Universitat Autònoma de Barcelona

Final Degree Project

# Differential Galois Theory

# Groups of symmetries in differential equations

*Author:*
Joan Claramunt Carós

*Supervisor:*
Dr. Pere Ara Bertran

*"Tu prieras publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité, mais sur l'importance des théorèmes.*
*Après cela, il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis."*

*(Ask Jacobi or Gauss publicly to give their opinion, not as to the truth, but as to the importance of these theorems. Later there will be, I hope, some people who will find it to their advantage to decipher all this mess.)*

Évariste Galois (1811-1832), two days before his death

Universitat Autònoma de Barcelona

# *Abstract*

Degree in Mathematics and Physics

**Differential Galois Theory**

The aim of this project is to study homogeneous linear differential equations through their own groups of symmetries, preserving both the algebraic and the differential structures of them. In order to do so, we develop a theory inspired by the Algebraic Galois Theory for polynomials. First, we introduce the differential structure over rings and fields, with some results about extending it through ring / field extensions. Then, we define the analogue concept of a splitting field, but for homogeneous linear differential equations, and we study some properties of it in depth. Having already dictated the fundamental tools, we will define the group of symmetries of a given homogeneous linear differential equation. Finally, by studying this group and its structure we will be able to provide some criteria about when such an equation has solutions expressible in terms of elementary functions: as we present, $\int e^{-w^2}$ is not expressible in terms of them.

# *Acknowledgements*

I would like to express my deep gratitude to Dr. Pere Ara, my research supervisor, for his patient guidance, enthusiastic encouragement and useful critiques of this research work. He gave me moral support and guided me in different matters regarding the topic, whilst suggesting to me some improvements on this project, and correcting my doubts. I really thank him for his overall support and dedication.

I would also like to thank Dr. Francesc Bars for his assistance and useful opinions, which have helped me in completing this project. My grateful thanks are also extended to Dr.'s Joan Eugeni Mateu Bennassar, Armengol Gasull, Marcel Nicolau and Wolfgang Pitsch for the valuable knowledge and bibliography provided in their respective fields.

Last but not least, I would like to thank my parents, sister and friends for their enormous support and encouragement without which this project would not have been possible.

To all of you, really thanks.

# Contents

# Preface

# Statement of the problem: the analogy with Algebraic Galois Theory

Évariste Galois faced the mathematical problem of characterizing the polynomials being solvable by radicals by introducing the mathematical concept of 'group'. Recall that a given polynomial with coefficients lying in the field of rational numbers $\mathbb{Q}$

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \quad , a_i \in \mathbb{Q} \;\; \forall i = 0, ..., n$$

is **solvable by radicals** if it has roots expressible by radicals and the basic arithmetic operations.
He gave a necessary and sufficient condition for this statement by studying the Galois group of $p(x)$, the set of automorphisms of the splitting field of $p(x)$ over $\mathbb{Q}$ (more intuitively, the group of symmetries of the roots that preserve all the algebraic relations among these roots):

**Theorem 0.1.** *Given* $p(x) \in \mathbb{Q}[x]$*,*

$p(x) = 0$ *is solvable by radicals* ***if and only if*** *its Galois group is solvable*

In this project we will develop a similar theory concerning not polynomials, but linear differential equations: given a linear differential equation of the form[1]

$$\mathcal{L}(y) = a_0(z) \cdot y(z) + a_1(z) \cdot y^{(1)}(z) + \cdots a_n(z) \cdot y^{(n)}(z) = 0 \quad , a_i(z) \in \mathbb{C}(z) \;\; \forall i = 0, ..., n$$

in what conditions its solutions are expressible by elementary functions?[2]
We can easily see the analogy between this problem and that which Galois faced. So, in order to answer this question (as well as other questions that will also come) we are going to follow a scheme analogous to the Algebraic Galois Theory with some, of course, differences and changes.

[1]The reader may have noticed that we are dealing with a homogeneous linear differential equation; we will prove, while properly studying linear differential equations, that this is the general case.

[2]We will formalise the idea of 'elementary function', but just to have an idea, an elementary function is a function built from a finite number of exponentials, logarithms, trigonometric functions and roots of polynomial equations, through compositions, sums, substractions, products and divisions.

The scheme we will follow, in analogy, is the following[3]:

- Since we are going to work with differential equations, we need a notion of what a differentiation is; so, first of all, we will set the concept of differentiation, and what a differential ring / field is.

| **A.G.T** | | **D.G.T** |
|---|---|---|
| $R$ ring / field | $\longleftrightarrow$ | $R$ differential ring / field |

- We will not deal with solutions to polynomial equations, but to (linear) differential ones: we need to understand what a linear differential equation means, and study the behavior of its solutions.

| **A.G.T** | | **D.G.T** |
|---|---|---|
| $\begin{cases} p(x) \in \mathbb{Q}[x] \\ p(x) = 0 \end{cases}$ | $\longleftrightarrow$ | $\begin{cases} \mathcal{L} \in K[d] \\ \mathcal{L}(y) = 0 \end{cases}$ |

- As we will see, a linear combination of solutions of a given linear differential equation is also a solution of the same linear differential equation, a property that we hadn't in the case of polynomial equations.

| **A.G.T** | | **D.G.T** |
|---|---|---|
| set of solutions of $p(x) = 0$ | $\longleftrightarrow$ | set of solutions of $\mathcal{L}(y) = 0$ |
| $\{x_1, ..., x_n\}$ | $\longleftrightarrow$ | $\langle y_1, ..., y_m \rangle$ (vect. space of dim $\leq n$) |

- Given a linear differential equation, we have an analogous concept of a splitting field, which will be the **Picard-Vessiot extension**.

| **A.G.T** | | **D.G.T** |
|---|---|---|
| splitting field of $p(x) = 0$<br>$E = \mathbb{Q}(x_1, ..., x_n)$ | $\longleftrightarrow$ | Picard-Vessiot ext. of $\mathcal{L}(y) = 0$<br>$L = K\langle y_1, ..., y_n \rangle$ |

- Having already dictated the fundamental tools of our theory, we will be ready to define what a Differential Galois Group is, and to study it and its properties.

| **A.G.T** | | **D.G.T** |
|---|---|---|
| Galois Group of the extension $L/K$<br>$\mathrm{Gal}(L/K)$ | $\longleftrightarrow$ | Differential Galois Group of the extension $L/K$<br>$\mathrm{DGal}(L/K)$ |

  We will be able to provide $\mathrm{DGal}(L/K)$ with a topology by thinking it as a subgroup of the general linear group $\mathrm{GL}_n(C_K)$, being $C_K$ the field of constants of the differential field $K$, and this fact will help us to study some interesting properties of our group.

- We will also study the analogue of the concept of radical extensions, the Liouvillian extensions, a concept which is deeply connected with the notion of elementary functions.

| **A.G.T** | | **D.G.T** |
|---|---|---|
| radical extensions | $\longleftrightarrow$ | Liouvillian extensions |

[3]Acronym A.G.T will be for Algebraic Galois Theory, and acronym D.G.T will be for Differential Galois Theory.

# Chapter 1

# Introduction. Constructing our worktable

Given a linear differential equation, the general idea is to associate it with a group of transformations (preserving the algebraic and differential structure) leaving it invariant: this group will give us information about its solutions.

In order to be able to follow the content of this work, the reader needs to have a basic knowledge of Group and Ring Theory, followed by a solid basis of Algebraic Galois Theory in general.

In this chapter we are going to introduce the reader to the notion of a derivation, followed by some algebraic properties.
First of all, we will study some important elements concerning the differential structure, such as differential morphisms, differential quotient rings or differential field extensions.
After that, we will introduce the key elements with whom we want to work: Linear Differential Equations. We will formalize the idea of what a LDE (Linear Differential Equation) is and where they "live" (ring of differential operators), as well as seeing that working with homogeneous linear differential equations will be enough for our purposes.
We will end this chapter by trying to understand some properties of their solutions, such as the main fact that the set of solutions of a LDE has a vector space structure, which will be crucial in the study of its Galois group.

In all this work we are going to deal with **commutative rings** and **fields of characteristic 0**, in order to avoid too technical demonstrations and make them easier.

## 1.1 Providing a differential structure over rings and fields

Since we are going to deal with LDE's, we need to have an idea of what a derivation is. In this section we will develop a simple theory about differential rings and fields, as well as giving some examples

and interesting results which we will exploit.
We already know what a differentiation (derivation) is, for example, in the context of differentiable real-valued functions defined on an open set $U \subseteq \mathbb{R}$:

$$\left\{ f : U \subseteq \mathbb{R} \longrightarrow \mathbb{R} \;\middle|\; \text{exists } \lim_{x \to a} \frac{f(x) - f(a)}{x - a} \equiv f'(a) \text{ for all } a \in U \right\}$$

We call $f'(a)$ the **derivative** of $f$ at point $a$. Some properties of this derivation that we already know are:

1) $(\alpha f + \beta g)'(a) = \alpha f'(a) + \beta g'(a)$ with $\alpha, \beta \in \mathbb{R}$ (linearity)

2) $(fg)'(a) = f'(a)g(a) + f(a)g'(a)$ (Leibniz's rule)

So, we can consider the abstract notion of a derivative, as follows:

**Definition 1.1.** *Let $R$ be a commutative ring (or a field). A **derivation** on $R$ is a map*

$$\begin{aligned} d_R : &R \longrightarrow R \\ &a \longmapsto d_R(a) \end{aligned}$$

*satisfying the following properties:*

*a)* $d_R(a + b) = d_R(a) + d_R(b)$ *(linearity)*

*b)* $d_R(ab) = d_R(a)b + a d_R(b)$ *(Leibniz's rule)*

*We say that $R$ is a **differential** ring (or a **differential** field) if we provide $R$ with a derivation.*

Some examples of differential rings and fields are given below.

**Examples 1.1.**

*1)* Every ring $R$ can be provided with the trivial derivation $d_R \equiv 0$.

*2)* Consider the field $R = \mathbb{C}(z)$ and the usual derivation $d_R \equiv \frac{d}{dz}$.

*3)* $R = C^\infty(\mathbb{R}^2)$, with the derivation

$$d_R(f) \equiv x\frac{\partial f}{\partial y} - y\frac{\partial f}{\partial x} \qquad \forall\, f \in C^\infty(\mathbb{R}^2)$$

is indeed a differential ring:

$$\begin{aligned} d_R(f+g) &= x\frac{\partial (f+g)}{\partial y} - y\frac{\partial (f+g)}{\partial x} = x\left(\frac{\partial f}{\partial y} + \frac{\partial g}{\partial y}\right) - y\left(\frac{\partial f}{\partial x} + \frac{\partial g}{\partial x}\right) = \\ &= d_R(f) + d_R(g) \end{aligned}$$

$$\begin{aligned} d_R(fg) &= x\frac{\partial (fg)}{\partial y} - y\frac{\partial (fg)}{\partial x} = x\left(\frac{\partial f}{\partial y}g + f\frac{\partial g}{\partial y}\right) - y\left(\frac{\partial f}{\partial x}g + f\frac{\partial g}{\partial x}\right) = \\ &= d_R(f)g + f d_R(g) \end{aligned}$$

Notice that, in this case, demanding the annihilation of the derivative of an element $f$ leads to the condition

$$\frac{1}{y}\frac{\partial f}{\partial y} = \frac{1}{x}\frac{\partial f}{\partial x}$$

which holds, for example, for the family of functions

$$f_\alpha(x,y) = \alpha(x^2+y^2) \qquad \alpha \in \mathbb{R}$$

The observation of the latter example shows that, depending on the derivation we provide on $R$, not only the "scalars" have the property of having zero derivative, as we are probably used to think, but some "non-scalar" elements.
This fact leads us to consider a general definition about what we mean by "constant elements".

**Definition 1.2.** *Given a differential ring (field) $R$, we define*

$$C_R \equiv \left\{ a \in R \;\middle|\; d_R(a) = 0 \right\} = Ker(d_R)$$

*the set of* ***constants*** *of the derivation $d_R$.*

**Property 1.1** (of the set $C_R$)**.**
*If $R$ is a (differential) ring, then $C_R$ is a subring.*
*If $R$ is a (differential) field, then $C_R$ is a subfield.*

*Proof.* Direct consequences of the definitions. □

What did we want to say before by "scalars"? The following fact is well-known and gives us a clearer interpretation of this meaning: given a commutative ring $R$, there exists a unique ring homomorphism $\psi$ mapping $\mathbb{Z}$ to $R$

$$\begin{aligned} \psi:\ & \mathbb{Z} \longrightarrow R \\ & n \longmapsto n \cdot 1 \end{aligned}$$

With this result we have a more abstract view of what we understand as "scalars" in a ring $R$. When $R$ is, in addition, a differential ring, it is therefore natural to ask if they are constants or not, as we are used to think.
The answer to this question is yes, as we shall see right now.

**Property 1.2** ("scalars" are constants)**.**
*If $R$ is a differential ring, then*

$$d_R(n \cdot 1) = 0$$

*Proof.* It is straightforward to prove that $d_R(0) = d_R(1) = d_R(-1) = 0$ because of linearity and Leibniz's rule:

$$\begin{aligned} d_R(0) = d_R(0+0) = d_R(0) + d_R(0) &\qquad \text{so} \qquad d_R(0) = 0 \\ d_R(1) = d_R(1\cdot 1) = 1\cdot d_R(1) + d_R(1)\cdot 1 = d_R(1) + d_R(1) &\qquad \text{so} \qquad d_R(1) = 0 \\ 0 = d_R(0) = d_R(1+(-1)) = d_R(1) + d_R(-1) = d_R(-1) &\qquad \text{so} \qquad d_R(-1) = 0 \end{aligned}$$

The property just holds from these facts due to linearity again. □

Given the basic ideas of a derivation, from now on we will study many of the most important results about extending them; first of all, let's set up some intuitive concepts of what a differential extension is [1].

Let $R$ be a differential ring (field). A **differential ring (field) extension of** $R$ is a differential ring (field) $T$ such that $R \subseteq T$ and $d_T\Big|_R = d_R$. On the other hand, a **differential subring (subfield) of** $R$ is a subring (subfield) $S$ which is closed under the derivation over $R$, $d_R(S) \subseteq S$.

### 1.1.1 Differential rational field $Quot(R)$

We now know the notion of a derivation acting on a ring $R$. In general, this $R$ will not be a field, since not all of their elements are invertible. However, we already have a way of constructing a new field given a ring $R$, with the condition on the ring of being an **integral domain**: this field is known as the **rational field of** $R$, $Quot(R)$. Recalling its construction,

$$Quot(R) = R \times R\backslash\{0\}/\sim \; = \left\{\overline{(a,b)} \;\Big|\; a, b \in R, b \neq 0\right\}$$

with the equivalence relation given by

$$(a,b) \sim (c,d) \iff ad = bc$$

We generaly use the notation

$$\frac{a}{b} \equiv \overline{(a,b)}$$

which is consistent with the idea we have for a fraction:

$$\frac{a}{b} = \frac{ac}{bc} = \overline{(ac,bc)} = \overline{(a,b)} \qquad \text{since } (ac)b = (bc)a$$

We would like to provide $Quot(R)$ with a differential structure taking advantage of the differential structure that could come from $R$. This is, indeed, possible to achieve; much more, there is only one way of extending the derivation from $R$ to $Quot(R)$.

**Proposition 1.1** (Extending derivations from $R$ to $Quot(R)$)**.**

*Let $R$ be an integral domain (a commutative ring without nonzero zero divisors) provided with a derivation $d_R$. Then $d_R$ extends to the rational field $Quot(R)$ in a unique way.*

*In other words, there exists only one derivation $d_{Quot(R)}$ on $Quot(R)$ such that $d_{Quot(R)}\Big|_R = d_R$.*

*Proof.* Let's define a derivation on $Quot(R)$ given by

$$\begin{aligned} \widetilde{d} : Quot(R) &\longrightarrow \quad Quot(R) \\ \frac{a}{b} \quad &\longmapsto \frac{d_R(a)b - a d_R(b)}{b^2} \end{aligned}$$

It is an easy exercice to show that it is well defined (the definition is independent of the choice of the representative) and a derivation over $Quot(R)$ with the property $\widetilde{d}\Big|_R = d_R$. It is also straightforward to see its uniqueness because of the relations

$$d_R(ab^{-1}) = d_R(a)b^{-1} + a d_R(b^{-1}) \quad \text{with} \quad d_R(b^{-1}) = -b^{-2} d_R(b)$$

The last one is due to $d_R(bb^{-1}) = d_R(1) = 0$. □

[1] We will revisit this concepts in **Section 1.1.4. Differential ring and field extensions**.

**Examples 1.2.**

*1)* Let $R$ be a differential ring. We can then consider the new ring

$$R[x_0, x_1, x_2, ..., x_n, ...]$$

that is, the ring of polynomials in the indeterminates $x_i$, $i \in \mathbb{Z}^+$ with coefficients in $R$.

A derivation on $R[x_i] \equiv R[x_0, x_1, x_2, ..., x_n, ...]$ can be given by extending the derivation over $R$ in the following way:

$$\begin{aligned} \widetilde{d}: \ R[x_i] &\longrightarrow R[x_i] \\ x_j &\longmapsto \widetilde{d}(x_j) = x_{j+1} \\ a &\longmapsto \widetilde{d}(a) = d_R(a) \quad \forall\, a \in R \end{aligned}$$

This definition determines the derivation totally, by extending it using linearity and product rule's properties. The ring $R[x_i]$ with this differential structure is called the **adjunction of a differential indeterminate $x$ in $R$**, and is denoted by

$$R\{x\} \equiv (R[x_i], \widetilde{d}) = R[x, \widetilde{d}(x), \widetilde{d}^2(x), ...., \widetilde{d}^n(x), ...]$$

($x$ and all its derivatives)

the **ring of differential polynomials in $x$**.

If $T$ is, in addition, a (differential) integral domain, so is $R\{x\}$, and we can consider its rational field, denoted by

$$R\langle x\rangle \equiv Quot(R\{x\})$$

which also becomes a differential field because of **Proposition 1.1**. It is called the **field of differential rational functions of $x$**.

Similarly, we can define the **field of differential rational functions of $x_1$,$x_2$,...,$x_n$** in a natural way:

$$R\langle x_1, x_2, ..., x_n\rangle \equiv (\cdots((R\langle x_1\rangle)\langle x_2\rangle)\cdots)\langle x_n\rangle$$

*2)* In general, let $T$ be a differential ring and $R \subseteq T$ a differential subring. Let $\alpha_1, ..., \alpha_n \in T$; we denote the smallest differential subring of $T$ that contains $R$ and each $\alpha_i$ and all its derivatives as

$$R\{\alpha_1, ..., \alpha_n\}$$

If $T$ is, in addition, a field, we denote the smallest differential subfield of $T$ that contains $R$ and each $\alpha_i$ and all its derivatives as

$$R\langle\alpha_1, ..., \alpha_n\rangle = Quot(R\{\alpha_1, ..., \alpha_n\})$$

### 1.1.2 Differential ideals and quotient rings

If $R$ is a ring and $I \subseteq R$ any subset, we already know the concept of being $I$ an ideal of $R$. We now want to extend this concept considering the differential structure coming from $R$.

**Definition 1.3.** *Let $R$ be a differential ring, and $I \subseteq R$ an ideal of $R$.*

*We say that $I$ is a* ***differential ideal*** *if $I$ is closed under derivation, that is, if*

$$d_R(I) \subseteq I$$

**Example 1.1.** Let $R$ be a differential ring, and $A \subseteq R$ a subset.

We define the **differential ideal generated by** $A$ as

$$(A)_d \equiv \bigcap_{\substack{A \subseteq I \\ I \text{ dif. ideal}}} I$$

We know it is an ideal. To see if it has a differential structure, consider $a \in (A)_d$; then $a \in I$ for every differential ideal containing $A$. Since $I$ are all differential ideal, $d_R(a) \in I$, in all of them, and so $d_R(a) \in (A)_d$ (the intersection), as we wanted. It is a simple exercice to show that

$$(A)_d = \left\{ \sum_{r=0}^{m} \sum_{i=0}^{n_r} b_{r,i} d_R^r(a_i) \;\middle|\; m, n_r \in \mathbb{N} \cup \{0\}, b_{r,i} \in R, a_i \in A \right\}$$

A particular case is when $A = \{a\}$. In this case, we denote

$$(a)_d \equiv (\{a\})_d = \left\{ \sum_{r=0}^{m} b_r d_R^r(a) \;\middle|\; m \in \mathbb{N} \cup \{0\}, b_r \in R \right\}$$

We could construct new rings by considering the quotient $R/I$ being $I$ an ideal. Now we have more: through the definition we have given of differential ideals, the quotient ring $R/I$, asking now $I$ to be a differential ideal, provided with the derivation induced by $R$, becomes a differential ring.

**Proposition 1.2** (Providing derivation to the quotient ring)**.**

*If $R$ is a differential ring, and $I \subseteq R$ a differential ideal, the quotient ring $R/I$ turns out to be a differential ring with the derivation*

$$\begin{aligned} \widetilde{d} \colon R/I &\longrightarrow R/I \\ \overline{a} &\longmapsto \widetilde{d}(\overline{a}) \equiv \overline{d_R(a)} \end{aligned}$$

*Proof.* We already know that $(R/I, +, \cdot)$ is a ring; we only need to prove that $\widetilde{d}$ is a derivation.

· It is well defined, since the definition is independent of the choice of the representative: having $\overline{a_1} = \overline{a_2}$, then $a_1 - a_2 \in I$, and so

$$d_R(a_1) - d_R(a_2) = d_R(a_1 - a_2) \in I$$

since $I$ is a differential ideal, which means that $\overline{d_R(a_1)} = \overline{d_R(a_2)}$.

· It is actually a derivation:

a) Linearity: $\widetilde{d}(\overline{a} + \overline{b}) = \overline{d_R(a+b)} = \overline{d_R(a) + d_R(b)} = \widetilde{d}(\overline{a}) + \widetilde{d}(\overline{b})$

b) Leibniz's rule: $\widetilde{d}(\overline{a} \cdot \overline{b}) = \overline{d_R(a \cdot b)} = \overline{d_R(a)b + a d_R(b)} = \widetilde{d}(\overline{a})\overline{b} + \overline{a}\widetilde{d}(\overline{b})$

□

We are interested in providing a differential structure on $K(\alpha) \cong K[x] \big/ (\mathrm{Irr}(\alpha, K)(x))$ extending the one on the differential field $K$ with derivation $d_K$, being $\alpha$ an algebraic element over $K$. Notice that, if such derivation $D$ on $K(\alpha)$ exists, the equality

$$\mathrm{Irr}(\alpha, K)(\alpha) = 0 = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n$$

determines it totally: deriving it,

$$\underbrace{\left(D(a_0) + D(a_1)\alpha + \cdots + D(a_{n-1})\alpha^{n-1}\right)}_{\mathrm{Irr}_D(\alpha,K)(\alpha) = \mathrm{Irr}_{d_K}(\alpha,K)(\alpha)\ \left(D\big|_K = d_K\right)} + \underbrace{\left(a_1 + 2a_2\alpha + \cdots + n\alpha^{n-1}\right)}_{\mathrm{Irr}(\alpha,K)'(\alpha)} D(\alpha) = 0$$

and so[2]

$$D(\alpha) = -\frac{\mathrm{Irr}_{d_K}(\alpha, K)(\alpha)}{\mathrm{Irr}(\alpha, K)'(\alpha)} = -\mathrm{Irr}_{d_K}(\alpha, K)(\alpha) \cdot \frac{1}{\mathrm{Irr}(\alpha, K)'(\alpha)}$$

Since the derivation $D$ over $K$ must be $d_K$, the element $D(\alpha)$ determines the derivation totally, as we have said. Much more, this last equality tells us that we can't define $D(\alpha)$ freely, and its definition involves the inverse of the element $\mathrm{Irr}(\alpha, K)'(\alpha)$.

This observation allows us to consider a particular derivation over $K[x]$ with an interesting property: it will become the previous derivation we have already defined over $K(\alpha)$; these results are given in **Theorem 1.1**.

**Theorem 1.1** (Differential structure over $K(\alpha)$)**.**

*Let $K$ be a differential field (of characteristic 0), and $K \subseteq L$ an algebraic field extension.*

*Given $\alpha \in L$, consider the field $K(\alpha)$, and its irreducible polynomial over $K$,*

$$Irr(\alpha, K)(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \quad a_i \in K$$

*Then*

*a) The derivation in $K$ can be extended to $K[x]$ by defining*

$$\begin{aligned} \widetilde{d} : K[x] &\longrightarrow K[x] \\ a &\longmapsto \widetilde{d}(a) \equiv d_K(a) \quad \forall\ a \in K \\ x &\longmapsto \widetilde{d}(x) = -Irr_{d_K}(\alpha, K)(x) \cdot q(x) \end{aligned}$$

*where*

$$Irr_{d_K}(\alpha, K)(x) = d_K(a_0) + d_K(a_1)x + \cdots + d_K(a_{n-1})x^{n-1}$$

*and $q(x) \in K[x]$ is such that*

$$Irr(\alpha, K)(x) \cdot p(x) + Irr(\alpha, K)'(x) \cdot q(x) = 1$$

*b) With the previous derivation, the ideal $(Irr(\alpha, K)(x))$ is a differential ideal, that is,*

$$(Irr(\alpha, K)(x))_d = (Irr(\alpha, K)(x))$$

[2]It could be helpful to remember that in all this work we are dealing with **fields of characteristic 0**.

c) *The quotient field* $K[x] \Big/ (Irr(\alpha, K)(x))$ *is a differential field. Much more, we have*

$$K[x] \Big/ (Irr(\alpha, K)(x)) \cong K(\alpha)$$

*as differential fields, with the derivation in* $K(\alpha)$ *induced by this isomorphism*

$$\begin{aligned} d_{K(\alpha)} : K(\alpha) &\longrightarrow K(\alpha) \\ a &\longmapsto d_{K(\alpha)}(a) \equiv d_K(a) \quad \forall\, a \in K \\ \alpha &\longmapsto d_{K(\alpha)}(\alpha) \equiv -\frac{Irr_{d_K}(\alpha, K)(\alpha)}{Irr(\alpha, K)'(\alpha)} \end{aligned}$$

*In fact, this is the only derivation we could provide over* $K(\alpha)$ *extending the one over* $K$.

*Proof.* It is an exercice to show that, if $d$ is a derivation, then $d(a^n) = na^{n-1}d(a)$ for all element $a$.

a) The derivation is completely determined by the definition of $\widetilde{d}(x)$: if $h(x) \in K[x]$,

$$\begin{aligned} \widetilde{d}(h(x)) &= \widetilde{d}(b_0 + b_1 x + \cdots + b_n x^n) = \\ &= \Big(\widetilde{d}(b_0) + \widetilde{d}(b_1)x + \cdots + \widetilde{d}(b_n)x^n\Big) + \Big(b_1\widetilde{d}(x) + b_2\widetilde{d}(x^2) + \cdots + b_n\widetilde{d}(x^n)\Big) = \\ &= (d_K(b_0) + d_K(b_1)x + \cdots + d_K(b_n)x^n) + \left(b_1 + 2b_2 x + \cdots + nb_n x^{n-1}\right)\widetilde{d}(x) \equiv \\ &\equiv h_{d_K}(x) + h'(x) \cdot \widetilde{d}(x) \end{aligned}$$

completely determined by $\widetilde{d}(b_i) = d_K(b_i)$ and $\widetilde{d}(x) = -\mathrm{Irr}_{d_K}(\alpha, K)(x) \cdot q(x)$.

b) Why have we chosen this definition of derivation specifically? This definition is the one which turns the ideal $(\mathrm{Irr}(\alpha, K)(x))$ into a differential ideal:

Consider $h(x) \in (\mathrm{Irr}(\alpha, K)(x))$, $h(x) = \mathrm{Irr}(\alpha, K)(x) \cdot h_1(x)$ with $h_1(x) \in K[x]$.

We need to show that $\widetilde{d}(h(x)) \in (\mathrm{Irr}(\alpha, K)(x))$. Let's first compute:

$$\begin{aligned} \widetilde{d}(h(x)) &= \widetilde{d}(\mathrm{Irr}(\alpha, K)(x) \cdot h_1(x)) = \\ &= \widetilde{d}(\mathrm{Irr}(\alpha, K)(x)) \cdot h_1(x) + \underbrace{\mathrm{Irr}(\alpha, K)(x) \cdot \widetilde{d}(h_1(x))}_{\text{multiple of } \mathrm{Irr}(\alpha,K)(x)} \end{aligned}$$

So, we only need to prove that $\widetilde{d}(\mathrm{Irr}(\alpha, K)(x)) \in (\mathrm{Irr}(\alpha, K)(x))$.

