $C[X_1, \ldots, X_n]$ por todos los $h_{\lambda\gamma}$, observamos que I es un ideal propio, ya que si se tuviera $1 \in I$, al anularse todos los $h_{\lambda\gamma}$ en $\boldsymbol{d}$, el polinomio constante 1 tendría que anularse también en $\boldsymbol{d}$, lo cual es evidentemente absurdo. Por el teorema de los ceros de Hilbert, $\mathcal{V}(I) \subset \mathbb{A}^n_C \neq \emptyset$, es decir, existen $c_1, \ldots, c_n \in C$ tales que $\boldsymbol{c} = (c_1, \ldots, c_n)$ anula todos los polinomios $h_{\lambda\gamma}$ y, por tanto, anula todos los f_λ.

Pongamos $g = \sum_{\gamma\in\Gamma} t_\gamma w_\gamma$ con $t_\gamma \in C[X_1, \ldots, X_n]$ para todo $\gamma \in \Gamma$. Si además, todas estas soluciones anulasen también a g, anularían a todos los t_γ y nuevamente, por el teorema de los ceros de Hilbert, se tendría que $t_\gamma \in \mathcal{I}(\mathcal{V}(I)) = \sqrt{I} \subset C[X_1, \ldots, X_n]$ para cada $\gamma \in \Gamma$, es decir, existiría $r_\gamma \in \mathbb{N}$ para cada $\gamma \in \Gamma$ tal que $t_\gamma^{r_\gamma} \in I$. Entonces, $t_\gamma^{r_\gamma}(\boldsymbol{d}) = 0$, luego $t_\gamma(\boldsymbol{d}) = 0$ y, por tanto, $g(\boldsymbol{d}) = 0$, llegando así a un absurdo ya que $\boldsymbol{d}$ era solución del sistema del enunciado. □

Vamos a ver que en este contexto, un isomorfismo admisible es, a todos los efectos, un automorfismo.

Lema 5.8. *Sea $L|K$ una extensión de Picard-Vessiot, $\{x_\lambda\}_{\lambda\in\Lambda}$ e $\{y_\lambda\}_{\lambda\in\Lambda}$ dos subconjuntos de L y $z \in L$. Supongamos que existe un isomorfismo diferencial admisible σ definido en L sobre K con $\sigma(x_\lambda) = y_\lambda$ para cada $\lambda \in \Lambda$ y que no deja fijo z. Entonces existe un automorfismo diferencial $\tau \in Gal(L|K)$ con $\tau(x_\lambda) = y_\lambda$ para cada $\lambda \in \Lambda$ y que no deja fijo z.*

Demostración. Pongamos que $L = K\langle\alpha_1, \ldots, \alpha_n\rangle$, siendo $\alpha_1, \ldots, \alpha_n$ soluciones linealmente independientes sobre las constantes de cierta ecuación diferencial lineal homogénea sobre K. Como σ es un isomorfismo diferencial admisible, existe una extensión diferencial M de L que contiene tanto a L como a $\sigma(L)$. Por el Lema 3.11, para cada $j = 1, \ldots, n$, $\sigma(\alpha_j) = \sum_{i=1}^n k_{ij}\alpha_i$, donde los elementos k_{ij} son constantes de M. Al definir un isomorfismo, la matriz $(k_{ij})_{i,j=1}^n$ es necesariamente invertible, luego $det(\{k_{ij}\}_{i,j=1}^n) \neq 0$. Por la Proposición 5.4, las constantes $\{k_{ij}\}_{i,j=1}^n$ de M dan lugar a un isomorfismo admisible entre $L \subset M$ y otro subcuerpo de M si, y solo si, son solución del sistema de ecuaciones impuesto por la anulación de los polinomios del conjunto $S \subset C\{[X_{ij}]_{i,j=1}^n] \subset L[\{X_{ij}\}_{i,j=1}^n]$ dado en la proposición.

