UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

Àlgebra diferencial: El teorema de Liouville

Autor: Sergi Sánchez Aragón

Tutora: Maria Teresa Crespo Vicente
Grau: Matemàtiques
Curs: 2021/2022, semestre de primavera

2020 Mathematics Subject Classification. 12H05, 12F05, 12F20, 12F99, 13-00, 13N15, 14-00

Índex

1 Introducció

Es tracta d'un dels primers resultats que es troben (indirectament) en el transcurs d'aprendre matemàtiques a nivell universitari. En aquelles primeres lliçons, és comú escoltar la frase "Aquesta funció, e^{-x^2}, no té primitiva; la seva integral només es pot aproximar numèricament."
Ara bé, quan diem que una funció donada als reals no té primitiva, que no existeix una funció en termes simples que n'expressi la integral en un cert interval, què volem dir? Què volem dir, tan sols, quan intentem acotar el significat d'expressar qualsevol funció als reals o als complexos en **termes simples**? Aprofundir en aquestes preguntes, i copsar-ne l'interès matemàtic, són els objectius d'aquest treball.
Emprant resultats de les matemàtiques modernes, es preté introduir un llenguatge i base teòrica on aquestes preguntes tinguin sentit, i on es pugui demostrar el teorema que històricament els donà resposta: el teorema de Liouville d'antiderivades.

1.1 Abstract

It's one of the first results a maths undergraduate hears about. The function e^{-x^2} does not have an antiderivative, the value of its integral on any given interval where it can be calculated can only be approximated via numerical methods. But what does it mean for a real function to not have an antiderivative, a function that expresses its integral in simple terms? When do we even consider a real or complex function to be expressible in **simple terms**?
These questions are the focus of this project. Using modern results in mathematics, mainly differential algebra, we aim to introduce a theoretical frame where these questions can be posed rigorously, one where we can prove the theorem that answers them: Liouville's theorem about antiderivatives.

2 Àlgebra diferencial

Com bé és enunciat al paràgraf introductori, l'objectiu del treball gira en torn a un teorema en particular, així com les seves conseqüències més immediates. Aquest resultat, el teorema de Liouville d'antiderivades, en la seva primera forma a nivell històric, determina la forma general -en un sentit algebraic que determinarem rigorosament- que ha de tenir una funció determinada per ser integrable en "termes elementals".
Si bé es podria pensar que aquest és un resultat inherentment lligat al càlcul, donat el context històric en què neix el problema i el seu contingut, els arguments que el demostren troben sustent i generalització actualment en una branca de l'àlgebra: específicament la coneguda com a *àlgebra diferencial*.
Aquesta secció del treball es dedica a introduir els fonaments i resultats clau d'aquesta branca de les matemàtiques; a proporcionar un llenguatge precís amb el qual perfilar el contorn de les nostres preguntes.

2.1 Anells diferencials

Pel cas que ens ocupa, ens referirem a anells commutatius cada cop que parlem d'anells.

Definició 2.1. *Anomenem anell diferencial a una parella (R,D) on R és un anell i* $D : R \longmapsto R$ *és una aplicació (que anomenarem derivació) que satisfà:*
1)$D(a+b) = D(a) + D(b)\ \forall a, b \in R$
2)$D(ab) = D(a)b + aD(b)\ \forall a, b \in R$

De la primera propietat es desprèn immediatament que $D(0) = 0$.
A la pràctica, normalment citarem només l'anell amb el qual treballem i direm que és diferencial quan el considerem amb una derivació determinada.

Obs. 1. *Sigui R un anell unitari, llavors* $D(1) = 0$

Demostració. Considerem la igualtat $1{\cdot}1 = 1$ i apliquem la propietat 2) de la definició, obtenint $2D(1) = D(1) \iff D(1) = 0$ □

Obs. 2. $D(x^n) = nx^{n-1}D(x)\ \ \forall n \in \mathbb{N}$

Demostració. Ho demostrem per inducció. El cas $n = 1$ és trivial per definició, de manera que només cal provar el pas inductiu. Suposem que es satisfà la propietat per n-1:
$D(x^n) = D(x^{n-1}x) = D(x^{n-1})x + x^{n-1}D(x)$
i, per la hipòtesi d'inducció
$D(x^n) = (n-1)x^{n-1}D(x) + x^{n-1}D(x) = nx^{n-1}D(x)$ □

Seguidament, passem a demostrar una sèrie de resultats bàsics relatius a anells diferencials.
A vegades denotarem $D(x)$ per x' per economia, i $D^{(n)}(x)$ com $x^{(n)}$.

Corol.lari 2.1. *Per la Obs.1 i les propietats d'una derivació respecte la suma, $D(n) = 0\ \forall n \in \mathbb{Z}$ on entenem per enters en aquest context els elements que són resultat de sumar 1 o -1 finites vegades.*

Proposició 2.1. *(Fòrmula de Leibniz)*
$(ab)^{(n)} = \sum_{i=1}^{n} \binom{n}{i} a^{(i)} b^{(n-i)}\ \forall n \in \mathbb{N}$

Demostració. Ho demostrem per inducció.
El cas $n = 1$ és la propietat 2) d'una derivació, de manera que l'obtenim trivialment. Demostrem el pas inductiu.
Suposem que és certa per a n-1:
$(ab)^{(n)} = ((ab)^{(n-1)})' = (\sum_{i=1}^{n-1} \binom{n-1}{i} a^{(i)} b^{(n-1-i)})'$
$(\sum_{i=1}^{n-1} \binom{n-1}{i} a^{(i)} b^{(n-1-i)})' = \sum_{i=1}^{n-1} \binom{n-1}{i} a^{(i+1)} b^{(n-1-i)} + \sum_{i=1}^{n-1} \binom{n-1}{i} a^{(i)} b^{(n-i)}$

on l'última igualtat és conseqüència del corol·lari 2.1. Procedim ara a observar detinguadament aquests dos sumatoris, i a reordenar-los de forma convenient.
Resulta clar que, si $i = n - 1$ o $i = 0$, ja tenim els sumands corresponents a la expressió que busquem en funció de n.
Per a la resta de casos, canviant l'índex ï"per "j"entre 1 i n-1, tindrem que el terme $a^{(j)} b^{(n-j)}$ ve dels termes $a^{(j-1)} b^{(n-j)}$ i $a^{(j)} b^{(n-1-j)}$ respectivament, de manera que el coeficient que li pertocarà a la suma serà $\binom{n-1}{j-1} + \binom{n-1}{j} = \binom{n}{j}$ per les propietats dels nombres combinatoris.
Per tant, reordenant les dues sumes segons aquest criteri, obtenim que
$(ab)^{(n)} = \sum_{j=1}^{n} \binom{n}{j} a^{(j)} b^{(n-j)}$ com voliem demostrar. □

Proposició 2.2. *(Identitat logarítmica de les derivacions)*
Sigui R un cos diferencial. Llavors:
$\frac{D(u_1^{e_1} \ldots u_n^{e_n})}{u_1^{e_1} \ldots u_n^{e_n}} = \sum_{i=1}^{n} e_i \frac{D(u_i)}{u_i} \quad n \in \mathbb{N}, u_i \in R, e_i \in \mathbb{Z}$

per a tot valor de i entre 1 i n.

Demostració. Ho veiem per inducció.
El cas inicial $n = 1$ és, de fet, la Obs.2, tenint en compte que podem interpretar els exponents negatius e_i com potències positives de l'invers multiplicatiu corresponent.
Demostrem llavors el pas inductiu, suposant que la proposició és certa per a n-1:

$$\frac{D(\prod_{i=1}^{n} u_i^{e_i})}{\prod_{i=1}^{n} u_i^{e_i}} = \frac{1}{u_n^{e_n}} \frac{D(\prod_{i=1}^{n} u_i^{e_i})}{\prod_{i=1}^{n-1} u_i^{e_i}} = \frac{1}{u_n^{e_n}} \frac{D(\prod_{i=1}^{n-1} u_i^{e_i}) u_n^{e_n} + \prod_{i=1}^{n-1} u_i^{e_i} D(u_n^{e_n})}{\prod_{i=1}^{n-1} u_i^{e_i}}$$

$$\iff \frac{D(\prod_{i=1}^{n} u_i^{e_i})}{\prod_{i=1}^{n} u_i^{0e_i}} = \frac{D(\prod_{i=1}^{n-1} u_i^{e_i})}{\prod_{i=1}^{n-1} u_i^{e_i}} + D(u_n^{e_n})$$

i, per la obs.2 i la hipòtesi d'inducció, tindrem

$$\frac{D(\prod_{i=1}^{n} u_i^{e_i})}{\prod_{i=1}^{n} u_i^{e_i}} = \sum_{i=1}^{n-1} e_i \frac{D(u_i)}{u_i} + \frac{e_n u_n^{e_{n-1}} D(u_n)}{u_n^{e_n}} = \sum_{i=1}^{n} e_i \frac{D(u_i)}{u_i}$$ □

Proposició 2.3. *Sigui (R,d) un anell diferencial amb R domini d'integritat. Sigui K el seu cos de fraccions. Llavors, d estén de forma única a una derivació a K.*

Demostració. Comencem demostrant la unicitat: sigui D una derivació a K satisfent les propietats volgudes, llavors tot b diferent de 0 complirà:
$0 = D(1) = D(b\frac{1}{b}) = bD(\frac{1}{b}) + \frac{1}{b}D(b) \iff D(\frac{1}{b}) = \frac{-D(b)}{b^2}$
de manera que, per a qualsevol element de K $\frac{a}{b}$, es tindrà
$D(\frac{a}{b}) = aD(\frac{1}{b}) + \frac{1}{b}D(a) = \frac{D(a)b - aD(b)}{b^2}$
de manera que aquesta D serà única, suposant que sigui també una derivació.
La part de la demostració relativa a la seva existència consistirà llavors en confirmar que D com la ja definida és, en efecte, una derivació a K. Comencem per veure que D està ben defnida, és a dir, que si dues parelles (a, b) i (c, d) pertanyen a la mateixa classe d'equivalència del cos de fraccions, tenen la mateixa imatge per D. Sigui $\frac{a}{b} \in K$

$D(\frac{sa}{sb}) = \frac{D(sa)sb - saD(sb)}{(sb)^2} = \frac{D(sa)b - aD(sb)}{sb^2} = \frac{(D(s)a + D(a)s)b - a(D(s)b + D(b)s)}{sb^2}$
$\iff D(\frac{sa}{sb}) = \frac{D(s)ab - D(s)ab + D(a)bs - D(b)as}{sb^2} = \frac{D(a)b - D(b)a}{b^2} = D(\frac{a}{b}) \quad \forall s \in R$
Finalment, comprovem que D és una derivació.

(1) $D(\frac{a}{b} + \frac{c}{d}) = D(\frac{ad+cb}{bd}) = \frac{D(ad+cb)bd - (ad+bc)D(bd)}{(bd)^2}$
$= \frac{D(a)bd^2 + D(d)abd + D(c)db^2 + D(b)bcd - ad^2D(b) - adbD(d) - bcdD(b) - D(d)cb^2}{(bd)^2}$

$= \frac{D(a)b - aD(b)}{b^2} + \frac{D(c)d - cD(d)}{d^2} = D(\frac{a}{b}) + D(\frac{c}{d}) \quad \forall \frac{a}{b}, \frac{c}{d} \in K$

(2) $D(\frac{a}{b}\frac{c}{d}) = D(\frac{ac}{bd}) = \frac{D(ac)bd - acD(bd)}{(bd)^2} = \frac{D(a)cbd + D(c)abd - D(b)dac - D(d)bac}{(bd)^2}$

$= \frac{D(a)bcd - aD(b)cd}{(bd)^2} + \frac{D(c)dab - D(d)cab}{(bd)^2} = \frac{D(a)b - aD(b)}{b^2}\frac{c}{d} + \frac{D(c)d - cD(d)}{d^2}\frac{a}{b}$

$= D(\frac{a}{b})\frac{c}{d} + D(\frac{c}{d})\frac{a}{b} \quad \forall \frac{a}{b}, \frac{c}{d} \in K$

□

Com és usual durant la construcció d'una branca de coneixement algebraic, no només ens resulten d'interès les estructures en si mateixes, sinó també com es relacionen entre elles, especialment a través de morfismes.
Al context de l'àlgebra diferencial, aquest enfoc ens porta a parlar de *morfismes diferencials.*

Definició 2.2. *Anomenem morfisme diferencial a una aplicació entre anells diferencials $f : A \longmapsto B$ (amb A, B anells diferencials) tal que f és morfisme d'anells:*
$f(a + b) = f(a) + f(b) \quad \forall a, b \in A$
$f(ab) = f(a)f(b) \quad \forall a, b \in A$ *(I $f(1) = 1$ si els anells són unitaris)*
$f(a') = (f(a))' \quad \forall a \in A$

Definició 2.3. *Si f morfisme diferencial és exhaustiu, l'anomenarem epimorfisme.*

Definició 2.4. *Si f morfisme diferencial és injectiu, l'anomenarem monomorfisme.*

Definició 2.5. *Seguint el conveni habitual, si f és monomorfisme i epimorfisme, direm que és un isomorfisme.*

Anàlogament, ens interessa un equivalent al concepte general d'anell quocient amb els anells diferencials, especialment per les necessitats del nostre treball, en tant que passar a quocients és una manera usual d'estudiar estructures o donar constructivament exemples d'algunes d'elles que satisfacin propietats especials.
Aquesta necessitat justifica llavors la definició del concepte d'*ideal diferencial*.

Definició 2.6. *Sigui un subconjunt I d'un anell diferencial A, direm que I és un ideal diferencial si I és ideal de A en el sentit usual i, a més, satisfà:*
$a' \in I \quad \forall a \in I$

Obs. 3. *Si f és un morfisme diferencial, llavors $Ker(f)$ és un ideal diferencial.*

Obs. 4. *Sigui A anell diferencial, I un ideal diferencial d'A, llavors l'anell quocient $\frac{A}{I}$ és un anell diferencial amb la derivació:*
$d([a]) = [D(a)] \quad \forall [a] \in \frac{A}{I}$

Demostració. d satisfarà les propietats d'una derivació tot heretant-les de D, de manera que només cal veure que està ben definida.
Ara bé, això també és directe, ja que $a, b \in A$ són de la mateixa classe si, i només si, $a - b \in I$ i, com I és ideal diferencial, llavors $D(a-b) = D(a) - D(b) \in I$. □

Obs. 5. *Com resulta d'esperar, l'aplicació $\pi : A \longmapsto \frac{A}{I}$ que envia cada element a la seva classe d'equivalència és, en els termes que acabem de definir, un epimorfisme diferencial.*

Obs. 6. *També es satisfà per a anells diferencials el primer teorema d'isomorfia, és a dir, $\frac{A}{Ker(f)} \cong Im(f)$ si f és un morfisme diferencial, ja que $Im(f)$ és un anell diferencial amb la derivació $(f(a))' = f(a') \ \forall \ a \in A$*

Un altre resultat usual amb versió referida a anells diferencials és l'existència d'elements maximals al conjunt dels ideals diferencials.
És a dir, existeixen en tot anell diferencial A ideals diferencials I amb la propietat que cap altre J ideal diferencial propi és tal que $I \subset J$.
La demostració d'aquest fet és anàloga a la del cas estàndard, constituint una aplicació directa del *Lema de Zorn*, amb l'afegit que l'element maximal de tota cadena ascendent d'ideals (la seva unió) és també un ideal diferencial quan tots els membres de la successió ho són.
Finalment, introduim ara un altre concepte bàsic propi del context diferencial:

Definició 2.7. *Anomemem constants al subconjunt d'A*
$Const_A := \{a \in A | D(a) = 0\}$

Proposició 2.4. *$Const_A$ és subanell d'A (o subcòs si A és cos)*

Demostració. Primerament, ja sabem que tant 0 com 1 ja pertanyen al subconjunt de constants, ja que es segueix directament de les propietats de les derivacions.
Que $a+b \in Const_A$ si a i b hi pertanyen és conseqüència directa de la propietat 1) d'una derivació, de manera que només ens queda veure que $Const_A$ és tancat respecte al producte i que, si A és cos, l'invers multiplicatiu d'una constant és també una constant. Ho demostrem per ordre:
Siguin a,b de $Const_A$, llavors $D(ab) = D(a)b + aD(b) = 0b + a0 = 0$
Quant al cas d'A cos, sigui $c \in Const_A$ invertible, llavors $D(c^{-1}) = -D(c)c^{-2}$ fet que ja vam deduir pel cas particular on K era el cos de fraccions d'un domini d'integritat A i voliem estendre'n la derivació.
La deducció és anàloga, ja que es dedueix del fet que $cc^{-1} = 1$ i $D(1) = 0$. □

2.2 Extensions de cossos diferencials

D'aquesta secció en endavant, ens centrarem en l'estudi de cossos diferencials, especialment aquells de característica 0.
Aquesta restricció és raonable, ja que el nostre objectiu és aplicar l'àlgebra diferencial a l'anell de funcions de variable real o complexa.
Més concretament, en aquesta nova terminologia d'àlgebra diferencial, donat un cos diferencial K i un dels seus elements f, ens preguntem quines propietats ha de tenir f perquè existeixi un cert cos diferencial L que contingui a K, contingui una antiderivada de f (g tal que $g' = f$) i, a més, sigui "elemental", que el poguem construir a partir de K afegint termes relativament simples.
Abans d'entrar en matèria i definir com han de ser aquests termes, resulta clar que ens manca un llenguatge per parlar d'aquests cossos que "estenen" K, la seva existència i en quin sentit ho fan.
En termes formals:

Definició 2.8. *Sigui (K, d) un cos diferencial, anomenem una extensió de cossos diferencials de K a un cos diferencial (L, D) tal que $K \subset L$ i la restricció de D a K és igual a d, és a dir:*
$D(a) = d(a) \quad \forall a \in A$

Quan A és un anell en general, parlem d'una extensió d'anells diferencials.
Havent introduit el concepte, llavors, resulta natural preguntar-se com trobar-ne a la pràctica; amb quins mètodes podem, en general, obtenir un cos diferencial extensió d'un altre.
Si ens emmirallem al cas de l'àlgebra convencional, les extensions de cossos més simples que hom pot trobar són les algebraiques, més concretament aquelles resultants de construir un cos que contingui una sola arrel d'un polinomi amb coeficients al cos.
Aquest precedent, juntament amb l'estudi de les equacions diferencials, ens porta a considerar les extensions de cossos diferencials que es formen afegint solucions d'equacions diferencials relativament simples, on per simples entendrem normalment lineals i homogènies.