As we have shown in the first section of this theorem, the derivative of $\mathrm{Irr}(\alpha, K)(x)$ is simply

$$\widetilde{d}(\mathrm{Irr}(\alpha, K)(x)) = \mathrm{Irr}_{d_K}(\alpha, K)(x) + \mathrm{Irr}(\alpha, K)'(x) \cdot \widetilde{d}(x)$$

and **using our definition of** $\widetilde{d}(x)$, we obtain

$$\begin{aligned} \widetilde{d}(\mathrm{Irr}(\alpha, K)(x)) &= \mathrm{Irr}_{d_K}(\alpha, K)(x) - \mathrm{Irr}(\alpha, K)'(x) \cdot \mathrm{Irr}_{d_K}(\alpha, K)(x) \cdot q(x) = \\ &= \mathrm{Irr}_{d_K}(\alpha, K)(x)\Big[1 - \mathrm{Irr}(\alpha, K)'(x) \cdot q(x)\Big] \end{aligned}$$

Now, since we are working with fields of characteristic 0, $\mathrm{Irr}(\alpha, K)'(x) \neq 0$, which leads to

$$\mathrm{mcd}\Big(\mathrm{Irr}(\alpha, K)(x), \mathrm{Irr}(\alpha, K)'(x)\Big) = 1 \quad \text{(because } \mathrm{Irr}(\alpha, K)(x) \text{ is irreducible)}$$

and from Bézout's Identity, there exist $p(x), q(x) \in K[x]$ such that[3]

$$\mathrm{Irr}(\alpha, K)(x) \cdot p(x) + \mathrm{Irr}(\alpha, K)'(x) \cdot q(x) = 1$$

Finally, we can return to the computation of the derivative of $\mathrm{Irr}(\alpha, K)(x)$:

$$\begin{aligned}\widetilde{d}(\mathrm{Irr}(\alpha, K)(x)) &= \mathrm{Irr}_{d_K}(\alpha, K)(x) \underbrace{\left[1 - \mathrm{Irr}(\alpha, K)'(x) \cdot q(x)\right]}_{\mathrm{Irr}(\alpha,K)(x)\cdot p(x)} = \\ &= \underbrace{\mathrm{Irr}_{d_K}(\alpha, K)(x) \cdot \mathrm{Irr}(\alpha, K)(x) \cdot p(x)}_{\text{multiple of } \mathrm{Irr}(\alpha,K)(x)}\end{aligned}$$

and so $\widetilde{d}(\mathrm{Irr}(\alpha, K)(x)) \in (\mathrm{Irr}(\alpha, K)(x))$, as we wanted to prove. Now it is easy to see the equality between ideals

$$(\mathrm{Irr}(\alpha, K)(x))_d = (\mathrm{Irr}(\alpha, K)(x))$$

using $\widetilde{d}^r(\mathrm{Irr}(\alpha, K)(x)) \in (\mathrm{Irr}(\alpha, K)(x))$, which is easily proven by induction.

c) By **Proposition 1.2.**, the quotient $K[x] \big/ (\mathrm{Irr}(\alpha, K)(x))$ becomes a differential ring, and in fact a differential field, since $(\mathrm{Irr}(\alpha, K)(x))$ is a maximal ideal of $K[x]$.

From the First Isomorphism Theorem, we already know that

$$K[x] \big/ (\mathrm{Irr}(\alpha, K)(x)) \cong K(\alpha)$$

are isomorphic as fields, with the isomorphism given by

$$\begin{aligned}\overline{f} : K[x] \big/ (\mathrm{Irr}(\alpha, K)(x)) &\longrightarrow K(\alpha) \\ \overline{p(x)} &\longmapsto p(\alpha)\end{aligned}$$

Furthermore, we can define a derivation over $K(\alpha)$ taking advantage of the differential structure over $K[x] \big/ (\mathrm{Irr}(\alpha, K)(x))$ and the previous isomorphism: we define a derivation $d_{K(\alpha)}$ which makes the following diagram commutative:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\ \overline{f}^{-1}\ } & K[x] \big/ (\mathrm{Irr}(\alpha, K)(x)) \\ {\scriptstyle d_{K(\alpha)}} \downarrow & & \downarrow {\scriptstyle \widetilde{d}} \\ K(\alpha) & \xleftarrow{\ \overline{f}\ } & K[x] \big/ (\mathrm{Irr}(\alpha, K)(x)) \end{array}$$

More specific,

$$\begin{aligned} d_{K(\alpha)} : K(\alpha) &\longrightarrow K(\alpha) \\ a &\longmapsto d_{K(\alpha)}(a) \equiv (\overline{f} \circ \widetilde{d} \circ \overline{f}^{-1})(a) = d_K(a) \quad \forall\ a \in K \\ \alpha &\longmapsto d_{K(\alpha)}(\alpha) \equiv (\overline{f} \circ \widetilde{d} \circ \overline{f}^{-1})(\overline{x}) = -\mathrm{Irr}_{d_K}(\alpha, K)(\alpha) \cdot q(\alpha) \end{aligned}$$

which we can rewrite as

$$\begin{aligned} d_{K(\alpha)} : K(\alpha) &\longrightarrow K(\alpha) \\ a &\longmapsto d_{K(\alpha)}(a) = d_K(a) \quad \forall\ a \in K \\ \alpha &\longmapsto d_{K(\alpha)}(\alpha) = -\frac{\mathrm{Irr}_{d_K}(\alpha, K)(\alpha)}{\mathrm{Irr}(\alpha, K)'(\alpha)} \end{aligned}$$

[3] $p(x)$ and $q(x)$ here are the polynomials we are using in our definition of the derivative.

taking into account Bézout's identity, evaluated on $\alpha$:

$$\underbrace{\mathrm{Irr}(\alpha, K)(\alpha)}_{\text{must be } 0} \cdot p(\alpha) + \mathrm{Irr}(\alpha, K)'(\alpha) \cdot q(\alpha) = 1 \quad \Longrightarrow \quad q(\alpha) = \frac{1}{\mathrm{Irr}(\alpha, K)'(\alpha)}$$

It is straightforward to see that this defines the derivation totally, and it is indeed a derivation. We already discussed, prior to this theorem, that this derivation over $K(\alpha)$ is unique, extending the one in $K$.

□

Another important aspect we need to keep in mind is the characterization of differential ideals in a quotient ring. Recalling the Second Isomorphism Theorem, if we have a ring $R$ and an ideal $I \subseteq R$, there exists a bijection

$$\begin{aligned} \{\text{ideals of } R \text{ containing } I\} &\longrightarrow \{\text{ideals of } R/I\} \\ J \qquad &\longmapsto \qquad \overline{J} = \pi(J) \end{aligned}$$

where $\pi : R \longrightarrow R/I$ is defined through $\pi(a) = \overline{a}$. If $R$ is, in addition, a differential ring, and $I$ a differential ideal, this fact induces a bijection between differential ideals of the two differential rings

$$\begin{aligned} \{\text{diff. ideals of } R \text{ containing } I\} &\longrightarrow \{\text{diff. ideals of } R/I\} \\ J \qquad &\longmapsto \qquad \overline{J} = \pi(J) \end{aligned}$$

Let's see how:

a) If $J$ is a differential ideal so is $\overline{J} = \pi(J)$, because if $\overline{a} \in \overline{J}$, $\widetilde{d}(\overline{a}) = \overline{d_R(a)} \in \overline{J}$ since $d_R(a) \in J$.

b) If $\overline{J}$ is a differential ideal so is $J = \pi^{-1}(\overline{J})$, because if $a \in J$, $\pi(d_R(a)) = \overline{d_R(a)} = \widetilde{d}(\overline{a}) \in \overline{J}$, so $d_R(a) \in \pi^{-1}(\overline{J}) = J$.

This will become a crucial property in order to study differential ideals in quotient rings.

Some definitions we also need to keep in mind concerning differential ideals are the following.

**Definition 1.4.** *Let $R$ be a differential ring, and $I \subseteq R$ a differential ideal.*

1) *We say $I$ is a **maximal differential ideal** if, given a differential ideal $J$ with the property*
$$I \subseteq J \subseteq R$$
*then $J = I$ or $J = R$.*

2) *We say $I$ is a **prime differential ideal** if it is a prime ideal, i.e.,*
$$ab \in I \Longrightarrow a \in I \text{ or } b \in I \qquad \forall\, a, b \in R$$

3) *We say $I$ is a **proper differential ideal** if*
$$\{0\} \subsetneq I \subsetneq R$$

**Study of prime differential ideals**

Since a prime differential ideal is both a prime ideal and a differential ideal, the following property is trivial.

**Property 1.3** (Caracterization of prime differential ideals).

*Let $R$ be a differential ring, and $I \subseteq R$ a differential ideal. Then*

$$I \text{ is a prime differential ideal } \iff R/I \text{ is an integral domain}$$

*Proof.* We already know the statement

$$I \text{ is a prime ideal } \iff R/I \text{ is an integral domain}$$

Since $I$ is a differential ideal, we are done. □

**Study of maximal differential ideals**

We can easily prove, applying Zorn's Lemma, the existence of maximal differential ideals. The proof is analogous to the one which proves the existence of maximal ideals.

An important result about maximal differential ideals is that, with some hypothesis, it turns out that they are prime differential ideals too.

**Property 1.4** (Of maximal differential ideals).

*Let $R$ be a differential ring, and $Quot(\mathbb{Z}) = \mathbb{Q} \subset R$.*

*Let $I \subseteq R$ be a maximal differential ideal. Then $I$ is also a prime differential ideal.*

*Proof.* Since $I$ is a differential ideal, $R/I$ turns out to be a differential ring; we denote the derivation on it by $\widetilde{d}$ (which is given by **Proposition 1.2**).

Let's prove our statement with some steps. Due to **Property 1.3**, we only need to prove that $R/I$ is an integral domain.

1) Let's first prove that every zero divisor in $R/I$ is nilpotent. Let $\overline{c} \in R/I$ be one of them, that is, there exists a nonzero $\overline{d} \in R/I$ such that $\overline{c}\overline{d} = \overline{0}$. Then

$$\overline{0} = \widetilde{d}(\overline{c}\overline{d}) = \widetilde{d}(\overline{c})\overline{d} + \overline{c}\widetilde{d}(\overline{d}) \underset{\text{multiplying by } \overline{d}}{\Longrightarrow} \widetilde{d}(\overline{c})\overline{d}^2 = \overline{0}$$

From similar arguments, it is not dificult to show by induction that $\widetilde{d}^k(\overline{c})\overline{d}^{k+1} = \overline{0}$ for all $k \geq 0$. Consider now the differential ideal generated by $\overline{d}$,

$$\overline{J} = (\overline{d})_d \subseteq R/I$$

and so $J = \pi^{-1}(\overline{J})$ is the differential ideal of $R$ containing $I$ that the bijection between differential ideals of $R$ containing $I$ and differential ideals of $R/I$ ensures. It is, then, clear that $I \subseteq J \subseteq R$, and since $I$ is a maximal differential ideal, we must have $J = I$ or $J = R$, but the first one is not

possible because $d \notin I$ ($\overline{d} \neq \overline{0}$).
Hence $J = R$, and $\overline{J} = R/I$, which means we can express $\overline{c}$ as

$$\overline{c} = \sum_{j=0}^{n} \overline{g}_j \widetilde{d}^j(\overline{d}) \qquad \text{for some } n \geq 0,\ \overline{g}_j \in R/I$$

and finally we obtain

$$\overline{c}^{n+2} = \sum_{j=0}^{n} \overline{g}_j \widetilde{d}^j(\overline{d}) \overline{c}^{n+1} = \overline{0}$$

as we wanted to show.

2) Let's prove our statement now: consider, then, $\overline{a}, \overline{b} \in R/I$, $\overline{a} \neq \overline{0}$ with $\overline{a}\overline{b} = \overline{0}$, and we want to prove that $\overline{b} = \overline{0}$. Let's prove it by contradiction: suppose $\overline{b} \neq \overline{0}$; then $\overline{a}$ will be a zero divisor, and hence nilpotent: there exists $n \geq 1$ such that $\overline{a}^n = \overline{0}$. Let's take $m$ to be the minimal number with such property.
Taking derivatives,

$$\overline{0} = \widetilde{d}(\overline{a}^m) = m\overline{a}^{m-1}\widetilde{d}(\overline{a})$$

Since $\mathbb{Q} \subset R$ and $m$ is minimal, $m\overline{a}^{m-1} \neq \overline{0}$, $\widetilde{d}(\overline{a})$ is again a zero divisor. Proceeding in the same way, we prove that $\widetilde{d}^k(\overline{a})$ is a zero divisor for all $k \geq 0$, and so all elements in $(\overline{a})_d$ are nilpotent.
Again, $I \subseteq \pi^{-1}((\overline{a})_d) \subseteq R$, so we must have $\pi^{-1}((\overline{a})_d) = I$ or $\pi^{-1}((\overline{a})_d) = R$, but the first one is not possible because $a \notin I$ ($\overline{a} \neq \overline{0}$).
Hence $\pi^{-1}((\overline{a})_d) = R$, so $(\overline{a})_d = R/I$, and we would have $\overline{1} \in (\overline{a})_d$ which gives a contradiction, since $\overline{1}$ is not nilpotent.
Therefore, $\overline{b} = \overline{0}$, as we wanted to prove.

□

### 1.1.3 Differential morphisms

To study relations between rings, we have the concept of ring homomorphism: a function between two rings which preserves the ring structure.

With a derivation defined in those two rings, we also want the differential structure to be preserved. For this purpose, we define the concept of differential homomorphisms. Remembering the last section of **Theorem 1.1**, a natural way of defining derivations through isomorphic rings / fields is via this isomorphism:

$$d_B = f \circ d_A \circ f^{-1}$$

or

$$d_B \circ f = f \circ d_A$$

This is the expression we are going to use to define the concept of differential homomorphisms. Notice that is the same concept as demanding the preservation of its differential structures.

**Definition 1.5.** *Let $R$ and $R'$ be two differential rings, with derivations $d_R$ and $d_{R'}$ respectively.*

*A function*

$$f : R \longrightarrow R'$$

*is said to be a* ***differential homomorphism*** *if*

*a) It is a ring homomorphism (preserves ring structure).*

*b) It preserves the derivations,*

$$f \circ d_R = d_{R'} \circ f$$

*The meaning of differential isomorphisms, automorphisms, etc. is clear.*

With this definition of preserving derivations, the First Isomorphism Theorem still holds.

**Theorem 1.2** (First Isomorphism Theorem for differential rings)**.**

*Let $R$ and $R'$ be differential rings, and*

$$f : R \longrightarrow R'$$

*a differential homomorphism. Then*

*a) $Ker(f)$ is a differential ideal of $R$.*

*b) $Im(f)$ is a differential subring of $R'$.*

*c) The isomorphism*

$$\begin{aligned} \overline{f} : R/Ker(f) &\longrightarrow Im(f) \\ \overline{a} &\longmapsto \overline{f}(\overline{a}) = f(a) \end{aligned}$$

*is a differential isomorphism.*

*Proof.*

a) We already know that $\mathrm{Ker}(f)$ is an ideal of $R$; we only need to check its differentiability.

Given an element $a \in \mathrm{Ker}(f)$, $f(d_R(a)) = (f \circ d_R)(a) = (d_{R'} \circ f)(a) = d_{R'}(f(a)) = d_{R'}(0) = 0$, and so $d_R(a) \in \mathrm{Ker}(f)$.

b) We already know that $\mathrm{Im}(f)$ is a subring of $R'$. We now need to check that $\mathrm{Im}(f)$ is closed under the derivation.

Given an element $a \in \mathrm{Im}(f)$, we need to prove that $d_{R'}(a) \in \mathrm{Im}(f)$. By definition, there exists an element $b \in R$ such that

$$f(b) = a$$

Let's now consider the element $d_R(b) \in R$; then, a simple computation shows that its image is precisely $d_{R'}(a)$:

$$f(d_R(b)) = (f \circ d_R)(b) = (d_{R'} \circ f)(b) = d_{R'}(f(b)) = d_{R'}(a)$$

and so $d_{R'}(a) \in \mathrm{Im}(f)$.

c) We know that

$$\begin{aligned} \overline{f} : R/\mathrm{Ker}(f) &\longrightarrow \mathrm{Im}(f) \\ \overline{a} &\longmapsto \overline{f}(\overline{a}) = f(a) \end{aligned}$$

is indeed an isomorphism; we need to check if it preserves the derivations. If we denote the derivation over the quotient ring $\widetilde{d}$ (which is given by **Proposition 1.2**), we need to see that $\overline{f} \circ \widetilde{d} = d_{R'} \circ \overline{f}$ , but it is straightforward to prove because of the definition of $\widetilde{d}$ and $\overline{f}$:

$$\overline{f}(\widetilde{d}(\overline{a})) = \overline{f}(\overline{d_R(a)}) = f(d_R(a)) = d_{R'}(f(a)) = d_{R'}(\overline{f}(\overline{a})) \quad \forall\, \overline{a} \in R/\mathrm{Ker}(f)$$

as we wanted to prove.

□

### 1.1.4 Differential ring / field extensions

We have already stated the concept of differential extension. However, let's remind it.

**Definition 1.6.** *Let $R$ be a differential ring (field).*

*A* ***differential ring (field) extension of*** *$R$ is a differential ring (field) $T$ such that*

*a)* $R \subseteq T$

*b)* $d_T\Big|_R = d_R$

*A* ***differential subring (subfield) of*** *$R$ is a subring (subfield) $S$ which is closed under the derivation over $R$, $d_R(S) \subseteq S$.*

Some examples of differential extensions and differential subrings (subfields) are given below.

**Examples 1.3.**

*1)* We already know, from **Proposition 1.1**, that if $R$ is a differential integral domain, $Q(R)$ is a differential ring extension of $R$; moreover, the extension of $d_R$ to $Q(R)$ is unique.

*2)* Consider the differential field $\left(F, \frac{d}{dt}\right)$ being $F = \mathbb{R}(t)\langle e^t \rangle$.
Then $L = \mathbb{R}(t)$ is a differential subfield, since $d(L) \subseteq L$.
Also, the ideal $I = (e^t)$ is a differential ideal of $L[e^t]$ because of the same reason, $d(I) \subseteq I$, and so $(e^t) = (e^t)_d$.

In this case, the set of constants is $C_F = \mathbb{R}$.

*3)* Now, let's consider the differential field $K = \mathbb{C}(z)$ with the usual derivation $\frac{d}{dz}$. We will adjoint to $K$ the function $e^{z^2}$ to obtain a new differential field $L$, extension of $K$; that is, remembering **Examples 1.2**, we consider

$$L = \mathbb{C}(z)\langle e^{z^2} \rangle = Q(\mathbb{C}(z)\{e^{z^2}\}) = \left\{ \textit{differential rational functions of } e^{z^2} \right\} =$$

$$= \left\{ \frac{a_{00} + \sum_{j=0}^{n} \sum_{k=1}^{m_j} a_{jk} \left( \frac{d^j}{dz^j}(e^{z^2}) \right)^k}{b_{00} + \sum_{j=0}^{\widetilde{n}} \sum_{k=1}^{\widetilde{m}_j} b_{jk} \left( \frac{d^j}{dz^j}(e^{z^2}) \right)^k} \;\middle|\; n, m_j, \widetilde{n}, \widetilde{m}_j \in \mathbb{N} \;,\; a_{ij}, b_{ij} \in \mathbb{C}(z) \right\}$$

Noticing that $\frac{d^j}{dz^j}(e^{z^2}) = p_j(z)\cdot e^{z^2}$, where $p_j(z)\in\mathbb{C}[z]$ is a polynomial of degree $j$, we can rewrite $L$ as

$$L = \left\{ \frac{\widetilde{a}_{00} + \sum_{j=0}^{n}\sum_{k=1}^{m_j}\widetilde{a}_{jk}\left(e^{z^2}\right)^k}{\widetilde{b}_{00} + \sum_{j=0}^{\widetilde{n}}\sum_{k=1}^{\widetilde{m}_j}\widetilde{b}_{jk}\left(e^{z^2}\right)^k} \;\middle|\; n, m_j, \widetilde{n}, \widetilde{m}_j \in \mathbb{N}\ ,\ \widetilde{a}_{ij}, \widetilde{b}_{ij} \in \mathbb{C}(z) \right\} =$$

$$= \left\{ \frac{\sum_{k=0}^{m}\widetilde{a}_k\left(e^{z^2}\right)^k}{\sum_{k=0}^{\widetilde{m}}\widetilde{b}_k\left(e^{z^2}\right)^k} \;\middle|\; m, \widetilde{m}\in\mathbb{N}\ ,\ \widetilde{a}_i, \widetilde{b}_i \in \mathbb{C}(z) \right\} = \mathbb{C}(z)(e^{z^2}) = \mathbb{C}(z, e^{z^2})$$

$$L = \mathbb{C}(z)\langle e^{z^2}\rangle = \mathbb{C}(z, e^{z^2})$$

Since we are interested in field extensions for our purposes, we are going to set two remarcable properties concerning both **algebraic** and **transcendental** field extensions, respectively. Before doing that, we need the following well-known result.

**Theorem 1.3.**

*Let $K \subseteq L$ be a field extension.*
*Then there exists a family $\{\alpha_i\}_{i\in I}$ of algebraically independent elements of $L$ such that the extension*

$$K(\{\alpha_i\}_{i\in I}) \subseteq L$$

*is algebraic, and the elements $\alpha_i$ are transcendental over $K$,*

$$K \subseteq K(\{\alpha_i\}_{i\in I}) \overset{\alpha_i \leftrightarrow x_i}{\cong} Quot(K[x_i]_{i\in I})$$

*In the case were $I$ is finite, we define the transcendence degree of the extension as*

$$\mathrm{trdeg}(L/K) \equiv |I|$$

**Theorem 1.4** (Extending derivation over fields)**.**

*Let $K$ be a differential field (of characteristic 0), and $K \subseteq L$ a field extension. Suppose that the extension has a finite transcendence degree, and let $\{x_1, ..., x_n\} \subseteq L$ be a transcendence basis. Then*

*a) For all $y_1, ..., y_n \in L$, there is a unique derivation*[4] *$\widetilde{d} : K[x_1, ..., x_n] \longmapsto L$ extending the one on $K$ and having the property*

$$\widetilde{d}(x_i) = y_i \quad \forall\ i = 1, ..., n$$

*This derivation $\widetilde{d}$ can also be extended on $K(x_1, ..., x_n)$ in a unique way.*

*b) $K(x_1, ..., x_n) \subseteq L$ is algebraic, so the derivation over $K(x_1, ..., x_n)$ extends uniquely to $L$.*

[4] We have defined a derivation over a ring $R$ as an application from $R$ to itself with two properties: linearity and Leibniz's rule. In this case we call $\widetilde{d}$ a derivation in the sense that only the two properties hold.

*Proof.*

a) The idea is quite the same as the one of **Theorem 1.1**. The definition

$$\begin{aligned} \widetilde{d}: K[x_1,...,x_n] &\longrightarrow L \\ a &\longmapsto \widetilde{d}(a) \equiv d_K(a) \quad \forall\, a \in K \\ x_i &\longmapsto \widetilde{d}(x_i) = y_i \end{aligned}$$

determines the derivation totally, because if $p \in K[x_1,...,x_n]$, then

$$p = \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}\ , \quad a_{k_1,\dots,k_n} \in K$$

and so

$$\begin{aligned} \widetilde{d}(p) &= \widetilde{d}\left(\sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}\right) = \\ &= \sum_{k_1,\dots,k_n} \widetilde{d}(a_{k_1,\dots,k_m}) x_1^{k_1} \cdots x_n^{k_n} + \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} \widetilde{d}(x_1^{k_1} \cdots x_n^{k_n}) = \\ &= \sum_{k_1,\dots,k_n} d_K(a_{k_1,\dots,k_n}) x_1^{k_1} \cdots x_n^{k_n} + \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} \left[\sum_{i=1}^n x_1^{k_1} \cdots x_{i-1}^{k_{i-1}} \cdot \widetilde{d}(x_i^{k_i}) \cdot x_{i+1}^{k_{i+1}} \cdots x_n^{k_n}\right] = \\ &= \sum_{k_1,\dots,k_n} d_K(a_{k_1,\dots,k_n}) x_1^{k_1} \cdots x_n^{k_n} + \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} \left[\sum_{i=1}^n x_1^{k_1} \cdots x_{i-1}^{k_{i-1}} \cdot k_i(x_i^{k_i-1}) \cdot x_{i+1}^{k_{i+1}} \cdots x_n^{k_n} \widetilde{d}(x_i)\right] = \\ &= \sum_{k_1,\dots,k_n} d_K(a_{k_1,\dots,k_n}) x_1^{k_1} \cdots x_n^{k_n} + \sum_{i=1}^n \left(\sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_{i-1}^{k_{i-1}} \cdot k_i(x_i^{k_i-1}) \cdot x_{i+1}^{k_{i+1}} \cdots x_n^{k_n}\right) \widetilde{d}(x_i) \end{aligned}$$

With the observation

$$\sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_{i-1}^{k_{i-1}} \cdot k_i(x_i^{k_i-1}) \cdot x_{i+1}^{k_{i+1}} \cdots x_n^{k_n} = \frac{\partial p}{\partial x_i}$$

and the notation

$$\sum_{k_1,\dots,k_n} d_K(a_{k_1,\dots,k_n}) x_1^{k_1} \cdots x_n^{k_n} \equiv p_{d_K}$$

we can rewrite $\widetilde{d}(p)$ as

$$\widetilde{d}(p) = p_{d_K} + \sum_{i=1}^n \frac{\partial p}{\partial x_i} \widetilde{d}(x_i)$$

completely determined by $\widetilde{d}(a_{k_1,\dots,k_n}) = d_K(a_{k_1,\dots,k_n})$ and $\widetilde{d}(x_i) = y_i$. This also proves its uniqueness.

Finally, the property on $K(x_1,...,x_n)$ holds by an argument similar to the proof of **Proposition 1.1**, since $K(x_1,...,x_n) = Quot(K[x_1,...,x_n])$.

b) <u>Finite case:</u> Suppose first that the extension is a finite one. Since our fields are of characteristic 0, from Galois' Theory we know that the extension is simple, that is, there exists $\alpha \in L$ such that

$$L = K(x_1, ..., x_n)(\alpha) = K'(\alpha)$$

where $K' \equiv K(x_1, .., x_n)$ is the differential field from the first part of this theorem, with derivation $d_{K'}$.
To prove the result, we will slightly modify the arguments given in **Theorem 1.1**: let's define

$$\widetilde{d} : K'[x] \xrightarrow{d_1} L[x] \xrightarrow{\text{av}_\alpha} L$$

with

$$\begin{aligned} d_1 : K'[x] &\longrightarrow L[x] \\ a &\longmapsto d_1(a) \equiv d_{K'}(a) \quad \forall\, a \in K' \\ x &\longmapsto d_1(x) = -\text{Irr}_{d_{K'}}(\alpha, K')(x) \cdot q(x) \end{aligned}$$

where

$$\text{Irr}_{d_{K'}}(\alpha, K')(x) = d_{K'}(a_0) + d_{K'}(a_1)x + \cdots + d_{K'}(a_{n-1})x^{n-1}$$

and $q(x) \in K'[x]$ is such that

$$\text{Irr}(\alpha, K')(x) \cdot p(x) + \text{Irr}(\alpha, K')'(x) \cdot q(x) = 1$$

With an argument similar to the one given in section (a) of **Theorem 1.1**, $d_1 : K'[x] \longrightarrow L[x]$ is a derivation. So, for $a(x), b(x) \in K'[x]$, $\widetilde{d} = \text{av}_\alpha \circ d_1$ satisfies

$$\begin{cases} \widetilde{d}(a(x)b(x)) = \text{av}_\alpha\Big(d_1(a(x)b(x))\Big) = \text{av}_\alpha\Big(d_1(a(x))b(x) + a(x)d_1(b(x))\Big) = \\ \qquad = \widetilde{d}(a(x))b(\alpha) + a(\alpha)\widetilde{d}(b(x)) \\ \widetilde{d}(a(x) + b(x)) = \text{av}_\alpha\Big(d_1(a(x) + b(x))\Big) = \text{av}_\alpha\Big(d_1(a(x)) + d_1(b(x))\Big) = \\ \qquad = \widetilde{d}(a(x)) + \widetilde{d}(b(x)) \end{cases}$$

Now, we would like to extend this derivation $\widetilde{d} : K'[x] \longrightarrow L$ to the quotient field, by defining

$$\begin{aligned} \overline{d} \ : K'[x] \Big/ (\text{Irr}(\alpha, K')(x)) &\longrightarrow \qquad L \\ \overline{a(x)} \qquad &\longmapsto \overline{d}(\overline{a(x)}) = \widetilde{d}(a(x)) \end{aligned}$$

From the previous properties of $\widetilde{d}$, $\overline{d}$ is indeed a derivation; we only need to prove that in this case it is well-defined, that is, $(\text{Irr}(\alpha, K')(x)) \subseteq \text{Ker}(\widetilde{d})$: let $h(x) \in K'[x]$; then

$$\widetilde{d}(\text{Irr}(\alpha, K')(x) \cdot h(x)) = \widetilde{d}(\text{Irr}(\alpha, K')(x))h(\alpha) + \underbrace{\text{Irr}(\alpha, K')(\alpha)}_{=0}\widetilde{d}(h(x))$$

so we only need to show that $\widetilde{d}(\text{Irr}(\alpha, K')(x)) = 0$, but this calculation is straightforward:

$$\begin{aligned} \widetilde{d}(\text{Irr}(\alpha, K')(x)) &= \text{Irr}_{d_{K'}}(\alpha, K')(\alpha) + \text{Irr}(\alpha, K')'(\alpha) \cdot \widetilde{d}(x) = \\ &= \text{Irr}_{d_{K'}}(\alpha, K')(\alpha) - \text{Irr}(\alpha, K')'(\alpha) \cdot \text{Irr}_{d_{K'}}(\alpha, K')(\alpha) \cdot q(\alpha) = \\ &= \text{Irr}_{d_{K'}}(\alpha, K')(\alpha) \underbrace{\Big[1 - \text{Irr}(\alpha, K')'(\alpha) \cdot q(\alpha)\Big]}_{=\text{Irr}(\alpha, K')(\alpha) \cdot p(\alpha) = 0} = 0 \end{aligned}$$

Hence, we have a derivation $\overline{d} : K'[x] \big/ (\mathrm{Irr}(\alpha, K')(x)) \longrightarrow L$. For $\overline{a(x)}, \overline{b(x)} \in K'[x] \big/ (\mathrm{Irr}(\alpha, K')(x))$, we have

$$\begin{cases} \overline{d}(\overline{a(x)} \cdot \overline{b(x)}) = \overline{d}(\overline{a(x)}) \cdot b(\alpha) + a(\alpha) \cdot \overline{d}(\overline{b(x)}) \\ \overline{d}(\overline{a(x)} + \overline{b(x)}) = \overline{d}(\overline{a(x)}) + \overline{d}(\overline{b(x)}) \end{cases}$$

Finally, we define a derivation over $K'(\alpha)$ taking advantage of the differential structure over $K'[x] \big/ (\mathrm{Irr}(\alpha, K')(x))$ and the isomorphism given by the First Isomorphism Theorem

$$K'(\alpha) \cong^{\overline{f}} K'[x] \big/ (\mathrm{Irr}(\alpha, K')(x))$$

So, we define a derivation $d_{K'(\alpha)}$ which makes the following diagram commutative:

$$\begin{array}{ccc} K'(\alpha) & \xrightarrow{\ \overline{f}\ } & K'[x] \big/ (\mathrm{Irr}(\alpha, K')(x)) \\ & \searrow^{d_{K'(\alpha)}} & \downarrow \overline{d} \\ & & L \end{array}$$

It is straightforward to see that this defines a derivation, and it is indeed unique, extending the one in $K'$.