Para cada par de elementos $x_\lambda, y_\lambda \in L$, como $L = K\langle \alpha_1, \ldots, \alpha_n \rangle$, existen polinomios diferenciales $P_\lambda, Q_\lambda, R_\lambda, S_\lambda \in K\{X_1, \ldots, X_n\}$, con $Q_\lambda, S_\lambda \neq 0$, tales que $x_\lambda = P_\lambda(\boldsymbol{\alpha})/Q_\lambda(\boldsymbol{\alpha})$ e $y_\lambda = R_\lambda(\boldsymbol{\alpha})/S_\lambda(\boldsymbol{\alpha})$, donde $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Entonces, si denotamos por $\sigma(\boldsymbol{\alpha})$ a $(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$, al ser σ un morfismo diferencial de cuerpos sobre K,

$$\begin{aligned} y_\lambda = \sigma(x_\lambda) &\iff \frac{R_\lambda(\boldsymbol{\alpha})}{S_\lambda(\boldsymbol{\alpha})} = \sigma\left(\frac{P_\lambda(\boldsymbol{\alpha})}{Q_\lambda(\boldsymbol{\alpha})}\right) = \frac{\sigma(P_\lambda(\boldsymbol{\alpha}))}{\sigma(Q_\lambda(\boldsymbol{\alpha}))} = \frac{P_\lambda(\sigma(\boldsymbol{\alpha}))}{Q_\lambda(\sigma(\boldsymbol{\alpha}))} \\ &\iff P_\lambda(\sigma(\boldsymbol{\alpha}))S_\lambda(\boldsymbol{\alpha}) = Q_\lambda(\sigma(\boldsymbol{\alpha}))R_\lambda(\boldsymbol{\alpha}) \\ &\iff P_\lambda(\sigma(\boldsymbol{\alpha}))S_\lambda(\boldsymbol{\alpha}) - Q_\lambda(\sigma(\boldsymbol{\alpha}))R_\lambda(\boldsymbol{\alpha}) = 0. \end{aligned}$$

Si sustituimos $\sigma(\alpha_j)$ por $\sum_{i=1}^n X_{ij}\alpha_i$, para cada $\lambda \in \Lambda$, obtenemos una ecuación de la forma $f_\lambda = 0$ donde $f_\lambda \in L[\{X_{ij}\}_{i,j=1}^n]$, de forma que $\{k_{ij}\}_{i,j=1}^n$ es una solución del sistema en D, el cuerpo de constantes de M. Además, un morfismo $\tau \in Gal(L|K)$, dado por $\tau(\alpha_j) = \sum_{i=1}^n c_{ij}\alpha_i$, cumple que $\tau(x_\lambda) = y_\lambda$ si, y solo si, $\{c_{ij}\}_{i,j=1}^n$ es una solución del sistema en C. Al sistema de ecuaciones $f_\lambda = 0\ \forall \lambda \in \Lambda$ le vamos a añadir el sistema dado por S, $f = 0\ \forall f \in S$. Además, si $z = P(\boldsymbol{\alpha})/Q(\boldsymbol{\alpha})$ con $P, Q \in K\{X_1, \ldots, X_n\}$ y $Q \neq 0$, la condición $\sigma(z) \neq z$ nos permite obtener una inecuación de la forma $\tilde{g} \neq 0$ con $\tilde{g} \in L[\{X_{ij}\}_{i,j=1}^n]$, de la misma forma que cuando obtuvimos las ecuaciones $f_\lambda = 0$. Observemos que las dos inecuaciones $det(\{X_{ij}\}_{i,j=1}^n) \neq 0$ y $\tilde{g} \neq 0$ se cumplen si, y solo si, se cumple la inecuación $g \neq 0$ donde $g(\{X_{ij}\}_{i,j=1}^n) = \tilde{g}(\{X_{ij}\}_{i,j=1}^n) \cdot det(\{X_{ij}\}_{i,j=1}^n)$ es un polinomio en $L[\{X_{ij}\}_{i,j=1}^n]$. Las constates $\{k_{ij}\}_{i,j=1}^n$ cumplen todas estas ecuaciones y esta inecuación como ya hemos visto, es decir, son una solución en D del sistema que definen. Por el Lema 5.7, este sistema admite una solución $\{c_{ij}\}_{i,j=1}^n$ en C, que proporciona un automorfismo diferencial $\tau \in Gal(L|K)$ que cumple todas las condiciones del enunciado. □