Abans d'introduir formalment què entenem per equació diferencial lineal i homogènia, i quines són les propietats que volem d'una extensió de cossos associada a ella, demostrem un primer resultat general d'utilitat que ens assegura l'existència d'extensió de cossos diferencials quan l'extensió L és algebraica.

Obs. 7. *Sigui (K, d) un cos diferencial, per estendre d a K[X] és suficient definir X'.*

Demostració. Per la propietat 1) de les derivacions, n'hi ha prou amb definir $(aX^n)'$ on a és un element de K i n natural.
Però, per la propietat 2), n'hi ha prou amb definir $(X^n)'$.
Ara bé, la observació 2 precisament ens diu que aquest resultat queda determinat pel valor de $(X)'$.

□

Proposició 2.5. *Sigui (K, d) un cos diferencial, i sigui L una extensió de cossos de K algebraica i separable* [1].
Llavors, la derivació d de K estén de manera única a L.
Encara més, tot K-automorfisme de L és diferencial.

Demostració. Considerem primer el cas corresponent a una extensió finita.
Llavors, per ser L una extensió separable i el teorema de l'element primitiu, existirà $\alpha \in K$ tal que $L = K(\alpha)$, en el llenguatge usual d'extensions de cossos, de manera que serà una extensió simple.
Sigui llavors $P(X) \in K[X]$ el polinomi mínim associat a α, considerant que $P(\alpha) = 0$ i derivant, obtindrem:
$(P(\alpha))' = 0$
Aplicant ara la propietat 2) d'una derivació, podem separar $(P(\alpha))'$ de la següent manera:
$0 = (P(\alpha))' = P^d(\alpha) + DP(\alpha)\alpha'$
on $P^d(X)$ és el polinomi tal que els seus coeficients són els coeficients de $P(X)$ derivats i $DP(X)$ és el polinomi derivada de $P(X)$ en el sentit algebraic usual.
Com $P(X)$ és el polinomi mínim associat a α, aquest element en serà una arrel simple, de manera que $DP(\alpha) \neq 0$ i obtenim $\alpha' = \frac{-P^d(\alpha)}{DP(\alpha)}$.
Com en aquest cas L és un K-espai vectorial finit amb base de potències d'α, aquest fet implica la unicitat d'una derivació de L.
Demostrem ara l'existència d'una tal derivació: com L és una extensió simple, és ben conegut el fet que $L \cong \frac{K[X]}{(P(X))}$, de manera que l'estratègia natural per definir-hi una derivació serà definir $D(X)$ (que determina una derivació D a $K[X]$ juntament amb la derivació d de K) i definir-la de manera que
$D(y) \in (P(X)) \quad \forall y \in (P(X))$ perquè $(P(X))$ sigui un ideal diferencial de $(K[X], D)$.
Una derivació D com la descrita es pot obtenir definint $D(X) := -P^d(X)h(X)$,

[1] Aqui exposem la prova general del teorema, malgrat que, al marc que hem fixat pel treball, podriem no esmentar la separabilitat, ja que tota extensió ho és per $Car(K) = 0$

on $h(X) \in K[X]$ és tal que $DP(X)h(X) \equiv 1 \pmod{P(X)}$
Si $h(X)$ és tal que $DP(X)h(X) = 1 + q(X)P(X)$, es tindrà:

$D(P(X)) = (P(X))' = P^d(X) + DP(X)X' = P^d(X) + DP(X)(-P^d(X)h(X))$
$= P^d(X) - P^d(X)(1 + q(X)P(X)) = -P^d(X)q(X)P(X) \in (P(X))$
Per tant (L, D) amb D definida d'aquesta manera serà una extensió de cossos diferencials de K.
La demostració del cas general és una aplicació del *Lema de Zorn* a partir del cas finit, que seguidament desenvolupem en profunditat.

Considerem ara el conjunt
$C := \{(F, \delta) | (F, \delta)$ és extensió diferencial algebraica de (K,d) i $F \subset L\}$
Clarament C és no buit, ja que (K, d) hi pertany, de manera que podem definir a C la següent relació d'ordre:
$(F, \delta) \geq (H, \epsilon) \iff H \subset F$ i δ és extensió d' ϵ.
Per a aplicar el Lema de Zorn, hem de veure que tot subconjunt D totalment ordenat de C té una cota superior a C. Sigui D tal conjunt totalment ordenat i no buit:
Prenem com a candidat a cota l'element $a = (\bigcup_{F \in D_1} F, \bigcup_{\delta \in D_2} \delta)$ amb
$D_1 := \{F \text{ cos} | \exists \delta$ tal que $(F, \delta) \in D\}$
$D_2 := \{\delta$ aplicació$| \exists F$ tal que $(F, \delta) \in D\}$
que són no buits perquè D ho és.
Pensem la unió de totes les deltes en un sentit conjuntista, interpretant una funció com el producte cartesià del seu domini i el seu recorregut.
Com totes les parelles de funcions de D_2 estan totalment ordenades en el sentit que una sempre és extensió de l'altra o viceversa, tal funció unió, que es comporta com cadascuna d'elles en els seus dominis respectius, és també una funció, amb domini la unió de tots els conjunts F de D_1.
I encara més, per ser totes les δ derivacions, la funció unió també ho serà, de manera que $a \in C$, ja que la unió de tots els F de D_1 està continguda a L. És a dir, a és cota superior de D a C i podem aplicar el Lema de Zorn: existeix un element maximal $y = (H, \epsilon)$ a C.
Comencem veient que $H = L$.
La primera inclusió és òbvia, ja que $y \in C$, de manera que ens falta únicament veure que $L \subset H$. Suposem que no fos així, que H estés estrictament contingut en L. Llavors, hi hauria un cert element α de L que no estaria a H.
Però, com hem demostrat prèviament, llavors podriem estendre ϵ a una derivació γ de $H(\alpha)$ i $(H(\alpha), \gamma)$ pertanyeria a C, clarament satisfent $(H(\alpha), \gamma) \geq y$, de manera que y no podria ser maximal. Per tant, $H = L$.
Per acabar, veiem la unicitat d'ϵ.
Considerem la possibilitat que hi hagués una altra parella (L, γ) a C tal que no fos comparable a y amb la relació d'ordre definida, de manera que no la poguéssim descartar per la maximalitat de y. Llavors, com L és una extensió algebraica, tot element $\beta \in L$ és algebraic respecte K, de manera que podem considerar l'extensió $(K(\beta), D)$ de (K, d). Ara bé, les restriccions de γ i ϵ a $K(\beta)$ són derivacions que estenen d, de manera que només poden ser D, ja que

hem provat la unicitat pel cas finit.
En particular, $\gamma(\beta) = D(\beta) = \epsilon(\beta)$
Com l'argument es pot fer per a tot β de L, tindrem que ambdues funcions coincidiran a tot el seu domini, de manera que $\epsilon = \gamma$ i $y = (L, \epsilon)$ és l'única extensió diferencial de cossos de (K, d) tal que la extensió de cossos que li correspon és L, com voliem demostrar.
Quant a l'última afirmació del teorema, sigui σ un K-automorfisme de L (això és, un morfisme de cossos de L en L bijectiu i tal que la seva restricció a K és la identitat), i sigui ϵ l'única derivació de L que estén a d, llavors resulta clar que $\sigma^{-1}\epsilon\sigma$ és una derivació de L, de manera que, de la unicitat, es segueix immediatament que $\sigma^{-1}\epsilon\sigma = \epsilon$ i $\sigma\epsilon = \epsilon\sigma$, de manera que σ és un isomorfisme diferencial de L en L.

□

2.2.1 Operadors diferencials lineals

Sigui (K, d) un cos diferencial amb derivació no trivial (això és $d \neq 0$ com a funció de K en K).
Podem considerar, llavors, les funcions $f : K \longmapsto K$ de la forma:
$f := \sum_{i=1}^{n} a_i D^{(i)} + a_0$ on $n \in \mathbb{N}$ i $a_i \in K\ \forall i \in \{1, 2, ..., n\}$
Anomenem a una funció f d'aquesta forma *Operador diferencial lineal.*
Sigui $V := \{f|\ f$ és operador diferencial lineal$\}$, llavors V és un anell que usualment denotarem com $K[D]$, un anell de polinomis no commutatiu amb coeficients a K, ja que definirem $Da = a' + aD\ \forall a \in K$.

Definició 2.9. *Si $a_n \neq 0$ direm que l'operador f té grau (denotat $Deg(f)$) n.*

Definició 2.10. *Si $a_n = 1$ direm que l'operador és mònic.*

Sota aquesta definició, és fàcil veure que $Deg(fg) = Deg(f) + Deg(g)\ \forall f, g \in K[D]$ i, de fet, tenim algoritmes de divisió semblants als presents als anells de polinomis convencionals, tot i que cal distingir entre divisió per la dreta i per l'esquerra.
En tot cas, els operadors diferencials lineals ens resulten interessants perquè ens permeten associar-los de manera natural a una equació diferencial i, en conseqüència, considerar les extensions de cossos diferencials que s'obtenen d'afegir a un cos diferencial base les solucions d'una equació d'aquesta forma. De forma rigorosa:

Definició 2.11. *Sigui un operador diferencial lineal $l := \sum_{i=1}^{n} a_i Y^{(i)}$, anomenem equació diferencial lineal associada a l a la expressió*
$l(Y) := \sum_{i=0}^{n} a_i Y^{(i)} = 0$
on $Y^{(0)} = Y$ per conveni.
A vegades també les anomenarem equacions diferencials lineals i homogènies, fent referència al fet que, si les considerem com a polinomi diferencial en funció de Y, tenen terme independent nul.
En general, assumirem que $a_n \neq 0$ i direm que l'equació en qüestió té ordre n.

Per a entendre l'estructura algebraica d'una tal extensió de cossos diferencial que incorpori les solucions d'una equació diferencial lineal homogènia, estudiem les propietats del seu conjunt de solucions.

Proposició 2.6. *Sigui (K, d) un cos diferencial, $l(Y) := \sum_{i=0}^{n} a_i Y^{(i)} = 0$ una equació diferencial lineal i homogènia amb coeficients a K i $K \subset L$ una extensió de cossos diferencial de K que contingui els conjunt de solucions A de $l(Y)$.*
Llavors, A és un C_L-espai vectorial, on $C_L := Const_L$

Demostració. Siguin x, y elements de A, per la propietat 1.) d'una derivació tindrem que
$\sum_{i=0}^{n} a_i(x+y)^{(i)} = \sum_{i=0}^{n} a_i y^{(i)} + \sum_{i=0}^{n} a_i Y^{(i)} = 0 + 0 = 0$ de manera que $x + y \in A$
D'altra banda, sigui x un element d'A i $c \in Const_L$,
$\sum_{i=0}^{n} a_i (cx)^{(i)} = \sum_{i=0}^{n} a_i \sum_{j=0}^{i} \binom{i}{j} c^{(i-j)} x^{(j)} = \sum_{i=0}^{n} a_i x^{(i)} = 0$
on el primer pas és degut a la fòrmula de Leibniz, el segon al fet que $c \in Const_L$ (només queden els sumands on c no apareix derivada) i l'últim pas és conseqüència directa del fet que $x \in A$, de manera que $cx \in A$, com voliem demostrar.
Per tant, A és tancat per la suma i el producte per escalars que hem proposat, i la resta de propietats que el fan espai vectorial són conseqüència directa de les propietats de L com a cos. □

Sabem, llavors, que el conjunt de solucions d'una equació diferencial lineal homogènia amb coeficients a K és un espai vectorial del conjunt de constants d'una extensió de cossos diferencials que el contingui.
Encara més, de fet, el cas que considerem té propietats tan convenients que resulta possible demostrar que aquest conjunt de solucions són un espai vectorial *finit* respecte al subcòs d'aquestes constants, i la seva dimensió és acotada superiorment per l'ordre de $l(Y)$.
Amb l'objecte de demostrar aquesta propietat, introduim el concepte de *wronskià*.

Definició 2.12. *Sigui K un cos diferencial, i siguin $y_1, ..., y_n$ elements de K per un cert $n \geq 1$ natural.*
Llavors, anomenarem el determinant:

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

Determinant wronskià de $y_1, ..., y_n$, o simplement wronskià dels elements $y_1, ..., y_n$.

Específicament, veiem que l'anulació del wronskià d'un conjunt d'elements de K caracteritza la seva dependència lineal sobre el conjunt C de constants del cos diferencial.

Proposició 2.7. *Sigui K un cos diferencial, i siguin $y_1, ..., y_n$ un conjunt d'elements de K.*
Llavors, $\{y_1, ...y_n\}$ és un conjunt linealment independent sobre el conjunt $Const_K := C$ si, i només si, $W(y_1, ..., y_n) \neq 0$.

Demostració. Veiem primer que la dependència lineal implica que el wronskià és igual a zero: si el conjunt $\{y_1, ..., y_n\}$ és linealment dependent sobre C, existiran $c_1, ..., c_n \in C$ tals que $\sum_{i=1}^{n} c_i y_i = 0$ i, llavors, derivant la identitat, obtindrem:
$(\sum_{i=1}^{n} c_i y_i)^{(j)} = \sum_{i=1}^{n} (c_i y_i)^{(j)} = \sum_{i=1}^{n} \sum_{l=0}^{j} \binom{j}{l} c_i^{(j-l)} y_i^{(l)}$
$\implies \sum_{i=1}^{n} c_i y_i^{(j)} = 0 \ \forall j \in \{1, 2, ..., n-1\}$
ja que, com hem fet servir a proposicions anteriors, aplicant la fòrmula de Leibniz i el fet que els valors c_i són constants, només queden els sumands on aquests elements no apareixen derivats.
D'aquesta manera, hem obtingut una relació de dependència lineal per les columnes de la matriu que defineix el wronskià i, per tant, $W(y_1, ..., y_n) = 0$.
Passem a demostrar el recíproc: considerem $W(y_1, ..., y_n) = 0$.
Com el wronskià està definit com el determinant d'una matriu, la igualtat implica que existeix una relació de dependència lineal entre les seves columnes, en principi amb coeficients a K, és a dir:
$\exists \{k_i\}_{i \in \{1,2,...,n\}} \subset K$ tals que $\sum_{i=1}^{n} k_i y_i^{(j)} = 0 \ \forall j \in \{1, 2, ..., n-1\}$
Com al menys un dels coeficients de la igualtat serà diferent a zero, podem assumir que és el corresponent a y_1 sense pèrdua de generalitat.
Per tant, multiplicant pel seu invers, podem suposar que $k_1 = 1$
També podem assumir que n és, de fet, el nombre natural mínim d'elements diferents de $\{y_1, ..., y_n\}$ que són linealment dependents. En cas contrari, com sabem que aquest nombre mínim existeix (n satisfà la propietat, i tot subconjunt dels naturals no buit té un mínim), simplement reescriuriem la proposició anomenant n a aquest nombre natural.
En síntesi, està justificat suposar que $W(y_2, ..., y_n) \neq 0$ i es segueix fàcilment que $\{y_2, ..., y_n\}$ és un conjunt K-linealment independent.
Amb aquestes simplificacions en ment, podem prendre la igualtat original per a $j = 0$ i, derivant, obtindrem:
$\sum_{i=1}^{n} k_i y_i' + \sum_{i=2}^{n} k_i' y_i = 0$ i, restant l'equació $\sum_{i=1}^{n} k_i y_i' = 0$, deduim que $\sum_{i=2}^{n} k_i' y_i = 0$ i, com el conjunt dels y_i amb i entre 2 i n és linealment independent, $k_i' = 0 \ \forall i \in \{1, 2, ..., n\}$ i els elements $y_1, ..., y_n$ són linealment dependents sobre el subcòs C de les constants de K. □

Obs. 8. *D'aquesta propietat s'obté, en el fons, una definició consistent d'independència lineal sobre el subcòs de les constants d'un cos diferencial, sense haver de calcular-lo explícitament o treballar-hi directament.*

Veiem ara que l'ordre n de la equació diferencial acota la dimensió del seu conjunt de solucions com C-espai vectorial, completant la subsecció.

Proposició 2.8. *Sigui $l(Y)$ una equació diferencial lineal i homogènia d'ordre n. Si $\{y_1, ..., y_{n+1}\}$ és un conjunt de solucions de $l(Y)$, llavors* $W(y_1, ..., y_{n+1}) = 0$

Demostració. Per la pròpia definició del wronskià com a determinant d'una matriu, serà igual a zero si, i només si, existeix una relació de dependència lineal entre les columnes (o files) d'aquesta. Ara bé, com el conjunt $\{y_1, ..., y_{n+1}\}$ és de solucions d'una equació diferencial lineal homogènia, $l(Y) := \sum_{i=0}^{n} a_i Y^{(i)} = 0$, resulta que $y_i^{(n)} = a_n^{-1}(\sum_{j=0}^{n-1} a_j y_i^{(j)})$ (com la equació és de ordre n, $a_n \neq 0$) per a tot i entre 1 i n+1, de manera que tenim una relació de dependència entre les files de la matriu que defineix el wronskià.
En conclusió, $W(y_1, ..., y_{n+1}) = 0$ □

Corol.lari 2.2. *Sigui A el conjunt de solucions d'una equació diferencial lineal homogènia d'ordre n.*
Llavors, per la proposició 2.6, A és un C-espai vectorial, i, a més, $n \geq dim(A)$.