<u>General case:</u> We can write $L$ as

$$L = \bigcup_{K' \underset{\text{finite}}{\subseteq} F \subseteq L} F$$

The inclusion $\supseteq$ is trivial. To prove the other one considers $\alpha \in L$: it's obvious that $\alpha \in K'(\alpha)$, and $K' \underset{\text{finite}}{\subseteq} K'(\alpha) \subseteq L$, so

$$\alpha \in \bigcup_{K' \underset{\text{finite}}{\subseteq} F \subseteq L} F$$

Now, let's define a derivation $\widetilde{d}$ over $L$. Given $\alpha \in L$, we define

$$\widetilde{d}(\alpha) \equiv d_F(\alpha) \quad \text{if } \alpha \in F \ , \ K' \subseteq F \text{ finite}$$

· It is well defined, since $\alpha \in F$ for some $F$ with $K' \subseteq F$ finite (from our previous observation); also, if $\alpha \in F_1, F_2$ with $K \subseteq F_1, F_2$ both finite, then $\alpha \in F_1 \cap F_2$ with $K \subseteq F_1 \cap F_2$ finite also, and from the finite case (unicity of the derivation),

$$d_{F_1 \cap F_2} = d_{F_1}\Big|_{F_1 \cap F_2} = d_{F_2}\Big|_{F_1 \cap F_2} \qquad \text{so} \qquad d_{F_1}(\alpha) = d_{F_2}(\alpha) = \widetilde{d}(\alpha$$

· $\widetilde{d}$ is obviously a derivation.
· It is also clear that $\widetilde{d}\Big|_K = d_K$, since $K \subseteq K$ is trivially finite.
· Because be have unicity in the finite case, this derivation $\widetilde{d}$ is also unique: consider another derivation $D$; then, for $\alpha \in L$,

$$D(\alpha) = D\Big|_{K(\alpha)}(\alpha) \underset{\text{unicity}}{=} d_{K(\alpha)}(\alpha) = \widetilde{d}(\alpha) \qquad \text{so} \qquad D = \widetilde{d}$$

□

**Examples 1.4.**

*1)* Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$, with $K = \mathbb{Q}$ provided with the trivial derivation (the only one we can provide over $K$), and $\alpha \in \overline{\mathbb{Q}}$.

Then, by uniqueness, the only derivation we can provide to $L = \mathbb{Q}(\alpha)$ is also the trivial one.

*2)* Consider the differential ring $K = \mathbb{R}(x)$ with the usual derivation

$$\begin{cases} d_K(a) = 0 \quad \forall\ a \in \mathbb{R} \\ d_K(x) = 1 \end{cases}$$

Let's now consider the element $\alpha = \sqrt[n]{x}$, for $n \geq 2$. It is algebraic over $\mathbb{R}(x)$, since the polynomial

$$y^n - x \in \mathbb{R}(x)[y]$$

has $\alpha$ as one of its roots. We can, in addition, say more: this polynomial is irreducible because of Eisenstein's criterion ($x \in \mathbb{R}[x]$ is a prime element). Then

$$\mathrm{Irr}(\sqrt[n]{x}, \mathbb{R}(x))(y) = y^n - x$$

So the only derivation we can provide to $L = \mathbb{R}(x, \sqrt[n]{x})$ is defined through

$$\begin{cases} d_L(a) = 0 \quad \forall\ a \in \mathbb{R} \\ d_L(x) = 1 \\ d_L(\sqrt[n]{x}) = -\frac{\mathrm{Irr}_{d_K}(\alpha,K)(\sqrt[n]{x})}{\mathrm{Irr}(\alpha,K)'(\sqrt[n]{x})} = -\frac{-1}{ny^{n-1}}\Big|_{\sqrt[n]{x}} = \frac{1}{n(\sqrt[n]{x})^{n-1}} \end{cases}$$

*3)* Take $K = \mathbb{R}(x)$ with the usual derivation. Let $y$ be an indeterminate (transcendental element over $K$) and consider the field extension

$$K = \underbrace{\mathbb{R}(x)}_{dif.field} \subseteq \mathbb{R}(x, y) = L$$

· From **Theorem 1.4**, we can define a derivation over $L$ through $\widetilde{d}(y) = \frac{1}{x}$. Intuitively, we are adjoining the natural logarithm $\ln(x)$ on $K$ with the usual derivation: $L = \mathbb{R}(x, \ln(x))$.
· Also from **Theorem 1.4**, we can define a derivation over $L$ through $\widetilde{d}(y) = 2xy$. Intuitively, we are adjoining the exponential function $e^{x^2}$ on $K$ with the usual derivation: $L = \mathbb{R}(x, e^{x^2})$.

## 1.2 An introduction to tensor product of algebras

In this section we are going to review some concepts concerning the tensor product of two $K$-algebras, being $K$ a field. Recall that a $K$-algebra is a vector space $R$ over $K$ equipped with a compatible notion of multiplication of elements of $R$; for example if we have $K$ a (differential) field and $K \subseteq R$ an extension of (differential) rings, then $R$ is a $K$-algebra.

We are interested in study the tensor product of two $K$-algebras $A$, $B$, denoted by $A \otimes_K B$. It is well known that, if we have a basis of $A$ as a $K$-vector space $\{a_i | i \in I\}$ and a basis of $B$ as a $K$-vector space $\{b_j | j \in J\}$, then the set $\{a_i \otimes b_j | i \in I, j \in J\}$ forms a basis of $A \otimes_K B$ as a $K$-vector space, and so the set

$$A \otimes_K B = \Big\{ \sum_{i,j} \lambda_{ij} a_i \otimes b_j | \lambda_{ij} \in K, i \in I, j \in J \Big\}$$

is again a $K$-vector space; furthermore, we can give to the tensor product the structure of a $K$-algebra if we define a product over $A \otimes_K B$ given by

$$\begin{array}{ccc} \cdot : A \otimes_K B \times A \otimes_K B & \longrightarrow & A \otimes_K B \\ \Big( (\sum_{i,j} \lambda_{ij} a_i \otimes b_j), (\sum_{k,l} \mu_{kl} a_k \otimes b_l) \Big) & \longmapsto & \sum_{i,j,k,l} \lambda_{ij} \mu_{kl} (a_i a_k) \otimes (b_j b_l) \end{array}$$

With that structure over $A \otimes_K B$, there are two natural morphisms from $A$, $B$ to $A \otimes_K B$ given by

$$\begin{array}{rcl} \phi_A : A & \longrightarrow & A \otimes_K B \\ a & \longmapsto & a \otimes 1 \end{array} \qquad \begin{array}{rcl} \phi_B : B & \longrightarrow & A \otimes_K B \\ b & \longmapsto & 1 \otimes b \end{array}$$

Finally, if we have a differential structure over $K$ (given by a derivation $d_K$) and over $A$ and $B$ (with derivations $d_A$, $d_B$ respectively, with $d_{A|K} = d_{B|K} = d_K$), we can also give to $A \otimes_K B$ a differential structure, given by the derivation

$$\begin{array}{rcl} d = d_A \otimes d_B : A \otimes_K B & \longrightarrow & A \otimes_K B \\ a \otimes b & \longmapsto & d(a \otimes b) \equiv d_A(a) \otimes b + a \otimes d_B(b) \end{array}$$

and extending it by linearity. It is a simple exercice to prove that $d$ is well defined, and it is indeed a derivation on $A \otimes_K B$. In fact, this differential structure converts the previous morphisms $\phi_A, \phi_B$ into differential morphisms.

We are going to use these results in order to prove some important theorems, like uniqueness of Picard-Vessiot extensions[5].

## 1.3 A brief introduction into Linear Differential Equations

We now have the concept of differential rings and fields, and we have given some important results about this differential theory, such as methods of extending derivations, or the study of differential quotient rings / fields through differential ideals.

We have also given some illustrative examples, in order to clarify our thoughts and ideas, and have a better understanding of the situation.

In this section we will define our key actor: linear differential operators $\mathcal{L} \in K[d]$.

Instead of doing a big discussion about them, we will only give a definition of where these operators "live", and after that we will focus on some results about the solutions of their associated linear differential equation $\mathcal{L}(y) = 0$, such as their linear independence as well as the structure of the set consisting of all of them.

In all this section, $K$ will represent a differential field (of characteristic 0) with derivation $d$.
We will also denote the derivation acting on an element $a \in K$ as $d^n(a) \equiv a^{(n)}$.

[5]See **Section 2.2. Uniqueness**.

### 1.3.1 The ring of linear differential operators

**Definition 1.7.** *A **linear differential operator** $\mathcal{L}$ **of order** $n$ is a polynomial in $d$ with coefficients in $K$*

$$\mathcal{L} = a_0 + a_1 d + \cdots + a_n d^n \quad \text{with } a_i \in K \quad \forall\ i$$

*which acts on $K$*

$$\begin{aligned} \mathcal{L} : K &\longrightarrow K \\ y &\longmapsto \mathcal{L}(y) \end{aligned}$$

*We then define the **ring of linear differential operators** as*

$$K[d] = \{\mathcal{L} \mid \mathcal{L} \text{ is a linear dif. operator over } (K, d)\}$$

*We associate to each $\mathcal{L}$ the equation $\mathcal{L}(y) = 0$,*

$$a_0 y + a_1 y' + \cdots + a_n y^{(n)} = 0 \quad \textbf{a homogeneous linear differential equation}$$

From now on, we will consider homogeneous linear differential equations (HLDE's) over a differential field $K$, with field of constants $C_K$. The reason to consider only HLDE's is that every LDE can be transformed into a homogeneous one, just deriving it once:

$$a_0 + a_1 y + a_2 y' + \cdots + a_n y^{(n-1)} + a_{n+1} y^{(n)} = 0 \quad \text{with } a_0 \neq 0$$

dividing it by $a_0$,

$$1 + \frac{a_1}{a_0} y + \frac{a_2}{a_0} y' + \cdots + \frac{a_n}{a_0} y^{(n-1)} + \frac{a_{n+1}}{a_0} y^{(n)} = 0$$

and now deriving,

$$\left(\frac{a_1}{a_0}\right)' y + \left[\frac{a_1}{a_0} + \left(\frac{a_2}{a_0}\right)'\right] y' + \cdots + \left[\frac{a_n}{a_0} + \left(\frac{a_{n+1}}{a_0}\right)'\right] y^{(n)} + \frac{a_{n+1}}{a_0} y^{(n+1)} = 0$$

a HLDE. Furthermore, if $y$ is a solution of the first one, it is also a solution of its homogeneous equation.

### 1.3.2 Studying the set of solutions of $\mathcal{L}(y) = 0$

It is well known that, if we have a differential extension $K \subseteq L$ and a linear differential operator $\mathcal{L} \in K[d]$, the set of solutions of $\mathcal{L}(y) = 0$ in $L$, denoted by $\text{Sol}(\mathcal{L})_L$, is a $C_L$ - vector space, where $C_L$ is the set of constants of $L$, which is also a field.
Moreover, we will prove that its dimension is at most equal to the order of the operator $\mathcal{L}$, $n$. To do so, we need to define what is called the Wronskian.

**Definition 1.8.** *Let $K$ be a differential field, and let $y_1, ..., y_n \in K$. We define the Wronskian of $y_1, ..., y_n$, $W(y_1, ..., y_n)$, as the determinant*

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

With this formalism, we have the following results.

**Proposition 1.3.** *If we have $y_1, ..., y_n \in K$, then*

$$y_1, ..., y_n \text{ are linearly independent over } C_K \iff W(y_1, ..., y_n) \neq 0$$

*Proof.* $\boxed{\Longleftarrow}$ Suppose that $y_1, ..., y_n$ are linearly dependent over $C_K$, that is, there exist $c_1, ..., c_n \in C_K$ not all 0 such that

$$c_1 y_1 + c_2 y_2 + \cdots + c_n y_n = 0$$

Since the $c_i$ are constants, we can differentiate the equality up to $n-1$ times, to get

$$\begin{cases} c_1 y_1 + c_2 y_2 + \cdots + c_n y_n = 0 \\ c_1 y_1' + c_2 y_2' + \cdots + c_n y_n' = 0 \\ \vdots \\ c_1 y_1^{(n-1)} + c_2 y_2^{(n-1)} + \cdots + c_n y_n^{(n-1)} = 0 \end{cases}$$

or, in matrix notation,

$$\begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Since the $c_i$ are not all 0, we must have $W(y_1, ..., y_n) = 0$, which is a contradiction, so $y_1, ..., y_n$ are linearly independent over $C_K$.

$\boxed{\Longrightarrow}$ We proceed by induction over $n$. The case $n = 1$ is trivial. So, assume that for all $z_1, ..., z_{n-1} \in K$ $C_K$-linearly independent we have $W(z_1, ..., z_{n-1}) \neq 0$.

Suppose now that $y_1, ..., y_n$ are $C_K$-linearly independent, but $W(y_1, ..., y_n) = 0$. Then the system

$$\begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

has a non-trivial solution $(\alpha_1, ..., \alpha_n) \in K^n$. Let $\alpha_i \neq 0$. By dividing the previous system by $\alpha_i$ and changing indices, we can assume without loss of generality $\alpha_1 = 1$. We have, for $0 \leq k \leq n-1$,

$$y_1^{(k)} + y_2^{(k)} \alpha_2 + \cdots + y_n^{(k)} \alpha_n = 0$$

and by deriving this equation for $0 \leq k \leq n-2$, we obtain

$$\underbrace{\left(y_1^{(k+1)} + y_2^{(k+1)} \alpha_2 + \cdots + y_n^{(k+1)} \alpha_n\right)}_{\text{is 0 by the preceding equation}} + \left(y_2^{(k)} \alpha_2' + \cdots + y_n^{(k)} \alpha_n'\right) = 0$$

$$y_2^{(k)} \alpha_2' + \cdots + y_n^{(k)} \alpha_n' = 0$$

Hence, $(\alpha'_2, ..., \alpha'_n) \in K^{n-1}$ is a solution for the system

$$\begin{pmatrix} y_2 & \cdots & y_n \\ y'_2 & \cdots & y'_n \\ \vdots & \ddots & \vdots \\ y_2^{(n-2)} & \cdots & y_n^{(n-2)} \end{pmatrix} \begin{pmatrix} x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

In particular,

$$y_2\alpha'_2 + \cdots + y_n\alpha'_n = 0$$

But $y_2, ..., y_n$ are $C_K$-linearly independent (by hypothesis), so $W(y_2, ..., y_n) \neq 0$ (by induction hypothesis), and so the solution of this system is trivial: $\alpha'_i = 0$ for $i = 2, ..., n$.
So $\alpha_i \in C_K$ for $i = 1, ..., n$ (remember $\alpha_1 = 1$) but we also have

$$y_1 + \alpha_2 y_2 + \cdots + \alpha_n y_n = 0$$

a contradiction. □

It is important to notice that the condition to have a non-zero Wronskian does not depend on the field we are working from.

**Proposition 1.4.** *Let $y_1, ..., y_{n+1}$ be solutions of $\mathcal{L}(y) = 0$ in $L$, having $\mathcal{L}$ degree $n$.*
*Then $W(y_1, ..., y_{n+1}) = 0$.*

*Proof.* Let's write $\mathcal{L}(y) = a_0 y + a_1 y' + \cdots + y^{(n)}$; then

$$\begin{cases} a_0 y_1 + a_1 y'_1 + \cdots + y_1^{(n)} = 0 \\ a_0 y_2 + a_1 y'_2 + \cdots + y_2^{(n)} = 0 \\ \qquad\vdots \\ a_0 y_{n+1} + a_1 y'_{n+1} + \cdots + y_{n+1}^{(n)} = 0 \end{cases} \Longrightarrow \begin{cases} y_1^{(n)} = -a_0 y_1 - a_1 y'_1 - \cdots - a_{n-1} y_1^{(n-1)} \\ y_2^{(n)} = -a_0 y_2 - a_1 y'_2 - \cdots - a_{n-1} y_2^{(n-1)} \\ \qquad\vdots \\ y_{n+1}^{(n)} = -a_0 y_{n+1} - a_1 y'_{n+1} - \cdots - a_{n-1} y_{n+1}^{(n-1)} \end{cases}$$

the last row of the Wronskian is a linear combination of the other rows, so $W(y_1, ..., y_{n+1}) = 0$. □

From these results, we can deduce that the set of solutions of $\mathcal{L}(y) = 0$ in $L$ has at most $n$ linearly independent solutions over $C_L$.

In the case of having exactly $n$ solutions in $L$ linearly independent over $C_L$, say $\{y_1, ..., y_n\}$, we will name this set of solutions a **fundamental set of solutions of $\mathcal{L}(y) = 0$ in $L$**.
Here, any other solution of $\mathcal{L}(y) = 0$ will be a $C_L$ - linear combination of these fundamental solutions $y_1, ..., y_n$. This property will play a fundamental role on studying the Picard-Vessiot extensions of $\mathcal{L}(y) = 0$ in the next chapter.

# Chapter 2

# Picard-Vessiot extensions

In this chapter we are going to work with linear differential operators $\mathcal{L}$ with coeficients in $K$, having exactly $n$ solutions in a differential extension $K \subseteq L$ linearly independent over $C_L$, denoted by $y_1, ..., y_n$, with $n$ denoting the degree of the operator $\mathcal{L}$.
Let's recall a crucial property involving the set of solutions of $\mathcal{L}$ in $L$:

Any other solution of $\mathcal{L}(y) = 0$ will be a $C_L$ - linear combination of these fundamental solutions $y_1, ..., y_n$:

$$\text{Sol}(\mathcal{L})_L = C_L \cdot y_1 \oplus C_L \cdot y_2 \oplus \cdots \oplus C_L \cdot y_n$$

That is, $Sol(\mathcal{L})_L$ is a $C_L$ - vector space generated by a fundamental set of solutions.

Here is an example that motivates the definition of what a Picard-Vessiot extension is.

**Example 2.1.** Let $K = \mathbb{C}(x)$ with the usual derivation $d = \frac{d}{dx}$. Let $\mathcal{L}(y) = y' - y$.
The element $e^x$ is a solution of the previous LDE, $\mathcal{L}(e^x) = 0$, and since the operator $\mathcal{L}$ has degree 1, the set of solutions here is

$$\text{Sol}(\mathcal{L})_L = C_L \cdot e^x \qquad \text{with } L = K\langle e^x\rangle = \mathbb{C}(x, e^x) \text{ and } C_L = C_K = \mathbb{C}$$

that is,

$$Sol(\mathcal{L})_L = \mathbb{C} \cdot e^x$$

which is clearly a $\mathbb{C}$ - vector space. Notice that here we have $C_K = C_L$.

We can, however, consider the same operator $\mathcal{L}$ thought with coeficients in $L$, and adjoin an indeterminate $z$ with derivation $z' = z$ (since $z$ is transcendental, **Theorem 1.4** guarantees us that this derivation is well defined).
Then, $F = L\langle z\rangle = \mathbb{C}(e^x)(z)$ contains two solutions of $\mathcal{L}(y) = 0$ that are not $C_F$ - linearly independent, since $\mathcal{L}$ has degree 1. More precisely, since it is easy to see that the element $\frac{e^x}{z}$ is a constant, we get the dependence of $e^x$ and $z$ through

$$e^x - \frac{e^x}{z} z = 0 \qquad 1, -\frac{e^x}{z} \in C_F$$

The clue here is the fact that we have

$$C_K = C_L \subsetneq C_F$$

that is, since we already had solutions of $\mathcal{L}(y) = 0$, the adjunction of a superfluous solution has resulted in the appearance of new constants in the extension, which leads to a $C_F$ - linear dependence of the solutions.

We can now define the Picard-Vessiot extensions, which are the analogous of the splitting fields of a polynomial in Algebraic Galois Theory.

**Definition 2.1.** *Let $K$ be a differential field, and $\mathcal{L}(y) = 0$ a lineal differential operator with coeficients in $K$ of order $n$.*
*We say that $K \subseteq L$ is a Picard-Vessiot extension of $K$ for $\mathcal{L}$ if*

*1) $\mathcal{L}$ has exactly $n$ solutions in $L$ linearly independent over $C_L$.*

*2) $L$ is generated over $K$, as a differential field, by the solutions of $\mathcal{L}(y) = 0$ in $L$, that is,*

$$L = K\langle y_1, y_2, ..., y_n \rangle$$

*where $\{y_1, ..., y_n\}$ is a fundamental set of solutions of $\mathcal{L}(y) = 0$ in $L$.*

*3) No new constants are added, i.e., $C_K = C_L$.*

From the previous example, it turns out that these are the appropriate extensions to study in Differential Galois Theory, since condition (3) in the definition guarantees its minimality (no superfluous solutions).

From now on in this chapter, we are going to study the existence and unicity of Picard-Vessiot extensions, and to consider some abstract and non-abstract examples in order to become more familiar with the definition.

## 2.1 Existence

**Theorem 2.1** (Existence of Picard-Vessiot extensions)**.**
*Let $K$ be a differential field with algebraically closed set of constants $C_K$. Let $\mathcal{L} \in K[d]$ be a linear differential operator.*

*Then there exists a Picard-Vessiot extension $L$ of $K$ for $\mathcal{L}$.*

We'll prove it by construction and with some steps. Firstly, put

$$\mathcal{L}(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y_1' + a_0 y \quad a_i \in K$$

The idea is to construct a $K$-algebra containing a full set of solutions of $\mathcal{L}(y) = 0$, and then make quotient by a maximal and prime differential ideal in order to get an integral domain. We'll see that its fraction field will not contain new constants.

1) Let's consider the polynomial ring on $n^2$ indeterminates

$$K[\{Y_{0,1}, Y_{0,2}, ..., Y_{0,n}\}, \{Y_{1,1}, Y_{1,2}, ..., Y_{1,n}\}, ..., \{Y_{n-1,1}, Y_{n-1,2}, ..., Y_{n-1,n}\}]$$

$$K[\{Y_{i,j}\}]_{\substack{i=0,...,n-1 \\ j=1,...,n}}$$

We extend the derivation of $K$ over it by defining

$$\begin{cases} Y'_{i,j} \equiv Y_{i+1,j} \quad \forall\ i = 0, ..., n-2 \\ Y'_{n-1,j} = -a_{n-1}Y_{n-1,j} - \cdots - a_1 Y_{1,j} - a_0 Y_{0,j} \end{cases} \quad \forall\ j = 1, ..., n$$

Intuitively, we are constructing solutions of $\mathcal{L}(y) = 0$: from the first set of the definition, we get $Y_{i,j} = Y_{0,j}^{(i)}\ \forall\ i, j$; combining this fact with the second set of the definition, we obtain

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

We can also see this polynomial ring with this differential structure as the quotient of the ring of differential polynomials in $Y_{0,1}, Y_{0,2}, ..., Y_{0,n}$ with the differential ideal generated by the previous linear differential equations, that is,

$$\Big(K[\{Y_{i,j}\}], \mathcal{L}\Big) \overset{\text{notation}}{\equiv} \Big(K[\{Y_{i,j}\}],'\Big) \cong K\{Y_{0,1}, ..., Y_{0,n}\} \Big/ \Big(\mathcal{L}(Y_{0,1}), ..., \mathcal{L}(Y_{0,n})\Big)_d$$

2) Intuitively, in order to convert the set $\{Y_{0,1}, ..., Y_{0,n}\}$ into a fundamental set of solutions of $\mathcal{L}(y) = 0$ they must be linearly independent over the constant field or, equivalently, we must have

$$\det(Y_{i,j}) = W(Y_{0,1}, ..., Y_{0,n}) \neq 0$$

This element is clearly a non-zero element in $K[\{Y_{i,j}\}]$, but we want it to continue being a non-zero element in the field we are constructing. Then, let's consider the algebra obtained by the adjunction of the element $\frac{1}{\det(Y_{i,j})}$ to $K[\{Y_{i,j}\}]$:

$$A \equiv K[\{Y_{i,j}\}]\Big[\frac{1}{\det(Y_{i,j})}\Big]$$

so the Wronskian $\det(Y_{i,j}) = W(Y_{0,1}, ..., Y_{0,n})$ becomes an invertible element on $A$.

3) So far we have defined what is called a **full universal solution algebra** for $\mathcal{L}$,

$$A \equiv K[\{Y_{i,j}\}]\Big[\tfrac{1}{\det(Y_{i,j})}\Big] \cong K\{Y_{0,1}, ..., Y_{0,n}\} \,/I\, \Big[\tfrac{1}{\det(Y_{i,j})}\Big]$$

$$\text{with } I = \Big(\mathcal{L}(Y_{0,1}), ..., \mathcal{L}(Y_{0,n})\Big)_d$$

Let now $J$ be a maximal differential ideal of $A$ (it exists from Zorn's lemma [1]).
Since $K \subseteq A$ is an extension of differential rings, from **Property 1.4** we have that $J$ is also a differential prime ideal, and so from **Property 1.3** $A/J$ becomes an integral domain.
Furthermore, we can also say that $A/J$ has no proper differential ideals: if that was the case, there

[1] See **Section 1.1.2. Study of maximal differential ideals**.

would exist a differential ideal $\overline{I}$ such that $\{\overline{0}\} \subsetneq \overline{I} \subsetneq A/J$; then, going from the quotient $A/J$ to $A$ via $\pi^{-1}$, we obtain

$$\begin{array}{ccccc} J & \subsetneq & \pi^{-1}(\overline{I}) & \subsetneq & A \\ \uparrow{\scriptstyle \pi^{-1}} & & \uparrow{\scriptstyle \pi^{-1}} & & \uparrow{\scriptstyle \pi^{-1}} \\ \{\overline{0}\} & \subsetneq & \overline{I} & \subsetneq & A/J \end{array}$$

and $\pi^{-1}(\overline{I})$ would be a proper differential ideal[2] of $A$ containing $J$, which is impossible.