Teorema 5.9. *Si $L|K$ es una extensión de Picard-Vessiot (de característica 0), entonces es una extensión normal.*

Demostración. Sea $\alpha \in L \setminus K$. Por el Teorema 2.6 existe un isomorfismo diferencial admisible sobre K definido en L que no deja fijo α. Entonces, por el Lema 5.8, existe un automorfismo de L sobre K (un automorfismo de $Gal(L|K)$) que no deja fijo α. □

Teorema 5.10. *Sea $L|K$ una extensión de Picard-Vessiot (de característica 0). Todo isomorfismo diferencial sobre K ente dos cuerpos diferenciales intermedios de la extensión puede extenderse a un automorfismo diferencial definido en todo L, es decir, de $Gal(L|K)$. En particular, si F es un cuerpo diferencial intermedio de la extensión, todo automorfismo de $Gal(F|K)$ puede extenderse a uno de $Gal(L|K)$.*

Demostración. Por el Teorema 2.5, este isomorfismo diferencial puede extenderse a un isomorfismo admisible definido en todo L. Por Lema 5.8, este isomorfismo admisible da

lugar a un automorfismo diferencial de $Gal(L|K)$ que extiende al isomorfismo diferencial original. □

Proposición 5.11. *Sea $L|K$ una extensión de Picard-Vessiot, entonces las correspondencias de Galois entre los subgrupos algebraicos de $Gal(L|K)$ (subgrupos de $Gal(L|K)$ cerrados para la topología de Zariski) y cuerpos diferenciales intermedios de $L|K$ son biyectivas e inversas la una de la otra.*

Demostración. Veamos primero que $F^{**} = F$ para todo cuerpo intermedio F de la extensión. Como hemos visto en el Lema 5.6, $L|F$ es también una extensión de Picard-Vessiot y por el Teorema 5.9, L es normal sobre F, es decir, ningún elemento de $L \setminus F$ queda fijo por todos los morfismos de $Gal(L|F) = F^*$, es decir, $Gal(L|F)^* = F^{**} \subset F$. Como siempre se tiene que $F^{**} \supset F$, concluimos que $F^{**} = Gal(L|F)^* = F$.

Finalmente, veamos que $H^{**} = H$ para todo subgrupo algebraico H de $Gal(L|K)$. Concretamente, vamos a ver que si $H \subset Gal(L|K)$ es un subgrupo cualquiera, entonces H^{**} es su clausura topológica en $Gal(L|K)$ para la topología de Zariski. Razonemos por reducción al absurdo. Sabemos que la clausura de H es $\mathcal{V}(\mathcal{I}(H))$, es decir, el conjunto de los morfismos de $Gal(L|K)$ donde se anulan todos los polinomios $f \in C[\{X_{ij}\}_{i,j=1}^n]$ que se anulan en H, es decir, con $f|_H = 0$. Cuando decimos que un polinomio $f \in C[\{X_{ij}\}_{i,j=1}^n]$ se anula en un morfismo, estamos utilizando la identificación de dicho morfismo con su matriz asociada, es decir, el polinomio se anula en los coeficientes de la matriz correspondiente a dicho morfismo, . Supongamos entonces que existe $f \in C[\{X_{ij}\}_{i,j=1}^n]$ con $f|_H = 0$ pero $f_{H^{**}} \neq 0$, es decir, $f(M(\sigma)) = 0\ \forall \sigma \in H$, pero $f(M(\sigma_0)) \neq 0$ para cierto $\sigma_0 \in H^{**}$. Si $L = K\langle \alpha_1, \dots \alpha_n \rangle$, vamos a considerar n indeterminadas diferenciales $Z_1, \dots, Z_n$ sobre L y las matrices fundamentales:

$$A = X(\alpha_1, \dots, \alpha_n) = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1' & \alpha_2' & \cdots & \alpha_n' \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{(n-1)} & \alpha_2^{(n-1)} & \cdots & \alpha_n^{(n-1)} \end{pmatrix},$$

$$X(Z_1, \dots, Z_n) = \begin{pmatrix} Z_1 & Z_2 & \cdots & Z_n \\ Z_1' & Z_2' & \cdots & Z_n' \\ \vdots & \vdots & \ddots & \vdots \\ Z_1^{(n-1)} & Z_2^{(n-1)} & \cdots & Z_n^{(n-1)} \end{pmatrix}.$$