Obs. 9. *Com A espai de solucions d'una equació diferencial lineal homogènia d'ordre n i, per tant, un C-espai vectorial finit, entre tot parell de bases $\mathbb{B}_1$ i $\mathbb{B}_2$ de A existeix una matriu M de coeficients a C tal que M és matriu de canvi de base entre $\mathbb{B}_1$ i $\mathbb{B}_2$. És a dir, que tot conjunt de solucions de l'equació esmentada que sigui generador de l'espai de solucions i linealment independent, es podrà expressar de forma única en funció d'un altre sistema de solucions d'aquesta forma, amb coeficients a C.*

Definició 2.13. *Sigui $\{y_1, ...y_n\}$ una base de l'espai de solucions d'una equació diferencial lineal i homogènia.*
A un conjunt de tals característiques l'anomenem conjunt de solucions fonamentals.

Tenim, llavors, un marc teòric suficient per estudiar les extensions de cossos diferencials associades a una certa equació diferencial lineal i homogènia però, un cop més, per analogia amb la teoria d'extensions de cossos usual, resulta natural preguntar-se si és aplicable a aquest tipus d'extensions de cossos diferencials una certa noció de *minimalitat*, si existeix un cert cos diferencial mínim en algun sentit amb la propietat de contenir el conjunt de solucions d'una equació com la descrita, un anàleg en cert sentit del cos de descomposició d'un polinomi aplicat al cas diferencial.
La resposta és, com a mínim pels casos que estudiarem a la pràctica, positiva, i la noció de minimalitat cercada es troba al conjunt C de les constants de K. Tot seguit, ho il·lustrem amb un exemple.

Obs. 10. *Sigui (K, d) un cos diferencial amb $d = 0$ i K algebraicament tancat, i considerem l'equació $l(Y) := Y' - Y = 0$. És clar que 0 és solució d'aquesta equació diferencial i $Const_K = K$, però, com hem vist a l'apartat anterior, un conjunt no trivial de solucions d'una extensió de (K, d) tindrà dimensió 1 sobre K com a espai vectorial.*
Construim l'extensió $L := K(y)$, on L és el cos de fraccions de $K[y]$, i la derivació de L és l'única extensió de la derivació D de $K[y]$ tal que la seva restricció a K és d i $D(y) = y$.
Clarament, aquesta extensió és una solució d'un cas molt particular del problema de construir una extensió de cossos diferencials que inclogui les solucions d'una equació diferencial lineal i homogènia.
Ara bé, sense una certa noció de minimalitat preestablerta, res ens impedeix construir una segona solució, igualment vàlida, prenent $H := L(z)$, on obtenim H d'aplicar el mateix mètode sobre L que sobre K, de manera que, en particular, $H \cong Q(K[y, z])$ com a cos i $z' = z$, on $Q(A)$ indica notació pel cos de fraccions d'A quan aquest és un domini d'integritat.
La diferència entre L i H radica, principalment, en què, en el procés de construcció de H, afegim constants que no teniem prèviament a K.
Procedim primer a demostrar que $Const_L = Const_K = K$, observant que la derivada d'un element x de $K[y]$, on $x := \sum_{i=0}^{n} a_i y^i$, és
$x' = \sum_{i=1}^{n} a_i' y^i + \sum_{i=1}^{n} i a_i y^i + a_0' = \sum_{i=1}^{n} i a_i y^i$,
de manera que serà igual a zero si, i només si, $ia_i = 0\ \forall i \in \{1, 2, ..., n\}$
Però, com ja hem establert clarament abans, considerem K tal que $Car(K) = 0$, de manera que cap dels valors de i pot ser zero.
En conseqüència, tots els a_i entre 1 i n hauran de ser zero i $x \in K$.
Fem servir aquest resultat per demostrar que les constants de L són elements de K:
sigui $\frac{f}{g} \neq 0$ una constant de L amb f i g coprimers (recordem que f i g són elements de $K[y]$, que com anell és un D.F.U, assegurant que els podem triar d'aquesta manera), resulta suficient veure que $g \in K$, de manera que l'element serà una constant de $K[y]$ i, com hem vist, un element de K.
$D(\frac{f}{g}) = \frac{D(f)g - fD(g)}{g^2} = 0 \iff D(f)g - fD(g) = 0 \iff fD(g) = gD(f)$
Com K algebraicament tancat, el resultat que volem veure equival a veure que g no té arrels a K, que cap factor de la forma $y - \lambda$ amb $\lambda \in K$ divideix a g.
Tot factor $y - \lambda$ és primer a $K[y]$, ja que $(y - \lambda)$ és maximal per ser un polinomi irreductible, de manera que podem aplicar el següent raonament:
sigui $y - \lambda$ un tal factor que divideix g, llavors, per la igualtat obtinguda del fet que $\frac{f}{g}$ constant, divideix a f o a $D(g)$. El primer cas és impossible, ja que hem triat f i g coprimers.
Quant al segon cas, si iterem el mateix raonament per a tots els factors de la forma establerta que divideixen g, obtindrem que $g|D(g)$.
Ara bé, sabem que $Deg(g) = Deg(D(g))$, de manera que $\frac{D(g)}{g} \in K$. Però això no és possible, ja que, com hem vist anteriorment, els coeficients de $D(g)$ són els coeficients de g multiplicats per l'index i que els pertoca, per la potència de y que els acompanya.

Com la contradicció sorgeix naturalment de suposar que g és divisible per algun factor lineal, es conclou que $g \in K$, completant la demostració.
Per tant, $Const_L \subset K$ i són el mateix conjunt.
Ara bé, H sí que afegeix constants que no són elements de K, com podem veure fàcilment considerant l'element $\frac{z}{y}$. És evident que no pertany a K, o tindriem que $z = \frac{z}{y}y$ seria tal que $z \in K[y] \subset L$
però $D(\frac{z}{y}) = \frac{D(z)y - zD(y)}{y^2} = \frac{zy-zy}{y^2} = 0$, del què es segueix que $Const_H \neq K$ immediatament.

2.3 L'extensió de Picard-Vessiot

L'exemple anterior, juntament amb la resta de conceptes i resultats que hem desenvolupat a la secció 2.2.1, ens permeten, finalment, definir aquest anàleg que buscàvem del cos de descomposició d'un polinomi al context de l'àlgebra diferencial, l'extensió de cossos diferencial minimal (en el sentit de mantenir el subcòs de constants del cos base) que conté les solucions d'una certa equació diferencial lineal homogènia. L'enunciem:

Definició 2.14. *Sigui (K, d) un cos diferencial, i considerem $l(Y) = 0$ una equació diferencial lineal i homogènia amb coeficients a K. Sigui L un cos amb una certa derivació D tal que $K \subset L$.*
Llavors, direm que L és una extensió de Picard-Vessiot de K associada a $l(Y) = 0$ si, i només si:
1.) (L, D) és una extensió de cossos diferencials de (K, d)
2.) $L = K < y_1, ..., y_n >$ per a un cert n natural (L és el mínim cos diferencial extensió de K que conté y_1,...,y_n, és a dir, el cos mínim en sentit d'inclusió conjuntista que conté aquests elements i les seves derivades), on $\{y_1, ..., y_n\}$ és un conjunt de solucions fonamental de $l(Y) = 0$ contingut a L
3.) $Const_L = Const_K$

Per suposat, la primera pregunta que hom es planteja davant d'un concepte matemàtic convenient és, de fet, si existeix i, si ho fa, quines propietats en garanteixen l'existència.
Seguint la mateixa línia de treball que hem plantejat de bon principi, ens centrarem en arribar al resultat teòric particular de la teoria de Picard-Vessiot que ens serveix per delimitar la nostra qüestió central.
Com veurem al capítol següent, considerarem cossos de funcions amb la derivació usual pròpia del càlcul diferencial i valors complexos en comptes de reals, amb una sèrie d'avantatges en ment.
El primer d'ells, tocant a aquest apartat, és que $\mathbb{C}$ és algebraicament tancat, i serà sempre el subcòs de constants d'aquests cossos de funcions.
En sintonia amb aquest marc de treball, a nivell teòric general, podrem assegurar que existeix una extensió de Picard-Vessiot per a un cos diferencial K quan $Const_K$ sigui algebraicament tancat.

Encara més, de fet, en aquest cas particular, l'extensió de Picard-Vessiot serà única excepte isomorfismes diferencials.

2.3.1 Nocions preliminars

La construcció d'una extensió de Picard-Vessiot emprant tècniques algebraiques dista de ser un afer trivial. La demostració constructiva de la seva existència requereix conèixer i fer referència a tot un conjunt de resultats i objectes d'ús comú entre la comunitat matemàtica, però que difícilment podrien ser obviats sense assumir cert bagatge.
En un intent per fer el treball el més autocontingut possible i no haver de referir la bibliografia al lector hipotètic innecessàriament, aquesta subsecció serveix com una sort d'annex, malgrat inclosa al treball per la seva relació directa amb els propers resultats.

Definició 2.15. *Sigui A un anell, i sigui $S \subset A$. Diem que S és un conjunt multiplicativament tancat si $1 \in S$, $0 \notin S$ i $st \in S \ \forall \ s,t \in S$*

Definició 2.16. *Sigui A un domini d'integritat*[2]*, $S \subset A$ un conjunt multiplicativament tancat. Considerem la relació d'equivalència definida a $A \times S$: $(a,s) \sim (r,w) \iff aw = rs \ \forall \ (a,s), (r,w) \in A \times S$*
Anomemem llavors al conjunt quocient d'aquesta relació d'equivalència, denotat per $S^{-1}A$, localització de A respecte S.
En general, emprarem notació de fraccions per referir-nos a la classe d'un element, així: $[(a,s)] := \frac{a}{s}$

Obs. 11. $(A \setminus \{0\})^{-1}A = Q(A)$
$S^{-1}A \subset Q(A)$ *en general.*

Obs. 12. *És especialment comú considerar els casos $S = \{1\} \cup \{x^n |\ n \geq 1\}$ amb $x \in A \setminus \{0\}$ i $S = A \setminus p$ on p és un ideal primer d'A.*
De fet, en el segon cas denotem $S^{-1}A = A_p$ ja que, històricament, és el cas que dóna nom al concepte, pel paper que tenen en àlgebra commutativa aquestes construccions a l'hora d'estudiar propietats locals de A; propietats de l'anell que es poden deduir de l'estudi de les localitzacions respecte els seus ideals primers.

Obs. 13. *Naturalment, $S^{-1}A$ és subanell de $Q(A)$, amb les operacions:*
1.) $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{ts}$
2.) $\frac{a}{s}\frac{b}{t} = \frac{ab}{ts}$
ja que el numerador de la fracció resultat és un element de A de manera trivial i el denominador pertany a S per ser aquest un conjunt multiplicativament tancat.

Obs. 14. *Per la proposició 2.3, com $S^{-1}A$ és subanell de $Q(A)$, podem estendre una derivació d de A únicament a una de $S^{-1}A$ prenent la restricció corresponent de l'única derivació del cos de fraccions de A que estén a d.*

[2]La localització respecte un conjunt multiplicativament tancat es pot definir en general per un anell A, però la relació d'equivalència canvia i el cas és més subtil quan A conté divisors de zero. A nivell pràctic, nosaltres només l'emprarem amb dominis d'integritat.

A més, $(\frac{a}{s})' \in S^1A \ \forall \ \frac{a}{s} \in S^{-1}A$ *per ser* $S \subset A$ *conjunt multiplicativament tancat, de manera que te sentit considerar les localitzacions com a extensions d'anells diferencials.*

Seguidament, introduim una sèrie de conceptes bàsics propis de l'àlgebra commutativa:

Definició 2.17. *Sigui* A *un anell amb unitat,* M *un conjunt.*
Diem que M *és un* A*-mòdul*[3] *si* $(M, +)$ *és un grup abelià amb una certa operació, i podem definir una aplicació* $\phi : A \times M \longmapsto M$ *que anomenarem producte per escalars i denotarem com* $\phi((a, m)) := am \ \forall a \in A, \forall m \in M$ *que satisfà:*
1.) $a(x + y) = ax + ay$
2.) $(a + b)x = ax + bx$
3.) $(ab)x = a(bx)$
4.) $1x = x$
$\forall \ x, y \in M, \ \forall \ a, b \in A$

Obs. 15. *Quan* A *és un cos, un* A*-mòdul és, de fet, el mateix que un* A*-espai vectorial.*

Definició 2.18. *Sigui* $N \subset M$*, si* N *és tancat respecte la suma i el producte d'escalars, diem que* N *és un submòdul de* M*.*
Quan aquest és el cas, podem considerar el mòdul quocient d'un mòdul respecte un submòdul: de manera anàloga al cas dels espais vectorials, serà el conjunt quocient associat a la relació d'equivalència $x \sim y \iff x - y \in N$*. El denotarem* $\frac{M}{N}$

Definició 2.19. *Sigui* M *un* A*-mòdul, diem que* M *és finitament generat si existeix un conjunt finit* $\{e_1, ..., e_n\}$ *tal que, per a tot element* $x \in M$*, existeixen valors* $a_i \in A \ \forall i \in \{1, 2, ..., n\}$ *de manera que* $x = \sum_{i=1}^{n} a_i e_i$

Definició 2.20. *Sigui* M *un* A*-mòdul, direm que* M *és lliure quan tingui una base, és a dir, un sistema de generadors que sigui linealment independent, en el mateix sentit que es defineixen aquests conceptes pels espais vectorials.*

Definició 2.21. *Sigui* X *un* A*-mòdul, direm que* X *és una* A*-àlgebra si existeix una aplicació* $\lambda : X \times X \longmapsto X$ *que anomenarem producte (i denotarem per* $\lambda((x, y)) = xy$*) amb les següents propietats:*
1.) $x(y + z) = xy + xz$
2.) $(y + z)x = yx + zx$
3.) $(ax)(by) = (ab)xy$
$\forall \ x, y, z \in X \ \forall \ a, b \in A$

Obs. 16. *Resulta clar que, si* X *és un anell commutatiu, les propietats 1.) i 2.) de la definició es satisfaran trivialment, de manera que un* A*-mòdul que a*

[3] En particular, aqui hem donat la definició d'un mòdul per l'esquerra d'A. Es poden definir de forma anàloga els mòduls per la dreta, encara que, a la majoria d'aplicacions pràctiques, els mòduls que considerem ho seran per l'esquerra i la dreta.

més sigui anell, només necessita satisfer la propietat 3.), una certa compatibilitat entre el seu producte intern i el producte amb escalars.

Definició 2.22. *Direm que una A-àlgebra X és finitament generada si el seu producte és commutatiu i associatiu i existeix un conjunt finit $\{x_1, ..., x_n\}$ tal que tot element de X es pot escriure en termes d'una expressió polinòmica en funció dels termes x_i amb i entre 1 i n, és a dir:*
sigui x un element de X, llavors existeix $p \in A[X_1, ..., X_n]$ (l'anell de polinomis de n variables amb coeficients a A) tal que $f(p) = x$, on $f : A[X_1, ..., X_n] \longmapsto X$ és el morfisme d'anells que, restringit a A és la identitat i envia X_i a x_i per a tot i, també conegut com a morfisme d'avaluació.

La raó principal per la qual introduim els mòduls i les àlgebres al context d'aquest treball és per construir el *producte tensorial* de dos A-mòduls, un mòdul particular assignable a una parella d'A-mòduls que conserva algunes propietats algebraiques interessants.
Primer, introduim una sèrie de definicions necessàries per a la seva construcció:

Definició 2.23. *Siguin M, N A-mòduls, diem que una aplicació $f : M \longmapsto N$ és A-lineal si satisfà:*
1.)$f(x + y) = f(x) + f(y)$
2.)$f(ax) = af(x)$
$\forall\ x, y \in M\ \forall\ a \in A$

Definició 2.24. *Sigui M un A-mòdul. Denotarem per $A^{(M)}$ l'A-mòdul lliure amb base del mateix cardinal que M, això és: a cada element m de M li assignem un únic element, x_m, i $A^{(M)}$ és el mòdul lliure resultant de prendre totes les sumes formals finites dels elements x_m amb coeficients a A, considerant els x_m linealment independents.*

Definició 2.25. *Sigui $f : M \times N \longmapsto Z$ amb M, N, Z A-mòduls.*
Diem que f és una aplicació A-bilineal si les aplicacions $f(x, .) : N \longmapsto Z$ i $f(., y) : M \longmapsto Z$ (les aplicacions resultants de restringir f a un sol valor a cadascuna de les seves components) són A-lineals $\forall x \in M\ \forall y \in N$

Finalment, demostrem la propietat que defineix el producte tensorial de dos mòduls:

Proposició 2.9. *Siguin M i N A-mòduls, existeix un únic A-mòdul T i una única aplicació $g : M \times N \longmapsto T$ A-bilineal satisfent la següent propietat:*
Per a tota aplicació $f : M \times N \longmapsto Z$ bilineal, amb Z A-mòdul, existeix una única funció $\overline{f} : T \longmapsto Z$ A-lineal tal que $f = \overline{f} \circ g$

Demostració. Comencem provant la unicitat (estructural, excepte isomorfismes de mòduls, és a dir, aplicacions A-lineals bijectives) d'una parella (T, g) amb la propietat enunciada: considerem (T', g') una altra parella amb la mateixa propietat.