4) We have already seen that $A/J$ is an integral domain, with no proper differential ideals. So, we can finally consider the fraction field of it

$$L = Quot(A/J)\ ^3$$

We can observe some properties about the field extension $K \subseteq L$:
· It is clearly finitely generated over $K$, as a differential field, by the $n$ solutions of $\mathcal{L}(y) = 0$ $\{Y_{0,1}, ..., Y_{0,n}\}$ and $\frac{1}{\det(Y_{i,j})}$, since $A$ is:

$$L = Quot(A/J) = Quot\Big(K[\{Y_{i,j}\}]\Big[\frac{1}{\det(Y_{i,j})}\Big]\,/J\Big) \cong Quot\Big(\Big(K\{Y_{0,1}, ..., Y_{0,n}\}\,/I\Big)\Big[\tfrac{1}{\det(Y_{i,j})}\Big]\,/J\Big)$$

· Since the Wronskian $\det(Y_{i,j})$ is invertible in $L$, it is non zero, so the set $\{Y_{0,1}, ..., Y_{0,n}\}$ is a fundamental set of solutions of $\mathcal{L}(y) = 0$ in $L$.
· We only need to check that $C_L = C_K$, and $K \subseteq L$ will become a Picard-Vessiot extension of $K$ for $\mathcal{L}$. But this is a consequence of **Proposition 2.1**, which we are going to announce below.

**Proposition 2.1.** *Let $K \subseteq R$ be a differential extension, being $K$ a differential field and $R$ an integral domain, finitely generated as a $K$-algebra, with no proper differential ideals. Suppose that $C_K$ is algebraically closed. Then*

$$C_{Quot(R)} = C_K$$

*i.e. we are adding no constants into the differential structure over $Quot(R)$.*

We are not going to prove it here, because a solid background of algebraic geometry is needed. A proof of it can be found at [1, Chapter 5].

With all this construction, we just have proven the Existence Theorem of Picard-Vessiot extensions.

## 2.2 Uniqueness

In order to prove uniqueness of a Picard-Vessiot extension, we will first prove a property, which will be also useful in furhter results.

[2] We already know that it is a differential ideal, from the study of them in the quotient. See **Section 1.1.2. Differential ideals and quotient rings**.

[3] Since $\det(Y_{i,j})$ is invertible on $A$, we are guaranteed to have $\det(Y_{i,j}) \notin J$, and hence it is a non-zero element in $L$.

**Property 2.1** (Normality property of Picard-Vessiot extensions).

*Let $K \subseteq L_1, L_2$ be Picard-Vessiot extensions for a linear differential operator $\mathcal{L} \in K[d]$ with order $n$, being $d$ the derivation over $K$.*
*Let $K \subseteq E$ be an extension with no new constants, that is $C_E = C_K$, and suppose that there exist injective differential $K$-morphisms*

$$\sigma_1 : \ L_1 \longrightarrow E$$
$$\sigma_2 : \ L_2 \longrightarrow E$$

*Then there exists a differential $K$-isomorphism between $L_1$ and $L_2$.*

*Proof.* We define $V_1 \equiv \mathcal{L}^{-1}(\{0\}) \subseteq L_1$, $V_2 \equiv \mathcal{L}^{-1}(\{0\}) \subseteq L_2$ and $V \equiv \mathcal{L}^{-1}(\{0\}) \subseteq E$.
Then $V_1$ and $V_2$ are $K$-vector spaces of dim $= n$ ($L_1$ and $L_2$ are Picard-Vessiot extensions), and $V$ is a $K$-vector space of dim $\leq n$ ($C_K = C_E$, but $E$ is not a Picard-Vessiot extension, we cannot guarantee equality)[4].
With that, since $\sigma_1(L_1), \sigma_2(L_2) \subseteq E$, we obtain $\sigma_1(V_1), \sigma_2(V_2) \subseteq V$. But $\sigma_1, \sigma_2$ are injective, and so $\sigma_1(V_1), \sigma_2(V_2)$ have also dim $= n$. Since the two are contained in $V$, which has dim $\leq n$, we must have that the three vector spaces coincide:

$$\sigma_1(V_1) = \sigma_2(V_2) = V$$

Furthermore, by definition of Picard-Vessiot extensions, wa can write $L_1 = K\langle V_1 \rangle$, $L_2 = K\langle V_2 \rangle$, and since $\sigma_1, \sigma_2$ are differential $K$-morphisms, we obtain

$$\sigma_1(L_1) = K\langle \sigma_1(V_1) \rangle = K\langle \sigma_2(V_2) \rangle = \sigma_2(L_2)$$

Finally, we obtain the result by restricting $\sigma_1, \sigma_2$ to their images:

$$L_1 \xrightarrow{\sim} \sigma_1(L_1) = \sigma_2(L_2) \xleftarrow{\sim} L_2$$

□

We are now ready to prove uniqueness.

**Theorem 2.2** (Uniqueness of Picard-Vessiot extensions).

*Let $K$ be a differential field with algebraically closed set of constants $C_K$.*
*Let $\mathcal{L} \in K[d]$ be a linear differential operator, and $L_1$, $L_2$ two Picard-Vessiot extensions of $K$ for $\mathcal{L}$. We can assume that $L_1$ is the one constructed in **Theorem 2.1**, that is,*

$$L_1 = Quot(A/J) \qquad being \quad \begin{cases} A = K[\{Y_{i,j}\}]\left[\frac{1}{\det(Y_{i,j})}\right] \\ J = maximal\ differential\ ideal\ of\ A \end{cases}$$

*Then there exists a differential $K$-isomorphism between $L_1$ and $L_2$.*

[4] See **Section 1.3.2. Studying the set of solutions of $\mathcal{L}(y) = 0$.**

*Proof.* Let's consider the differential ring

$$R \equiv A/J \otimes_K L_2 \qquad \text{with derivation defined in } \textbf{Section 1.2.}$$

Since $A/J$ is finitely generated over $K \subseteq L_2$ (we know this for the $4th$ step in the proof of **Theorem 2.1**), $R$ is clearly finitely generated over $L_2$.
We can now do the same construction we made in the $3th$ step in the proof of **Theorem 2.1** to obtain a maximal differential ideal $I \subseteq R$, being $R/I$ an integral domain with no proper differential ideals.
Let's consider the maps

$$\begin{array}{ccccc} A/J & \xrightarrow{\phi_{A/J}} & R & \xrightarrow{\pi} & R/I \\ a & \longmapsto & a \otimes 1 & \longmapsto & \overline{a \otimes 1} \end{array} \qquad \begin{array}{ccccc} L_2 & \xrightarrow{\phi_{L_2}} & R & \xrightarrow{\pi} & R/I \\ b & \longmapsto & 1 \otimes b & \longmapsto & \overline{1 \otimes b} \end{array}$$

· Let's see that the first one is injective: we know that $\phi^{-1}_{A/J}(I)$ is a differential ideal of $A/J$, which has no proper differential ideals, so we must have $\phi^{-1}_{A/J}(I) = A/J$ or $\{0\}$.
If $\phi^{-1}_{A/J}(I) = A/J$, the unity element $1 \otimes 1$ would be in $I$ since $\phi_{A/J}(1) = 1 \otimes 1 \in I$, which would lead to a contradiction ($I = R$, but $I$ is a maximal differential ideal). Then, $\phi^{-1}_{A/J}(I) = \{0\}$.

Let's consider now two elements $a, a' \in A/J$ such that $(\pi \circ \phi_{A/J})(a) = (\pi \circ \phi_{A/J})(a')$, that is,

$$\overline{a \otimes 1} = \overline{a' \otimes 1}$$

$$(a - a') \otimes 1 \in I$$

then $a - a' \in \phi^{-1}_{A/J}(I) = \{0\}$, so $a = a'$ as we wanted to prove.

· The second map is clearly non-zero and, since $L_2$ is a field, it is injective.

We obtain two embeddings

$$A/J \hookrightarrow R/I \qquad\qquad L_2 \hookrightarrow R/I$$

which can be extended to their rational fields ($R/I$ is an integral domain, so we can construct its rational field $E = Quot(R/I)$)

$$\begin{array}{ccc} A/J & \hookrightarrow & R/I \\ \downarrow & & \downarrow \\ L_1 = Quot(A/J) & \hookrightarrow & E = Quot(R/I) \end{array} \qquad\qquad \begin{array}{ccc} L_2 & \hookrightarrow & R/I \\ \downarrow & & \downarrow \\ L_2 & \hookrightarrow & E = Quot(R/I) \end{array}$$

We have obtained two injective differential $K$-morphisms $\sigma_1 : L_1 \longrightarrow E$, $\sigma_1 : L_1 \longrightarrow E$. Moreover, using **Proposition 2.1**, $C_E = C_{Quot(R/I)} = C_{L_2}$ [5], and since $L_2$ is a Picard-Vessiot extension, $C_{L_2} = C_K$. Hence $C_E = C_K$, and by **Property 2.1** we are done.

□

[5] This fact is due to the embedding $L_2 \hookrightarrow R/I \hookrightarrow E = Quot(R/I)$, since $R/I$ is finitely generated over $L_2$ because $R$ is.

## 2.3 Some (abstract) examples

In order to work the concept of Picard-Vessiot extensions, in this section we will treat some examples about that, some of them abstract and others more applied.
From now on, we are going to work with differential fields with algebraically closed set of constants.

### 2.3.1 Adjunction of the integral

Consider a differential field $K$, and let $a \in K$ be an element which is not a derivative of any element, i.e. does not exist $b \in K$ such that $b' = a$.

We can consider the differential equation

$$\tilde{\mathcal{L}}(y) = y' - a = 0, \quad \tilde{\mathcal{L}} \in K[d] \text{ , being } d \text{ the derivation in } K,$$

which has no solution in $K$. Converting it into a homogeneous one, we get

$$\mathcal{L}(y) = y'' - \frac{a'}{a} y' = 0, \quad \mathcal{L} \in K[d]$$

We can, however, take an indeterminate $\alpha$ (transcendental element over $K$) and consider the field extension

$$K \subseteq K(\alpha) = L$$

which is also a differential field extension by defining a derivation over $L$ through $\alpha' = a$ [6].
We shall prove that the extension $K \subseteq K(\alpha) = K\langle 1, \alpha \rangle$ is a Picard-Vessiot extension of $K$ for $\mathcal{L}$:

1. It is clear that $\mathcal{L}$ has exactly 2 solutions in $L$, $\{1, \alpha\}$, which are linearly independent over $C_K$.
2. $L = K\langle 1, \alpha \rangle = K(\alpha)$, being $\{1, \alpha\}$ a fundamental set of solutions of $\mathcal{L}(y) = 0$ in $L$.
3. No new constants are added. Suppose we have a constant element in $L$

   $$\frac{p(\alpha)}{q(\alpha)} = \frac{\sum_{i=0}^{m_1} a_i \alpha^i}{\sum_{j=0}^{m_2} b_j \alpha^j} \quad a_i, b_j \in K \text{ with } a_{m_1} \neq 0, b_{m_2} = 1$$

   We can assume $\gcd(p(X), q(X)) = 1$ with $p(X), q(X) \in K[X]$.

   Then, assuming that $q(\alpha)$ is not a constant itself ($q(\alpha)' \neq 0$), we must have, since $\frac{p(\alpha)}{q(\alpha)}$ is indeed a constant,

   $$0 = \left(\frac{p(\alpha)}{q(\alpha)}\right)' = \frac{p(\alpha)' q(\alpha) - p(\alpha) q(\alpha)'}{q(\alpha)^2} \Longrightarrow \frac{p(\alpha)}{q(\alpha)} = \frac{p(\alpha)'}{q(\alpha)'}$$

   with degree of $q' <$ degree of $q$, which gives a contradiction with $\gcd(p(X), q(X)) = 1$. Then, $q(\alpha)$ must be a constant:

   $$0 = q(\alpha)' = \Big(\sum_{j=0}^{m_2} b_j \alpha^j\Big)' = \Big(b_{m_2} \alpha^{m_2}\Big)' + \Big(b_{m_2-1} \alpha^{m_2-1}\Big)' + \Big(\sum_{j=0}^{m_2-2} b_j \alpha^j\Big)' =$$

   $$= a m_2 \alpha^{m_2-1} + b'_{m_2-1} \alpha^{m_2-1} + (m_2 - 1) b_{m_2-1} a \alpha^{m_2-2} + \underbrace{\Big(\sum_{j=0}^{m_2-2} b_j \alpha^j\Big)'}_{\text{terms of degree } \leq m_2 - 2}$$

[6] Remember **Theorem 1.4**.

Since $\alpha$ is transcendental, the coefficients of $\alpha^j$ must vanish for all $j$, in particular for $j = m_2 - 1$:

$$m_2 a + b'_{m_2-1} = 0 \Longrightarrow a = -\frac{b'_{m_2-1}}{m_2} = \Big(-\frac{b_{m_2-1}}{m_2}\Big)'$$

which is a contradiction, since $a$ is not a derivative of any element in $K$. Hence, no new constants are added.

Finally, we have just proven that the extension $K \subseteq K\langle 1, \alpha\rangle = K(\alpha)$ is a Picard-Vessiot extension of $K$ for $\mathcal{L}(y) = y'' - \frac{a'}{a}y'$.

We can make an observation about this differential equation, which we will study in a general context in the next section. If we consider the "change of variables" induced by the following isomorphism

$$\begin{aligned} \sigma : & L \longrightarrow L \\ & b \longmapsto b \qquad\qquad \forall\, b \in K \\ & \alpha \longmapsto \widetilde{\alpha} = \alpha + c \qquad c \in C_K \text{ a constant} \end{aligned}$$

then the differential equation **remains unchanged**:

$$\mathcal{L}(\alpha) = \alpha'' - \frac{a'}{a}\alpha' = 0 \longrightarrow \mathcal{L}(\widetilde{\alpha}) = \widetilde{\alpha}'' - \frac{a'}{a}\widetilde{\alpha}' = \alpha'' - \frac{a'}{a}\alpha' = \mathcal{L}(\alpha) = 0$$

in other words, the previous automorphism is a **symmetry** of the differential (operator) equation $\mathcal{L}(y) = 0$.

Notice also that our "change of variables" involves a $C_K$ **- linear combination** of $\{1, \alpha\}$, which are the solutions of $\mathcal{L}$ linearly independent over $C_K$.

As we have already said, we will formalise all these concepts in the next chapter.

### 2.3.2 Adjunction of the exponential of the integral

Consider a differential field $K$, and let $a \in K$ be an element such that does not exist $b \in K \backslash \{0\}$ and $n \in \mathbb{Z}\backslash\{0\} \subset \mathbb{Q} \hookrightarrow K$ such that $b' = nab$.

We can consider the differential equation

$$\mathcal{L}(y) = y' - ay = 0, \quad \mathcal{L} \in K[d] \text{ , being } d \text{ the derivation in } K$$

which has no solution in $K$.

We can, however, take an indeterminate $\alpha$ (transcendental element over $K$) and consider the field extension

$$K \subseteq K(\alpha) = L$$

which is also a differential field extension by defining a derivation over $L$ through $\alpha' = a\alpha$ [7].

We shall prove that the extension $K \subseteq K(\alpha) = K\langle\alpha\rangle$ is a Picard-Vessiot extension of $K$ for $\mathcal{L}$:

1. It is clear that $\mathcal{L}$ has exactly 1 solution in $L$, $\{\alpha\}$, which is trivially linearly independent over $C_K$.

[7] Remember **Theorem 1.4**.

2. $L = K\langle\alpha\rangle = K(\alpha)$, being $\{\alpha\}$ a fundamental set of solutions of $\mathcal{L}(y) = 0$ in $L$.

3. No new constants are added; we shall prove it using the same arguments as the example above: suppose we have a constant element in $L$

$$\frac{p(\alpha)}{q(\alpha)} = \frac{\sum_{i=0}^{m_1} a_i \alpha^i}{\sum_{j=0}^{m_2} b_j \alpha^j} \quad a_i, b_j \in K \text{ with } a_{m_1} \neq 0, b_{m_2} = 1$$

   We can assume $\gcd(p(X), q(X)) = 1$ with $p(X), q(X) \in K[X]$.

   Then, assuming that $q(\alpha)$ is not a constant itself ($q(\alpha)' \neq 0$), we must have, since $\frac{p(\alpha)}{q(\alpha)}$ is indeed a constant,

$$0 = \left(\frac{p(\alpha)}{q(\alpha)}\right)' = \frac{p(\alpha)'q(\alpha) - p(\alpha)q(\alpha)'}{q(\alpha)^2} \Longrightarrow \frac{p(\alpha)}{q(\alpha)} = \frac{p(\alpha)'}{q(\alpha)'} \Longrightarrow p(\alpha)q(\alpha)' = p(\alpha)'q(\alpha)$$

   Since $\gcd(p(X), q(X)) = 1$, $q(\alpha)$ has to divide $q(\alpha)'$. Let's write

$$\begin{cases} q(\alpha) = \alpha^{m_2} + b_{m_2-1}\alpha^{m_2-1} + \cdots + b_1\alpha + b_0 \\ q(\alpha)' = am_2\alpha^{m_2} + \left[a(m_2-1)b_{m_2-1} + b'_{m_2-1}\right]\alpha^{m_2-1} + \cdots + \left[ab_1 + b'_1\right]\alpha + b'_0 \end{cases}$$

   so, we must have

$$q(\alpha)' = am_2 q(\alpha)$$

   because $q(\alpha) \mid q(\alpha)'$, with a factor of $am_2$ if we compare the terms of degree $m_2$. But if we compare their independent terms, we obtain

$$b'_0 = am_2 b_0$$

   which is a contradiction with our choice of $a$. Then, $q(\alpha)$ must be a constant. Let's study this case:

$$0 = q(\alpha)' = \Big(\sum_{j=0}^{m_2} b_j\alpha^j\Big)' = \sum_{j=0}^{m_2}\Big(b'_j\alpha^j + jb_j\alpha^{j-1}\alpha'\Big) = \sum_{j=0}^{m_2}\Big(b'_j + jb_j a\Big)\alpha^j$$

   Since $\alpha$ is transcendental, the coefficients of $\alpha^j$ must vanish for all $j$:

$$b'_j = -jb_j a \quad \forall\ j = 0, ..., m_2$$

   which, by hypothesis, has no non-zero solution. This is a contradiction, since $q(X) \in K[X]$ is a non-zero polynomial. Hence, no new constants are added.

Finally, we have just proven that the extension $K \subseteq K\langle\alpha\rangle = K(\alpha)$ is a Picard-Vessiot extension of $K$ for $\mathcal{L}(y) = y' - ay$.

### 2.3.3 A brief study of differential equations over $\mathbb{C}(z)$

Consider the differential field $\mathbb{C}(z)$ provided with the usual derivation $\frac{d}{dz}$. Consider then a differential equation

$$\mathcal{L}(y) = y^{(n)} + a_{n-1}(z)y^{(n-1)} + \cdots + a_1(z)y' + a_0(z)y = 0 \quad , \quad \mathcal{L} \in \mathbb{C}(z)[d]$$

Since $a_i(z) \in \mathbb{C}(z)$ $\forall i = 0, ..., n-1$, they are meromorphic functions, defined over $\mathbb{C}\backslash\{z_{i,0}, ..., z_{i,N_i}\}$, from **Existence and Independence of Solutions** and **Analyticity of Matrix Solutions in a Star**[8] we know that if we take a simply connected bounded open set

$$U \subset \mathbb{C}\backslash\{z_{0,1}, ..., z_{0,N_0}, ..., z_{n-1,1}, ..., z_{n-1,N_{n-1}}\}$$

and initial conditions, there exist $n$ unique linearly independent holomorphic solutions of $\mathcal{L}(y) = 0$ defined in all $U$.

Denote this set of fundamental solutions $\{f_1(z), ..., f_n(z)\}$. We can think these solutions in the ring of holomorphic functions defined over the previous simply connected open set $U$

$$\text{Hol}(U) = \Big\{ f : U \longrightarrow \mathbb{C} \;\Big|\; f \text{ is holomorphic in } U \Big\}$$

We can finally consider the differential extension $\mathbb{C}(z) \subseteq \mathbb{C}(z)\langle f_1, ..., f_n\rangle = L$, extending the derivation over $\mathbb{C}(z)$ in the usual way (considering the usual derivation $\frac{d}{dz}$ on $L$), thinking $L$ as a subfield of the field of meromorphic functions defined over the previous simply connected bounded open set $U$

$$\text{Mer}(U) = \Big\{ f : U \longrightarrow \mathbb{C} \;\Big|\; f \text{ is meromorphic in } U \Big\}$$

We shall prove that the extension $\mathbb{C}(z) \subseteq \mathbb{C}(z)\langle f_1, ..., f_n\rangle = L$ is a Picard-Vessiot extension of $\mathbb{C}(z)$ for $\mathcal{L}$:

1. By hypothesis, $\mathcal{L}$ has exactly $n$ solutions in $L$, $\{f_1(z), ..., f_n(z)\}$ linearly independent over $\mathbb{C}$.
2. $L = \mathbb{C}(z)\langle f_1, ..., f_n\rangle$, being $\{f_1, ..., f_n\}$ a fundamental set of solutions of $\mathcal{L}(y) = 0$ in $L$.
3. No new constants are added, since we know that with the usual derivation we have

$$\frac{df(z)}{dz} = 0 \quad \text{for } f \in L \subset \text{Mer}(U) \Longrightarrow f(z) = \text{ constant } \in \mathbb{C}$$

[8]See [4, Chapter 9], **Linear *nth* Order and Matrix Differential Equations**.

# Chapter 3

# Differential Galois Group

In the last two chapters we have developed a general theory of differentiability over rings and fields, as well as some important results about extending them through ring and field extensions, setting the concept of differential ideals and studying the derivation over quotient rings, etc.
These results were necessary in order to have enough tools to study in depth the main goal in this work, which are the homogeneous linear differential equations, or HLDE's, and the symmetries of their solutions.

We have also set the fundamental concept of a Picard-Vessiot extension associated with a HLDE $\mathcal{L}(y) = 0$ over $K$, which can be understood to be the analogous of the splitting field of a polynomial equation $p(x) = 0$ in Algebraic Galois Theory: the **minimal** differential field in where the solutions of $\mathcal{L}(y) = 0$ "live".[1]
We have given some examples concerning the construction of Picard-Vessiot extensions of some easy differential equations, having used some results of our differential theory already exposed to do so.

We are now ready to begin our study about the symmetries of a given HLDE.
In this chapter we are going to define what we understand as a symmetry of a differential equation, and we will associate to each of them a group of transformations (preserving the **algebraic** and **differential** structure) leaving it invariant: this group will give us important information about the properties of the solutions. We will call this group the Differential Galois Group of the Picard-Vessiot extension associated to our differential equation.

First of all, we will study an important representation of this (in general continuous) group, and we shall show that it can be viewed as a group of matrices with some properties.

After that, we will do some instructive examples in the computation of the Differential Galois Group, and we will see that there doesn't exist any general method to construct symmetries[2] of a given differential equation. However, we will be able to provide a specific topology in this Differential Galois Group, and this fact will give us some (theoretical) information and properties about the group.

[1]With **minimal** we understand an extension $K \subseteq L$ with $C_L = C_K$, no new constants are added.

[2]Notice that in Algebraic Galois Theory we had a property which tells us how to construct automorphisms from an algebraic extension of a given field $K$ onto itself.

From now on in this work $K$ will denote a differential field **of characteristic 0 with algebraically closed set of constants** $C_K$ in order to have existence and unicity of Picard-Vessiot extensions for HLDE's.

## 3.1 Identifying the Differential Galois Group

As we have already said, we want to study the symmetries of solutions of a given HLDE $\mathcal{L}(y) = 0$ preserving all **algebraic** and **differential** structure.

**Definition 3.1.** *Let $K$ be a differential field with algebraically closed set of constants $C_K$.*

*Let $\mathcal{L} \in K[d]$ be a linear differential operator, and $K \subseteq L$ be its Picard-Vessiot extension.*

*We define the Differential Galois Group of $\mathcal{L}$ as*

$$\begin{aligned}\mathrm{DGal}(\mathcal{L}) = \mathrm{DGal}(L/K) &= \Big\{ \textit{differential } K\textit{-automorphisms of } L \Big\} = \\ &= \Big\{ \sigma : L \longrightarrow L \;\Big|\; \sigma|_K = Id_K \textit{ differential isomorphism} \Big\}\end{aligned}$$

It is straightforward to check that it is indeed a group. Let's study in depth this definition and extract some crucial properties. Since $K \subseteq L$ is a Picard-Vessiot extension for $\mathcal{L}$, we can put

$$L = K\langle y_1, ..., y_n\rangle \quad , \quad \text{where } \{y_1, ..., y_n\} \text{ is a fundamental set of solutions of } \mathcal{L}(y) = 0 \text{ in } L$$

with $C_K = C_L$.

Now, given a symmetry $\sigma \in \mathrm{DGal}(\mathcal{L})$, it is completely determined by the images of the solutions $\{y_1, ..., y_n\}$ since it is a differential automorphism (it preserves addition, substraction, multiplication, division and derivation, and over $K$ is the identity automorphism). So, we can write $\sigma$ in a more compact form as

$$\begin{aligned}\sigma : K\langle y_1, ..., y_n\rangle &\longrightarrow K\langle y_1, ..., y_n\rangle \\ \alpha &\longmapsto \alpha \qquad\qquad \forall\, \alpha \in K \\ y_i &\longmapsto \sigma(y_i)\end{aligned}$$

Why have we chosen this definition of symmetries of a differential equation? These particular symmetries are the ones which send solutions of $\mathcal{L}(y) = 0$ onto solutions of the same differential equation: if we write

$$\mathcal{L}(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y \quad , \quad a_i \in K$$

then, given $y_i$ a (fundamental) solution, we get

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

and $\sigma(y_i)$ is again a solution of the differential equation.

The big difference between studying polynomials and differential equations is that we have more structure over the solutions of the last one: they form a vector space over the field of constants $C_L = C_K$, denoted by

$$\mathrm{Sol}(\mathcal{L})_L = C_K \cdot y_1 \oplus C_K \cdot y_2 \oplus \cdots \oplus C_K \cdot y_n$$

This fact leads us to be able to express $\sigma(y_i)$ as a $C_K$-combination of our basis of $\mathrm{Sol}(\mathcal{L})_L$, $\{y_1, ..., y_n\}$:

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

that is, we can rewrite $\sigma$ in a more suitable way

$$\begin{aligned} \sigma : K\langle y_1, ..., y_n\rangle &\longrightarrow K\langle y_1, ..., y_n\rangle \\ \alpha \quad &\longmapsto \quad \alpha \qquad\qquad \forall\ \alpha \in K \\ (y_1, ..., y_n) &\longmapsto (y_1, ..., y_n) \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} \end{aligned}$$

It is easy to see now, with all this study, that we can associate to each $\sigma \in \mathrm{DGal}(\mathcal{L})$ a matrix $C$. We are now ready to prove the following theorem.

**Theorem 3.1** (Identifying $\mathrm{DGal}(\mathcal{L})$).

*We have an embedding*

$$\begin{aligned} \phi : \mathrm{DGal}(\mathcal{L}) &\hookrightarrow \mathrm{GL}_n(C_K) \\ \sigma \quad &\longmapsto \quad (C)_{ji} \end{aligned}$$

*i.e., we have a representation of* $\mathrm{DGal}(\mathcal{L})$ *through the invertible matrices with coefficients in* $C_K$, $\mathrm{GL}_n(C_K)$.

*Proof.*

1) We initially have $\phi$ defined between $\mathrm{DGal}(\mathcal{L})$ and $\mathrm{M}_n(C_K)$, $\phi : \mathrm{DGal}(\mathcal{L}) \longrightarrow \mathrm{M}_n(C_K)$. If we have the representations

$$\sigma \to \phi(\sigma) = C_\sigma$$
$$\tau \to \phi(\tau) = C_\tau$$

the composition has the representation

$$\begin{aligned} (\sigma \circ \tau)(y_i) = \sigma(\tau(y_i)) = \sigma\Big(\sum_{j=1}^{n}(C_\tau)_{ji} y_j\Big) = \sum_{j=1}^{n}(C_\tau)_{ji}\sigma(y_j) = \sum_{j=1}^{n}(C_\tau)_{ji}\Big(\sum_{k=1}^{n}(C_\sigma)_{kj} y_k\Big) = \\ = \sum_{j=1}^{n}\sum_{k=1}^{n}(C_\sigma)_{kj}(C_\tau)_{ji} y_k = \sum_{k=1}^{n}\Big(\sum_{j=1}^{n}(C_\sigma)_{kj}(C_\tau)_{ji}\Big) y_k = \sum_{k=1}^{n}(C_\sigma C_\tau)_{ki} y_k \quad \forall i = 1, ..., n \end{aligned}$$

$$\sigma \circ \tau \to \phi(\sigma \circ \tau) = C_\sigma C_\tau = \phi(\sigma)\phi(\tau)$$

Also, $\phi(Id) = Id$ trivially. With these observations, since every $\sigma \in \mathrm{DGal}(\mathcal{L})$ is an isomorphism, $C_\sigma$ has to be invertible, i.e. $C_\sigma \in \mathrm{GL}_n(C_K)$, because

$$Id = \phi(Id) = \phi(\sigma \circ \sigma^{-1}) = \phi(\sigma) \cdot \phi(\sigma^{-1}) = C_\sigma \cdot C_{\sigma^{-1}}$$

2) Hence, $\phi(\mathrm{DGal}(\mathcal{L})) \subseteq \mathrm{GL}_n(C_K)$, and we can consider $\phi : \mathrm{DGal}(\mathcal{L}) \longrightarrow \mathrm{GL}_n(C_K)$. Much more, we have also already proved that

$$\begin{cases} \phi(\sigma \circ \tau) = \phi(\sigma)\phi(\tau) \\ \phi(Id) = Id \end{cases}$$

and so $\phi$ is a homomorphism between the groups $(\mathrm{DGal}(\mathcal{L}), \circ)$ and $(\mathrm{GL}_n(C_K), \cdot)$.