Como $\alpha_1, \dots, \alpha_n$ son linealmente independientes sobre las constantes, su wronskiano $W(\alpha_1, \dots, \alpha_n) = det(A)$ es no nulo, luego A es invertible. Vamos a considerar el polinomio diferencial $F \in L\{Z_1, \dots, Z_n\}$ dado por $F(Z_1, \dots, Z_n) = f(A^{-1}X(Z_1, \dots, Z_n))$. Para cada $\sigma \in Gal(L|K)$ y cada $i, j \in 1, \dots, n$, si $M(\sigma) = (c_{ij})_{i,j=1}^n$ se observa que

$\sigma(\alpha_j)^{(i)} = \left(\sum_{k=1}^n c_{kj}\alpha_k\right)^{(i)} = \sum_{k=1}^n c_{kj}\alpha_k^{(i)}$, que es el elemento (i,j) del producto de matrices $A \cdot M(\sigma)$, es decir, $X(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) = A \cdot M(\sigma)$. Por tanto, $\forall\, \sigma \in Gal(L|K)$, $F(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) = f(A^{-1}X(\sigma(\alpha_1),\dots,\sigma(\alpha_n))) = f(A^{-1}AM(\sigma)) = f(M(\sigma))$, luego, por la elección de f, el polinomio diferencial F cumple que $F(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) = 0$ para todo morfismo $\sigma \in H$, pero $F(\sigma_0(\alpha_1),\dots,\sigma_0(\alpha_n)) \neq 0$. Existen, por tanto, polinomios diferenciales $F \in L\{Z_1,\dots,Z_n\}$ tales que $F(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) = 0$ para todo $\sigma \in H$, pero no todo $\sigma \in H^{**}$. Sea $G \in L\{Z_1,\dots,Z_n\}$ un polinomio con esta propiedad con el menor número de monomios no nulos posible y, salvo producto por un escalar de L, supongamos que uno de sus monomios tiene coeficiente 1. Para un morfismo $\tau \in H$, vamos a considerar el polinomio diferencial G_τ obtenido de G al aplicar τ al coeficiente de cada uno de sus monomios, es decir, si $G = \sum_{i=1}^m \lambda_i G_i$, con $\lambda_i \in L$ y G_i monomio mónico en $L\{Z_1,\dots,Z_n\}$ para cada $i = 1,\dots,m$, entonces $G_\tau = \sum_{i=1}^m \tau(\lambda_i)G_i$. Por ser τ un automorfismo de L, G_τ tiene el mismo número de monomios no nulos que G y, dado que $\tau(1) = 1$, uno de sus monomios es idéntico. Además, $\forall \sigma \in H$, se tiene que $\tau^{-1}\sigma \in H$, luego

$$G_\tau(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) = \sum_{i=1}^m \tau(\lambda_i)G_i(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) =$$

$$\tau\Big(\sum_{i=1}^m \lambda_i G_i(\tau^{-1}\sigma(\alpha_1),\dots,\tau^{-1}\sigma(\alpha_n))\Big) = \tau(G(\tau^{-1}\sigma(\alpha_1),\dots,\tau^{-1}\sigma(\alpha_n))) = \tau(0) = 0.$$