Com (T, g) té la propietat i g' és bilineal, existirà una única $\overline{g'}$ lineal de T a T' tal que $g' = \overline{g'} \circ g$
Anàlogament, existeix una única $\overline{g}$ de T' a T lineal tal que $g = \overline{g} \circ g'$
Per la primera igualtat, $g' = \overline{g'} \circ \overline{g} \circ g'$, de manera que $\overline{g'} \circ \overline{g} = id_{T'}$
Aplicant el mateix argument a la segona igualtat, obtenim que $g = \overline{g} \circ \overline{g'} \circ g$, de manera que $\overline{g} \circ \overline{g'} = id_T$, així que són inverses i $T \cong T'$ com A-mòduls.
Sobre la unicitat que atribuim a l'enunciat a la funció g, és en el sentit que existeix j isomorfisme d'A-mòduls tal que $g' = j \circ g$. En aquest cas, $j = \overline{g'}$.
Quant a l'existència, la demostrem de manera constructiva: considerem, en la notació que hem preestablert, $R := A^{(M \times N)}$ i fem pas al quocient per S, que és com denotarem el submòdul més petit (en el sentit d'inclusió conjuntista) que conté els elements de la forma:
$(x, y + y') - (x, y) - (x, y')$
$(x + x', y) - (x, y) - (x', y)$
$(ax, y) - a(x, y)$
$(x, ay) - a(x, y)$
$\forall\ x, x' \in M\ \forall\ y, y' \in N\ \forall a \in A$
Cal notar que fem un abús de notació, ja que, en la notació anterior, quan parlem de (x, y) fem referència a l'element $x_{(x,y)}$ de $A^{(M \times N)}$.
Per fi, prenem $T := \frac{R}{S}$ com el nostre candidat a satisfer la propietat enunciada, i denotem $[(x, y)] := x \otimes y$ com a element de T.
Prenem també $g : M \times N \longmapsto T$ tal que $g((x, y)) = x \otimes y$ per a tot (x, y) i resulta clar que g és A-bilineal per construcció, per com hem triat S.
Només queda veure que satisfà la propietat:
sigui $f : M \times N \longmapsto Z$ bilineal, amb Z A-mòdul.
Per la definició de R, podem estendre per linealitat qualsevol funció de $M \times N$ a Z a una de R a Z. Si f és bilineal, en particular s'anul·larà en tots els generadors de S, de manera que definirà una aplicació A-lineal entre T i Z.
Aplicar aquest procediment a una funció determinada ens dóna una única aplicació lineal $\overline{f}$ que satisfarà $\overline{f}(x \otimes y) = f((x, y))$ per a tot $(x, y) \in M \times N$, de manera que és l'aplicació que busquem, satisfent $f = \overline{f} \circ g$ □

Definició 2.26. *A la parella (T, g) com l'enunciada a la proposició anterior l'anomenem producte tensorial de M i N respecte A, i podem denotar el A-mòdul corresponent per $T := M \otimes N$, indicant-se a vegades sobre quin anell es prenen els mòduls amb un subíndex situat al signe de producte.*
A la propietat que satisfà la parella esmentada l'anomemem propietat universal del producte tensorial.
Als elements de $M \otimes N$ de la forma $x \otimes y$ els anomenem tensors purs.

Obs. 17. *Si M i N són A-àlgebres, $M \otimes N$ és també una A-àlgebra, amb el producte definit per $(x \otimes y)(z \otimes t) := xz \otimes yt\ \forall\ x, z \in M\ \forall\ y, t \in M$*

Obs. 18. *Siguin A i B sistemes de generadors de M i N mòduls, respectivament, (això és, subconjunts que puguin generar amb les seves combinacions lineals tots els elements del mòdul), llavors el conjunt $\{e \otimes v |\ e \in A\ v \in B\}$ és un sistema de generadors de $M \otimes N$.*

En particular, si M i N són finitament generats, el seu producte tensorial també ho serà.

Obs. 19. *A més del propi anell A i els ideals d'A com a exemples de A-mòduls, també podem considerar A com a C-mòdul, on $C \subset A$ és un dels seus subanells.*

Proposició 2.10. *Siguin (R, d_1), (F, d_2) extensions de cossos diferencials d'un cert cos K amb una derivació d. Llavors, considerant R i F com K-mòduls, $R \otimes F$ és un anell diferencial amb la derivació D que satisfà $D(x \otimes y) = d_1(x) \otimes y + x \otimes d_2(y)\ \forall\ x \in R,\ y \in F$ i envia tota suma de tensors purs a la suma de les seves imatges per D.*

Demostració. Que $R \otimes F$ és un anell és conseqüència directa de la observació 17, ja que tant R com F són K-àlgebres i anells commutatius.
D'aquesta manera, només és necessari demostrar que D com la definida és una derivació. Hem aprofitat que els tensors purs són un sistema de generadors de $R \otimes F$ per definir per bilinealitat D que satisfaci la propietat 1.) per construcció, de manera que només cal veure com es comporta el producte de tensors respecte D.
Siguin $p, q \in R \otimes F$, llavors existeixen $n, m \geq 1$ naturals i conjunts $\{a_i\}_{1 \leq i \leq n} \subset K$, $\{b_j\}_{1 \leq j \leq m} \subset K$ tals que $p = \sum_{i=1}^{n} a_i x_i \otimes y_i$ i $q = \sum_{j=1}^{m} b_j z_j \otimes t_j$ on tots els $x_i, z_j \in R$ i tots els $y_i, t_j \in F$
Per tant, tindrem:
$D(pq) = D(\sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j (x_i \otimes y_i)(z_j \otimes t_j))$
per la binealitat dels tensors purs, podem definir $x'_i := a_i x_i$ per a tot i i $z'_j := b_j z_j$ per a tot j, de manera que simplifiquem l'expressió per a manipular-la còmodament:
$D(pq) = D(\sum_{i=1}^{n} \sum_{j=1}^{m} (x'_i \otimes y_i)(z'_j \otimes t_j)) = D(\sum_{i=1}^{n} \sum_{j=1}^{m} x'_i z'_j \otimes y_i t_j)$
$= \sum_{i=1}^{n} \sum_{j=1}^{m} D(x'_i z'_j \otimes y_i t_j)$
$= \sum_{i=1}^{n} \sum_{j=1}^{m} d_1(x'_i z'_j) \otimes y_i t_j + x'_i z'_j \otimes d_2(y_i t_j) =$
$\sum_{i=1}^{n} \sum_{j=1}^{m} d_1(x'_i) z'_j \otimes y_i t_j + x'_i d_1(z'_j) \otimes y_i t_j + x'_i z'_j \otimes d_2(y_i) t_j + x'_i z'_j \otimes y_i d_2(t_j) =$
$\sum_{i=1}^{n} \sum_{j=1}^{m} d_1(x'_i) z'_j \otimes y_i t_j + x'_i z'_j \otimes d_2(y_i) t_j + x'_i d_1(z'_j) \otimes y_i t_j + x'_i z'_j \otimes y_i d_2(t_j) =$
$\sum_{i=1}^{n} \sum_{j=1}^{m} (d_1(x'_i) + x'_i) z'_j \otimes (d_2(y_i) + y_i) t_j + x'_i (d_1(z'_j) + z'_j) \otimes y_i (t_j + d_2(t_j)) =$
$\sum_{i=1}^{n} \sum_{j=1}^{m} (D(x'_i \otimes y_i))(z'_j \otimes t_j) + (x'_i \otimes y_i)(D(z'_j \otimes t_j))$
$= D(p)q + pD(q)\ \forall\ p, q \in R \otimes F$ □

Obs. 20. *A la situació descrita pel teorema anterior, el tensor pur $1 \otimes 1$ és una unitat de $R \otimes F$ com a anell i, si un tensor pur $x \otimes y$ és tal que els elements x i y són invertibles (pel cas que ens ocupa, serà suficient que siguin diferents de zero per ser R i F cossos), llavors $x \otimes y$ és invertible amb el producte definit al tensorial.*

Per a acabar la secció, introduim una sèrie de resultats bàsics referents a l'àmbit de la geometria algebraica.

Definició 2.27. *Sigui K un cos, K^n el producte cartesià de n còpies de K amb $n \geq 1$ i sigui $K[X_1, ..., X_n]$ l'anell de polinomis en n variables amb coeficients a K.*
Anomenem varietat afí a un subconjunt $V \subset K^n$ de la forma $V = V(I) := \{p \in K^n |\ f(p) = 0\ \forall\ p \in I\}$, on I és un ideal de $K[X_1, ..., X_n]$.

Proposició 2.11. *Els conjunt de varietats afins de K^n, denotat per τ, és un conjunt de tancats d'una topologia.*

Demostració. Clarament, $\emptyset \in \tau$, ja que $V(K[X_1, ..., X_n]) = \emptyset$ (cap punt de K^n pot anul·lar un element de K diferent de zero, per exemple).
Anàlogament, $K^n \in \tau$, ja que $V(\{0\}) = K^n$.
Només queda veure que, per a tot conjunt $\{V(I_i)\}_{i \in I} \subset \tau$, $\bigcap_{i \in I} V(I_i) \in \tau$
Aquesta propietat, però, es segueix directament del fet que $\bigcap_{i \in I} V(I_i) = V(\bigoplus_{i \in I} I_i)$, on $\bigoplus_{i \in I} I_i$ denota la suma directa d'un conjunt d'ideals de $K[X_1, ..., X_n]$. En general, anomenem suma directa d'un conjunt d'ideals al conjunt d'elements que es poden escriure com sumes finites d'elements de cadascun dels I_i, rigorosament el podem definir com $\bigoplus_{i \in I} I_i :=< \bigcup_{i \in I} I_i >$, que, com és natural, es redueix a la suma d'ideals convencional quan el conjunt I és finit.
Demostrem la propietat enunciada: prenem p de la intersecció de totes les $V(I_i)$. Com $f(p) = 0\ \forall\ f \in I_i$ per a tot i de I, és clar que p anul·larà tota suma finita d'elements d'aquests ideals i, per tant, $p \in V(\bigoplus_{i \in I} I_i)$
Recíprocament, tot element p de K^n que anul·li tots els elements de $\bigoplus_{i \in I} I_i$ anul·larà en particular els elements de $\bigcup_{i \in I} I_i$ i, per tant, també els de cada I_i. □

Definició 2.28. *A la topologia sobre K^n que té per tancats les varietats afins l'anomenem topologia de Zariski.*

Definició 2.29. *Sigui $V \subset K^n$, resulta directe demostrar que el conjunt de polinomis f de $K[X_1, ..., X_n]$ tals que $f(p) = 0\ \forall\ p \in V$ és un ideal.*
El denotem per $\mathbb{I}(V)$ i l'anomenem ideal associat a V.

Definició 2.30. *Diem que una varietat afí és irreductible si no es pot expressar com la unió de dos subconjunts tancats de la seva toopologia induida.*

En el context de les varietats afins, la irreductibilitat d'una varietat és caracteritzable en termes del seu ideal associat.

Proposició 2.12. *Sigui V un tancat de la topologia de Zariski de K^n. Llavors, V és irreductible si, i només si, $\mathbb{I}(V)$ és un ideal primer.*

Demostració. Escrivim I per a referir-nos a $\mathbb{I}(V)$ per abreujar.
Considerem V irreductible, i prenem $p, q \in K[X_1, ..., X_n]$ tals que $pq \in I$, de manera que $p(a)q(a) = 0\ \forall\ a \in V$. Com K és un domini d'integritat, llavors $p(a) = 0$ o $q(a) = 0$ per a tot a de V, de manera que $a \in V((p))$ o $a \in V((q))$, $V \subset V((p)) \cup V((q))$, de manera que $V \subset V((p))$ o $V \subset V((q))$

per ser V irreductible (en cas contrari, tindriem que V és unió de dos tancats de la seva topologia induida), i, en conseqüència, $p(\alpha) = 0 \ \forall \ \alpha \in V$ o $q(\alpha) = 0$ $\forall \ \alpha \in V$, és a dir, o bé $p \in I$ o $q \in I$ i, per tant, I és un ideal primer.
Demostrem el recíproc per reducció a l'absurd: suposem que $V = V_1 \cup V_2$ amb V_i tancats de V, $i \in \{1, 2\}$, i I ideal primer.
Com suposem que la descomposició de V nega la seva irreductibilitat, no pot ser trivial, de manera que cap de les V_i pot contenir V. Per tant, podem prendre f i g elements de $\mathbb{I}(V_1)$ i $\mathbb{I}(V_2)$, respectivament, que no pertanyin a l'ideal associat de l'altra varietat.
Resulta clar, llavors, que ni f ni g pertanyen a I, però fg sí per ser V unió de les V_i, de manera que I no pot ser primer i obtenim una contradicció. □

Quan K és algebraicament tancat, a més, comptem amb un resultat especialment il·lustre, el $Nullstellensatz$, que estableix bijeccions entre certs tipus d'ideals de $K[X_1, ..., X_n]$ i varietats afins.

Lema 2.1. *(Nullstellensatz[4]) Sigui K un cos algebraicament tancat, $A := K[X_1, ..., X_n]$, llavors:*
a.) Tots els ideals maximals de A són de la forma $(X_1 - y_1, ..., X_n - y_n)$ amb $p := (y_1, ..., y_n) \in K^n$
b.) Tot ideal propi de A, I, és tal que $V(I) \neq \emptyset$
c.) Sigui I ideal de A, $\mathbb{I}(V(I)) = \sqrt{I}$, on $\sqrt{I} := \{x \in A | \ \exists n \in \mathbb{N}$ tal que $x^n \in I\}$

Citem aquest resultat com a lema en tant que tindrà un paper auxiliar en el context d'aquesta secció, i és un resultat prou destacat i conegut com per no necessitar una secció dedicada a demostrar-lo, malgrat una demostració detallada es pot trobar al capítol 1 de [C-H].
De fet, emprarem de manera concreta el corol·lari següent de la secció c.) del teorema:

Corol.lari 2.3. *Sigui K un cos algebraicament tancat, existeix una correspondència bijectiva entre el ideals radicals de $K[X_1, ..., X_n]$ i les varietats afins de K^n.*

Abans d'aplicar-la, però, definim el context en què la necessitarem, parlem del concepte d'*anell de coordenades* d'una varietat V i la relacionem amb un tipus específic de K-àlgebra.

Definició 2.31. *Sigui f un element de $K[X_1, ..., X_n]$. Podem interpretar f com la funció $f : K^n \longmapsto K$ que envia $p \in K^n$ a $f(p)$. Considerem ara una varietat afí V, i interpretem f com a funció restringint el seu domini a V, $f : V \longmapsto K$. El conjunt de totes aquestes restriccions polinòmiques és clarament un anell, heretant aquesta estructura de les operacions usuals amb polinomis.*
Denotat per $K[V]$, l'anomenem anell de coordenades de V.

[4]"Teorema dels zeros", en alemany. Teorema cabdal en geometria algebraica clàssica, demostrat originalment per David Hilbert(1862-1943).

Proposició 2.13. *Sigui V una varietat afí de K^n, $K[V] \cong \frac{K[X_1,...,X_n]}{\mathbb{I}(V)}$ com a anell.*

Demostració. Considerem $\phi : K[X_1, ..., X_n] \longmapsto K[V]$ la funció que envia cada polinomi en n variables f a la seva funció de valoració restringida a V, tal com hem considerat prèviament. Resulta clar llavors que ϕ és exhaustiva, de manera que només ens cal veure que $Ker(\phi) = \mathbb{I}(V)$ i aplicar el primer teorema d'isomorfia d'anells.
Però això és senzill de deduir, ja que un element g de $K[X_1, ..., X_n]$ és tal que $\phi(g) = 0$ si, i només si, com a polinomi, satisfà $g(p) = 0 \ \forall \ p \in V$, per definició del què vol dir que una funció sigui igual a la funció zero.
Ara bé, aquesta condició és equivalent a dir que $g \in \mathbb{I}(V)$ i, en conseqüència, $K[V] \cong \frac{K[X_1,...,X_n]}{\mathbb{I}(V)}$ □

Proposició 2.14. *Sigui K un cos, X una K-àlgebra finitament generada tal que* [5] *$K \subset X$ amb conjunt de generadors $A := \{1, x_1, ..., x_n\}$ i $n \geq 1$ natural. Llavors, existeix un ideal I de $K[X_1, ..., X_n]$ tal que $X \cong \frac{K[X_1,...,X_n]}{I}$*

Demostració. Prenem $\phi : K[X_1, ..., X_n] \longmapsto X$ tal que $\phi(X_i) = x_i$ per a tot i entre 1 i n i $\phi(1) = 1$ satisfent $\phi(p + q) = \phi(p) + \phi(q)$ i $\phi(pq) = \phi(p)\phi(q)$ per a tot p, q de $K[X_1, ..., X_n]$.
Com X és finitament generada amb sistema de generadors A, ϕ queda totalment determinada com a funció per aquestes propietats i, a més, serà exhaustiva.
Encara més, per les propietats de X com a K-àlgebra, 1 serà l'element neutre del producte de X, de manera que ϕ envia el neutre del producte de l'anell de polinomis al neutre de X, satisfent les propietats de definició d'un morfisme d'anells.
Per aquest motiu, podem considerar $I = Ker(\phi)$ i, aplicant el primer teorema d'isomorfia d'anells, obtenim la relació desitjada, $X \cong \frac{K[X_1,...,X_n]}{I}$ □

Proposició 2.15. *Sigui K un cos algebraicament tancat, i sigui X una K-àlgebra finitament generada tal que $K \subset X$ i, a més, sigui domini d'integritat.*
Llavors, existeix una varietat afí V tal que $K[V] \cong X$

Demostració. Sigui A amb la notació del teorema anterior un sistema de generadors de X com a K-àlgebra.
Per la proposició 2.14, existeix un cert ideal I de $K[X_1, ..., X_n]$ tal que $X \cong \frac{K[X_1,...,X_n]}{I}$
D'aquesta relació d'isomorfia, i perquè X és domini d'integritat, es segueix que I és un ideal primer i, per tant, radical.
Com K és algebraicament tancat, podem aplicar el corol.lari 2.3 i deduir que, de fet, $I = \mathbb{I}(V)$ per a una certa varietat afí V de K^n.