3) Finally, if we have $\sigma, \tau$ such that $\phi(\sigma) = \phi(\tau) = (C)_{ji}$, then

$$\begin{cases} \sigma(y_i) = \sum_{j=1}^{n} (C)_{ji} y_j \\ \tau(y_i) = \sum_{k=1}^{n} (C)_{ki} y_k \end{cases} \quad \forall i = 1, ..., n$$

but the elements of $\mathrm{DGal}(\mathcal{L})$ are completely determined by their behavior on the basis $\{y_1, ..., y_n\}$, and so $\sigma = \tau$, i.e. $\phi$ is injective.

□

In conclusion, we can understand $\mathrm{DGal}(\mathcal{L})$ as a subgroup of the invertible $n \times n$ matrices with coefficients in $C_K$.

## 3.2 Examples of some Differential Galois Groups

Just to get an insight of these symmetries of a given differential equation, we are going to give the continuation of some previous examples by computing its Differential Galois Group.

### 3.2.1 Adjunction of the integral

Consider a differential field $K$, and let $a \in K$ be an element which is not a derivative of any element, i.e. it does not exist $b \in K$ such that $b' = a$.

We can consider the differential equation

$$\mathcal{L}(y) = y'' - \frac{a'}{a} y' = 0, \quad \mathcal{L} \in K[d] \text{ , being } d \text{ the derivation in } K,$$

Taking an indeterminate $\alpha$ (transcendental element over $K$) and considering the differential field extension

$$K \subseteq K(\alpha) = L$$

by defining a derivation over $L$ through $\alpha' = a$, the extension $K \subseteq K(\alpha) = K\langle 1, \alpha \rangle$ becomes a Picard-Vessiot extension of $K$ for $\mathcal{L}$, as we have already proved in **Section 2.3.1. Adjunction of the integral**.

Let's find it's $\mathrm{DGal}(\mathcal{L})$: we know that, given an element $\sigma \in \mathrm{DGal}(\mathcal{L})$, we can represent it as an invertible matrix $C \in \mathrm{GL}_2(C_K)$ in the following way:

$$\begin{aligned} \sigma : & K\langle 1,\alpha\rangle \longrightarrow K\langle 1,\alpha\rangle \\ & k \longmapsto k \qquad \forall\, k \in K \\ & (1,\alpha) \longmapsto (1,\alpha) \underbrace{\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}}_{C} \end{aligned}$$

that is,

$$\begin{cases} \sigma(1) = c_{11} + c_{21}\alpha \\ \sigma(\alpha) = c_{12} + c_{22}\alpha \end{cases}$$

**but** we have restrictions: since $\sigma$ is a **differential** $K$**-automorphism of** $K\langle 1,\alpha\rangle$,

- $\sigma(1) = 1 = c_{11} + c_{21}\alpha$, and so $\boxed{c_{11} = 1}$ , $\boxed{c_{21} = 0}$, since 1 and $\alpha$ are linearly independent.
- $\sigma(\alpha)' = \sigma(\alpha')$,

$$c_{22}a = c_{22}\alpha' = \sigma(\alpha)' = \sigma(\alpha') = \sigma(a) = a \qquad \text{and so } \boxed{c_{12} \text{ free}}\ ,\ \boxed{c_{22} = 1}$$

Finally, every element of $\mathrm{DGal}(\mathcal{L})$ is of the form

$$\begin{aligned} \sigma : & K\langle 1,\alpha\rangle \longrightarrow K\langle 1,\alpha\rangle \\ & k \longmapsto k \qquad \forall\, k \in K \\ & \alpha \longmapsto \alpha + c \qquad c \in C_K \end{aligned}$$

and it is straightforward to check that every morphism of the previous form is indeed a differential $K$-automorphism of $L = K\langle 1,\alpha\rangle$.
In this case,

$$\mathrm{DGal}(\mathcal{L}) \cong \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \;\middle|\; c \in C_K \right\} \cong (C_K, +) \quad \text{the additive group}$$

Now we can relate this result with the observation we already did about some "change of variables" we can do to our differential equation: we have found that those "change of variables" are valid, and that they are the only ones we can do to the differential equation in order to leave it invariant.

### 3.2.2 Adjunction of the exponential of the integral

Consider a differential field $K$, and let $a \in K$ be an element such that it does not exist $b \in K\backslash\{0\}$ and $n \in \mathbb{Z}\backslash\{0\} \subset \mathbb{Q} \hookrightarrow K$ such that $b' = nab$.
We can consider the differential equation

$$\mathcal{L}(y) = y' - ay = 0, \quad \mathcal{L} \in K[d] \text{ , being } d \text{ the derivation in } K$$

which has no solution in $K$.

Taking an indeterminate $\alpha$ (transcendental element over $K$) and considering the differential field extension

$$K \subseteq K(\alpha) = L$$

by defining a derivation over $L$ through $\alpha' = a\alpha$, the extension $K \subseteq K(\alpha) = K\langle\alpha\rangle$ becomes a Picard-Vessiot extension of $K$ for $\mathcal{L}$, as we have already proved in **Section 2.3.2. Adjunction of the exponential of the integral.**.

Let's find it's $\mathrm{DGal}(\mathcal{L})$: we know that, given an element $\sigma \in \mathrm{DGal}(\mathcal{L})$, we can represent it as an invertible matrix $C \in \mathrm{GL}_1(C_K) = C_K^*$ in the following way:

$$\begin{aligned} \sigma : K\langle\alpha\rangle &\longrightarrow K\langle\alpha\rangle \\ k \quad &\longmapsto \quad k \qquad \forall\, k \in K \\ \alpha \quad &\longmapsto \quad c\alpha \qquad c \in C_K^* \end{aligned}$$

Again, it is straightforward to check that every morphism of the previous form is indeed a differential $K$-automorphism of $L = K\langle\alpha\rangle$, and so we do not need to impose any relations between the coefficients of the matrix (we only have one parameter here).

In this case,

$$\mathrm{DGal}(\mathcal{L}) \cong \{c \mid c \in C_K^*\} = (C_K^*, \cdot) \quad \text{the multiplicative group}$$

### 3.2.3 Concrete examples involving $\mathbb{C}(z)$

All the examples we will expose in this section are referred over the differential field $K = \mathbb{C}(z)$ provided with the usual derivation $\frac{d}{dz}$, and the Picard-Vessiot extensions are viewed in the same way as in **Section 2.3.3. A brief study of differential equations over** $\mathbb{C}(z)$, where we have already proven that they are indeed Picard-Vessiot extensions.

1) Let's consider the differential equation given by

$$0 = \mathcal{L}(y) = y'' + y, \quad \mathcal{L} \in \mathbb{C}(z)\Big[\frac{d}{dz}\Big]$$

Its solutions are $y_1(z) = \sin(z)$ and $y_2(z) = \cos(z)$ defined over $\mathbb{C}$; so,

$$\mathrm{Sol}(\mathcal{L})_L = \mathbb{C}\cdot\cos(z) \oplus \mathbb{C}\cdot\sin(z) \qquad \text{with} \begin{cases} L = \mathbb{C}(z)\langle\cos(z),\sin(z)\rangle = \mathbb{C}(z,\cos(z),\sin(z)) \\ C_L = C_K = \mathbb{C} \end{cases}$$

and so $\mathbb{C}(z,\cos(z),\sin(z))/\mathbb{C}(z)$ is a Picard-Vessiot extension for $\mathcal{L}$. Its Differential Galois Group is given by

$$\mathrm{DGal}(\mathcal{L}) = \{\sigma : L \longrightarrow L \text{ differential } \mathbb{C}(z)\text{-automorphisms}\}$$

Given an element $\sigma \in \mathrm{DGal}(\mathcal{L})$, we can represent it as an invertible matrix $C \in \mathrm{GL}_2(\mathbb{C})$ through

$$\begin{aligned} \sigma :\ \mathbb{C}(z,\cos(z),\sin(z)) &\longrightarrow \mathbb{C}(z,\cos(z),\sin(z)) \\ k \qquad &\longmapsto \qquad k \qquad\qquad \forall\, k \in \mathbb{C}(z) \\ (\sin(z),\cos(z)) &\longmapsto (\sin(z),\cos(z)) \underbrace{\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}}_{C} \end{aligned}$$

that is,

$$\begin{cases} \sigma(\sin(z)) = c_{11}\sin(z) + c_{21}\cos(z) \\ \sigma(\cos(z)) = c_{12}\sin(z) + c_{22}\cos(z) \end{cases}$$

**but** we have restrictions: since $\sigma$ is a **differential** $\mathbb{C}(z)$**-automorphism of** $L$,

- $\sigma(\sin(z))' = \sigma(\sin(z)')$,

  $$c_{11}\cos(z) - c_{21}\sin(z) = \sigma(\sin(z)') = \sigma(\cos(z)) = c_{12}\sin(z) + c_{22}\cos(z)$$

  and so $\boxed{c_{11} = c_{22}}$ , $\boxed{c_{12} = -c_{21}}$, since $\sin(z)$ and $\cos(z)$ are linearly independent.
- $\sigma(\cos(z))' = \sigma(\cos(z)')$,

  $$c_{12}\cos(z) - c_{22}\sin(z) = \sigma(\cos(z)') = -\sigma(\sin(z)) = -c_{11}\sin(z) - c_{21}\cos(z)$$

  and so $\boxed{c_{11} = c_{22}}$ , $\boxed{c_{12} = -c_{21}}$. They are the same relations as before.

For the moment, every element of $\mathrm{DGal}(\mathcal{L})$ is of the form

$$\begin{aligned} \sigma:\ \mathbb{C}(z,\cos(z),\sin(z)) &\longrightarrow \mathbb{C}(z,\cos(z),\sin(z)) \\ k &\longmapsto k \qquad \forall\ k \in \mathbb{C}(z) \\ (\sin(z),\cos(z)) &\longmapsto (\sin(z),\cos(z)) \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad a,b \in \mathbb{C} \text{ with } a^2+b^2 \neq 0 \end{aligned}$$

In this case, we have another restriction, which comes from the **algebraic relation** between $\sin(z)$ and $\cos(z)$

$$\sin(z)^2 + \cos(z)^2 = 1$$

Applying $\sigma$, we get

$$\sigma(\sin(z))^2 + \sigma(\cos(z))^2 = 1$$

and with a bit of algebra we get to the restriction $a^2 + b^2 = 1$.
Finally, every element of $\mathrm{DGal}(\mathcal{L})$ is of the form

$$\begin{aligned} \sigma:\ \mathbb{C}(z,\cos(z),\sin(z)) &\longrightarrow \mathbb{C}(z,\cos(z),\sin(z)) \\ k &\longmapsto k \qquad \forall\ k \in \mathbb{C}(z) \\ (\sin(z),\cos(z)) &\longmapsto (\sin(z),\cos(z)) \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad a,b \in \mathbb{C} \text{ with } a^2+b^2 = 1 \end{aligned}$$

and it is straightforward to check that every morphism of the previous form is indeed a differential $\mathbb{C}(z)$-automorphism of $L = \mathbb{C}(z,\cos(z),\sin(z))$.
In this case,

$$\mathrm{DGal}(\mathcal{L}) \cong \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \ \middle|\ a,b \in \mathbb{C}, a^2+b^2 = 1 \right\}$$

2) Now we consider the differential equation

$$0 = \mathcal{L}(y) = y''' - y', \quad \mathcal{L} \in \mathbb{C}(z)\Big[\frac{d}{dz}\Big]$$

Its solutions are $y_1(z) = 1$, $y_2(z) = e^z$ and $y_3(z) = e^{-z}$ defined over $\mathbb{C}$; so,

$$\mathrm{Sol}(\mathcal{L})_L = \mathbb{C}\cdot 1 \oplus \mathbb{C}\cdot e^z \oplus \mathbb{C}\cdot e^{-z} \qquad \text{with} \begin{cases} L = \mathbb{C}(z)\langle 1, e^z, e^{-z}\rangle = \mathbb{C}(z, e^z) \\ C_L = C_K = \mathbb{C} \end{cases}$$

and so $\mathbb{C}(z, e^z)/\mathbb{C}(z)$ is a Picard-Vessiot extension for $\mathcal{L}$. Let's find its Differential Galois Group: given an element $\sigma \in \mathrm{DGal}(\mathcal{L})$, we can represent it as an invertible matrix $C \in \mathrm{GL}_3(\mathbb{C})$ trough

$$\begin{aligned} \sigma :\ \mathbb{C}(z, e^z) &\longrightarrow \mathbb{C}(z, e^z) \\ k &\longmapsto k \qquad\qquad \forall\, k \in \mathbb{C}(z) \\ (1, e^z, e^{-z}) &\longmapsto (1, e^z, e^{-z}) \underbrace{\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}}_{C} \end{aligned}$$

that is,

$$\begin{cases} \sigma(1) = c_{11} + c_{21}e^z + c_{31}e^{-z} \\ \sigma(e^z) = c_{12} + c_{22}e^z + c_{32}e^{-z} \\ \sigma(e^{-z}) = c_{13} + c_{23}e^z + c_{33}e^{-z} \end{cases}$$

**but** we have restrictions: since $\sigma$ is a **differential** $\mathbb{C}(z)$**-automorphism of** $L$,

- $\sigma(1) = 1 = c_{11} + c_{21}e^z + c_{31}e^{-z}$, and so $\boxed{c_{11} = 1}$ , $\boxed{c_{21} = c_{31} = 0}$ since 1, $e^z$ and $e^{-z}$ are linearly independent.
- $\sigma(e^z)' = \sigma((e^z)')$,

$$c_{22}e^z - c_{32}e^{-z} = \sigma((e^z)') = \sigma(e^z) = c_{12} + c_{22}e^z + c_{32}e^{-z}$$

  and so $\boxed{c_{12} = c_{32} = 0}$ , $\boxed{c_{22} \text{ free}}$.
- $\sigma(e^{-z})' = \sigma((e^{-z})')$,

$$c_{23}e^z - c_{33}e^{-z} = \sigma((e^{-z})') = -\sigma(e^{-z}) = -c_{13} - c_{23}e^z - c_{33}e^{-z}$$

  and so $\boxed{c_{13} = c_{23} = 0}$ , $\boxed{c_{33} \text{ free}}$.

For the moment, every element of $\mathrm{DGal}(\mathcal{L})$ is of the form

$$\begin{aligned} \sigma :\ \mathbb{C}(z, e^z) &\longrightarrow \mathbb{C}(z, e^z) \\ k &\longmapsto k \qquad\qquad \forall\, k \in \mathbb{C}(z) \\ (1, e^z, e^{-z}) &\longmapsto (1, e^z, e^{-z}) \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{pmatrix} \quad a, b \in \mathbb{C}^* \end{aligned}$$

Like the previous example, we have another restriction coming from the **algebraic relation** between $e^z$ and $e^{-z}$

$$e^z \cdot e^{-z} = 1$$

Applying $\sigma$, we get

$$1 = \sigma(e^z) \cdot \sigma(e^{-z}) = ab \qquad \text{that is, } b = \frac{1}{a}$$

Finally, every element of $\mathrm{DGal}(\mathcal{L})$ is of the form

$$\begin{aligned} \sigma :\ \mathbb{C}(z, e^z) &\longrightarrow \mathbb{C}(z, e^z) \\ k &\longmapsto k \qquad\qquad\qquad \forall\, k \in \mathbb{C}(z) \\ (1, e^z, e^{-z}) &\longmapsto (1, e^z, e^{-z}) \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & \frac{1}{a} \end{pmatrix} \qquad a \in \mathbb{C}^* \end{aligned}$$

and it is straightforward to check that every morphism of the previous form is indeed a differential $\mathbb{C}(z)$-automorphism of $L = \mathbb{C}(z, e^z)$.
In this case,

$$\mathrm{DGal}(\mathcal{L}) \cong \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & \frac{1}{a} \end{pmatrix} \;\middle|\; a \in \mathbb{C}^* \right\} \cong \mathbb{C}^* \qquad \text{the multiplicative group}$$

3) Consider the following differential equation

$$0 = \mathcal{L}(y) = y' - \frac{1}{nz} y, \quad \mathcal{L} \in \mathbb{C}(z)\Big[\frac{d}{dz}\Big]$$

whose coefficients are analytic on a simply connected open set $U \subset \mathbb{C}\backslash\{0\}$; for example, let's take the region

$$U = \{ z \in \mathbb{C} \mid |z+1| < 1 \}$$

Its solution is $y(z) = \sqrt[n]{z}$ defined over $U$ if we take an analytic branch of $y(z)$ there; so,

$$\mathrm{Sol}(\mathcal{L})_L = \mathbb{C} \cdot \sqrt[n]{z} \qquad \text{with} \begin{cases} L = \mathbb{C}(z)\langle \sqrt[n]{z} \rangle = \mathbb{C}(\sqrt[n]{z}) \\ C_L = C_K = \mathbb{C} \end{cases}$$

and so $\mathbb{C}(\sqrt[n]{z})/\mathbb{C}(z)$ is a Picard-Vessiot extension for $\mathcal{L}$. Let's find its Differential Galois Group: an element $\sigma \in \mathrm{DGal}(\mathcal{L})$ can be represented through an invertible matrix $C \in \mathrm{GL}_1(\mathbb{C})$

$$\begin{aligned} \sigma :\ \mathbb{C}(\sqrt[n]{z}) &\longrightarrow \mathbb{C}(\sqrt[n]{z}) \\ k &\longmapsto k \qquad \forall\, k \in \mathbb{C}(z) \\ \sqrt[n]{z} &\longmapsto c\sqrt[n]{z} \quad\; c \in \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^* \end{aligned}$$

**but** we have restrictions: since $\sigma$ is a **differential** $\mathbb{C}(z)$**-automorphism of** $L$,

- $\sigma(\sqrt[n]{z})' = \sigma((\sqrt[n]{z})')$,

$$\frac{c}{nz}\sqrt[n]{z} = \sigma((\sqrt[n]{z})') = \sigma\Big(\frac{1}{nz}\sqrt[n]{z}\Big) = \frac{c}{nz}\sqrt[n]{z}$$

  and so $\boxed{c \text{ free}}$; this tells us that all values of $c$ are compatible of being $\sigma$ a differential $\mathbb{C}(z)$-automorphism.

But, since in this case $\sqrt[n]{z}$ is **algebraic** over $\mathbb{C}(z)$ [3], with $\mathrm{Irr}(\sqrt[n]{z},\mathbb{C})(X) = X^n - z$, we have the **algebraic relation**

$$(\sqrt[n]{z})^n - z = 0$$

Applying $\sigma$, we get

$$0 = \sigma(\sqrt[n]{z})^n - z = z(c^n - 1)$$

that is, $c$ has to be an **nth root of unity**, $c = e^{2\pi i \frac{m}{n}}$ for $m = 0, ..., n-1$.
Finally, every element of $\mathrm{DGal}(\mathcal{L})$ is of the form

$$\begin{aligned} \sigma: \ \mathbb{C}(\sqrt[n]{z}) &\longrightarrow \mathbb{C}(\sqrt[n]{z}) \\ k &\longmapsto k \qquad\qquad \forall\, k \in \mathbb{C}(z) \\ \sqrt[n]{z} &\longmapsto e^{2\pi i \frac{m}{n}} \sqrt[n]{z} \qquad m \in \{0, ..., n-1\} \end{aligned}$$

and it is straightforward to check that every morphism of the previous form is indeed a differential $\mathbb{C}(z)$-automorphism of $L = \mathbb{C}(\sqrt[n]{z})$.
In this case,

$$\mathrm{DGal}(\mathcal{L}) \cong \left\{1, e^{2\pi i \frac{1}{n}}, e^{2\pi i \frac{2}{n}}, ..., e^{2\pi i \frac{n-1}{n}}\right\} \subset \mathbb{C}^* \qquad \text{a finite cyclic group of order } n$$

4) The last example we are going to study concerns the differential equation

$$0 = \mathcal{L}(y) = y'' - (1+z^2)y, \quad \mathcal{L} \in \mathbb{C}(z)\left[\frac{d}{dz}\right]$$

Its solutions are $y_1(z) = e^{\frac{1}{2}z^2}$ and $y_2(z) = f(z)e^{\frac{1}{2}z^2}$ with $f(z) = \int_0^z e^{-w^2}dw$, defined over $\mathbb{C}$; so,

$$\mathrm{Sol}(\mathcal{L})_L = \mathbb{C}\cdot e^{\frac{1}{2}z^2} \oplus \mathbb{C}\cdot f(z)e^{\frac{1}{2}z^2} \qquad \text{with} \begin{cases} L = \mathbb{C}(z)\langle e^{\frac{1}{2}z^2}, f(z)e^{\frac{1}{2}z^2}\rangle = \mathbb{C}(z, e^{\frac{1}{2}z^2}, f(z), e^{-z^2}) \\ C_L = C_K = \mathbb{C} \end{cases}$$

and so $\mathbb{C}(z, e^{\frac{1}{2}z^2}, f(z), e^{-z^2})/\mathbb{C}(z)$ is a Picard-Vessiot extension for $\mathcal{L}$. Let's find its Differential Galois Group; an element $\sigma \in \mathrm{DGal}(\mathcal{L})$ is represented through an invertible matrix $C \in \mathrm{GL}_2(\mathbb{C})$

$$\begin{aligned} \sigma: \ \mathbb{C}(z, e^{\frac{1}{2}z^2}, f(z), e^{-z^2}) &\longrightarrow \mathbb{C}(z, e^{\frac{1}{2}z^2}, f(z), e^{-z^2}) \\ k &\longmapsto k \qquad\qquad \forall\, k \in \mathbb{C}(z) \\ (e^{\frac{1}{2}z^2}, f(z)e^{\frac{1}{2}z^2}) &\longmapsto (e^{\frac{1}{2}z^2}, f(z)e^{\frac{1}{2}z^2}) \underbrace{\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}}_{C} \end{aligned}$$

that is,

$$\begin{cases} \sigma(e^{\frac{1}{2}z^2}) = c_{11}e^{\frac{1}{2}z^2} + c_{21}f(z)e^{\frac{1}{2}z^2} \\ \sigma(f(z)e^{\frac{1}{2}z^2}) = c_{12}e^{\frac{1}{2}z^2} + c_{22}f(z)e^{\frac{1}{2}z^2} \end{cases}$$

**but** we have restrictions: since $\sigma$ is a **differential** $\mathbb{C}(z)$**-automorphism of** $L$,

- $\sigma(e^{\frac{1}{2}z^2})' = \sigma((e^{\frac{1}{2}z^2})')$,

$$c_{11}ze^{\frac{1}{2}z^2} + c_{21}zf(z)e^{\frac{1}{2}z^2} + c_{21}e^{\frac{1}{2}z^2}e^{-z^2} = c_{11}ze^{\frac{1}{2}z^2} + c_{21}zf(z)e^{\frac{1}{2}z^2}$$

  and so $\boxed{c_{11} \text{ free}}$ , $\boxed{c_{21} = 0}$. In particular, we need $c_{11} \in \mathbb{C}^*$.

[3] See **Examples 2.4, Part 2**.

- $\sigma(f(z)e^{\frac{1}{2}z^2})' = \sigma((f(z)e^{\frac{1}{2}z^2})')$,

$$c_{12}ze^{\frac{1}{2}z^2} + c_{22}zf(z)e^{\frac{1}{2}z^2} + c_{22}e^{\frac{1}{2}z^2}e^{-z^2} = c_{12}ze^{\frac{1}{2}z^2} + c_{22}zf(z)e^{\frac{1}{2}z^2} + \frac{1}{c_{11}}\frac{1}{e^{\frac{1}{2}z^2}}$$

and so $\boxed{c_{12} \text{ free}}$, $\boxed{c_{22} = \frac{1}{c_{11}}}$.

Since there are no algebraic relations of the solutions (not involving derivatives), we obtain finally that every element of $\text{DGal}(\mathcal{L})$ is of the form

$$\begin{aligned} \sigma:\ \mathbb{C}(z, e^{\frac{1}{2}z^2}, f(z), e^{-z^2}) &\longrightarrow \mathbb{C}(z, e^{\frac{1}{2}z^2}, f(z), e^{-z^2}) \\ k &\longmapsto k \qquad\qquad \forall\, k \in \mathbb{C}(z) \\ (e^{\frac{1}{2}z^2}, f(z)e^{\frac{1}{2}z^2}) &\longmapsto (e^{\frac{1}{2}z^2}, f(z)e^{\frac{1}{2}z^2}) \begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix} \qquad a \in \mathbb{C}^*, b \in \mathbb{C} \end{aligned}$$

and it is straightforward to check that every morphism of the previous form is indeed a differential $\mathbb{C}(z)$-automorphism of $L = \mathbb{C}(z, e^{\frac{1}{2}z^2}, f(z), e^{-z^2})$.
In this case,

$$\text{DGal}(\mathcal{L}) \cong \left\{ \begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix} \;\middle|\; a \in \mathbb{C}^*, b \in \mathbb{C} \right\}$$

## 3.3 Introduction to Linear Algebraic Groups

Remembering **Theorem 3.1**, we can always see $\text{DGal}(\mathcal{L})$ as a subgroup of the group of invertible matrices $\text{GL}_n(C_K)$ through the embedding

$$\begin{aligned} \phi: \text{DGal}(\mathcal{L}) &\hookrightarrow \text{GL}_n(C_K) \\ \sigma &\longmapsto (C)_{ji} \end{aligned}$$

But we have more: we can provide this subgroup with a topology, induced by the topology of the invertible matrices $\text{GL}_n(C_K)$. In this section we are going to present the basic concepts involving this topology, and in **Section 3.4. $\text{DGal}(\mathcal{L})$ as a Linear Algebraic Group** we will prove that we can truly equip $\text{DGal}(\mathcal{L})$ with this topology.

### 3.3.1 Topology of affine $n$-space

Given a field $K$, the set $K^n$ will be called the **affine $n$-space** over $K$, and will be denoted by $\mathbb{A}^n$ when it is clear from the context what is $K$. Let's provide this set with a topology.

**Definition 3.2** (The Zariski topology).

*A subset $X$ of $\mathbb{A}^n$ is said to be* ***Zariski closed*** *if there exists a finite set of polynomials in $n$ variables*

$$f_1, ..., f_r \in \mathbb{A}[x_1, ..., x_n]$$

*such that $X$ is the "zero set" of these polynomials, that is,*

$$X = \{(a_1, ..., a_n) \in \mathbb{A}^n | f_i(a_1, ..., a_n) = 0 \ \forall i = 1, ..., r\}$$

This definition of closed subsets indeed defines a topology in $\mathbb{A}^n$ (defining the open sets as $X^c = \mathbb{A}^n \backslash X$ with $X$ a closed subset) called the **Zariski topology**.

The following theorem will become a crucial element when providing $\mathrm{DGal}(\mathcal{L}) \subseteq \mathrm{GL}_n(C_K)$ the Zariski topology.

**Theorem 3.2** (Hilbert's basis theorem).

*Let $I \subseteq \mathbb{A}[x_1, ..., x_n]$ an ideal. Then $I$ is finitely generated: there exist $f_1, .., f_s \in \mathbb{A}[x_1, ..., x_n]$ such that*

$$I = (f_1, ..., f_s)$$

### 3.3.2 Topology in the general linear group $\mathrm{GL}_n(\mathbb{A})$

We can take advantage of the topology already given in $\mathbb{A}^n$ (Zariski topology), and provide a topology on $\mathrm{GL}_n(\mathbb{A})$ induced by this one, by embedding it into an affine space $\mathbb{A}^m$ for an appropriate $m$; specifically,

$$\begin{array}{ccc} \psi : \mathrm{GL}_n(\mathbb{A}) & \hookrightarrow & \mathbb{A}^{n^2+1} \\ C = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} & \longmapsto & \left( c_{11}, c_{12}, ..., c_{nn}, \dfrac{1}{\det(C)} \right) = (\underbrace{z_{11}, ..., z_{nn}}_{n^2}, \underbrace{z_{n^2+1}}_{1}) \end{array}$$

In particular, we can see

$$\mathrm{GL}_n(\mathbb{A}) \cong \psi(\mathrm{GL}_n(\mathbb{A})) = \{(z_{11}, ..., z_{nn}, z_{n^2+1}) \mid z_{n^2+1} \cdot \det(z_{ij}) - 1 = 0\} \subset \mathbb{A}^{n^2+1}$$

as the zero set of the polynomial $X_{n^2+1} \cdot \det(X_{ij}) - 1 \in \mathbb{A}[X_{11}, ..., X_{nn}, X_{n^2+1}]$.
So $\mathrm{GL}_n(\mathbb{A}) \cong \psi(\mathrm{GL}_n(\mathbb{A}))$ is a Zariski closed subset of $\mathbb{A}^{n^2+1}$.