Por tanto, $(G - G_\tau)(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) = 0$ para todo $\sigma \in H$. Como $G - G_\tau$ tiene al menos un monomio no nulo menos que G, por la propiedad que define a G, tiene que ser también que $(G - G_\tau)(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) = 0$ para todo $\sigma \in H^{**}$. Si $G - G_\tau$ no fuera idénticamente nulo, podríamos encontrar un escalar $\lambda \in L$ tal que $\lambda(G - G_\tau)$ tuviera algún monomio idéntico a G y, en este caso, $G - \lambda(G - G_\tau)$ tendría al menos un monomio no nulo menos que G y cumpliría las mismas condiciones que G, lo cual es absurdo. Por tanto, $G - G_\tau \equiv 0$ para todo $\tau \in H$, luego los coeficientes de G son invariantes por todos los morfismos de H, es decir, están en $H^* = (H^{**})^*$, así que también son invariantes por todos los morfismos de H^{**} y $G \equiv G_\tau$ para todo $\tau \in H^{**}$. Entonces, para todo $\sigma \in H^{**}$,

$$G(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) = G_\sigma(\sigma(\alpha_1),\dots,\sigma(\alpha_n)) = \sigma(G(\sigma^{-1}\sigma(\alpha_1),\dots,\sigma^{-1}\sigma(\alpha_n))) =$$

$$\sigma(G(id_L(\alpha_1),\dots,id_L(\alpha_n))) = \sigma(0) = 0,$$

ya que $id_L \in H$, contradiciendo la definición de G y llegando así a un absurdo.

Entonces, H^{**} es la clausura topológica de H en $Gal(L|K)$ para cualquier subgrupo $H \subset Gal(L|K)$ y, en particular, todo subgrupo algebraico de $Gal(L|K)$ es cerrado para las correspondencias de Galois de la extensión.

□

Proposición 5.12. *Sea $L|K$ una extensión de Picard-Vessiot. Entonces un subgrupo algebraico $H \subset Gal(L|K)$ es normal en $Gal(L|K)$ si, y solo si, su cuerpo diferencial intermedio correspondiente F es normal sobre K.*

Demostración. Sean $H \subset Gal(L|K)$ un subgrupo algebraico de $Gal(L|K)$ y F un cuerpo diferencial intermedio de la extensión, correspondientes mutuamente por las correspondencias de Galois de la extensión.

Por el Teorema 5.9, $L|K$ es una extensión normal, al ser de Picard-Vessiot. Por el Lema 3.5, si H es normal en $Gal(L|K)$, entonces $H^* = F$ es normal sobre K.

Supongamos ahora que F es normal sobre K. Entonces, como por el Teorema 5.10 todo automorfismo de $Gal(F|K)$ puede extenderse a uno de $Gal(L|K)$, solo falta probar que el normalizador de H en $Gal(L|K)$, $N(H) = \{\sigma \in Gal(L|K) : \sigma^{-1}H\sigma = H\}$ es cerrado para las correspondencias de Galois, y podremos aplicar el Lema 3.8 para concluir que H es un subgrupo normal de $Gal(L|K)$. Como vimos en la Proposición 5.11, basta ver que el subgrupo $N(H) \subset Gal(L|K)$ es cerrado en $Gal(L|K)$ para la topología de Zariski. vamos a considerar los morfismos de grupos $f_1^\tau, f_2^\tau : Gal(L|K) \to Gal(L|K)$ para cada $\tau \in H$, dados por $f_1^\tau(\sigma) = \sigma^{-1}\tau\sigma$ y $f_2^\tau(\sigma) = \sigma\tau\sigma^{-1}$. Además de ser morfismos de grupos, son aplicaciones continuas para la topología de Zariski al serlo las aplicaciones $\iota : \sigma \mapsto \sigma^{-1}$, $\mu_1 : \sigma \mapsto \sigma\tau$ y $\mu_2 : \sigma \mapsto \tau\sigma$. Entonces, como H es un subgrupo algebraico de $Gal(L|K)$, es cerrado para la topología de Zariski, luego $(f_1^\tau)^{-1}(H) = \{\sigma \in Gal(L|K) : \sigma^{-1}\tau\sigma \in H\}$ y $(f_2^\tau)^{-1}(H) = \{\sigma \in Gal(L|K) : \sigma\tau\sigma^{-1} \in H\}$ son cerrados en $Gal(L|K)$ para cada $\tau \in H$. Entonces:

$$\begin{aligned}
N(H) &= \{\sigma \in Gal(L|K) : \sigma^{-1}H\sigma = H\} \\
&= \{\sigma \in Gal(L|K) : \sigma^{-1}H\sigma \subset H\} \cap \{\sigma \in Gal(L|K) : \sigma^{-1}H\sigma \supset H\} \\
&= \{\sigma \in Gal(L|K) : \sigma^{-1}H\sigma \subset H\} \cap \{\sigma \in Gal(L|K) : \sigma H\sigma^{-1} \subset H\} \\
&= \{\sigma \in Gal(L|K) : \sigma^{-1}\tau\sigma \in H \ \forall \tau \in H\} \cap \{\sigma \in Gal(L|K) : \sigma\tau\sigma^{-1} \in H \ \forall \tau \in H\} \\
&= \Big(\bigcap_{\tau\in H} \{\sigma \in Gal(L|K) : \sigma^{-1}\tau\sigma \in H\}\Big) \cap \Big(\bigcap_{\tau\in H} \{\sigma \in Gal(L|K) : \sigma\tau\sigma^{-1} \in H\}\Big) \\
&= \Big(\bigcap_{\tau\in H} (f_1^\tau)^{-1}(H)\Big) \cap \Big(\bigcap_{\tau\in H} (f_2^\tau)^{-1}(H)\Big)
\end{aligned}$$

Concluimos que $N(H)$ es cerrado en $Gal(L|K)$ para la topología de Zariski al ser una intersección de cerrados, luego es cerrado para las correspondencias de Galois y podemos aplicar el Lema 3.8 para finalizar la prueba. □

Estos últimos resultados se recopilan en el teorema fundamental de esta teoría:

Teorema 5.13 (**Teorema fundamental de la teoría de Galois diferencial**).
Sea $L|K$ una extensión de Picard-Vessiot:

1) Las correspondencias de Galois entre los subgrupos algebraicos de $Gal(L|K)$ y los cuerpos diferenciales intermedios de la extensión son biyectivas e inversas la una de la otra.

ii) Un cuerpo diferencial intermedio F de la extensión es normal sobre K si, y solo si, su subgrupo correspondiente $F^* = Gal(L|F)$ es normal en $Gal(L|K)$. En este caso, el morfismo de restricción (en el dominio y la imagen):

$$\begin{aligned} Gal(L|K) &\longrightarrow Gal(F|K) \\ \sigma &\longmapsto \sigma|_F, \end{aligned}$$

induce un isomorfismo $\frac{Gal(L|K)}{Gal(L|F)} \cong Gal(F|K)$.

***Nota* 5.14.** El teorema fundamental puede refinarse aún más incluyendo un resultado: si $L|K$ es una extensión de Picard-Vessiot (de característica 0) y F es normal sobre K, entonces F es a su vez una extensión de Picard-Vessiot de $L|K$ [4, pág 891]. Ya sabíamos el recíproco (Teorema 5.9), luego podemos afirmar que, en las correspondencias de Galois de una extensión de Picard-Vessiot, subgrupos algebraicos normales se corresponden con subextensiones de Picard-Vessiot (que son exactamente los subcuerpos diferenciales normales de la extensión).

Referencias

[1] D. Blázquez-Sanz. La evolución de la teoría de grupos en las ecuaciones diferenciales. *Lecturas matemáticas*, 29(2):83–93, 2008.

[2] W. Fulton. *Curvas algebraicas : introducción a la geometriía algebraica*. Reverteé, Barcelona, 1971.

[3] I. Kaplansky. *An introduction to differential algebra*. Actualiteés scientifiques et industrielles ; 1251. Hermann, París, 2nd ed. edition, 1971.

[4] E. R. Kolchin. On the galois theory of differential fields. *American Journal of Mathematics*, 77(4):868–894, 1955.

[5] F. Delgado y C. Fuertes y S. Xambó. *Introducción al Álgebra*. Paraninfo, Madrid, 2ª ed. edition, 2021.

[6] F. Galindo y J. Sanz y L. A. Tristán. *Guía práctica de cálculo infinitesimal en varias variables*. Thomson, Madrid, 2005.

[7] T. Crespo y Z. Hajto. *Algebraic groups and differential Galois theory*. Graduate studies in mathematics ; v. 122. American Mathematical Society, Providence, R.I, 2011.