[5] Aquesta condició, que és formulada en sentit algebraic, és equivalent a dir que existeix un cert morfisme d'anells $h : K \longmapsto X$, de manera que X serà una K-àlgebra en el sentit definit a [A-M], en comptes de la definició més general que hem escollit pel treball.

Per la proposició 2.13, resulta clar que $X \cong K[V]$ □

Definició 2.32. *Sigui X un espai topològic, diem que un conjunt B és localment tancat si existeix un parell de conjunts A i C tals que A és obert i C tancat que satisfacin $B = A \cap C$*

Definició 2.33. *Sigui X un espai topològic, diem que un subconjunt de X és constructible si és unió finita de conjunts localment tancats.*

Proposició 2.16. *Sigui K un cos, considerat com a espai topològic amb la topologia de Zariski.*
Llavors, tot conjunt $D \subset K$ constructible és finit o el complementari d'un conjunt finit.

Demostració. Com és constructible, llavors és unió finita de de conjunts localment tancats. Sigui un conjunt B localment tancat de K amb la topologia de Zariski, $B = A \cap C$ amb A obert i C tancat, si $C \neq K$, llavors C és el conjunt d'arrels d'un polinomi p de $K[X]$.
Això passa perquè, si C tancat, $C = V(I)$ per un cert ideal de $K[X]$, però $K[X]$ és un domini d'ideals principals, de manera que $I = (p)$ per un cert polinomi i, clarament, C és el seu conjunt d'arrels a K.
A més, es segueix del fet que K sigui un cos que el conjunt de les seves arrels a K ha de ser finit, de manera que C també ho serà.
En conclusió, si B és localment tancat i el conjunt C que el defineix no és K, llavors B és finit per estar-hi contingut.
Resulta clar que, si això aplica per tots els conjunts localment tancats que componen D, llavors serà finit. En cas contrari, hi haurà com a mínim un cert B localment tancat tal que serà la intersecció d'un obert A amb K i, per tant, serà obert. Si B és obert, llavors o és el buit i no aporta res a la unió o bé és el complementari d'un tancat diferent del total i, per l'observació que hem fet abans, ha de ser el complementari d'un finit.
Com el resultat de la unió del complementari d'un finit amb un altre complementari d'un finit o amb un conjunt finit continua sent el complementari d'un finit, en aquest cas tindrem que D és el complementari d'un conjunt finit. □

Lema 2.2. *(Chevalley)*[6] *Sigui $f : K^n \longmapsto K$ una funció polinòmica (la funció d'avaluació associada a un polinomi).*
Llavors, per a tot $D \subset K^n$ constructible, $f(D)$ és constructible.

[6] De manera anàloga al cas anterior pel Nullstellensatz, citem aquest resultat com a lema pel seu paper fonamentalment auxiliar. L'anotació *Chevalley* fa referència al fet que és un corol·lari del teorema de Chevalley, un resultat profund que s'enuncia i demostra generalment al context de la teoria de varietats algebraiques, de manera que s'escapa del focus d'atenció del treball.
Un desenvolupament exhaustiu de la teoria que fonamenta aquest resultat, a més d'una demostració de la versió general, es pot trobar al capítol 2 de [C-H].

2.3.2 Existència

En tota la secció considerarem (K, d) el cos diferencial a estendre, amb $Const_K$ algebraicament tancat.
Acabada la presentació i demostració de la majoria de resultats teòrics necessaris per fer una demostració constructiva de l'existència de l'extensió de Picard-Vessiot[7], hi procedim seguint l'estratègia següent: construirem una K-àlgebra convenient que contingui les solucions d'una equació diferencial lineal i homogènia, i assegurarem a través de diferents modificacions algebraiques que sigui un cos i tingui el mateix subcòs de funcions que K, a més de procurar que la derivació que hi definim sigui una extensió de la definida sobre K.

Definició 2.34. *Sigui (A, d) un anell diferencial, sigui $A[X_i]_{i\in\mathbb{N}}$ l'anell de polinomis amb una quantitat infinita comptable d'incògnites. Llavors, definint $D(X_i) = X_{i+1}$ per a tot i, $D(a) = d$, i canviant la notació per $X_0 = X$, $X_i = X^{(i)}$ per a tot $i \geq 1$, obtenim un anell diferencial de polinomis en una variable i les seves derivades per D, el qual anomenem anell de polinomis diferencials amb coeficients a A, denotat per $A\{X\}$. Iterant el mateix procediment prenent coeficients a l'anells de polinomis diferencials amb $n-1$ incògnites, podem definir $A\{X_1, ..., X_n\}$ per a tot $n \geq 1$*

Considerem ara una equació diferencial lineal i homogènia amb coeficients a K $l(Y) = \sum_{i=0}^{n} a_i Y^{(i)}$ amb $a_n = 1$ per a un cert $n \geq 1$, i considerem l'anell de polinomis en n^2 variables $K[Y_{ij}, i \in \{0, 1, ...n-1\}, j \in \{1, 2, ..., n\}]$. Podem estendre la derivació d de K a una de $K[Y_{ij}]$ definint:
$Y'_{ij} = Y_{i+1j}$, $\forall\ i \in \{1, ..., n-2\}$
$Y'_{n-1j} = -a_{n-1}Y_{n-1j} - ... - a_1 Y_{1j} - a_0 Y_{0j}$
per a tot valor de j entre 1 i n.
Resulta clar que tenim una extensió d'anells diferencials de (K, d) construida de manera específica perquè les incògnites es comportin com solucions de $l(Y) = 0$, de manera que constitueix un bon punt de partida per a obtenir la extensió de Picard-Vessiot.
Una altra manera de construir el mateix anell i comprovar la validesa del nostre argument és considerar $K\{X_1, ..., X_n\}$ i fer el quocient per l'ideal diferencial generat pels elements de la forma $X_j^n - a_{n-1}X_j^{(n-1)} - ... - a_0 X_j$ per a tot j entre 1 i n, que és, de fet, l'ideal generat per aquests elements i les seves derivades (de manera que el terme d'ideal diferencial generat per un subconjunt es pot plantejar en termes d'ideals generats convencionals, sense haver de recórrer a nous conceptes).
Aquest anell, juntament amb les nocions referents a localització detallades a la secció anterior, ens permeten introduir la següent definició, que serà l'anell base a partir del qual obtindrem l'extensió desitjada.

[7] La nomenclatura es deu a Ernest Vessiot(1865-1952) i a Émile Picard (1856-1941), generalment considerats els precursors de la teoria relativa a aquest tipus d'extensions.

Definició 2.35. *Sigui $K[Y_{ij}]$ l'anell diferencial que acabem de construir, i sigui $W = det((Y_{ij}))$, la matriu amb coeficients Y_{ij} a la posició (i, j). Resulta clar que, amb la derivació que hem definit a $K[Y_{ij}]$, W és el wronskià de $\{Y_{01}, ..., Y_{0n}\}$, i prenent $S := \{1\} \cup \{W^n |\ n \geq 1\}$, podem definir $R := S^{-1}K[Y_{ij}]$, que és un anell diferencial amb l'única derivació de la localització que estén la definida a $K[Y_{ij}]$.*
En aquestes condicions, diem que R és l'àlgebra de solucions universal de $l(Y) = 0$

El següent pas del procés és passar al cocient per un ideal diferencial convenient, veure que el resultat és un domini d'integritat i prendre com a extensió el seu cos de fraccions.
El treball que ens queda és veure com triar aquest ideal i que, en efecte, es conserva el subcòs de les constants.
Abans, però, demostrem un resultat auxiliar d'utilitat:

Proposició 2.17. *Sigui (K, d) un cos diferencial, L una extensió de cossos diferencials de K. Llavors, sigui una constant α de L algebraica i separable sobre K, α és algebraic sobre $C := Const_K$.*

Demostració. Com α és algebraic i separable sobre K, podem considerar el seu polinomi mínim $P(X)$ de $K[X]$ i podem considerar-lo mònic. Si
$P(X) = \sum_{i=0}^{n} c_i X^i$, tindrem:
$P(\alpha) = 0 \implies (P(\alpha))' = 0 \implies \sum_{i=1}^{n} c_i' \alpha^i + c_0' + \alpha'(\sum_{i=1}^{n} i a_i X^{i-1}) = 0$
Com $\alpha' = 0$ i $c_n = 1$, deduim que
$P(\alpha) = 0 \implies \sum_{i=0}^{n-1} c_i' \alpha^i = 0$, de manera que α és arrel d'un polinomi amb coeficients a K de grau menor a n, fet que no és possible excepte si el polinomi és zero, per la tria de $P(X)$.
Així, $c_i' = 0\ \forall \in \{1, 2, ...n\}$ i α és algebraic sobre C. □

Proposició 2.18. *Sigui (K, d_1) un cos diferencial, R una extensió diferencial d'anells de K amb derivació d.*
Llavors, si I és un ideal diferencial propi de R amb la propietat de ser maximal dins el conjunt d'ideals diferencials, és un ideal primer de R.

Demostració. Primerament, passem al quocient $\frac{R}{I}$. Com tot ideal diferencial de R és també, en particular, un ideal, per la correpondència bijectiva entre els ideals de R i els ideals de $\frac{R}{I}$ que contenen I, el fet que I sigui maximal al conjunt dels ideals diferencials propis ens assegura que el cocient no tindrà cap ideal diferencial propi. Amb aquesta consideració en ment, l'objectiu és deduir que $A := \frac{R}{I}$ és un domini d'integritat. Ho veiem per reducció a l'absurd: assumim que existeixen elements a, b de A tals que $a, b \neq 0$ i $ab = 0$
Per començar, ens resulta interessant demostrar l'afirmació $d^{(k)}(a)b^{k+1} = 0$, $\forall\ n \geq 1$ natural. Emprem inducció matemàtica: del fet que $d(ab) = 0$ deduim que $d(a)b + ad(b) = 0$ per ser d derivació i, multiplicant per b, obtenim que $d(a)b^2 = 0$
Quant al pas d'inducció, si suposem que la condició és certa per a un cert k natural, podem deduir
$d(d^k(a)b^{k+1}) = 0 \implies d^{k+1}(a)b^{k+1} + d^k(a)(k+1)b^k d(b) = 0$

i, multiplicant per b, deduim que $d^{k+1}(a)b^{k+2}$ com a conseqüència de la hipòtesi inductiva, provant la propietat.
Considerem ara J l'ideal diferencial generat per a, és a dir, l'ideal generat pel conjunt de a i les seves derivades, $\{d^k(a)|\ k \geq 1\} \cup \{a\}$. Suposem que $b \notin \eta(A)$, el conjunt dels nilpotents de A. Llavors, per la propietat que acabem de demostrar, totes les derivades de a i a mateix són divisors de zero de A, de manera que tots els elements de J són divisors de zero i, en particular, $J \neq A$ (per exemple, J no pot contenir cap element diferent de 0 pertanyent a K). A més, $a \in J$ amb $a \neq 0$ per definició, de manera que tampoc és l'ideal trivial. És a dir, en aquestes condicions, J és un ideal diferencial propi de A, contradint les seves propietats definitòries. En consequència, ha de ser $b \in \eta(A)$. Ara bé, hem triat b un divisor de zero qualsevol de A, de manera que tot divisor de zero de A és nilpotent. En particular $a \in \eta(A)$.
Triem n natural mínim tal que $a^n = 0$. Aplicant propietats bàsiques de les derivacions, deduim ràpidament que $na^{n-1}d(a) = 0$ i, com $a \neq 0$ i $Car(K) = 0$, ha de ser que $d(a)$ és un divisor de zero i, per tant, també nilpotent.
Recuperant J l'ideal diferencial anterior, aquesta propietat implica que $J \subset \eta(A)$, de manera que no pot ser A (cap element de K diferent de 0 és nilpotent) i, un cop més, podem deduir que tampoc és l'ideal nul del fet que contingui a a. Així, també en aquest context tindriem que J és un ideal diferencial propi de A, contradint les seves propietats.
Com aquesta disjunció de casos contradictoris sorgeix naturalment d'assumir que existeixen elements de A a i b com els triats anteriorment, aquest succés no és possible.
Per tant, A és un domini d'integritat i I és un ideal primer de R. □

Demostrem ara el resultat principal de la secció, la proposició que ens permet construir una extensió de cossos diferencials de (K, d) amb les seves mateixes constants. És aquí on fem valer tota la secció de nocions preliminars:

Proposició 2.19. *Sigui K un cos diferencial, C el seu subcòs de constants, amb la propietat de ser algebraicament tancat.*
Considerem R una extensió d'anells diferencials de K tal que, a més, és una K-àlgebra finitament generada i un domini d'integritat.
Denotem per L el seu cos de fraccions. Llavors, si a més suposem que R no té ideals diferencials propis, $Const_L = C$.

Demostració. Primer observem que cap element de $Const_L \setminus C$ pot ser algebraic sobre K ja que, per la proposició 2.17, seria algebraic sobre C i, com és algebraicament tancat, pertanyeria a C.
A més, $Const_L \subset R$. En efecte, sigui $b \in Const_L$, tindrem $b = \frac{f}{g}$ per a uns certs f, g de R. Considerem ara el conjunt de denominadors de b, $J := \{h \in R|\ hb \in R\}$ i observem que J és un ideal, fet que és fàcilment demostrable.
Sigui D la derivació de R, el fet que $h \in J$ implica $hb \in R$ i, per tant, $D(hb) = h'b + hb' = h'b$ (b constant) pertany a R, de manera que $h' \in J$ i J és un ideal diferencial. Ara bé, J no pot ser l'ideal trivial, ja que g hi pertany i

$g \neq 0$ per ser denominador d'una fracció de L. Com R no pot tenir ideals diferencials propis per hipòtesi, ha de ser $J = R$ i es segueix directament que $1b = b \in R$.
Finalment, demostrem que, per a tot b de $Const_L$, existeix un element c de C tal que $b - c$ no és una unitat de R. Llavors, $(b - c)R$ serà un ideal diferencial diferent del total de R i, per tant, serà $\{0\}$, d'on es desprèn que $b = c$.
Introduim algunes simplificacions gràcies als resultats previs: considerem $\overline{K}$ la clausura algebraica de K, $\overline{R} := R \otimes \overline{K}$, on el producte tensorial es pren sobre ambdós conjunts en tant que K-àlgebres. Per les propietats que hem vist del producte tensorial, si $b \otimes 1 - c \otimes 1 = (b - c) \otimes 1$ no és una unitat, $b - c$ tampoc ho serà a R (per la Obs.20). A més, el conjunt de generadors de $\overline{R}$ $A := \{r \otimes 1 | r \in R\}$ isomorf a R (i, per tant, domini d'integritat i finitament generat) és una $\overline{K}$-àlgebra amb el producte per escalars definit per $k(r \otimes 1) = r \otimes k$ per a tot $k \in \overline{K}$. No només això, sinó que també podem considerar a $\overline{R}$ com anell diferencial tal que $K \subset \overline{R}$ (en sentit algebraic) amb la derivació definida a 2.10.
És a dir, a efectes del què volem demostrar, podem canviar R per $\overline{R}$ i considerar que estem treballant amb una K-àlgebra finitament generada sobre un cos K algebraicament tancat.
Assumir que treballem sobre un cos algebraicament tancat ens permet introduir la potència dels resultats de la geometria algebraica, de manera que, pel teorema 2.15, existeix una varietat afí V de K^n tal que R és isomorf al seu anell de coordenades. Per tant, podem interpretar b com una funció d'avaluació polinòmica f amb domini V.
Ara, pel lema 2.2 (Chevalley), $f(V)$ serà constructible, en tant que tot conjunt tancat és localment tancat i, com $f(V) \subset K$, serà finit o complement d'un finit per la proposició 2.16. Al segon cas, per ser C infinit (conseqüència del fet que 1 és constant i $Car(K) = 0$), existirà algun $v \in V$ tal que $f(v) = c$ per a c constant, de manera que $f - c$ s'anul·la a c i, pel Nullstellensatz, $b - c$ pertany a l'ideal maximal definit per v. En particular, per pertànyer a un ideal propi, $b - c$ no és una unitat.
Al primer cas, com $f(V)$ finit i R domini d'integritat, $\mathbb{I}(V)$ primer i, com hem vist, V irreductible i, en conseqüència ha de ser un sol punt (Els punts són conjunts tancats amb la topologia de Zariski, de manera que un conjunt finit amb més d'un no serà mai irreductible), de manera que f constant i b haurà de pertànyer a K, essent llavors $b \in C$ directament.
Això completa la demostració. □

Corol.lari 2.4. *Sigui R l'àlgebra de solucions universal de $l(Y) = 0$ una equació diferencial lineal i homogènia amb coeficients a K, P un ideal diferencial maximal de R, llavors $L := Q(\frac{R}{P})$ és una extensió de Picard-Vessiot de (K, d)*

Demostració. Resulta evident que, per construcció, L és un cos amb un subcòs isomorf a K i amb una derivació obtinguda a través de processos ben coneguts (estendre la derivació de K a una de R, prendre la derivació al quocient per P

i estendre-la únicament a L). A més, per la proposició anterior, $Const_L = C$. Quant a les solucions de l'equació, R les conté per construcció, i la localització per les potències del wronskià assegura que no pugui pertànyer a P per ser invertible, de manera que conservem el conjunt de solucions fonamental en passar a classes mòdul P, arribant així a ser elements de L que satisfan la igualtat desitjada.
Per tant L satisfà totes les condicions i és una extensió de Picard-Vessiot de (K, d). □

2.3.3 Unicitat

Demostrada l'existència de l'extensió de Picard-Vessiot associada a una certa equació, només queda demostrar-ne la unicitat com a estructura, provar que tota parella d'estrcutures satisfent les propietats d'una extensió de Picard-Vessiot d'un cos diferencial K associada a una equació $l(Y) = 0$ són isomorfes en sentit diferencial.
Abans d'abordar el resultat principal, però, en demostrem un d'auxiliar:

Proposició 2.20. *Siguin L_1, L_2 extensions de Picard-Vessiot d'un cos diferencial (K, d) assocaides a una equació $l(Y) = 0$ d'ordre n, i L una extensió de cossos diferencials de K tal que $Const_K = Const_L$.*
Llavors, siguin $\sigma_1 : L_1 \longmapsto L$ i $\sigma_2 : L_2 \longmapsto L$ K-morfismes diferencials (morfismes diferencials tals que la seva restricció a K és la identitat), $\sigma_1(L_1) = \sigma_2(L_2)$

Demostració. Siguin $V_i := \{y \in L_i |\ l(y) = 0\}$ per a i 1 i 2, $V := \{y \in L |\ l(y) = 0\}$. Com hem vist a les seccions prèvies, tant V com els dos V_i són $Const_K$-espais vectorials, els segons de dimensió exactament n (l'ordre de l'equació) i el primer de dimensió com a molt n.
Com $Const_L = Const_K$ i els σ_i són, en particular morfismes de cossos, són injectius i envien els tres conjunts a espais vectorials sobre el subcòs de constants de L de la mateixa dimensió que les seves antimatges. Llavors, com $\sigma_i(V_i) \subset V$ i es conserven les dimensions, ha de ser $dim(V) = n$ i $\sigma_1(V_1) = V = \sigma(V_2)$. Del fet que els L_i són generats com a K-espais vectorials pels V_i corresponents i que les σ_i són K-morfismes, obtenim la igualtat desitjada. □

Proposició 2.21. *Sigui (K, d) un cos diferencial, C el seu subcòs de funcions, que suposem algebraicament tancat. Sigui $l(Y) = 0$ una equació diferencial lineal i homogènia d'ordre n amb coeficients a K. Si L_1, L_2 són dues extensions de Picard-Vessiot de K associades a $l(Y) = 0$, existeix un K-isomorfisme diferencial entre L_1 i L_2.*

Demostració. Prenem L_1 l'extensió de Picard-Vessiot que hem construit a la secció d'existència. L'estratègia a seguir per a dur a terme la demostració és la següent: cosntruirem E una extensió de cossos diferencials de K tal que $Const_E = C$ i trobarem K-morfismes diferencials entre els L_i $i \in \{1, 2\}$ que ens permetin aplicar la proposició 2.20.