**Definition 3.3** (The Zariski topology in $\mathrm{GL}_n(\mathbb{A})$).

*A subset $X$ of $GL_n(\mathbb{A})$ is said to be* ***Zariski closed*** *if it is closed in the Zariski topology as a subset of $\mathbb{A}^{n^2+1}$, that is, if $\psi(X) \subseteq \mathbb{A}^{n^2+1}$ is Zariski closed.*

This definition of closed subsets indeed defines a topology in $\mathrm{GL}_n(\mathbb{A})$, induced by the one in $\mathbb{A}^{n^2+1}$.
We are now ready to define what a **linear algebraic group** is.

**Definition 3.4** (Linear Algebraic Groups). [4]

*A* ***linear algebraic group*** *is a Zariski closed* ***subgroup*** *of $GL_n(\mathbb{A})$ for some $n$.*

[4] This definition is sufficient for our purposes. For an abstract definition of linear algebraic groups the reader can consult [1, Chapter 3].

### 3.3.3 Some examples to gain intuition

Here we briefly study some examples concerning concepts about Zariski topology, in order to understand them with a little more of depth.

1) **About the Zariski topology in $\mathbb{R}^2$:**

We can consider the unitary circle

$$U = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

It is a Zariski closed subset of $\mathbb{R}^2$ because it is the “zero set“ of the polynomial $f(X, Y) = X^2 + Y^2 - 1 \in \mathbb{R}[X, Y]$:

$$U = \{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\}$$

2) **Consequence of Hilbert's basis theorem:**

Suppose we have a subset $X \subseteq A^n$ and a (maybe infinite) set of indices $S$ such that

$$X = \{(a_1, ..., a_n) \in \mathbb{A}^n \mid f_\alpha(a_1, ..., a_n) = 0 \ \forall \alpha \in S\} \qquad \text{with } f_\alpha \in \mathbb{A}[x_1, ..., x_n] \ \forall \alpha \in S$$

Let's consider the ideal of $\mathbb{A}[x_1, ..., x_n]$ generated by all the polynomials with indexes in $S$, that is,

$$I = (\{f_\alpha\}_{\alpha \in S}) \subseteq \mathbb{A}[x_1, ..., x_n]$$

From Hilbert's basis theorem, $I$ is finitely generated: there exist $f_1, ..., f_r \in \{f_\alpha\}_{\alpha \in S}$ such that

$$I = (f_1, ..., f_r)$$

With this result, we can now prove the following equality:

$$X = \{(a_1, ..., a_n) \in \mathbb{A}^n \mid f_i(a_1, ..., a_n) = 0 \ \forall i = 1, ..., r\} \equiv \mathcal{N}(I)$$

The inclusion $\subseteq$ is clear. To prove the other one, consider $a = (a_1, ..., a_n) \in \mathcal{N}(I)$ such that $f_i(a) = 0 \ \forall i = 1, ..., r$. We want to prove that $a$ is a root of all the polynomials of the set $\{f_\alpha\}_{\alpha \in S}$. Given $f_\beta \in \{f_\alpha\}_{\alpha \in S} \subset I = (f_1, ..., f_r)$ it can be written as

$$f_\beta = \sum_{i=1}^{r} b_i f_i \in \mathbb{A}[x_1, ..., x_n] \qquad b_1, ..., b_r \in \mathbb{A}$$

and so we obtain

$$f_\beta(a) = \sum_{i=1}^{r} b_i f_i(a) = 0$$

as we wanted to prove.

This result is telling us that $X$ is a **Zariski closed** subset of $\mathbb{A}^n$.

3) **Some basic examples of Linear Algebraic Groups:**

a) The additive group $\mathbb{G}_a(\mathbb{A})$ can be identified with the Zariski closed subgroup

$$\mathbb{G}_a(\mathbb{A}) \cong \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \Big| a \in \mathbb{A} \right\} \subset \mathrm{GL}_2(\mathbb{A})$$

hence is a linear algebraic group. We will simply write it as $\mathbb{G}_a$ if the field $\mathbb{A}$ is clear from the context.

b) The multiplicative group $\mathbb{G}_m(\mathbb{A})$ can be identified with the Zariski closed subgroup

$$\mathbb{G}_m(\mathbb{A}) \cong \mathbb{A}^* \cong \mathrm{GL}_1(\mathbb{A})$$

hence is a linear algebraic group. We will simply write it as $\mathbb{G}_m$ if the field $\mathbb{A}$ is clear from the context.

c) It is left as an exercice (and not dificult to prove) that the direct product of two algebraic groups is again an algebraic group, so

$$\mathbb{G}_a^r \times \mathbb{G}_m^s$$

is again an algebraic group, for all $r, s \in \mathbb{N}$.

## 3.4 DGal($\mathcal{L}$) as a Linear Algebraic Group

We are now in a position to prove an essential property of DGal($\mathcal{L}$).

**Proposition 3.1.**

*Let $K$ be a differential field with algebraically closed set of constants $C_K$, and let $\mathcal{L} \in K[d]$ be a linear differential operator of degree $n$, and $K \subseteq L$ its Picard-Vessiot extension. Let DGal($\mathcal{L}$) be its Differential Galois Group. Then there exist a set $S$ of polynomials*

$$f(X_{ij}) \in C_K[\{X_{ji}, i, j = 1, ..., n\}]$$

*such that*

*1) For every $\sigma \in$ DGal($\mathcal{L}$) and $\phi(\sigma) = (C)_{ji} \in GL_n(C_K)$ its representation, we have*

$$f(C_{ji}) = 0 \quad \forall f \in S$$

*2) Given a matrix $(C)_{ji} \in GL_n(C_K)$ with $f(C_{ji}) = 0\ \forall f \in S$, then the morphism $\sigma$ defined through*

$$\sigma(y_i) = \sum_{j=1}^{n} C_{ji} y_j \quad \forall i = 1, ..., n$$

*is an element of DGal($\mathcal{L}$).*

*Proof.* Let's first construct the set $S$. Since $K \subseteq L$ is a Picard-Vessiot extension, we can write

$$L = K\langle y_1, ..., y_n \rangle = Quot(K\{y_1, ..., y_n\})$$

Let $K\{Z_1, ..., Z_n\}$ be the ring of differential polynomials in the indeterminates $Z_1, ..., Z_n$. We then have a natural differential $K$-morphism

$$\begin{array}{rccc} \psi: & K\{Z_1, ..., Z_n\} & \longrightarrow & K\{y_1, ..., y_n\} \subseteq L \\ & Z_i & \longmapsto & y_i \end{array}$$

The idea is to work in the (universal) object $K\{Z_1, ..., Z_n\}$, and then translate it into $L$.
We will consider the ring of differential polynomials in the indeterminates $X_{ji}$, $K\{y_1, ..., y_n\}[X_{ji}] \subseteq L[X_{ji}]$, with a derivation defined through $X'_{ji} = 0$. Then we have the differential $K$-morphism

$$\begin{array}{rccc} \phi: & K\{Z_1, ..., Z_n\} & \longrightarrow & K\{y_1, ..., y_n\}[X_{ji}] \subseteq L[X_{ji}] \\ & Z_i & \longmapsto & \displaystyle\sum_{j=1}^{n} X_{ji} y_j \end{array}$$

We have the following diagram:

$$\begin{array}{ccc} K\{Z_1, ..., Z_n\} & \xrightarrow{\quad \psi \quad} & K\{y_1, ..., y_n\} \subseteq L \\ \phi \downarrow & \swarrow \overline{\psi} & \\ K\{y_1, ..., y_n\}[X_{ji}] \subseteq L[X_{ji}] & & \end{array}$$

We define $\Delta \equiv \phi(\text{Ker}(\psi)) \subseteq K\{y_1, ..., y_n\}[X_{ji}] \subseteq L[X_{ji}]$.

With all this preparation, we are ready to construct the set $S$: since $C_K \subseteq K \subseteq L$ are field extensions, $L$ is a $C_K$- vector space, with (maybe infinite) basis denoted by $\{l_i | i \in I\}$, and so every $\delta \in \Delta \subseteq L[X_{ji}]$ can be written as a $C_K[X_{ji}]$-linear combination

$$\delta = \sum_{k=1}^{m_\delta} f_k^{(\delta)} \cdot l_k \qquad \text{with } f_k^{(\delta)} \in C_K[X_{ji}] \quad \forall k = 1, ..., m_\delta$$

Let's define $S$ to be

$$S \equiv \{f_1^{(\delta)}, ..., f_{m_\delta}^{(\delta)} | \delta \in \Delta\} \subseteq C_K[X_{ji}] \subseteq L[X_{ji}]$$

1) Let $\sigma \in \text{DGal}(\mathcal{L})$, $\sigma : L \longrightarrow L$ be written by

$$\sigma(y_i) = \sum_{j=1}^{n} C_{ji} y_j$$

It is clear that, if we define the evaluation differential $K\{y_1, ..., y_n\}$-morphism (or $L$-morphism) (it is indeed a differential one beacuse of the definition of the derivation $X'_{ji} = 0$)

$$\begin{array}{rccc} ev: & K\{y_1, ..., y_n\}[X_{ji}] \subseteq L[X_{ji}] & \longrightarrow & K\{y_1, ..., y_n\} \subseteq L \\ & X_{ji} & \longmapsto & C_{ji} \end{array}$$

we can consider the following diagram

$$\begin{array}{ccc} K\{Z_1,...,Z_n\} & \xrightarrow{\quad\psi\quad} & K\{y_1,...,y_n\} \subseteq L \\ \Big\downarrow \phi & & \Big\downarrow \sigma \\ K\{y_1,...,y_n\}[X_{ji}] \subseteq L[X_{ji}] & \xrightarrow{\quad ev \quad} & K\{y_1,...,y_n\} \subseteq L \end{array}$$

which is commutative:

$$\begin{cases} (\sigma \circ \psi)(Z_i) = \sigma(\psi(Z_i)) = \sigma(y_i) = \sum_{j=1}^n C_{ji} y_j \\ (ev \circ \phi)(Z_i) = ev(\phi(Z_i)) = ev\Big( \sum_{j=1}^n X_{ji} y_j \Big) = \sum_{j=1}^n C_{ji} y_j \end{cases}$$

so, if we consider any element $\delta \in \Delta = \phi(\text{Ker}(\psi))$,

$$\delta = \sum_{k=1}^{m_\delta} f_k^{(\delta)} \cdot l_k \qquad \text{with } f_k^{(\delta)} \in C_K[X_{ji}] \quad \forall k = 1, ..., m_\delta$$

then there exists an element $\chi \in \text{Ker}(\psi)$ such that $\phi(\chi) = \delta$, with this information, we get

$$0 = \sigma(0) = \sigma(\psi(\chi)) = (\sigma \circ \psi)(\chi) = (ev \circ \phi)(\chi) = ev(\phi(\chi)) =$$
$$ev(\delta) = ev\Big( \sum_{k=1}^{m_\delta} f_k^{(\delta)} \cdot l_k \Big) = \sum_{k=1}^{m_\delta} ev(f_k^{(\delta)}) \cdot l_k = \sum_{k=1}^{m_\delta} f_k^{(\delta)}(C_{ji}) \cdot l_k$$

and so $f_k^{(\delta)}(C_{ji}) = 0$ for all $k = 1, ..., m_\delta$ (since $\{l_k\}$ are linearly independent), and for all $\delta \in \Delta$. This is precisely what we wanted to prove: $f(C_{ji}) = 0 \ \forall f \in S$.

2) Conversely, consider a matrix $(C)_{ji} \in \text{GL}_n(C_K)$ such that $f(C_{ji}) = 0 \ \forall f \in S$. From the previous diagram, let's consider the differential $K$-morphism

$$\begin{array}{rccc} ev \circ \phi : & K\{Z_1, ..., Z_n\} & \longrightarrow & K\{y_1, ..., y_n\} \subseteq L \\ & Z_i & \longmapsto & \displaystyle\sum_{j=1}^n C_{ji} y_j \end{array}$$

that is,

$$\begin{array}{ccc} K\{Z_1,...,Z_n\} & \xrightarrow{\quad\psi\quad} & K\{y_1,...,y_n\} \subseteq L \\ & \searrow^{ev\circ\phi} & \Big\downarrow \text{we want to construct it} \\ & & K\{y_1,...,y_n\} \subseteq L \end{array}$$

It is easy to prove that $\text{Ker}(\psi) \subseteq \text{Ker}(ev \circ \phi)$: given $\chi \in \text{Ker}(\psi)$, the element $\delta \equiv \phi(\chi)$ is in $\Delta \subseteq L[X_{ji}]$, and just like before we can write it as

$$\delta = \sum_{k=1}^{m_\delta} f_k^{(\delta)} \cdot l_k \qquad \text{with } f_k^{(\delta)} \in C_K[X_{ji}] \quad \forall k = 1, ..., m_\delta$$

then

$$(ev \circ \phi)(\chi) = ev(\phi(\chi)) = ev(\delta) = ev\Big( \sum_{k=1}^{m_\delta} f_k^{(\delta)} \cdot l_k \Big) = \sum_{k=1}^{m_\delta} ev(f_k^{(\delta)}) \cdot l_k = \sum_{k=1}^{m_\delta} f_k^{(\delta)}(C_{ji}) \cdot l_k = 0$$

where the last equality holds by hypothesis. We can, then, construct a differential $K$-morphism given by

$$\begin{aligned} \sigma :\ K\{y_1,...,y_n\} &\longrightarrow K\{y_1,...,y_n\} \\ y_i \quad &\longmapsto \quad \sum_{j=1}^{n} C_{ji} y_j \end{aligned}$$

The next step is to prove that $\sigma$ is bijective:

· Since the matrix $(C)_{ji}$ is invertible, $\sigma$ is clearly surjective, because the image contains $\{y_1,...,y_n\}$.
· To prove the injectiveness, we have the following **Result** (the proof can be found in any book concerning Commutative Algebra, for example **Commutative ring theory, Theorem 2.4 (Hideyuki Matsumura)**)

If $f : R \longrightarrow R$ is a surjective $K-$algebra homomorphism, with $R$ domain and finitely generated as a $K-$algebra, then $f$ is also injective.

Since we are in this case, with $R = K\{y_1,...,y_n\}$, $\sigma$ is injective.

Finally, we have a bijective differential $K$-morphism

$$\begin{aligned} \sigma :\ K\{y_1,...,y_n\} &\longrightarrow K\{y_1,...,y_n\} \\ y_i \quad &\longmapsto \quad \sum_{j=1}^{n} C_{ji} y_j \end{aligned}$$

and so it can be extended to a differential $K$-automorphism defined over the quotient differential field $Quot(K\{y_1,...,y_n\}) = K\langle y_1,...,y_n\rangle$:

$$\begin{aligned} \sigma :\ K\langle y_1,...,y_n\rangle &\longrightarrow K\langle y_1,...,y_n\rangle \\ y_i \quad &\longmapsto \quad \sum_{j=1}^{n} C_{ji} y_j \end{aligned}$$

as we wanted to prove.

□

# Chapter 4

# The Fundamental Theorem of Differential Galois Theory

So far we have been studying the Differential Galois Group $\mathrm{DGal}(\mathcal{L})$ of a given linear differential equation $\mathcal{L} \in K[d]$, giving a representation of it as a subgroup of the invertible matrices with coefficients in $C_K$, the field of constants of $K$. We have also proven that it has more structure than that of a subgroup: it is a linear algebraic group, a Zariski closed subgroup of $\mathrm{GL}_n(C_K)$.

In this chapter we are going to establish the analogue of the Fundamental Theorem of Algebraic Galois Theory, which is stated below and a proof of it can be found in any introductory book about Field Theory and Galois Theory.

**Theorem 4.1** (Galois Correspondence).

*Let $L/K$ be a finite Galois extension. Then*

1. *The correspondences*

$$\begin{array}{ccc} \{\textit{subgroups of } Gal(L/K)\} & \longrightarrow & \{\textit{subfields } F \textit{ of } L \textit{ containing } K\} \\ H & \stackrel{\Phi}{\longmapsto} & \Phi(H) = L^H = \{x \in L \mid \sigma(x) = x \ \forall \sigma \in H\} \\ \Psi(F) = Aut_F(L) = Gal(L/F) & \stackrel{\Psi}{\longleftarrow\!\!\shortmid} & F \end{array}$$

   *define inclusion inverting mutually inverse maps.*

2. *The intermediate field $F$ defines a Galois extension $F/K$ if and only if $Gal(L/F) \triangleleft Gal(L/K)$. In this case, the restriction morphism*

$$\begin{array}{rccc} \varphi: & Gal(L/K) & \longrightarrow & Gal(F/K) \\ & \sigma & \longmapsto & \sigma_{|F} \end{array}$$

   *induces an isomorphism*

$$Gal(F/K) \cong Gal(L/K) \big/ Gal(L/F)$$

The theorem we are going to prove is analogous to this one, in the sense that the same results hold, just by adding the concepts of Zariski closed subgroups of $\mathrm{DGal}(\mathcal{L})$ and intermediate differential field $F$.

## 4.1 The Fundamental Theorem

In all this section $K \subseteq L$ will be a Picard-Vessiot extension of a linear differential operator $\mathcal{L} \in K[d]$, being $d$ the derivation on $K$, and $\mathrm{DGal}(\mathcal{L})$ its Differential Galois Group.
We start by proving a proposition which will lead us to define the previous correspondences in the context of differential fields and Zariski closed subgroups of $\mathrm{DGal}(\mathcal{L})$.

**Proposition 4.1.**

*In the situation mentioned before, we have the following results:*

1) *If $F$ is an intermediate differential subfield of $L$ containing $K$, then $F \subseteq L$ is again a Picard-Vessiot extension of the same operator $\mathcal{L}$.*
2) *If $H \leq DGal(\mathcal{L})$, then the field*

$$L^H \equiv \{x \in L \mid \sigma(x) = x \ \forall \sigma \in H\}$$

*is a differential subfield of $L$, that is, $L^H$ is closed under the derivation over $L$.*

*Proof.*

1) The result holds easily by thinking $\mathcal{L}$ defined ofer $F$, $\mathcal{L} \in K[d] \subseteq F[d]$, and taking into account that if $K \subseteq F \subseteq L$, we obtain a tower of constant fields $C_K \subseteq C_F \subseteq C_L$, so $C_K = C_F = C_L$ using that $K \subseteq L$ is a Picard-Vessiot extension.
2) Take $x \in L^H$; then

$$\sigma(x') = (\sigma(x))' = x' \qquad \forall \ \sigma \in H \text{ (differential morphisms)}$$

so $x' \in L^H$.

□

We are now ready to state the Fundamental Theorem (note that the correspondences are well-defined due to **Proposition 4.1**).

**Theorem 4.2** (Differential Galois Correspondence)**.**

*Let $K \subseteq L$ be the Picard-Vessiot extension of $\mathcal{L} \in K[d]$, and $DGal(\mathcal{L}) = DGal(L/K)$ its Differential Galois Group. Then*

1. *The correspondences*

$$\left\{\begin{matrix} \textit{Zariski closed} \\ \textit{subgroups of } DGal(\mathcal{L}) \end{matrix}\right\} \longrightarrow \left\{\begin{matrix} \textit{differential subfields} \\ \textit{of } L \textit{ containing } K \end{matrix}\right\}$$

$$\begin{array}{ccc} H & \stackrel{\widetilde{\Phi}}{\longmapsto} & \widetilde{\Phi}(H) = L^H \\ \widetilde{\Psi}(F) = DGal(L/F) & \stackrel{\widetilde{\Psi}}{\longleftarrow\!\!\!\dashv} & F \end{array}$$

*define inclusion inverting mutually inverse maps.*

2. *The intermediate differential field $F$ defines a Picard-Vessiot extension $K \subseteq F$ if and only if $DGal(L/F) \triangleleft DGal(L/K)$.*
   *In this case, the restriction morphism*

$$\begin{aligned} \varphi : \ DGal(L/K) &\longrightarrow DGal(F/K) \\ \sigma \quad &\longmapsto \quad \sigma_{|F} \end{aligned}$$

*induces an isomorphism*

$$DGal(F/K) \cong DGal(L/K) \Big/ DGal(L/F)$$

*Proof.* By definition, we have the inclusions

$$\begin{cases} H \leq \mathrm{DGal}(L/L^H) & \text{for all } H \leq \mathrm{DGal}(L/K) \\ F \subseteq L^{\mathrm{DGal}(L/F)} & \text{for all intermediate field } F \end{cases}$$

and a direct consequence of these facts are the equalities $L^H = L^{\mathrm{DGal}(L/L^H)}$ and $\mathrm{DGal}(L/L^{\mathrm{DGal}(L/F)}) = \mathrm{DGal}(L/F)$.

Again by definition, the correspondences invert inclusions,

$$\begin{cases} \text{if } K \subseteq F_1 \subseteq F_2 \subseteq L, \text{ then } \mathrm{DGal}(L/F_2) \leq \mathrm{DGal}(L/F_1) \\ \text{if } H_1 \leq H_2 \leq \mathrm{DGal}(L/K), \text{ then } L^{H_2} \subseteq L^{H_1} \end{cases}$$

The rest of the proof requires different results from algebraic geometry that go further than what we intend to study in this work, so we won't prove them here. For a proof of them the reader may consult [1, Chapter 6], [2, Chapter 6] or [6, Section 1.3.].

□

## 4.2 Some easy examples of the Differential Galois Correspondence

### 4.2.1 Adjunction of the exponential of the integral

Here we are going to briefly study an example, which will be a continuation of the example in **Section 3.2.2. Adjunction of the exponential of the integral**.

To be more specific, consider the differential field $\mathbb{C}(z)$ (with the usual derivation $\frac{d}{dz}$), and $z \in \mathbb{C}(z)$. It is easy to prove that does not exist an element $b \in \mathbb{C}(z) \backslash \{0\}$ and $n \in \mathbb{Z} \backslash \{0\} \subset \mathbb{Q} \hookrightarrow K$ such that $b' = nzb$. If that would be the case, we would have $b = \frac{p(z)}{q(z)}$ with

$$\frac{p(z)'q(z) - p(z)q(z)'}{q(z)^2} = nz\frac{p(z)}{q(z)}$$

If we define $n = \deg(p(z)), m = \deg(q(z))$,

$$\underbrace{(p(z)'q(z) - p(z)q(z)')}_{\text{degree}\leq\max\{(n-1)\cdot m, n\cdot(m-1)\}<n\cdot m} = \underbrace{nzp(z)q(z)}_{\text{degree}=n\cdot m+1}$$

which gives a contradiction.
Consider the differential equation

$$\mathcal{L}(y) = y' - zy = 0, \quad \mathcal{L} \in \mathbb{C}(z)\Big[\frac{d}{dz}\Big]$$

which has no solution in $\mathbb{C}(z)$, as we have already mentioned.

We already know from this example that, if we consider the differential field extension $\mathbb{C}(z) \subseteq L = \mathbb{C}(z)\langle e^{\frac{1}{2}z^2}\rangle = \mathbb{C}(z)(e^{\frac{1}{2}z^2}) = \mathbb{C}(e^{\frac{1}{2}z^2})$, the extension $\mathbb{C}(z) \subseteq L$ becomes a Picard-Vessiot extension of $\mathbb{C}(z)$ for $\mathcal{L}$, with Differential Galois Group given by

$$\mathrm{DGal}(\mathcal{L}) \cong \{c \mid c \in C^*_{\mathbb{C}(z)}\} = \mathbb{C}^* \qquad \text{the multiplicative group}$$

Let's now find all the closed non-trivial subgroups of $\mathbb{C}^*$. They are given by the roots of a finite family of polynomials

$$G = \{a \in \mathbb{C}^* \mid f_i(a) = 0, f_i(z) = z^{n_i} + a_{n_i-1}z^{n_i-1} + \cdots + a_0, i \in I \text{ finite } \}$$

We know that every polynomial $f_i(z)$ has exactly $n_i$ roots in $\mathbb{C}$ (counting multiplicity), so

$$|G| \leq \min\{n_i | i \in I\} < +\infty$$

that is, $G$ is a finite subgroup of $\mathbb{C}^*$; let's put $n = |G|$. From Lagrange's Theorem, for every $g \in G$, we must have

$$g^{|G|} = g^n = 1 \qquad \text{so } g \text{ is an } n\text{th root of unity}$$

So, every closed subgroup $G$ of $\mathbb{C}^*$ must be

$$G = \mu_n \equiv \left\{e^{2\pi i\frac{k}{n}} \mid k = 0, ..., n-1\right\} \subset \mathbb{C}^*$$

With that, we get the relation between the lattice of closed subgroups of $\mathbb{C}^*$ and differential intermediate fields $F$

$$\begin{array}{ccc}
\{1\} & \longleftrightarrow & L = \mathbb{C}(e^{\frac{1}{2}z^2}) \\
\Big| & & \Big| \\
\mu_n & \longleftrightarrow & L^{\mu_n} = \mathbb{C}(e^{\frac{n}{2}z^2}) \\
\Big| & & \Big| \\
\mathrm{DGal}(\mathcal{L}) = \mathbb{C}^* & \longleftrightarrow & K = \mathbb{C}(z)
\end{array}$$

### 4.2.2 An example with finite DGal($\mathcal{L}$)

Recall **Example 3 of Section 3.2.3. Concrete examples involving** $\mathbb{C}(z)$: consider the differential equation

$$0 = \mathcal{L}(y) = y' - \frac{1}{nz}y, \quad \mathcal{L} \in \mathbb{C}(z)\Big[\frac{d}{dz}\Big]$$

whose coefficients are analytic on a simply connected open set $U \subset \mathbb{C}\backslash\{0\}$; for example, let's take the region

$$U = \{z \in \mathbb{C} \mid |z+1| < 1\}$$

Its solution is $y(z) = \sqrt[n]{z}$ defined over $U$ if we take an analytic branch of $y(z)$ there; so,

$$\mathrm{Sol}(\mathcal{L})_L = \mathbb{C} \cdot \sqrt[n]{z} \qquad \text{with} \begin{cases} L = \mathbb{C}(z)\langle \sqrt[n]{z} \rangle = \mathbb{C}(\sqrt[n]{z}) \\ C_L = C_K = \mathbb{C} \end{cases}$$

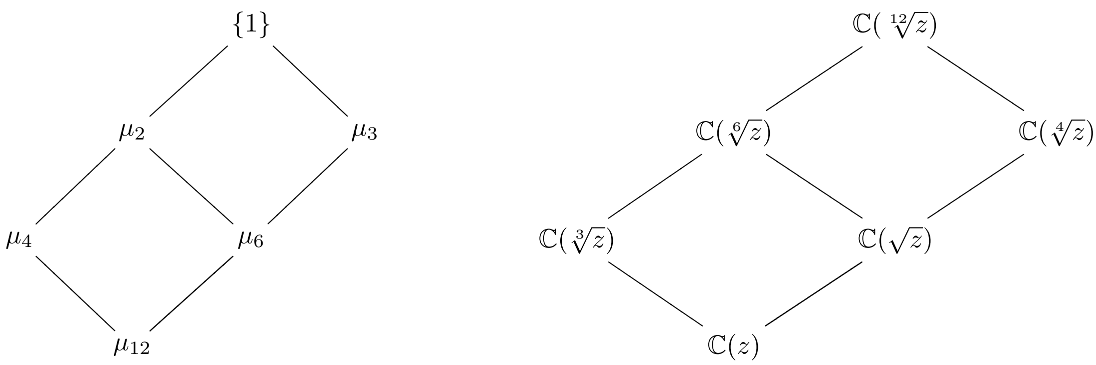
and so $\mathbb{C}(\sqrt[n]{z})/\mathbb{C}(z)$ is a Picard-Vessiot extension for $\mathcal{L}$. Its Differential Galois Group is given by

$$\mathrm{DGal}(\mathcal{L}) \cong \mu_n = \left\{ e^{2\pi i \frac{k}{n}} \mid k = 0, ..., n-1 \right\} \subset \mathbb{C}^* \qquad \text{a finite cyclic group of order } n$$

It is straightforward to prove that every closed subgroup of $\mu_n$ is $\mu_m$ with $m|n$. So, here we have the lattices

$$\begin{array}{ccc} \{1\} & \longleftrightarrow & L = \mathbb{C}(\sqrt[n]{z}) \\ | & & | \\ \mu_m & \longleftrightarrow & L^{\mu_m} = \mathbb{C}(\sqrt[n/m]{z}) \\ | & & | \\ \mathrm{DGal}(\mathcal{L}) = \mu_n & \longleftrightarrow & K = \mathbb{C}(z) \end{array}$$

For example, if $n = 12$, we obtain the complete lattices given by



# Chapter 5

# Liouvillian extensions: the analogue of radical extensions

In this last chapter we will finally study some particular differential field extensions, which are the analogues of radical extensions in the Algebraic Galois Theory: the Liouvillian extensions. These extensions will provide us some criteria in order to decide when a given linear differential equation over $\mathbb{C}(z)$ is **solvable by quadratures**[1].