Considerem ara l'anell $A := (\frac{R}{P}) \otimes L_2$, on R és l'àlgebra de solucions universal de $l(Y) = 0$ i P un ideal diferencial maximal de R. Prenem el producte tensorial en tant que K-àlgebres. Clarament, pel teorema 2.10, A és un anell diferencial equipat amb la derivació usual del producte tensorial. A més, el podem interpretar com una L_2-àlgebra finitament generada amb el producte escalar definit com al teorema anterior d'existència, enviant $l(r \otimes k)$ a $r \otimes lk$ per a tot tensor pur de A i considerant que $\frac{R}{P}$ és finitament generada com a K-àlgebra.
Sigui Q un ideal diferencial propi i maximal de A, i sigui la funció $\frac{R}{P} \longmapsto A$ que envia a a $a \otimes 1$ per a tot a de $\frac{R}{P}$. Considerem l'antimatge de Q per a aquesta funció: ha de ser igual a $\{0\}$, ja que $\frac{R}{P}$ no té ideals diferencials propis i no podria ser tot l'anell, o $Q = A$.
Per tant, prenent el cocient per Q i composant la funció descrita amb el morfisme de pas al quocient, obtenim un K-morfisme diferencial injectiu de $\frac{R}{P}$ a $\frac{A}{Q}$.
De manera similar, podem obtenir un K-morfisme diferencial injectiu de L_2 a $\frac{A}{Q}$, composant amb el morfisme de pas al quocient el K-morfisme injectiu que envia tot element l de L_2 a $1 \otimes l$.
Per la proposició 2.18, Q és un ideal primer i $\frac{A}{Q}$ és un domini d'integritat; podem considerar E el seu cos de fraccions. Com, a més, E satisfà les hipòtesis de la proposició 2.19, $C = Const_{L_2} = Const_E$
Finalment, podem estendre els K-morfismes diferencials de L_1 i $\frac{R}{P}$ a $\frac{A}{Q}$ definits anteriorment a K-morfismes diferencials entre L_1, $\frac{R}{P}$ i E, composant-los amb l'inclusió natural d'un anell al seu cos de fraccions.
Ara, aplicant la proposició 2.20, obtenim que les imatges de L_1 i L_2 pels K-morfismes definits són iguals, i, per tant, diferencialment isomorfes. Però, per ser els morfismes injectius, aquestes imatges són isomorfes a les seves antiimatges, de manera que $L_1 \cong L_2$ com a cossos diferencials. □

3 El teorema de Liouville

3.1 El cos de les funcions meromorfes

Al capítol anterior hem desenvolupat els fonaments de l'àlgebra diferencial, des de la definició d'un cos diferencial a com extendre'ls, tractant les dues maneres més senzilles de fer-ho: considerant extensions de cossos algebraiques o, si el subcòs de les constants és algebraicament tancat, considerant l'extensió de Picard-Vessiot associada a alguna equació diferencial lineal i homogènia.
L'objectiu, ara, és capturar algebraicament la pregunta bàsica del treball, en principi plantejada en termes purament analítics, i respondre-la demostrant el Teorema de Liouville, més concretament, la versió abstracta sobre cossos diferencials de la generalització demostrada per Ostrovsky (1946) del teorema clàssic de Liouville (1835).
Per començar, adrecem la qüestió d'expressar una funció en *termes simples*, o en forma tancada.
Sigui una funció de variable real o complexa definida en una *regió* (un conjunt connex, obert i no buit, en la topologia corresponent), intuitivament parlant, considerem que una funció és *elemental*, o expressable en *forma tancada* si és una funció en una variable que es pot construir combinant consecutivament un nombre finit d'operacions algebraiques, composicions per exponencials, composicions per logaritmes (que sempre assumirem que són en base e) i composicions per funcions trigonomètriques o funcions trigomètriques inverses, en definitiva, una funció que, col·loquialment, considerariem que té una forma simple; raonable.
El primer problema són les funcions trigonomètriques i les seves inverses, ja que és fàcil caracteritzar un logaritme (o una determinació del seu logaritme en el cas complex) d'una funció determinada definida en una certa regió en termes de les seves propietats diferencials (de fet, podem definir els logaritmes i exponencials d'un element d'un cos diferencial en termes de la seva derivació), però la tasca resulta molt més complicada en el cas d'aqueste funcions, de manera que ens resulta estratègicament interessant poder expressar-les algebraicament en funció de la resta d'operacions permeses, combinacions finites d'operacions algebraiques, composicions per logaritmes i composicions per exponencials.
Aquest interès motiva l'ús de *funcions a valors complexos*.
És a dir, permetre que les funcions amb les quals treballem, encara que tinguin domini real, puguin tenir recorregut potencialment complex.
Pel cas general on parlem de funcions a variable complexa és clar que el problema és inexistent. L'avantatge més immediat que obtenim considerant aquesta definició ampliada de funció de variable real és, efectivament, evitar el problema de les funcions trigonomètriques i les seves inverses, ja que, per exemple, de les fòrmules de *De Moivre* obtenim expressions com a funcions a valors complexos de les funcions trigonomètriques bàsiques en funció de l'exponencial:

$sin(x) = \frac{e^{ix}-e^{-ix}}{2i}$; $cos(x) = \frac{e^{ix}+e^{-ix}}{2}$; $tan(x) = \frac{e^{ix}-e^{-ix}}{i(e^{ix}+e^{-ix})}$
i, pel cas de les funcions trigonomètriques inverses, tindrem:
$arcsin(x) = -i\sqrt{ln(1-x^2+ix)}$; $arccos(x) = -i\sqrt{ln(1-x^2+x)}$;
$arctan(x) = -\frac{i}{2}ln(\frac{i-x}{i+x})$;
pels seus valors principals, on $ln(z)$ és la determinació principal del logaritme complex. Tenim, llavors, una noció més o menys sòlida de què entenem com a funció principal, però ens falta traduir-la a un context algebraic particular; hem d'aconseguir una estructura de cos diferencial amb les funcions amb les quals volem treballar.
La part de definir una derivació és senzilla: si considerem les funcions de variable complexa, tenim la derivada usual sorgida del concepte del límit del quocient incremental i ens interessa els conjunt de les funcions holomorfes en una regió complexa Ω determinada.
Quant al cas de les funcions a valors complexos f, podem considerar la igualtat $f = u + iv$ amb u, v funcions de variable real, i assignar-li la derivació $f' = u' + iv'$ on derivem u, v en el sentit real usual, i llavors ens interessa la classe de les funcions diferenciables dins el conjunt de les funcions a valors complexos. Per a obtenir l'estructura de cos, ens centrem en el cas de variable complexa de les funcions meromorfes en una regió Ω, i pensarem les funcions del cas real, generalment, com restriccions d'aquestes funcions complexes a regions reals on siguin diferenciables:

Definició 3.1. *Sigui Ω una regió complexa, diem que una funció f és meromorfa si és holomorfa a Ω exceptuant un conjunt finit de punts, que seran pols de la funció (recordem que un pol d'una funció de variable complexa és un punt z_0 tal que $\lim_{z \longmapsto z_0} |f(z)| = \infty$). El conjunt de funcions meromorfes d'una regió Ω es denota per $M(\Omega)$.*

Obs. 21. $H(\Omega) \subset M(\Omega)$

Proposició 3.1. *$M(\Omega)$ és un cos.*

Demostració. Siguin f, g elements de $M(\Omega)$, al conjunt resultant de restar a Ω la unió dels conjunts dels seus pols, $f + g$ serà holomorfa. A més, sigui z_0 un pol de f i no de g o viceversa, serà un pol de $f + g$, ja que $||f(z)| - |g(z)|| \leq |f(z) + g(z)| \ \forall \ z \in \mathbb{C}$ i, passant al límit quan z tendeix a z_0, obtenim que z_0 és un pol de $f + g$. Si fos un pol compartit per f i g, podria ser que no ho fos de la suma, però, en tot cas, els pols de $f + g$ són subconjunt de la unió dels pols de f i g i, per tant, un conjunt finit.
Quant a fg, els seus pols són exactament la unió dels pols de f i g, ja que $|f(z)g(z)| = |f(z)||g(z)|$ per a tot nombre complex i, passant al límit quan z tendeix a algun pol de f o g, tindrem que és sempre un pol de fg.
Finalment, si f és una funció meromorfa diferent de zero, la seva inversa multiplicativa serà una funció holomorfa excepte a la unió dels pols de f (on tindrà singularitats puntuals) i als zeros de f, on tindrà pols. Com és conegut que una funció holomorfa en una regió Ω tindrà un conjunt finit de zeros aïllats, $\frac{1}{f}$ tindrà un nombre finit de pols i serà, per tant, una funció meromorfa. □

Corol.lari 3.1. $Q(H(\Omega)) \subset M(\Omega)$

Resulta clar, llavors, que el cos de les funcions racionals $\mathbb{C}(z)$ està contingut a $M(\Omega)$ per a tota regió, de manera que serà l'elecció natural de cos diferencial (amb la derivada usual $\frac{d}{dz}$) a partir del qual considerar extensions amb propietats convenients.
Per començar, podem capturar la noció de ser una funció *elemental* en termes d'extensions de cossos:

Definició 3.2. *Sigui $\mathbb{C}(z) = C \subset L$ una extensió de cossos. Direm que L és una extensió elemental si $L := C(f_1, ..., f_n)$ per a $n \geq 1$ i, emprant la notació $C(f_1, ..., f_i) = C_i$ per a tot i entre 1 i n, es satisfà $C_{j+1} = C_j(f_{j+1})$ amb f_{j+1} algebraic sobre C_j, $f_{j+1} = ln(f)$ amb $f \in C_j$ i $ln(z)$ determinació del logaritme o $f_{j+1} = e^g$ per a algun $g \in C_j$, j entre 0 i $n-1$, $C_0 := C$.*

Evidentment, f és una funció elemental si pertany a alguna extensió elemental de $\mathbb{C}(z)$. Aquesta manera de tornar la nostra qüestió principal en una essencialment algebraica té els seus inconvenients per a tractar amb funcions, però, ja que prendre logaritmes, exponencials o elements algebraics de cossos de funcions pot obligar-nos a modificar la seva regió de definició, sigui de manera mínima (sigui f holomorfa a Ω, $ln(f)$ només ho serà allà on f no s'anul·li, per exemple, malgrat continuarà sent meromorfa) o profunda, per exemple si f és un element algebraic sobre un cos de funcions, és a dir, si és la solució d'una equació polinòmica amb coeficients que són funcions meromorfes. El teorema de la funció implícita assegura l'existència d'una regió on f està definida i és holomorfa, però f podria no ser meromorfa com a funció de la regió Ω inicial. Per tant, tota funció que obtinguem com a element d'una extensió elemental d'una altra s'ha de considerar com a funció amb certa precaució, estudiant quan sigui possible com canvia el seu domini.
A canvi, però, hem guanyat un marc teòric algebraic on considerar el nostre problema i, a més, un d'equipat amb una derivació tal que el subcòs de les constants, $\mathbb{C}$, és algebraicament tancat, de manera que el podrem veure com un cas particular d'una teoria general d'extensions de cossos diferencials elementals.

3.2 Extensions elementals

Establertes les bases per a transformar la nostra pregunta sobre funcions en una sobre extensions de cossos, anem a generalitzar-la a una qüestió general i teòrica relativa a extensions de cossos diferencials.
Comencem definint alguns termes:

Definició 3.3. *Sigui F un cos diferencial, $a, b \in F$. Diem que b és un logaritme de a si $b' = \frac{a'}{a}$*

Definició 3.4. *Sigui F un cos diferencial, $a, b \in F$. Diem que a és una exponencial de b si $a' = ba$*

Obs. 22. *Noti's que a és exponencial de b si b és logaritme de a, i viceversa.*

Resulta també clar que aquestes nocions generalitzen naturalment les nocions comuns d'exponencial i logaritme com a funcions, en un sentit purament diferencial.
Això ens permet introduir la noció d'extensió de cossos diferencials elemental:

Definició 3.5. *Sigui (K, d) un cos diferencial, $K \subset L$ una extensió de cossos diferencials. Llavors, diem que L és una extensió elemental de (K, d) si $L := K(f_1, ..., f_n)$ per a algun $n \geq 1$ com a extensió de cossos amb una derivació D, i, si denotem $K(f_1, ..., f_i) := K_i$ per a tot i entre 1 i n, satisfà: $K_{j+1} := K_j(f_{j+1})$ $(1 \leq j \leq n-1)$ amb f_{j+1} algebraic sobre K_j o bé f_{j+1} exponencial o logaritme d'un element $b \in K_j$ amb la derivació obtinguda de restringir D a K_j.*

Si, a més, considerem el cas particular $C := Const_K$ algebraicament tancat, obtenim una propietat important i profunda, resultat directe de la teoria que hem demostrat prèviament.

Proposició 3.2. *Sigui (K, d) un cos diferencial amb subcòs de constants C algebraicament tancat, $K \subset L$ amb $L = K(f_1, ..., f_n)$ $(n \geq 1)$ extensió de cossos diferencials elemental.*
Llavors, la derivació de D de L queda determinada per d i, a més, és minimal, en el sentit que $Const_L = C$

Demostració. L'estratègia és simple: veiem que cadascun dels tipus d'extensions simples que componen una extensió elemental satisfan les propietats que requerim: volem demostrar que, sigui F un cos diferencial amb $C' = Const_F$, $F(t)$ elemental és una extensió de cossos diferencials única (en sentit algebraic) i conserva el subcòs de constants de F. Si f és algebraic sobre F, podrem estendre de manera única la derivació de F a $F(f)$ per la proposició 2.5 i, per la proposició 2.17, com tota constant de $F(t)$ seria algebraica sobre F, ho seria també sobre C' i, com és algebraicament tancat, seria un element de C'.
Quant al segon cas, si f és una exponencial transcendental d'un cert element $a \in F$, llavors $F[f] \cong F[X]$ i $F(f) \cong Q(F[f])$ com a anells, de manera que, com a més tenim determinada f' pel fet que sigui una exponencial d'un element de F, la derivació de $F[t]$ queda totalment determinada, i com la extensió al cos de fraccions és única pel teorema 2.3, la derivació obtinguda en aquest tipus d'extensió també ho és. Quant al subcòs de les constants, $F(t)$ és el mínim cos que extensió de F que conté t, de manera que, si considerem L l'extensió de Picard-Vessiot associada a $Y' - aY = 0$ que conté a t, haurà de contenir a $F(t)$, i en particular $Const_{F(t)} \subset Const_L = C$, de manera que és el mateix que el de F. En particular, $F(t)$ en aquestes condicions satisfà les propietats d'una extensió de Picard-Vessiot associada a l'equació esmentada, de manera que $L = F(t)$
L'últim cas, quan f és logaritme d'un cert element b de F, és més complex. Primerament, descartem els casos trivials: com f logaritme de b de F,

$f' = \frac{b'}{b} = \eta \in F$ i, si hi ha algun altre element $g \in F$ logaritme de b, llavors no caldria estendre F per a incloure-hi un logaritme de b, de manera que podem suposar que, si estem considerant una extensió d'aquest tipus i no és la trivial, no hi ha cap element de F amb derivada η. A més, si f no és un logaritme trivial, és transcendent sobre K, ja que, en cas contrari, tindrem un polinomi mínim de $K[X]$ amb arrel f, anomenem-lo $P(X)$, que podem escollir mònic. Llavors, si $P(X) := \sum_{i=0}^{n} m_i X^i$, $0 = (P(f))'$ i, com $m_n = 1$, tindrem un polinomi de grau $n-1$ que anul·la f i, per la tria de $P(X)$, ha de ser el polinomi zero. En particular, observant el coeficient $n-1$-èsim d'aquest polinomi derivat de $P(X)$, tenim que $m'_{n-1} + nm_n f' = 0$ i
$f' = \frac{-m'_{n-1}}{n} = (\frac{-m'_{n-1}}{n})'$, negant que sigui un logaritme de no trivial d'un element de K.
Amb això en ment, repetim l'argument del cas anterior: si f és un element transcendent, f només s'anul·la a $0 \in F[X]$ i, per tant, $F[f] \cong F[X]$ com a anell. Per la Obs.7, podem estendre una derivació de F a una de $F(f)$ sempre i quan definim f', però, en aquest cas, f' queda determinada per ser f logaritme de b, de manera que l'extensió és única. A més, com $F[f]$ és un domini d'integritat per ser F cos, $F(f) = Q(F[f])$ i la derivació de $F[t]$ estén únicament a una de $F(f)$ per la proposició 2.3. Queda per veure que, en aquest cas, l'extensió no afegeix constants.
Comencem veient que $C' = Const_{F[f]}$. Sigui $c = \sum_{i=0}^{n} c_i f^i$ una constant de grau n ($c_n \neq 0$), llavors $0 = c' = \sum_{i=0}^{n} c'_i f^i + f'(\sum_{j=1}^{n-1} ((j+1)c_{j+1} f^j)$
com $f' \in F$ i f és transcendent, el polinomi en funció de f ha de ser zero, de manera que, en particular, $c'_{n-1} = f' n c_n$, i llavors
$f' = \frac{-c'_{n-1}}{nc_n} = \frac{-c'_{n-1} nc_n + nc_{n-1} c'_n}{nc_n^2} = (\frac{-c_{n-1}}{c_n})'$ per ser $c'_n = 0$ com a coeficient líder del polinomi en funció de f descrit prèviament, de manera que ja hi hauria un element de F logaritme de b, causant una contradicció.
Finalment, per a veure que $Const_{F(f)} = C'$, considerem $c = \frac{h}{g}$ amb h, g polinomis en funció de f coprimers, $g \neq 0$ i el triem mònic. La demostració és molt semblant a la de l'exemple de la pàgina 15, on es construeix una extensió de Picard-Vessiot per una equació en particular. Repetim el raonament:
$0 = c' = \frac{h'g - hg'}{g^2} \iff h'g = hg'$
Com h, g coprimers i $F[f]$ D.F.U, si g no és un element de F (que ens reduiria al cas anterior), és producte de potències de primers de $F[f]$. Per la igualtat que acabem de veure, un primer que divideixi a g dividirà a g', perquè no podrà dividir a f per coprimalitat. Iterar aquest raonament amb tots els factors primers que divideixen a g ens porta a deduir $g | g'$, però, com $f' \in F$ i g mònic, $Deg(g') < Deg(g)$, de manera que arribem a una contradicció i ha de ser $g = 1$ (escollit mònic, però no el poden dividir factors primers), essent llavors que $Const_{F(t)} \subset Const_{F[t]} = C'$.
Aplicar aquest raonament a cadascun dels passos $K_{j+1} = K_j[f_{j+1}]$ per a tot j entre 0 i $n-1$, amb $K_0 := K$ completa la demostració. □

Per a poder aplicar la proposició 3.2 i entendre bé les extensions principals de $\mathbb{C}(z)$, ens queda demostrar que les extensions de cossos elementals són

extensions de cossos diferencials en aquest cas, hem de veure que són conjunts tancats per $\frac{d}{dz}$

Proposició 3.3. *Sigui $L := C(f_1, ..., f_n)$ en la notació anterior una extensió elemental, amb $n \geq 1$. Llavors, L és tancat per $\frac{d}{dz}$, la derivada de tot element de L pertany a L.*

Demostració. Ho veiem per inducció. Quant al cas inicial, si considerem $\mathbb{C}(z) = C_0$, és clar que el cos de les funcions racionals en una variable complexa és tancat per $\frac{d}{dz}$.
Demostrem el pas d'inducció: suposem que la porpietat es satisfà per a $n-1$ i la veiem per a n. Denotem $C(f_1, ..., f_{n-1}) := C$, de manera que $C(f_1, ..., f_n) = C(f_n)$ amb $f_n := f$ algebraic sobre C, logaritme o exponencial d'un element de C.
Simplifiquem primer lleugerament la demostració veient que és suficient amb veure que $f' \in C(f)$.
En efecte, sigui $x \in C[f]$, $x = \sum_{i=0}^{n} a_i f^i$ per a algun n natural, $x' = \sum_{i=0}^{n} a_i' f^i + f'(\sum_{j=1}^{n-1} j a_j f^j)$, de manera que, si $f' \in C(f)$, llavors $x' \in C(f)$. Com $C(f)$ és el cos de fraccions de $C[f]$, aplicant la regla del quocient veiem automàticament que $f' \in C(f) \implies (\frac{h}{g})' \in C(f)$ per a tot $\frac{h}{g}$ de $C(f)$.
Per tant, només ens queda veure que $f' \in C(f)$ per als tres tipus d'element que pot ser f. Si f és exponencial d'un element a de C, llavors $f' = af$ i, evidentment, $f' \in C(f)$ perquè a i f hi pertanyen. Si f és logaritme de b de C, llavors $f' = \frac{b'}{b}$ i $f' \in C(t)$ perquè, per hipòtesi, C és tancat per $\frac{d}{dz}$.
Finalment, sigui f algebraic sobre C, llavors serà separable sobre C perquè $Car(C) = 0$ per ser extensió de cossos dels complexos i podem considerar $P(X)$ el polinomi mínim de f.
El raonament és anàleg a l'emprat al cas finit de la proposició 2.5, de manera que, reciclant la mateixa notació pel polinomi derivat $DP(X)$ i el polinomi amb coeficients les derivades dels coeficients de $P(X)$, $P^d(X)$, tindrem que $f' = \frac{-P^d(f)}{DP(f)}$, que té sentit perquè $DP(f) \neq 0$ per ser $P(X)$ polinomi mínim de f, i es segueix de manera immediata que $f' \in C(f)$. □

Així, hem demostrat que podem aplicar la teoria d'extensions diferencials elementals al cas particular dels cossos de funcions meromorfes en una regió, amb les precaucions ja descrites.
Estem, per fi, en situació de formular de manera unívoca la nostra pregunta inicial, i demostrar-la introduint el teorema de Liouville. Introduim la noció d'integral d'un element i d'extensió simple integral.

Definició 3.6. *Sigui $f \in K$, K un cos diferencial, i $K(g)$ una extensió simple de cossos diferencials.*
Llavors, diem que g és una integral de f, o una antiderivada de f, si $g' = f$.

Definició 3.7. *Si $K(g)$ extensió de cossos diferencials de (K, d) amb g integral d'un element $f \in K$, diem que l'extensió és integral.*

Es segueix d'aquesta definició i tot el treball previ que hem fet per definir les extensions elementals que, la nostra pregunta original, en termes algebraics, és formulable com: sigui f un element de (K, d) un cos diferencial, i sigui g una integral de f en alguna extensió de K. És sempre $K(g)$ una extensió de cossos diferencials elemental? En cas negatiu, quines propietats ha de satisfer f per tal que així sigui? Com és d'esperar, la resposta és, en general, negativa i, de fet, perquè aquesta propietat es satisfaci, f ha de satisfer condicions bastant restrictives sobre la seva forma, s'ha de poder expressar d'una manera específica.
Ens disposem, llavors, a enunciar formalment el teorema que dóna resposta a aquesta pregunta i a demostrar-lo. Abans, però, provem un lema important:

Proposició 3.4. *Sigui F un cos diferencial, $F(t)$ una extensió diferencial de cossos simple amb $Const_{F(t)} = Const_F$ tal que t és transcendental respecte F i, a més, es té que t és integral d'un element b de F o $\frac{t'}{t} \in F$ (t és una exponencial d'un element de F).*
Llavors, si t és integral d'un element de F, qualsevol polinomi p de $F[t]$ és tal que la seva derivada p' té el mateix grau que p o exactament el grau de p menys u, depenent de si el seu coeficient líder (aquell que acompanya el terme de grau màxim) és o no una constant de F.
En el segon cas, si t és una exponencial d'un element de F, llavors, per a tot $a \neq 0$ de F i tot $n \geq 1$ natural, tindrem $(at^n)' = ht^n$ per a algun h no nul de F. Encara més, per a tot p no nul de $F[t]$, $Deg(p') = Deg(p)$ i p és múltiple de p' (el seu quocient és de F) si, i només si, són monomis.

Demostració. Considerem primer el cas $t' = b$ amb b de F.
Sigui $p \in F[t]$, $p = \sum_{i=0}^{n} a_i t^i$ per a algun $n \geq 1$ derivant, tenint en compte que $t' = b$, obtenim que $p' = a_n' t^n + b\sum_{i=1}^{n-1}(a_i' + (i+1)a_{i+1})t^i + a_0'$, que, per descomptat, pertany a $F[t]$ i té grau n si a_n no és una constant. Si $a_n' = 0$ i p' no té grau $n-1$, llavors $a_{n-1}' + na_n b = 0$ i, com na_n serà una constant, $0 = a_{n-1}' + na_n b = (a_{n-1} + na_n t)'$, de manera que $a_{n-1} + na_n t$ és una constant i, per hipòtesi, pertany a F, així que, manipulant algebraicament l'expressió, deduim immediatament que ha de ser $t \in F$, contradient la hipòtesi que diu que és transcendent sobre F. Per tant, $Deg(p') = n-1$
Quant al segon cas, sigui $b = \frac{t'}{t} \in F$, i considerem a de F no nul, a més d'un enter n igual o més gran que 1.
Tenim $(at^n)' = a't^n + ant't^{n-1} = (a' + anb)t^n$, i $a' + anb$ no pot ser zero, o $at^n \in F$ i $t^n \in F$, de manera que $t \in \overline{F}$, contradient la hipòtesi.
Sigui de nou p de $F[t]$, amb la mateixa notació que abans. Com $a_n \neq 0$, $(a_n t^n)' = ht^n$ amb $h \in F$ no nul, de manera que $Deg(p) = Deg(p')$. Acabem de veure que un monomi és múltiple de la seva derivada en aquest cas, de manera que només falta veure el recíproc. Sigui p un element de $F[t]$ tal que $p = kp'$ amb $k \in F$ no nul.
Suposem que no són monomis, i considerem $a_n t^n$ monomi de p i $ka_m t^m$ monomi de p', amb $n > m$, que sempre és possible si no són monomis. Com la derivada de p serà múltiple de p amb quocient a F, tindrem la igualtat pels

seus coeficients:
$\frac{a'_n+na_nb}{a_n} = \frac{a'_m+ma_mb}{a_m} \iff \frac{a'_n}{a_n} + n\frac{t'}{t} = \frac{a'_m}{a_m} + m\frac{t'}{t}$
i, per tant $(\frac{a_nt^n}{a_mt^m})' = \frac{\frac{a'_n+na_nb}{a_n}a_na_mt^{n+m} - \frac{a'_m+ma_mb}{a_m}a_ma_nt^{n+m}}{a_m^2t^{2m}} = 0$
i, llavors, el quocient de monomis pertany a F per hipòtesi, i t ha de ser algebraic sobre F, generant una contradicció.
Com aquesta contradicció ha sorgit de suposar que p no és un monomi, hem demostrat allò que voliem veure. □

Proposició 3.5. *(Teorema de Liouville)*
Sigui (K, d) un cos diferencial, f de K i sigui $K(g)$ una extensió de cossos diferencials tal que $g' = f$.
Llavors, $K(g)$ és una extensió elemental tal que $Const_{K(g)} = Const_K = C$ [8] *(i, per tant, totes les subextensions tenen subcòs de constants C) si, i només si, existeixen conjunts $\{g_i\}_{1\leq i\leq n} \subset K$ (diferents de zero), $\{\alpha_i\}_{1\leq i\leq n} \subset Const_{K(g)} = C$ ($n \geq 1$) i un element $h \in K$ tals que:*
$f = \sum_{i=1}^n \alpha_i \frac{g'_i}{g_i} + h'$

Demostració. Resulta evident que una de les direccions de la implicació és molt més simple de demostrar que l'altra, concretament, si existeix per f una expressió com l'enunciada, resulta clar que un element $g = \sum_{i=1}^n \alpha_i b_i + h$ amb b_i logaritme de g_i per a tot i és una integral de f i, clarament, g és element d'una extensió elemental que afegeix un nombre finit de logaritmes d'elements de K que no siguin trivials (l'extensió podria ser potencialment K). Com hem vist demostrant la proposició 3.2, una extensió que afegeixi un logaritme no trivial, és transcendent i conserva el subcòs de les constants, de manera que obtenim la propietat desitjada.
Quant al recíproc, el veiem per inducció, suposant $K(g) = K(f_1, ..., f_N)$, prenent la notació $K_i := K(f_1, ..., f_i)$ per a tot i entre 1 i N. Amb el conveni $K_0 = K$, resulta clar que el cas $n = 0$ és trivial, si f té una integral a K, té la forma general desitjada.
Passem a demostrar el pas d'inducció, suposant que el teorema es satisfà per a tot element que pertany a una extensió elemental del cos diferencial al qual pertany que s'aconsegueixi afegint $N - 1$ elements.
Aplicant aquesta hipòtesi veient f com a element de K_1 i considerant l'extensió $K_1 \subset K_N$ de $N - 1$ elements, tenim que, en efecte,
$f = \sum_{i=1}^n \alpha_i \frac{g'_i}{g_i} + h'$, amb els elements α_i constants de K i algun $n \geq 1$, però els g_i i h a $K_1 = K(f_1)$. D'ara endavant, simplifiquem la notació prenent $f_1 = t$ i, considerant les de t en cadascun dels tres casos possibles, busquem una expressió amb els termes que la defineixen a K.
Comencem pel cas f algebraic sobre K: en els termes que hem vist abans, existeixen $U_i[X]$, $H[X]$ polinomis de $K[X]$ tals que $U_i[t] = u_i$, $H'[t] = h'$ per a tot i entre 1 i N. Considerem ara $\{\tau_1 = t, ..., \tau_s\}$ les arrels del polinomi mínim

[8] Gràcies al teorema 3.2 no és necessari veure aquesta condició com una necessitat purament tècnica, sinó més bé com una relaxació de la condició que C sigui algebraicament tancat, ja que, en aquest cas, sabem que tota extensió elemental conserva les constants.

de t sobre K a alguna clausura algebraica de $F(t)$ (en el cas que parlem de funcions, les τ_k estaran definides en alguna subregió convenient de la regió original pel teorema de la funció implícita, de manera que hi haurà prou amb canviar la regió on considerem les funcions per a continuar la demostració), llavors, per la proposició 2.5, la derivació de $F(t)$ estén únicament a una derivació d'aquesta clausura algebraica, i, a més, es satisfarà la propietat: $\sum_{i=1}^{n} \alpha_i \frac{U_i'[\tau_j]}{U_i[\tau_j]} + H'[\tau_j]$ per a tot j entre 1 i s. Això és conseqüència del fet que, al cos de descomposició d'un polinomi, les arrels del polinomi estan relacionades entre si per K-isomorfismes que envien una arrel a una altra diferent. En particular, juntament amb la proposició 2.5, aquests K-isomorfismes són diferencials i $K[\tau_k] \cong K[\tau_j]$ per a $k \neq j$ entre 1 i s com a cossos diferencials amb aquests K-isomorfismes de canvi d'arrel, de manera que, en particular, les imatges dels elements $U_i[\tau_j]$ i $H'[\tau_j]$ satisfan la mateixa igualtat per a tot j entre 1 i s perquè $\tau_1 = t$ la satisfà.
Sumant totes les igualtats entre 1 i s i dividint per s, obtindrem:
$f = \sum_{i=1}^{n} \frac{\alpha_i}{s} \frac{(U_i[\tau_1]...U_i[\tau_s])'}{(U_i[\tau 1]...U_i[\tau_s])} + \frac{\sum_{i=j}^{s} H'[\tau_j]}{s}$, com a conseqüència d'aplicar la identitat logarítmica de les derivacions sobre els $U_i[\tau_j]$.
És clar que aquesta expressió és un polinomi simètric en les variables $\{\tau_1, ..., \tau_s\}$ amb coeficients a K i, com és sabut (és un dels resultats més egregis sobre polinomis simètrics), tots aquests elements han de ser de K, de manera que hem obtingut una expressió com la que demana l'enunciat del teorema.
D'ara endavant, podem considerar t transcendental sobre K, de manera que $K(t) \cong Q(K[t])$ i podem introduir diferents simplificacions: com $K[t]$ és D.F.U, cadascun dels u_i serà un producte de potències enteres (també negatives) d'elements irreductibles i mònics de $K[t]$ i una constant de K, emprant de nou la identitat logarítmica de les derivacions, podem separar els termes corresponents a cada u_i en sumes d'expressions iguals on el polinomi corresponent és un element de K, un element mònic i irreductible de $K[t]$. Sumant els elements de K a h' i canviant el nom a les variables de manera adequada, podem assumir que f és igual a una expressió de la mateixa forma que la anterior, però on cada u_i és mònic i irreductible i α_i és sempre no nul. A més, podem considerar la descomposició de h en forma reduïda, és a dir, com a suma de polinomis de $K[t]$ de la forma $\frac{p(t)}{q(t)^r}$, amb $p(t)$ mònic i irreductible i $q(t)$ polinomi no nul amb grau menor que del de $p(t)$ (vegi's [Bro.97] per aprofundir més en diferents descomposicions de funcions racionals i demostrar la descomposició en fraccions parcials, que podem emprar perquè K[X] sobre un cos és un domini euclidià).
Ateses aquestes modificacions, considerem els casos restants, que resoldrem emprant la proposició 3.4 com a lema.
Considerem primer el cas en què t és un logaritme no trivial d'un element a de K, $f' = \frac{b'}{b}$. Sigui $f(t)$ un polinomi irreductible i mònic, llavors, pel què hem vist al teorema 3.4, $f'(t) \in K[t]$ i té grau menor que $f'(t)$, de manera que $f(t)$ no divideix a $f'(t)$. Si $u_i = f(t)$, llavors la fracció $\frac{u_i'}{u_i}$ ja no es pot simplificar més, amb denominador $f(t)$. Quant a h, si el factor $\frac{g(t)}{f(t)^r}$ apareix en la