We are not going to prove all the results announced, but we will use them in order to develop our study in a more deeper way.

First of all, we will state some important results about linear algebraic groups, for example some properties concerning its irreducible components (which will be of crucial importance in the study of elementary functions). We will also introduce a new operation between groups: the semi-direct product (a generalization of the classical direct product): this will be important to study because some Differential Galois Groups will be of this form.

After that, we will define the notion of Liouvillian extensions in an abstract context and state, as in Algebraic Galois Theory, a fundamental theorem relating Liouvillian extensions and solvability of its Differential Galois Group [2].

Moreover, we would be ready to give some physical examples concerning linear differential equations solvable by quadratures, for example the quantum harmonic oscillator, studying them by using Kovacic's criterion, which characterizes what type of solutions we can get in a linear differential equation of order 2.

Finally, we will focus our efforts in the study of linear differential equations over $\mathbb{C}(z)$, giving a formal definition of what we understand as elementary functions, through a field called a **field of elementary functions**. We will focus on the definition given by [2, Chapter 6]. There are other definitions for elementary functions that are more familiar and intuitive, for example the ones given in [19, Section 1] or [20]; we will only focus on Magid's definition, which does not allow all the standard elementary

[1] We will define this concept lately.

[2] More precisely, solvability of its irreducible component containing the identity, $\mathrm{DGal}(\mathcal{L})^0$.

functions, but this restriction will give us a beautiful criterion concerning its Differential Galois Group. We will end this study by proving the well-known result that the function

$$\int e^{-z^2} dz$$

cannot be expressed in terms of elementary functions (in Magid's sense)[3]. In order to answer this question, we will study the symmetries of the linear differential equation

$$0 = y'' + 2zy \in \mathbb{C}(z)\left[\frac{d}{dz}\right]$$

which in particular has the previous function as a solution.

## 5.1 A continuation in the study of Linear Algebraic Groups

We have already seen in **Section 3.3.3. Introduction to Linear Algebraic Groups** that for any $r, s \in \mathbb{Z}^+$, the direct product $\mathbb{G}_a^r \times \mathbb{G}_m^s$ is a linear algebraic group; in matrix form, it can be viewed as a subgroup of $\mathrm{GL}_{2r+s}(\mathbb{A})$ via

$$\begin{pmatrix} \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \begin{pmatrix} 1 & a_r \\ 0 & 1 \end{pmatrix} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \begin{pmatrix} b_1 \end{pmatrix} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \begin{pmatrix} b_s \end{pmatrix} \end{pmatrix} \qquad a_1, ..., a_r \in \mathbb{A}; b_1, ..., b_s \in \mathbb{A}^*$$

Some other examples of linear algebraic groups are the following.

**Examples 5.1.**

*1) The* ***special linear group****, defined as*

$$SL_n(\mathbb{A}) \equiv \{A \in GL_n(\mathbb{A}) \mid \det(A) = 1\}$$

*2) The* ***upper triangular group****, defined as*

$$T_n(\mathbb{A}) \equiv \{A \in GL_n(\mathbb{A}) \mid a_{ij} = 0 \text{ for } i > j\}$$

*3) The* ***upper triangular unipotent group****, defined as*

$$U_n(\mathbb{A}) \equiv \{A \in T_n(\mathbb{A}) \mid a_{ii} = 1 \ \forall i\}$$

[3] It is also true for the standard definition but, as we have already said, we will not study it in this work.

*4) The **diagonal group**, defined as a particular case of the previous product*

$$D_n(\mathbb{A}) \equiv \{A \in GL_n(\mathbb{A}) \mid a_{ij} = 0 \text{ for } i \neq j\} \cong \mathbb{G}_m^n$$

In general, we can define

**Definition 5.1.** *Let $G \subseteq GL_n(\mathbb{A})$ be a linear algebraic group.*

- *a) We say $G$ is **diagonalizable** if it is isomorphic (via conjugation) to a subgroup of $D_n(\mathbb{A})$.*
- *b) We say $G$ is **trigonalizable** if it is isomorphic (via conjugation) to a subgroup of $T_n(\mathbb{A})$.*
- *c) We say $G$ is **unipotent** if it is isomorphic (via conjugation) to a subgroup of $U_n(\mathbb{A})$.*

### 5.1.1 Irreducible components of (Linear) Algebraic Groups

In this part we are going to quickly review a concept which will be important in the study of Liouvillian extensions.

**Definition 5.2** (Connectedness).

*Let $X$ be a topological space. It is said to be irreducible if it cannot be decomposed as*

$$X = X_1 \cup X_2 \qquad \text{being } X_1, X_2 \textbf{ proper closed} \text{ subsets of } X$$

*It is said to be reducible if it is not irreducible. In this case, if we can put $X = X_1 \cup X'$ being $X_1$, $X'$ proper closed sets of $X$, and $X_1$ irreducible, we say $X_1$ is an **irreducible component** of $X$.*

The following proposition will provide us the basic study of connectedness in the case of (linear) algebraic groups. A proof of it can be found at [1, Chapter 3] or [13, Chapter 1].

**Proposition 5.1.**

*Let $G \subseteq GL_n(\mathbb{A})$ be a (linear) algebraic group. Then $G$ has a unique irreducible component $G^\circ$ containing the identity element. Also, the following statements hold:*

- *1) $G^\circ$ is a normal subgroup of $G$, with $[G : G^\circ] < +\infty$.*
- *2) Each closed subgroup $H \subseteq G$ with $[G : H] < +\infty$ contains $G^\circ$.*

**Definition 5.3.** *We will call a (linear) algebraic group **connected** if $G = G^0$.*

The following proposition gives us different examples of some connected linear algebraic groups. Again, a proof can be found at [1, Chapter 3].

**Proposition 5.2.**

*The following linear algebraic groups are connected:*

- *1) $\mathbb{G}_a$ and $\mathbb{G}_m$, and hence any direct product $\mathbb{G}_a^r \times \mathbb{G}_m^s$.*
- *2) The linear alebraic groups of **Examples 5.1**: $SL_n(\mathbb{A})$, $T_n(\mathbb{A})$, $U_n(\mathbb{A})$, $D_n(\mathbb{A})$.*

Finally, an important theorem we will use is the **Lie-Kolchin Theorem**, which gives the structure of linear algebraic groups that are connected and solvable[4].

**Theorem 5.1** (Lie-Kolchin Theorem)**.**

*Let $G \subseteq GL_n(\mathbb{A})$ be a connected solvable linear algebraic group.*

*Then $G$ is trigonalizable, that is*[5]*,*

$$G \cong U \rtimes \mathbb{G}_m^r \qquad \textit{for some } r \leq n \text{ , } \textit{where } U \textit{ is unipotent}$$

An intuition of the descomposition of this theorem is the following: if $G$ is trigonalizable, we can think of elements in the group as being of the form

$$\begin{pmatrix} ** & * & * & * \\ \mathbf{0} & ** & * & * \\ \mathbf{0} & \mathbf{0} & ** & * \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & ** \end{pmatrix} = \begin{pmatrix} 1 & * & * & * \\ \mathbf{0} & 1 & * & * \\ \mathbf{0} & \mathbf{0} & 1 & * \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 \end{pmatrix} \cdot \begin{pmatrix} ** & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ** & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & ** & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & ** \end{pmatrix} \qquad * \in \mathbb{A}; ** \in \mathbb{A}^*$$

The first matrix of this descomposition is an element of $U_n(\mathbb{A})$, and hence unipotent. The second matrix is an element of $D_n(\mathbb{A})$, and hence diagonal; in fact, if this matrix has $r$ independent elements in the diagonal different from 1, the group which they formed is isomorphic to $\mathbb{G}_m^r$, such as the theorem says.

For a complete proof of **Lie-Kolchin Theorem**, the reader may consult [1, Chapter 4], [13, Chapter 4] or [14, Chapter 1.4].

### 5.1.2 Direct and Semidirect product of groups

**Definition 5.4.** *Let $G$ be a subgroup, and $H, K \leq G$.*

*We say $G$ is the **semidirect product** of $H$ by $K$ if $G = HK$, with the properties*

$$\begin{cases} H \lhd G \\ H \cap K = \{e\} \end{cases}$$

*We will denote it by $H \rtimes K$.*[6]

**Examples 5.2.**

*1)* We already know that

$$\mathbb{Z}/(6) \cong \mathbb{Z}/(3) \times \mathbb{Z}/(2)$$

In this case we obtain the direct product, since both $\mathbb{Z}/(3), \mathbb{Z}/(2) \lhd \mathbb{Z}/(6)$ (the group is abelian).

[4]For linear algebraic groups, the definition of being solvable is quite the same as in finite groups, but more restrictive: that is, a linear algebraic group $G$ is solvable if there exists a chain of **closed** subgroups $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$ such that $G_{i-1} \lhd G_i$ and $G_i/G_{i-1}$ is abelian for $i = 1, ..., m$.

[5]We will introduce the concept of semidirect product $\rtimes$ in the following **Section 5.1.2. Direct and Semidirect product of groups**. It is a generalization of the common direct product.

[6]Note that we do not assume $K$ to be normal; in fact, if $K \lhd G$, then $G$ is the usual direct product, denoted by $H \times K$.

*2)* Taking again $\mathbb{Z}/(3)$ and $\mathbb{Z}/(2)$, viewed as subgroups of $S_3$, we know that $\mathbb{Z}/(3) \lhd S_3$ (has index 2) but not $\mathbb{Z}/(2)$. It is not difficult to prove that

$$S_3 \cong \mathbb{Z}/(3) \rtimes \mathbb{Z}/(2)$$

*3)* Consider the linear algebraic group

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} |c \in \mathbb{C}, d \in \mathbb{C}^* \right\} \subseteq GL_2(\mathbb{C})$$

We can easily see that any element in $G$ can be written as

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \qquad \text{with } \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in U_2(\mathbb{C}) \cong \mathbb{G}_a \ , \ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \in G \cap D_2(\mathbb{C}) \cong \mathbb{G}_m$$

and so $G \cong \mathbb{G}_a \cdot \mathbb{G}_m$. Also, for any elements $g = \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \in G$ and $h = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \in U_2(\mathbb{C})$,

$$ghg^{-1} = \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -cd^{-1} & d^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ ad & 1 \end{pmatrix} \in U_2(\mathbb{C})$$

and hence $U_2(\mathbb{C}) \lhd G$. On the contrary, if we take $g = \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \in G$ and $k = \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \in G \cap D_2(\mathbb{C})$,

$$gkg^{-1} = \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -cd^{-1} & d^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c(1-b) & b \end{pmatrix}$$

which in general is not an element $G \cap D_2(\mathbb{C})$, and hence $G \cap D_2(\mathbb{C})$ is not a normal subgroup of $G$. Finally, it is clear that $(G \cap D_2(\mathbb{C})) \cap U_2(\mathbb{C}) = \{Id\}$. With all these properties, we can write $G \cong \mathbb{G}_a \rtimes \mathbb{G}_m$ and we obtain a non-abelian group, as we already knew. We will revisit this example lately in this work.

## 5.2 Liouvillian extensions

Let's finally define the concept of a Liouvillian extension.

**Definition 5.5.** *Let $K$ be a differential field with algebraically closed set of constants $C_K$, and let $K \subseteq L$ be an extension of differential fields. The extension is said to be* ***Liouvillian*** *if $C_L = C_K$, i.e. no new constants are added, and if there exists a finite tower of differential fields*

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{l-1} \subseteq K_l = L$$

*such that $K_i$ is obtained from $K_{i-1}$ either by*

*1) adjunction of an integral: $K_i = K_{i-1}(t_i)$ with $t_i' \in K_{i-1}$.*

*2) adjunction of the exponential of an integral: $K_i = K_{i-1}(t_i)$ with $t_i \neq 0$ and $\frac{t_i'}{t_i} \in K_{i-1}$.*

*3) adjunction of an algebraic element: $K_i = K_{i-1}(t_i)$ with $t_i$ algebraic over $K_{i-1}$.*

**Definition 5.6.**

*In the same notation as before, let now $\mathcal{L} \in K[d]$ be a linear differential operator, and $K \subseteq E$ its Picard-Vessiot extension.*

*We say the solutions of $\mathcal{L}(y) = 0$ in $E$ are* ***Liouvillian*** *if there exists a Liouvillian extension $K \subseteq L$ such that $E$ is contained in it, that is, $K \subseteq E \subseteq L$.*

This is the idea that a linear differential equation is **solvable by quadratures**: if its solutions are Liouvillian, that is, they are expressible through integrals, exponentials of integrals and algebraic elements.[7]

### 5.2.1 Returning to the abstract examples in section 3.2.

**Adjunction of the integral**

Here we have a differential field $K$ and $a \in K$ an element which is not a derivative of any element, i.e. it does not exist $b \in K$ such that $b' = a$.

We already know that the extension $K \subseteq K(\alpha) = L$, being $\alpha$ an indeterminate, with the derivation $\alpha' = a$, is a Picard-Vessiot extension of $K$ for $\mathcal{L}(y) = y'' - \frac{a'}{a}y'$, with Differential Galois Group given by

$$\mathrm{DGal}(\mathcal{L}) \cong \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \;\middle|\; c \in C_K \right\} \cong (C_K, +) \cong \mathbb{G}_a \quad \text{the additive group}$$

In fact, this is general: given any transcendental element $t$ over $K$, with $t' \in K$, the extension $K \subseteq K(t)$ will be a Picard-Vessiot extension (for $\mathcal{L}(y) = y'' - \frac{t''}{t'}y'$), and its Differential Galois Group will be

$$\mathrm{DGal}(K(t)/K) \cong \mathbb{G}_a$$

It is obvious that all solutions of $\mathcal{L}$ are Liouvillian, since we are only **adjoining an integral** in $K$, and hence $K \subseteq K(t)$ is itself a Liouvillian extension.

As an example over $\mathbb{C}(z)$ with the usual derivation, we have

$$\mathrm{DGal}(\mathbb{C}(z, \ln(z))/\mathbb{C}(z)) \cong \mathbb{G}_a$$

since $\ln(z)' = \frac{1}{z} \in \mathbb{C}(z)$, and hence any symmetry, preserving the derivation, of the differential equation $y'' + \frac{1}{z}y'$ will be of the form

$$\ln(z) \longmapsto \ln(z) + c \quad , \quad c \in \mathbb{C}$$

**Adjunction of the exponential of the integral**

Here we have a differential field $K$ and $a \in K$ an element such that it does not exist $b \in K \backslash \{0\}$ and $n \in \mathbb{Z} \backslash \{0\} \subset \mathbb{Q} \hookrightarrow K$ such that $b' = nab$.

[7] This is not the common definition of solvability by quadratures: the common one does not admit algebraic extensions. We will allow this kind of extensions.

We already know that the extension $K \subseteq K(\alpha) = L$, being $\alpha$ an indeterminate, with derivation $\alpha' = a\alpha$, is a Picard-Vessiot extension of $K$ for $\mathcal{L}(y) = y' - ay$, with Differential Galois Group given by

$$\mathrm{DGal}(\mathcal{L}) \cong \{c \mid c \in C_K^*\} = (C_K^*, \cdot) \cong \mathbb{G}_m \quad \text{the multiplicative group}$$

As before, this is general: given any transcendental element $t$ over $K$, with $t'/t \in K$, the extension $K \subseteq K(t)$ will be a Picard-Vessiot extension (for $\mathcal{L}(y) = y' - \frac{t'}{t}y$), and its Differential Galois Group will be

$$\mathrm{DGal}(K(t)/K) \cong \mathbb{G}_m$$

It is obvious that all solutions of $\mathcal{L}$ are Liouvillian, since we are only **adjoining the exponential of an integral** in $K$, and hence $K \subseteq K(t)$ is itself a Liouvillian extension.

Again, as an example over $\mathbb{C}(z)$ with the usual derivation, we have

$$\mathrm{DGal}(\mathbb{C}(z, e^{-z^2})/\mathbb{C}(z)) \cong \mathbb{G}_m$$

since $\frac{(e^{-z^2})'}{e^{-z^2}} = -2z \in \mathbb{C}(z)$, and hence any symmetry, preserving the derivation, of the differential equation $y' + 2zy$ will be of the form

$$e^{-z^2} \longmapsto c \cdot e^{-z^2} \quad , \quad c \in \mathbb{C}^*$$

### 5.2.2 Characterization of liouvillian solutions

The following theorem is the main result of this section and will not be proven (see [3, Chapter 1.5] fot a complete proof of it). It states a criteria about when the solutions of a given linear differential equation are liouvillian through the Differential Galois Group of its Picard-Vessiot extension.

**Theorem 5.2** (Characterizing liouvillian solutions)**.**

*Let $\mathcal{L} \in K[d]$ be a linear differential operator of degree $n$ defined over a differential field $K$ with derivation $d$.*

*Let $K \subseteq E$ be its Picard-Vessiot extension, and DGal($\mathcal{L}$) its Differential Galois Group.*

*Then the following statements are equivalent:*

*1) The irreducible component of DGal($\mathcal{L}$) containing the identity, DGal($\mathcal{L}$)$^0$, is solvable* [8]*.*

*2) The solutions of $\mathcal{L}(y) = 0$ in $E$ are Liouvillian, i.e., $\mathcal{L}(y) = 0$ is solvable by quadratures.*

*In this case, and due to **Lie-Kolchin Theorem 5.1**,*

$$DGal(\mathcal{L})^0 \cong U \rtimes \mathbb{G}_m^r \qquad \textit{for some } r \text{ , } \textit{where } U \textit{ is unipotent}$$

[8] In such a case, when the irreducible component $G^0$ of a linear algebraic group $G$ is solvable, we say $G$ is **virtually solvable**.

### 5.2.3 Kovacic's criterion for linear differential equations of degree 2

In this section we shall present a direct application of Differential Galois Theory in the case of linear differential equations of the form

$$\mathcal{L}(y) = y''(z) + a(z)y(z) = 0 , \quad a(z) \in \mathbb{C}(z)$$

that is, linear differential equations of degree 2.[9]

We start by finding all linearly independent solutions of $\mathcal{L}(y) = 0$, by noting that if $y_1(z)$ is a solution, so is $y_2(z) = y_1(z) \int \frac{dw}{y_1^2(w)}$:

$$\begin{aligned} y_2''(z) + a(z)y_2(z) &= y_1''(z) \int \frac{dw}{y_1^2(w)} + \frac{y_1'(z)}{y_1^2(z)} - \frac{y_1'(z)}{y_1^2(z)} + a(z)y_1(z) \int \frac{dw}{y_1^2(w)} = \\ &= \Big( y_1''(z) + a(z)y_1(z) \Big) \int \frac{dw}{y_1^2(w)} = 0 \end{aligned}$$

and it is clear that they are linearly independent over $\mathbb{C}$, since

$$W(y_1, y_2) = \begin{vmatrix} y_1 & y_2 \\ y_1' & y_2' \end{vmatrix} = \begin{vmatrix} y_1 & y_1 \int \frac{1}{y_1^2} \\ y_1' & y_1' \int \frac{1}{y_1^2} + \frac{1}{y_1} \end{vmatrix} = 1 \neq 0$$

This tells us that, if a solution is Liouvillian ($y_1(z)$), they all are ($y_1(z)$ and $y_2(z)$).
Much more, $W$ is constant, and hence for any differential $\mathbb{C}(z)$-automorphism $\sigma \in \mathrm{DGal}(\mathcal{L})$ we must have

$$\sigma(W) = W$$

If we put, as for every Differential Galois Group,

$$\Big(\sigma(y_1), \sigma(y_2)\Big) = \Big(y_1, y_2\Big) \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \Big(y_1, y_2\Big) C_\sigma \qquad \text{with } C_\sigma \in \mathrm{GL}_2(\mathbb{C})$$

we obtain

$$\begin{aligned} W = \sigma(W) = \sigma(y_1 y_2' - y_2 y_1') &= (c_{11}y_1 + c_{21}y_2)(c_{12}y_1' + c_{22}y_2') - (c_{12}y_1 + c_{22}y_2)(c_{11}y_1' + c_{21}y_2') = \\ &= (c_{11}c_{22} - c_{12}c_{21})(y_1 y_2' - y_2 y_1') = \det(C_\sigma)W \end{aligned}$$

and hence $\det(C_\sigma) = 1$, which means that $\mathrm{DGal}(\mathcal{L})$ is a closed subgroup not only of $\mathrm{GL}_2(\mathbb{C})$ but of $\mathrm{SL}_2(\mathbb{C})$, the special linear group.

This observation is really important, because in order to study properties of the solutions of the previous differential equation we only need to study the closed subgroups of $\mathrm{SL}_2(\mathbb{C})$; this study is given in the following proposition, and a proof of it can be found in [1, Chapter 4] or [16, Section 1.4]:

[9] This is the most general form we can study, since every equation of the form

$$y''(z) + a(z)y'(z) + b(z)y(z) = 0$$

can be transformed by $y(z) \longmapsto e^{\int \frac{a}{2}} y(z) = Y(z)$ in

$$Y''(z) + \Big(b(z) - \frac{1}{2}a(z)' - \frac{1}{4}a(z)^2\Big)Y(z) = 0$$

**Proposition 5.3** (Classification of the closed subgroups of $\mathrm{SL}_2(\mathbb{C})$).

*Let $G$ be an algebraic subgroup of $SL_2(\mathbb{C})$. Then one of the following cases holds:*

*1) $G$ is trigonalizable.*

*2) $G$ is isomorphic (via conjugation) to a subgroup of*

$$D^+ = \Big\{ \begin{pmatrix} c & 0 \\ 0 & \frac{1}{c} \end{pmatrix} \Big| c \in \mathbb{C}^* \Big\} \cup \Big\{ \begin{pmatrix} 0 & c \\ -\frac{1}{c} & 0 \end{pmatrix} \Big| c \in \mathbb{C}^* \Big\}$$

*and* 1) *does not hold.*

*3) $G$ is finite and* 1), 2) *do not hold.*

*4) $G = SL_2(\mathbb{C})$.*

With this classification, we can now study the different situations and solutions of the linear differential equation

$$\mathcal{L}(y) = y''(z) + a(z)y(z) = 0 \qquad a(z) \in \mathbb{C}(z)$$

**Case** 1) If $\mathrm{DGal}(\mathcal{L})$ is trigonalizable,

$$\mathrm{DGal}(\mathcal{L}) \cong \Big\{ \begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix} \Big| a \in \mathbb{C}^*, b \in \mathbb{C} \Big\}$$

and hence there is a solution $y_1(z)$ such that, for every $\sigma \in \mathrm{DGal}(\mathcal{L})$,

$$\sigma(y_1(z)) = \frac{1}{a_\sigma} y_1(z)$$

so

$$\sigma\Big(\frac{y_1(z)'}{y_1(z)}\Big) = \frac{\sigma(y_1(z))'}{\sigma(y_1(z))} = \frac{y_1(z)'}{y_1(z)} \qquad \forall \sigma \in \mathrm{DGal}(\mathcal{L})$$

hence the elemeny $\frac{y_1'}{y_1}$ is fixed for every $\mathrm{DGal}(\mathcal{L})$, which by the Galois Correspondence implies that $w = \frac{y_1'}{y_1} \in \mathbb{C}(z)$, so it has a solution of the form $y_1(z) = e^{\int w}$; the solutions in this case are

$$\begin{cases} y_1(z) = e^{\int w} \\ y_2(z) = e^{\int w} \int e^{-2\int w} \end{cases} \qquad \text{with } w \in \mathbb{C}(z) \text{ ; Liouvillian solutions}$$

**Case** 2) If

$$\mathrm{DGal}(\mathcal{L}) \cong G \subseteq \Big\{ \begin{pmatrix} c & 0 \\ 0 & \frac{1}{c} \end{pmatrix} \Big| c \in \mathbb{C}^* \Big\} \cup \Big\{ \begin{pmatrix} 0 & c \\ -\frac{1}{c} & 0 \end{pmatrix} \Big| c \in \mathbb{C}^* \Big\}$$

and Case 1) does not hold, there are solutions $y_1(z)$ and $y_2(z)$ such that for any $\sigma \in \mathrm{DGal}(\mathcal{L})$,

$$\begin{cases} \sigma(y_1(z)) = c_\sigma y_1(z) \\ \sigma(y_2(z)) = \frac{1}{c_\sigma} y_2(z) \end{cases} \qquad \text{or} \qquad \begin{cases} \sigma(y_1(z)) = c_\sigma y_2(z) \\ \sigma(y_2(z)) = -\frac{1}{c_\sigma} y_1(z) \end{cases}$$

Now, if we define $w_1 = \frac{y_1'}{y_1}$ and $w_2 = \frac{y_2'}{y_2}$, we obtain

in the first case, $\begin{cases} \sigma(w_1) = w_1 \\ \sigma(w_2) = w_2 \end{cases}$ and in the second case, $\begin{cases} \sigma(w_1) = w_2 \\ \sigma(w_2) = w_1 \end{cases}$ $\forall \sigma \in \mathrm{DGal}(\mathcal{L})$

Minimally, both cases are handled by

$$\sigma^2(w_1) = w_1 \quad \sigma^2(w_2) = w_2$$

Observe that, in this case,

$$\mathrm{DGal}(\mathcal{L})^2 \equiv \{\sigma^2 | \sigma \in \mathrm{DGal}(\mathcal{L})\} \subseteq \left\{ \begin{pmatrix} c & 0 \\ 0 & \frac{1}{c} \end{pmatrix} \Big| c \in \mathbb{C}^* \right\}$$

is a closed normal subgroup of index 2, and so again by Galois Correspondence $w_1, w_2$ are algebraic over $\mathbb{C}(z)$ with degree 2; finally, at least one solution is of the form $y_1(z) = e^{\int w}$, and hence the solutions are

$\begin{cases} y_1(z) = e^{\int w} \\ y_2(z) = e^{\int w} \int e^{-2\int w} \end{cases}$ with $w$ algebraic of degree 2 over $\mathbb{C}(z)$ ; Liouvillian solutions

**Case** 3) If $\mathrm{DGal}(\mathcal{L})$ is finite and Cases 1), 2) do not hold, there are only a finite number of differential $\mathbb{C}(z)$-automorphisms $\sigma_1, ..., \sigma_n$; then, for every $r = 1, ..., n$, the element

$$Y_r = \sum_{1 \le i_1 < i_2 < \cdots < i_r \le n} \sigma_{i_1}(y_1)\sigma_{i_2}(y_1) \cdots \sigma_{i_r}(y_1)$$

is invariant under $\mathrm{DGal}(\mathcal{L})$, since if $\sigma_j \in \mathrm{DGal}(\mathcal{L})$,

$$\begin{aligned} \sigma_j(Y_r) = \sigma_j\Big( & \sum_{1 \le i_1 < i_2 < \cdots < i_r \le n} \sigma_{i_1}(y_1)\sigma_{i_2}(y_1) \cdots \sigma_{i_r}(y_1)\Big) = \\ &= \sum_{1 \le i_1 < i_2 < \cdots < i_r \le n} (\sigma_j \circ \sigma_{i_1})(y_1)(\sigma_j \circ \sigma_{i_2})(y_1) \cdots (\sigma_j \circ \sigma_{i_r})(y_1) = \\ &= \sum_{1 \le j_1 < j_2 < \cdots < j_r \le n} \sigma_{j_1}(y_1)\sigma_{j_2}(y_1) \cdots \sigma_{j_r}(y_1) = Y_r \end{aligned}$$

Then, by the Galois Correspondence, $Y_r \in \mathbb{C}(z)$ for $r = 1, ..., n$.
Consider now the polynomial

$$P(y) = \prod_{i=1}^{n} (y - \sigma_i(y_1)) = y^n - Y_1 y^{n-1} + Y_2 y^{n-2} + \cdots + (-1)^n Y_n \in \mathbb{C}(x)[y]$$

It is a monic polynomial with coefficients in $\mathbb{C}(z)$ which has $y_1$ as one of its roots, because one of the $\sigma's$ has to be the identity element. So $y_1$ is algebraic over $\mathbb{C}(z)$.
Since the same argument can be made for $y_2$, we obtain that all the solutions are algebraic over $\mathbb{C}(z)$.

**Case** 4) Finally, let's study the case when

$$\mathrm{DGal}(\mathcal{L}) \cong \mathrm{SL}_2(\mathbb{C})$$

Here it is necessary to announce some properties about the linear algebraic group $\mathrm{SL}_2(\mathbb{C})$: it is well-known that $\mathrm{SL}_2(\mathbb{C})$ is a non-abelian group, and from **Proposition 5.2**, it is also **connected**. Moreover, as the reader can verify in [1, Chapter 4], it is also a **non-solvable** group.
Then, we have $\mathrm{DGal}(\mathcal{L})^0 = \mathrm{DGal}(\mathcal{L}) = \mathrm{SL}_2(\mathbb{C})$ which is not solvable: by **Theorem 5.2**, the solutions of the linear differential equation we are treating are not liouvillian, and hence it is not solvable by quadratures.