descomposició en forma reduïda amb $g(t)$ de grau menor a $f(t)$, amb $r > 0$ màxim amb aquesta propietat, llavors h' descomposarà en la suma d'una sèrie de factors amb $f(t)$ al denominador amb exponent com a màxim r i el sumand de $(\frac{g(t)}{f(t)^r})'$ següent, $-rg(t)\frac{(f'(t)}{(f(t))^{r+1})}$. Com $f(t)$ no divideix a $g(t)f'(t)$, llavors definitivament hi haurà un element a la banda dreta de la igualtat amb denominador $f(t)$ amb exponent $r+1 \geq 2$ que no es pot cancel·lar amb cap dels elements que aporten les descomposicions dels elements $\frac{u_i'}{u_i}$, de manera que tal factor hauria d'aparèixer a la descomposició de f de K, fet que és impossible. Per tant, $f(t)$ no pot aparèixer al denominador de h i llavors tampoc ho podrà fer al de cap $\frac{u_i'}{u_i}$ per un i fix, ja que no apareixeria cap altre factor corresponent a u_j per un altre valor de j que el pogués anul·lar i hauria d'aparèixer a la descomposició de f.
En conclusió, tenim que tots els u_i només poden ser de K per com els hem simplificat, i $h \in K[t]$. A més, per la proposició 3.4, $h = ct + d$ amb c a C i d a K i $h' = c\frac{b'}{b} + d$ element de K.
Com tots els u_i són de K i f també, l'expressió que hem trobat ha de tenir grau 0 en t, i això només s'aconsegueix si $c = 0$ i $h \in K$, obtenint una igualtat de la forma desitjada.
Finalment, considerem el cas en què t és una exponencial d'un element a' de K, de manera que $\frac{t'}{t} = a'$ de K (podem fer aquesta simplificació pel raonament següent: sigui t exponencial d'un element a de K, a és un logaritme de t. Com $a \in K \subset K(t)$, no pot ser un element transcendent respecte $K(t)$, de manera que ha de ser una integral trivial, pel contrarrecíproc del què hem demostrat pel cas dels logaritmes al toerema 3.2 i, en conseqüència, ha d'existir $b \in K(t)$ tal que $b' = a$ i, pel teorema 3.4, com han de tenir el mateix grau, $b \in K$).
Ara, per la proposició 3.4, si $f(t)$ és un element mònic irreductible diferent de t de $K[t]$, no pot dividir $f'(t)$, de manera que podem repetir l'argument del cas anterior sobre l'aparició de $f(t)$ al denominador corresponent al descompondre qualsevol dels factors u_i i h, així que, com a molt un u_i per a i fix (que podem triar 1 sense pèrdua de generalitat) és tal que $u_1 = t$, i h ha de ser tal que $h = \sum_{j\in I}^{s} a_j t^j$, on I és un conjunt finit d'enters (pot contenir negatius).
Si $\frac{u_i'}{u_i} \in K$ per a tot i, llavors de l'expressió obtinguda deduim que $h' \in K$. Pel teorema 3.4, això vol dir que $h \in K$. En cas contrari, si es dóna el cas particular $u_1 = t$, tindrem que $\frac{u_1'}{u_1} = \frac{t'}{t} = a'$, de manera que podem canviar h per $v = h + c_1 a \in K$ i obtindrem una igualtat amb la forma desitjada. □

Corol.lari 3.2. *La integral d'una funció racional de $\mathbb{C}(z)$ és elemental si, i només si, la funció en qüestió és la suma de la derivada d'una funció racional i una combinació lineal finita de logaritmes de funcions racionals.*
En particular, quan provem de calcular-ne una antiderivada, fem referència a trobar la part racional i la part transcendental de la integral.

Demostrat el teorema principal, veiem les virtuts de considerar el teorema de Liouville com un resultat particular en el marc de la teoria d'extensions diferencials, aprofitant també l'estudi de les extensions de Picard-Vessiot.

Tornant a la proposició 2.19, utilitzem la hipòtesi que C és algebraicament tancat per a justificar que cap constant de l'extensió L de Picard-Vessiot és algebraica sobre K, o ho seria també sobre C i hi hauria de pertànyer.
En el cas general, no podem descartar aquesta possibilitat, però la demostració continua sent certa aplicada a elements transcendentals de $Const_L$, de manera que, allò que realment ens diu la proposició sobre el cas general és que, sigui una extensió de Picard-Vessiot (fem un cert abús de notació, en realitat parlem més bé d'una extensió construida seguint el procediment de Kolchin), $Const_L \subset \overline{C}$, la clausura algebraica del subcòs de constants de K.
Això ens permet enunciar una propietat general de les extensions elementals de forma natural:

Proposició 3.6. *Sigui (K, d) un cos diferencial, C el seu subcòs de constants, i sigui $K \subset L$ una extensió elemental de K.*
Llavors, $Const_L \subset \overline{C}$

Demostració. Com ja sabem, una extensió és elemental si és finita i a cada pas simple, afegeix una exponencial, un element algebraic o un logaritme no trivial al cos base de l'extensió.
Quan l'element afegit és un logaritme no trivial, l'extensió simple associada a ell no afegeix constants, i, a la resta de casos, només pot afegir constants algebraiques sobre C, ja que bé és una extensió algebraica (i tota constant algebraica sobre K ho és sobre C, com vam veure) o és una extensió de Picard-Vessiot si afegeix una exponencial, de manera que només pot afegir constants algebraiques pel què acabem d'observar. □

I no només això, sinó que, a més, la proposició 3.4, admet una versió amb la condició $Const_{F(t)} = Const_F$ relaxada a $Const_{F(t)} \subset \overline{Const_F}$. Això passa perquè les propietats que aconseguim són conseqüència de veure que un monomi en funció de t, o un polinomi de grau 1 en t és una constant de $F(t)$ i deduir que t ha de ser algebraic sobre F, aconseguint una contradicció amb el fet que t sigui transcendent sobre F.
Ara bé, amb la condició relaxada que proposem, aquestes igualtats ens diuen que t pertany a $\overline{Const_F} \subset \overline{F}$, de manera que acabem deduint que t és algebraic sobre $\overline{F}$, pertany a $\overline{\overline{F}}$. Però és ben conegut el fet que $\overline{\overline{F}} = \overline{F}$, de manera que t hauria de ser algebraic sobre F, obtenint les mateixes contradiccions. És a dir:

Corol.lari 3.3. *La proposició 3.4 també és certa si relaxem la hipòtesi a $Const_{F(t)} \subset \overline{Const_F}$*

Aquestes observacions, juntament amb una versió de la proposició 3.4 modificada que ens pot ajudar a demostrar els casos d'extensions simples de logaritmes no trivials i exponencials no trivials, ens donen una certa intuició sobre com podria ser una versió generalitzada del teorema de Liouville sense suposar restriccions o relacions entre els subcossos de constants de les extensions, prenent elements de $\overline{C}$ per fer el seu paper en el cas general.
Aquest cas general, però, particularment quan tractem el pas d'inducció per a una extensió simple algebraica, no funciona si considerem una expressió amb

elements de K com al cas anterior, i requereix una hipòtesi extra a més dels dos resultats enunciats, els termes que componen l'expressió de f han de pertànyer a $K(\alpha_i, ..., \alpha_n)$, el mínim cos que conté els termes que fan el paper de les constants al cas particular.
En tot cas, la teoria de Picard-Vessiot ens dóna una bona intuició sobre com modificar les hipòtesis per traslladar el resultat al cas general.
Enunciem el teorema sense desenvolupar la demostració, referint a on trobar-ne una prova alternativa a la bibliografia.

Proposició 3.7. *(Teorema de Liouville general) Sigui (K, d) un cos diferencial, f de K i sigui $K(g)$ una extensió de cossos diferencials tal que $g' = f$.*
Llavors, $K(g)$ és una extensió elemental si, i només si, existeixen conjunts $\{\alpha_i\}_{1\leq i\leq n} \subset \overline{C}$, $\{g_i\}_{1\leq i\leq n} \subset K(\alpha_1, .., \alpha_n)$ (diferents de zero), ($n \geq 1$) i un element $h \in K$ tals que:
$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$

Una demostració rigorosa d'aquest resultat, malgrat que des d'un enfoc molt diferent a la del nostre treball, es pot trobar a [Bro,97].

3.3 Aplicacions

Per a acabar el treball, tornem a considerar els espais de funcions meromorfes a una regió Ω, en particular aquelles de la forma fe^g amb f, g racionals.
L'objecte de l'apartat és aplicar el teorema de Liouville a aquestes funcions i trobar exemples de funcions elementals sobre el cos de les funcions racionals $\mathbb{C}(z)$ sense antiderivada elemental.
Primer, veiem un resultat preliminar:

Proposició 3.8. *Sigui $e^{g(z)}$ amb g racional no constant. Llavors, $e^{g(z)}$ no és algebraica sobre $\mathbb{C}(z)$.*

Demostració. Ho veiem fàcilment aplicant resultats d'anàlisi complexa. Com g és una funció racional, tindrà com a mínim un pol a algun punt $z_0 \in \mathbb{C}$, de manera que e^g tindrà una singularitat essencial a z_0, propietat que no satisfà cap funció racional de variable complexa. □

Per tant, fe^g tal que g no constant i f racional serà una exponencial transcendent sobre $\mathbb{C}(z)$, i estem en posició d'aplicar la proposició 3.4 i el teorema de Liouville per a determinar com de restrictiva és la forma en què la podem expressar, obtenint un criteri.
Si denotem $t = e^g$, podem veure ft com un element de $\mathbb{C}(z, t)$

Proposició 3.9. *Sigui $x = fe^g$, amb f i g racionals i g no constant. Llavors, una extensió $\mathbb{C}(z, t, g)$ integral serà primitiva si, i només si, existeix $a \in \mathbb{C}(z)$ tal que $f = a' + ag'$*

Demostració. Denotem $\mathbb{C}(z) := F$, de manera que treballem a l'extensió $F(t)$. Pel teorema del Liouville, existeixen $u_i \in F(t)$, $c_i \in \mathbb{C}$, $h \in F(t)$ per a tot i

entre 1 i un cert n més gran o igual que 1 tals que $ft = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + h'$ com els elements de la expressió són a $F(t)$ amb t exponencial transcendental, podem aplicar la proposició 3.4 de manera anàloga al cas anterior i, simplificant les expressions (com abans, tot simplificant els u_i a elements de $F[t]$ mònics i irreductibles), tindrem que només pot existir, com a molt, un sol u_i (suposem u_1) igual a t i la resta han de pertànyer a F. Quant a h, com hem vist abans, ha de ser de la forma $h = \sum_{j \in I} b_j t^j$ per a un conjunt I finit d'enters. Ara bé, com ft és un monomi a $F(t)$ de grau 1 i $\sum_{i=1}^{n} c_i \frac{u_i'}{u_i} \in F$ (també per a $u_1 = t$, per ser t exponencial d'una funció racional) serà zero i l'únic coeficient no nul de la expressió de h serà b_1 (o la derivada conservaria monomis d'altres graus, com hem demostrat prèviament), de manera que $h' = (b_1' + b_1 g')t$ i, com és una igualtat de polinomis en t, tindrem $f = b_1' + b_1 g'$ amb $b_1 \in F$. Prendre $a = b_1$ completa la demsotració.
Quant al recíproc, si existeix $a \in F$ tal que $f = a' + ag'$, tindrem que at és una integral de ft. En efecte, $(at)' = ag't + a' = ag't + ft - ag't = ft$, que clarament és un integral elemental de ft. □

Obtinguda aquesta caracterització de les funcions d'aquest tipus que tenen antiderivada elemental, aprofitem el resultat per demostrar alguns casos particulars destacables.

Proposició 3.10. *Les funcions e^{-z^2} i $e^{\frac{1}{z}}$ no tenen integrals elementals.*

Demostració. Per la proposició 3.9, tenim que e^{-z^2} tindrà la seva antiderivada a una extensió elemetnal del cos de les funcions racionals si, i només si, existeix una funció racional sobre els complexos a tal que $1 = a' - 2za$, en la notació preestablerta.
Veiem primer que a no és un polinomi en funció de z. En efecte, si fos així i fos de grau $n \geq 1$, el seu coeficient líder $a_n \neq 0$ hauria de ser el coeficient líder de $a' - 2za$ (perquè $Deg(a) > Deg(a')$), però llavors hauria de ser $a_n = 0$, contradient les seves propietats de definicíó. Només quedaria el cas en què a fos una constant, però llavors $a' = 0$ i tindriem que 1 és igual a un monomi de grau 1 o a 0, ambdues situacions acabant en contradicció.
Quant al cas general, sigui $a = \frac{h}{g}$ amb h, g polinomis en la variable z tals que són coprimers, tindrem: $1 = \frac{h'g - hg' - 2zgh}{g^2}$, de manera que
$g^2 = h'g - hg' - 2zgh$ i, sigui p un factor primer que divideix a g, llavors divideix a $h'g$ i $2zgh$, i tindrem que $p | hg'$. Però p no pot dividir a h, de manera que dividirà a g'. Repetint el mateix raonament per a tots els factors primers de g, i emprant que $\mathbb{C}[X]$ és un D.F.U, arribem ràpidament a la situació $g | g'$, que no és possible, ja que la derivada de g té grau estrictament menor que el de g. Es segueix, llavors, que la normal no té una expressió elemental.
Quant al segon cas, si l'extensió integral corresponent fos elemental, tindriem $1 = za' + za = z(a' + a)$ per a una certa funció a racional. Seguint la notació anterior, tindriem que $1 = \frac{zh'g - zhg' + zhg}{g^2}$, de manera que, per a tot factor primer de g, diem-li p, tenim, de nou, que $p | zhg'$. Llavors, o bé $p = z$ o $p | g'$. Però això voldrà dir que $g | zg'$ i, com tenen el mateix grau, el seu quocient

haurà de ser una constant de $\mathbb{C}$, k. En particular, s'hauran de satisfer les igualtats $ka_i = ia_i$ per a i entre n i 1 i $a_0 = 0$, on els a_i són els coeficients de g. Però això voldria dir que $i = k = j$ per a $i \neq j$ si hi ha a_i, a_j diferents no nuls, obtenint una contradicció. Per tant, g hauria de ser un monomi, de manera que g no tingués realment cap factor primer diferent de z a la seva descomposició. Ara bé, en aquest cas, com z estaria al denominador de a i a', ens podriem reduir al cas $1 = a' + a$ simplificant la z que multiplica, i no pot haver cap funció racional en la variable z satisfent aquesta igualtat, ja que obtindriem una contradicció molt similar a la del primer cas: si $a = \frac{h}{g}$ amb h, g coprimers, acabariem deduint que $g|g'$ de nou, obtenint la contradicció desitjada.

□

Emprant diferents canvis de variable i raonant de forma similar per a altres igualtats simples, podem demostrar que moltes integrals conegudes no són elementals, com les de les funcions $\frac{ln(z)}{z}$ i $\frac{sin(z)}{z}$.
L'existència d'aquest tipus de criteri suggereix un problema de decisió més general, el dubte de si és possible decidir sempre (deduir) si una funció donada té integral elemental o no, en especial aplicant algun tipus d'algoritme. Aquesta pregunta, juntament amb la tasca de calcular integrals indefinides elementals quan aquestes existeixen, dubtes importants dins el camp de les matemàtiques aplicades, són plantejades aprofitant el marc teòric proporcionat pel teorema de Liouville, posant de rellevància que, si bé és un teorema generalment oblidat a les aules de les universitats com subratllem al paràgraf introductori, val la pena demostrar-lo i posar-lo en context adequadament.

4 Bibliografia

[$M-H$]-M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[$C-H$]-T.Crespo, Z.Hajto, *Algebraic groups and Differential Galois Theory*, ISBN 978-0-8218-5318-4, Graduate Studies in Mathematics, American Mathematical Society, 2011.

[I]-K. Irwin, *An introduction to differential algebra*, ISBN 2-7056-1251-3, Hermann, 1976.

[A]-Magid R. Andy, *Lectures on Differential Galois Theory*, ISBN 0-8218-7004-1, American Mathematical Society, 1994.

[$Bro, 97$]-M. Bronstein, *Symbolic Integration I, Transcendental Functions*, ISBN 3-540-21493-3, Springer, 2005.
[B]-A. Borel, *Essays in the History of Lie Groups and Algebraic Groups*, ISBN 0-8218-0288-7, American Mathematical Society, London Mathematical Society, 2001.

[Ro]- M. Rosenlicht, *Integration in finite terms*, American Mathematical Monthly 79, pp.963–972, 1972.

[Co]-B. Conrad, *Impossibility theorems for elementary integration*, disponible online a https://math.stanford.edu/ conrad/papers/elemint.pdf