The classification of solutions we have already done is referred to as **Kovacic's criterion**.

It is possible to compute explicitly Liouvillian solutions by applying **Kovacic's algorithm**; if the reader is interested in this topic, the algorithm is given in [1, Chapter 7], [16] or [17].

Much more, Kovacic established necessary conditions for each of the three first cases to hold; in order to provide some applications into physics in the next section we shall announce here these conditions, although they will not be proven.[10]

Since $a(z) = \frac{p(z)}{q(z)} \in \mathbb{C}$ is a rational function, we shall speak of the poles of it (meaning the poles in the complex plane): remember that the poles of $a(z)$ are the zeros of $q(z)$, and the order of every pole is the multiplicity of the zero of $q(z)$; by the order of $a(z)$ at infinity we are referring to $-(\deg(p) - \deg(q))$.

**Theorem 5.3** (Kovacic's necessary conditions)**.**

*The following conditions are necessary (though not sufficient) for each of the respective cases in* ***Kovacic's criterion*** *to hold:*

***Case*** *1) Every pole of $a(z)$ must have* ***even order*** *or* ***order 1****.*
*The order of $a(z)$ at infinity must be* ***even*** *or* ***greater than 2****.*

***Case*** *2) $a(z)$ must have at least one pole that either has* ***odd order greater than 2*** *or* ***order 2****.*

***Case*** *3) The order of a pole of $a(z)$* ***cannot exceed 2****.*
*The order of $a(z)$ at infinity must be* ***at least 2****.*

### 5.2.4 Integrable systems in physics: an application to Kovacic's criterion

An interesting application of **Kovacic's criterion** is whenever a system of homogeneous linear differential equations is solvable by quadratures or not. We are dealing with linear differential equations of the form

$$\mathcal{L}(y) = y''(z) + a(z)y(z) = 0 \qquad a(z) \in \mathbb{C}(z)$$

[10] Again, the proof of these conditions can be found at [1, Chapter 7], [16] or [17].

Equations of this type are typical in physics, for example the harmonic oscil·lator

$$y''(z) + \frac{k}{m}y(z) = 0$$

the Airy equation

$$y''(z) - zy(z) = 0$$

or the quantum harmonic oscil·lator

$$y''(z) + \frac{m^2w^2}{\hbar^2}\Big(\frac{2E}{mw^2} - z^2\Big)y(z) = 0$$

Let's study these differential equations as examples.

**The harmonic oscillator**

Here we have the linear differential equation

$$y''(z) + \frac{k}{m}y(z) = 0 \qquad \text{and} \qquad a(z) = \frac{k}{m} \equiv w_0^2 \in \mathbb{C}$$

In this case $a(z)$ has no poles in $\mathbb{C}$, and has order 0 at infinity. Hence Cases 2) and 3) cannot hold, and so it can only be Case 1), $\text{DGal}(\mathcal{L})$ trigonalizable, or Case 4), $\text{DGal}(\mathcal{L}) \cong \text{SL}_2(\mathbb{C})$.

In fact, we already know that two linearly independent solutions are

$$\begin{cases} e^{iw_0z} \\ e^{-iw_0z} \end{cases} \qquad \text{or} \qquad \begin{cases} \sin(w_0z) = \frac{e^{iw_0z}-e^{-iw_0z}}{2i} \\ \cos(w_0z) = \frac{e^{iw_0z}+e^{-iw_0z}}{2} \end{cases} \qquad \text{which are clearly Liouvillian}$$

and hence $\text{DGal}(\mathcal{L})$ is trigonalizable; furthermore, this example is exactly the same as **Example 1) of Section 3.2.3. Concrete examples involving** $\mathbb{C}(z)$, which leads to

$$\text{DGal}(\mathcal{L}) \cong \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\Big|\; a, b \in \mathbb{C}, a^2+b^2 = 1 \right\} \underbrace{\cong}_{\text{via conjugation}} \left\{ \begin{pmatrix} a+\sqrt{a^2-1} & 0 \\ 0 & a-\sqrt{a^2-1} \end{pmatrix} \;\Big|\; a \in \mathbb{C} \right\}$$

We have solutions of the form given by Kovacic's criterion in this case, $e^{\pm iw_0z} = e^{\int \pm iw_0}$, as it should be.

**The Airy equation**

Here we have the linear differential equation

$$y''(z) - zy(z) = 0 \qquad \text{and} \qquad a(z) = -z \in \mathbb{C}(z)$$

In this case $a(z)$ has no poles in $\mathbb{C}$, and has order $-1$ at infinity. Hence Cases 1), 2) and 3) cannot hold, and so it can only be Case 4), $\text{DGal}(\mathcal{L}) \cong \text{SL}_2(\mathbb{C})$. The equation **is not solvable by quadratures**, it **has no Liouvillian solutions**.

**The quantum harmonic oscillator**

Here we have the linear differential equation

$$y''(z) + \frac{m^2w^2}{\hbar^2}\Big(\frac{2E}{mw^2} - z^2\Big)y(z) = 0$$

By doing the change of variables

$$z \longmapsto Z = \sqrt{\frac{mw}{\hbar}}z$$

the equation transforms to

$$\ddot{y}(Z) + \Big(\frac{2E}{\hbar w} - Z^2\Big)y(Z) = 0 \qquad \text{and} \qquad a(Z) = \frac{2E}{\hbar w} - Z^2 \in \mathbb{C}(Z)$$

In this case $a(Z)$ has no poles in $\mathbb{C}$, and has order $-2$ at infinity. Hence Cases 2) and 3) cannot hold, and so it can only be Case 1), $\mathrm{DGal}(\mathcal{L})$ trigonalizable, or Case 4), $\mathrm{DGal}(\mathcal{L}) \cong \mathrm{SL}_2(\mathbb{C})$.

In fact, if we apply Kovacic's algorithm in solving this differential equations, since we are in Case 1) (if there exist Liouvillian solutions), we would get that it is solvable by quadratures when the number $\frac{2E}{\hbar w}$ is an odd integer, $2n+1$, and in particular for $n \geq 0$, we would arrive at a solution[11]

$$y_1(Z) = e^{\int\left(\frac{H_n'(z)}{H_n(z)} - z\right)} = H_n(Z)e^{-\frac{Z^2}{2}}$$

where $H_n(Z)$ denotes the classical Hermite's polynomials. These solutions are the physical ones (referring to that are the solutions which give positive energies, the only valid energies in the harmonic oscillator).
However, mathematically other solutions are also possible, as we can see if we notice that this example is a generalization of the particular case ($n = -1$) **Example 4) of Section 3.2.3. Concrete examples involving** $\mathbb{C}(z)$:

$$y''(z) - (1 + z^2)y(z) = 0$$

its solutions are $y_1(z) = e^{\frac{1}{2}z^2}$ and $y_2(z) = f(z)e^{\frac{1}{2}z^2}$ with $f(z) = \int e^{-w^2}dw$. In this particular case, we can see that the equation is **solvable by quadratures** (as we already knew, $2n + 1 = -1$ is an odd integer here), and in fact its Differential Galois Group is

$$\mathrm{DGal}(\mathcal{L}) \cong \Big\{ \begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix} \;\Big|\; a \in \mathbb{C}^*, b \in \mathbb{C} \Big\}$$

hence trigonalizable.

[11]The procedure to do so can be found in [18, Section 2.2].

## 5.3 Field of elementary functions

In the two previous sections of this chapter we have reviewed some concept of linear algebraic groups that will be of great importance in order to study elementary functions, as well as characterizing Liouvillian extensions, a result which, together with Kovacic's criterion, has helped us to study different linear differential equations present in the world of physics.

In this section we are going to study, as promised, elementary functions over $\mathbb{C}(z)$, and we will state when a given linear differential equation has its solutions expressible by elementary functions, a more restrictive property than being a liouvillian solution.

So, we begin by defining the concept of elementary field (field of elementary functions):[12] we want rational functions, exponential functions and algebraic functions to be elementary, as well as integrals of rational functions (logarithmic functions), and sums, substractions, products and divisions of them should also be elementary.
This idea of elementary functions can be formalized in the following way.

**Definition 5.7.**

*Consider the differential field $\mathbb{C}(z)$ with the usual derivation $\frac{d}{dz}$.*
*A differential field extension $K \subseteq \mathcal{E}$ is called a field of elementary functions (an* ***elementary field****) if*

$$\mathcal{E} = \mathbb{C}(z; f_1, ..., f_n; g_1, ..., g_m)$$

*with*

1) *$f_i$ an integral of a rational function, that is $f_i' \in \mathbb{C}(z)$, for $i = 1, ..., n$.*

2) *a tower of differential fields for the $g's$*

$$\mathbb{C}(z) \subseteq \mathbb{C}(z)(g_1) \subseteq \cdots \subseteq \mathbb{C}(z)(g_1, ..., g_m)$$

*with either $\frac{g_j'}{g_j} \in \mathbb{C}(z)(g_1, ..., g_{j-1})$ or $g_j$ algebraic over $\mathbb{C}(z)(g_1, ..., g_{j-1})$, for $j = 1, ..., m$ (understanding $g_0 = 1$).*

*An elementary function is an element of a field of elementary functions.*

**Observation 5.1.** *Some important observations about the definition are the following:*

- *The differential field $\mathbb{C}(z)$ itself contains the rational functions; the first condition adjoins logarithm functions, and the second condition adjoins algebraic elements and exponential functions.*
- *We are working with fields in order to obtain also elementary functions through sums, substractions, products and divisions of another ones.*

[12] Here we will follow the definition from Magid's book [2, Chapter 6], which is not the standard one, but it leads to a remarkable result concerning the Differential Galois Group.

- *The idea of a tower differential field in the definition gives us the understanding of composition. However, an important fact we shall notice in the definition is the following: we are adjoining the elements $f_i$ as integrals of the base field $\mathbb{C}(z)$, we are not considering a tower of differential fields here, in contrast with the elements $g_j$ in which we are considering compositions of them.*

Next we state some examples of different elementary functions according to our definition:

**Examples 5.3.**

*1)* We clearly have rational functions as elementary functions, as well as $n$th roots of them through the tower

$$\mathbb{C}\underbrace{(z)\subset\mathbb{C}(z)}_{\text{algebraic}}\left(\sqrt[n]{p(z)}\right)\qquad p(z)\in\mathbb{C}(z)$$

*2)* We also have exponentials of rational functions, $e^p$, since we can write it as $e^{\int p'}$ and so we have the tower

$$\mathbb{C}\underbrace{(z)\subset\mathbb{C}(z)}_{\text{exp. of int.}}(e^p)\qquad p(z)\in\mathbb{C}(z)$$

*3)* We have logarithms of rational functions: let $p(z),q(z)\in\mathbb{C}[z]$, with $q(z)\neq 0$; then we can write them as ($\mathbb{C}$ is algebraically closed)

$$p(z)=a\prod_{i=0}^{\deg(p)}(z-\alpha_i)\quad a,\alpha_i\in\mathbb{C}\qquad,\qquad q(z)=b\prod_{j=0}^{\deg(q)}(z-\beta_j)\quad b,\beta_j\in\mathbb{C}$$

and so

$$\ln\left(\frac{p(z)}{q(z)}\right)=\ln(a)-\ln(b)+\sum_{i=0}^{\deg(p)}\ln(z-\alpha_i)-\sum_{j=0}^{\deg(q)}\ln(z-\beta_j)$$

hence we have a tower

$$\mathbb{C}\underbrace{(z)\subset\mathbb{C}(z)(\ln(z-\alpha_i),}_{\text{integrals from }\mathbb{C}(z)}\ln(z-\beta_j))=\mathbb{C}(z)\Big(\ln(z-\alpha_i),\ln(z-\beta_j),\ln\left(\frac{p(z)}{q(z)}\right)\Big)$$

*4)* Of course, we also include $e^{\pm iz}=e^{\int\pm i}$, and hence we also have as elementary functions the trigonometric ones

$$\sin(z)=\frac{1}{2i}\Big(e^{iz}-e^{-iz}\Big)\qquad,\qquad\cos(z)=\frac{1}{2}\Big(e^{iz}+e^{iz}\Big)$$

through the tower

$$\mathbb{C}\underbrace{(z)\subset\mathbb{C}(z)(e^{iz},}_{\text{exp. of int. from }\mathbb{C}(z)}\ e^{-iz})=\mathbb{C}(z)(\sin(z),\cos(z))$$

An analogous tower, with $e^{\pm z}=e^{\int\pm 1}$, leads to the hyperbolic functions

$$\sinh(z)=\frac{1}{2}\Big(e^{z}-e^{-z}\Big)\qquad,\qquad\cosh(z)=\frac{1}{2}\Big(e^{z}+e^{z}\Big)$$

The essential property about this definition of elementary functions is contained in the following theorem, a proof of which can be found in Magid's book [2, Chapter 6].

**Theorem 5.4** (Elementary functions)**.**

*Let $\mathcal{L} \in \mathbb{C}(z)\left[\frac{d}{dz}\right]$ be a linear differential operator, and $\mathbb{C}(z) \subseteq E$ its Picard-Vessiot extension. Suppose that there exists a field of elementary functions*

$$\mathcal{E} = \mathbb{C}(z; f_1, ..., f_n; g_1, ..., g_m)$$

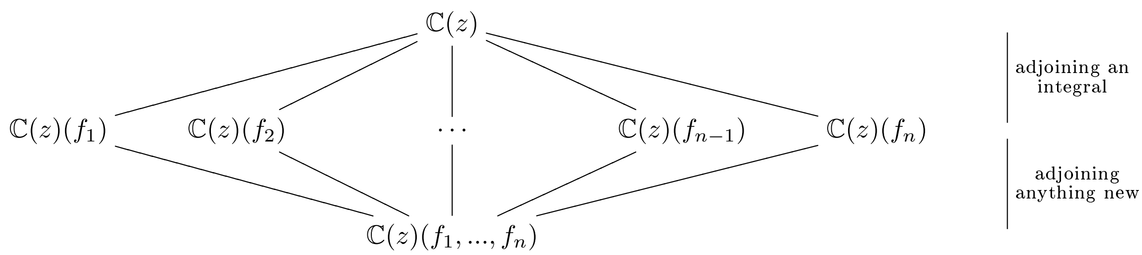
*that contains $E$, that is, $\mathbb{C}(z) \subseteq E \subseteq \mathcal{E}$.*
*Then the irreducible component of DGal$(\mathcal{L})$ containing the identity, DGal$(\mathcal{L})^0$, is abelian.*

*Intuition of Theorem 5.4.*

We already know, thanks to the examples of **Section 5.2.1.**, that adjoining an integral will provide an additive group $\mathbb{G}_a$ into the Differential Galois Group, and by adjoining the exponential of an integral will lead to a multiplicative group $\mathbb{G}_m$ into the Differential Galois Group.
With that, we can now think with the following tower

$$\mathbb{C}\underbrace{(z) \subseteq \mathbb{C}(z; f_1,}_{\text{integrals}} \overbrace{\underbrace{..., f_n) \subseteq E}_{} \subseteq}^{\text{alg. elements and exp. of integrals}} \mathcal{E} = \mathbb{C}(z; f_1, ..., f_n)(g_1, ..., g_m)$$

For the first sequence, every element $f_i$ has its derivative over $\mathbb{C}(z)$




In this first chain is easy to compute its DGal, since for every $\sigma \in \text{DGal}(\mathbb{C}(z)(f_1, ..., f_n)/\mathbb{C}(z))$ we have

$$(\sigma(f_i) - f_i)' = \sigma(f_i') - f_i' = f_i' - f_i' = 0 \quad \Longrightarrow \quad \sigma(f_i) - f_i = c_i^\sigma \in \mathbb{C}$$

and hence we can construct an injective morphism

$$\begin{aligned} \text{DGal}(\mathbb{C}(z)(f_1, ..., f_n)/\mathbb{C}(z)) &\hookrightarrow \mathbb{C}^n \cong \mathbb{G}_a^n \\ \sigma \qquad\qquad &\longmapsto (c_1^\sigma, c_2^\sigma, ..., c_n^\sigma) \end{aligned}$$

As already said, this part of the tower is responsible of the adjunctions of integrals, and therefore the corresponding Differential Galois Group is a subgroup of $\mathbb{G}_a^n$.
For the second chain

$$\mathbb{C}(z; f_1, \overbrace{\underbrace{..., f_n) \subseteq E}_{} \subseteq}^{\text{alg. elements and exp. of integrals}} \mathcal{E} = \mathbb{C}(z; f_1, ..., f_n)(g_1, ..., g_m)$$

and due to **Theorem 5.2**,

$$\mathrm{DGal}(E/\mathbb{C}(z;f_1,...,f_n))^0 \cong \mathbb{G}_m^r \qquad \text{for some } r$$

since here we do not adjoin any integral (as already said, $\mathbb{G}_m^r$ is responsible of the adjunctions of exponentials of integrals).

Furthermore, we can think of $\mathrm{DGal}(\mathbb{C}(z;f_1,...,f_n)/\mathbb{C}(z))$ as a subgroup of $\mathrm{DGal}(E/\mathbb{C}(z))$,

$$\mathrm{DGal}(\mathbb{C}(z;f_1,...,f_n)/\mathbb{C}(z)) \hookrightarrow \mathrm{DGal}(E/\mathbb{C}(z))$$

by simply extending every $\sigma \in \mathrm{DGal}(\mathbb{C}(z;f_1,...,f_n)/\mathbb{C}(z))$ by $\sigma(g_i) = g_i\ \forall i = 1,...,m$. Hence, by the Galois Correspondence, we can think

$$\mathrm{DGal}(E/\mathbb{C}(z)) \Big/ \mathrm{DGal}(E/\mathbb{C}(z;f_1,...,f_n)) \cong \mathrm{DGal}(\mathbb{C}(z;f_1,...,f_n)/\mathbb{C}(z))$$

so we have an equality of the irreducible components containing the identity

$$\begin{aligned}\mathrm{DGal}(E/\mathbb{C}(z))^0 &\cong \mathrm{DGal}(\mathbb{C}(z;f_1,...,f_n)/\mathbb{C}(z))^0 \cdot \mathrm{DGal}(E/\mathbb{C}(z;f_1,...,f_n))^0 \cong \\ &\cong \mathrm{DGal}(\mathbb{C}(z;f_1,...,f_n)/\mathbb{C}(z))^0 \cdot \mathbb{G}_m^r\end{aligned}$$

Finally, we also have the property

$$\sigma \circ \tau = \tau \circ \sigma \qquad \begin{cases} \forall\ \sigma \in \mathrm{DGal}(\mathbb{C}(z;f_1,...,f_n)/\mathbb{C}(z)) \equiv \mathrm{DGal}(E/\mathbb{C}(z;g_1,...,g_m)) \\ \forall\ \tau \in \mathrm{DGal}(E/\mathbb{C}(z;f_1,...,f_n)) \end{cases}$$

because

$$\begin{cases} \sigma(f_i) \in \mathbb{C}(z;f_1,...,f_n) \\ \sigma(g_j) = g_j \end{cases} \qquad \text{and} \qquad \begin{cases} \tau(f_i) = f_i \\ \tau(g_j) \in \mathbb{C}(z;g_1,...,g_m) \end{cases}$$

hence

$$\begin{cases} (\sigma\circ\tau)(f_i) = \sigma(\tau(f_i)) = \sigma(f_i) = \tau(\sigma(f_i)) = (\tau\circ\sigma)(f_i) \\ (\sigma\circ\tau)(g_j) = \sigma(\tau(g_j)) = \tau(g_j) = \tau(\sigma(g_j)) = (\tau\circ\sigma)(g_j) \end{cases}$$

This tells us that the previous group product is indeed a direct product (no relations between $f's$ and $g's$, they are not connected by any algebraic or differential relation):

$$\mathrm{DGal}(E/\mathbb{C}(z))^0 \cong \mathrm{DGal}(\mathbb{C}(z;f_1,...,f_n)/\mathbb{C}(z))^0 \times \mathbb{G}_m^r$$

being $\mathrm{DGal}(\mathbb{C}(z;f_1,...,f_n)/\mathbb{C}(z))^0$ abelian, and hence $\mathrm{DGal}(E/\mathbb{C}(z))^0$ is.

As a summary, we have intuitively done the following scheme:

$$\mathbb{C}\overbrace{\underbrace{(z) \subseteq \mathbb{C}(z;f_1,}_{\substack{H\subseteq\mathbb{G}_a^n \\ \text{adjoining integrals}}}\ \underbrace{...,f_n) \subseteq \mathbb{C}(z;f_1,...,f_n)}_{\substack{\mathbb{G}_m^r \\ \text{adjoining exp. of integrals}}}}^{\mathrm{DGal}(E/\mathbb{C}(z))^0}\overbrace{\underbrace{(g_1,...,g_r) \subseteq \mathcal{E} = \mathbb{C}(z;f_1,...,f_n)}_{\text{algebraic elements}}}^{\mathrm{DGal}(E/\mathbb{C}(z))/\mathrm{DGal}(E/\mathbb{C}(z))^0}(g_1,...,g_m)$$

· The first part is referred as the part which adjoints integrals and exponentials of integrals, the first one related to the group $\mathbb{G}_a^n$ and the second one related to the group $\mathbb{G}_m^r$.
· The second part, and due to **Proposition 5.1**, the quotient group

$$\mathrm{DGal}(E/\mathbb{C}(z)) \Big/ \mathrm{DGal}(E/\mathbb{C}(z))^0$$

is finite, and hence is related to the adjunctions of algebraic elements. □

### 5.3.1 The function $\int e^{-z^2}dz$ cannot be expressed in terms of elementary functions

Finally, we are ready to prove one of the main results in this section: the function

$$\int e^{-z^2}dz$$

cannot be expressed in terms of elementary functions (in Magid's sense). To do so, as we have mentioned, let's study the linear differential equation

$$0 = \mathcal{L}(y) = y'' + 2zy', \quad \mathcal{L} \in \mathbb{C}(z)\Big[\frac{d}{dz}\Big]$$

Its solutions are $y_1(z) = 1$ and $y_2(z) \equiv f(z) = \int_0^z e^{-w^2}dw$ defined over $\mathbb{C}$; so,

$$\mathrm{Sol}(\mathcal{L})_L = \mathbb{C}\cdot 1 \oplus \mathbb{C}\cdot f(z) \qquad \text{with} \begin{cases} L = \mathbb{C}(z)\langle 1, f(z)\rangle = \mathbb{C}(z, e^{-z^2}, f(z)) \\ C_L = C_K = \mathbb{C} \end{cases}$$

and so $\mathbb{C}(z, e^{-z^2}, f(z))/\mathbb{C}(z)$ is a Picard-Vessiot extension for $\mathcal{L}$. Its Differential Galois Group is given by

$$\mathrm{DGal}(\mathcal{L}) = \{\sigma : L \longrightarrow L \text{ differential } \mathbb{C}(z)\text{-automorphisms}\}$$

Given an element $\sigma \in \mathrm{DGal}(\mathcal{L})$, we can represent it as an invertible matrix $C \in \mathrm{GL}_2(\mathbb{C})$ through

$$\begin{aligned} \sigma :\ \mathbb{C}(z, e^{-z^2}, f(z)) &\longrightarrow \mathbb{C}(z, e^{-z^2}, f(z)) \\ k &\longmapsto k \qquad \forall\, k \in \mathbb{C}(z) \\ (1, f(z)) &\longmapsto (1, f(z)) \underbrace{\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}}_{C} \end{aligned}$$

that is,

$$\begin{cases} \sigma(1) = c_{11} + c_{21}f(z) \\ \sigma(f(z)) = c_{12} + c_{22}f(z) \end{cases}$$

**but** we have restrictions: since $\sigma$ is a **differential** $\mathbb{C}(z)$**-automorphism of** $L$,

- $\sigma(1) = 1 = c_{11} + c_{21}f(z)$, and so $\boxed{c_{11} = 1}$, $\boxed{c_{21} = 0}$, since 1 and $f(z)$ are linearly independent.
- $\sigma(f(z))' = \sigma(f(z)') = \sigma(e^{-z^2})$,

$$\sigma(e^{-z^2}) = \sigma(f(z))' = c_{22}f'(z) = c_{22}e^{-z^2}$$

Since $\sigma$ has to be a differential $\mathbb{C}(z)$-automorphism of $L$, we define the image of $e^{-z^2}$ for $\sigma$ through the previous relation, so $\boxed{c_{12} \text{ free}}$, $\boxed{c_{22} \text{ free}}$.

Finally, every element of $\mathrm{DGal}(\mathcal{L})$ is of the form

$$\begin{aligned} \sigma :\ \mathbb{C}(z, e^{-z^2}, f(z)) &\longrightarrow \mathbb{C}(z, e^{-z^2}, f(z)) \\ k &\longmapsto k \qquad \forall k \in \mathbb{C}(z) \\ (1, f(z)) &\longmapsto (1, f(z)) \begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix} \qquad c \in \mathbb{C}\ ,\ d \in \mathbb{C}^* \end{aligned}$$

and it is straightforward to check that every morphism of the previous form is indeed a differential $\mathbb{C}(z)$-automorphism of $L = \mathbb{C}(z, e^{-z^2}, f(z))$.
In this case,

$$\mathrm{DGal}(\mathcal{L}) \cong \left\{ \begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix} \;\middle|\; c \in \mathbb{C} \,,\, d \in \mathbb{C}^* \right\} \underbrace{\cong}_{\text{via } A \mapsto A^t} \left\{ \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \;\middle|\; c \in \mathbb{C} \,,\, d \in \mathbb{C}^* \right\}$$

The reader may notice that we have already studied this group in **Examples 5.2., 3)**; hence we obtain a group isomorphism

$$\mathrm{DGal}(\mathcal{L}) \cong \mathbb{G}_a \rtimes \mathbb{G}_m$$

We already know that this group is **non-abelian**; much more, it is a **connected** group: [13]

$$\mathrm{DGal}(\mathcal{L})^0 \cong \mathbb{G}_a \rtimes \mathbb{G}_m \qquad \textbf{not abelian}$$

By **Theorem 5.4**, $L$ cannot be embedded in any field of elementary functions $\mathcal{E}$, and as a consequence at least one of the solutions of $\mathcal{L}(y) = 0$ cannot be expressible in terms of elementary functions; since 1 is trivially an elementary function, we must have

$$\boxed{f(z) = \int_0^z e^{-w^2} dw \qquad \textbf{cannot be expressed in terms of elementary functions}}$$

[13]See Magid's book [2, Chapter 6] for a general proof of it: $\mathbb{G}_a \rtimes \mathbb{G}_m$ is indeed the Borel subgroup of $\mathrm{GL}_2(\mathbb{C})$, and hence connected.

# Bibliography


[1] T. Crespo and Z. Hajto, *Algebraic Groups and Differential Galois Theory.* Graduate Studies in Mathematics, Volume 122. American Mathematical Society.

[2] A. R. Magid, *Lectures on Differential Galois Theory.* University Lecture Series, Volume 7. American Mathematical Society.

[3] M. van der Put and M. F. Singer, *Galois Theory of Linear Differential Equations.* Singer-Verlay, 2003.

[4] E. Hille, *Ordinary Differential Equations in the Complex Domain.* A Wiley-Interscience Publication, John Wiley & Sons.

[5] R. C. Churchill and J. J. Kovacic, *Introduction to Differential Galois Theory.* Kolchin Seminar in Differential Algebra, Posted Papers.

[6] M. F. Singer, *Introduction to the Galois Theory of Linear Differential Equations.* Lectures at London Mathematical Society Invited Lecture Series, Heriot-Watt University, 2006 (expanded version).

[7] J. H. Hubbard and B. E. Lundell, *A First Look at Differential Algebra.* American Mathematical Society, Volume 118, Number 3, pp. 245 - 261 (17), 2011.

[8] J. M. Murphy, *Differential Galois Theory.* UChicago 2010 REU, University of Chicago.

[9] M. Kamensky, *Differential Galois Theory.* Lecture Notes

[10] T. Crespo, *The Origins of Differential Galois Theory.* Łojasiewicz Lecture, Preparatory Workshop, Jegiellonian University, 2012.

[11] J. J. Kovacic, *Picard-Vessiot Theory, Algebraic Groups and Group Schemes.* Kolchin Seminar in Differential Algebra, Lecture Notes.

[12] B. H. Matzat and M. van der Put, *Constructive Differential Galois Theory.* Mathematical Science Research Institute, Publications, Volume 41, 2003.

[13] G. Malle and D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type.* Cambridge Studies in Advanced Mathematics, 2011.

[14] A. L. Onishchik and E. B. Vinberg, *Lie Groups and Algebraic Groups.* Springer-Verlag Berlin Heidelberg, 1990. Translated from the Russian edition Seminar po Gruppam Li i Algebraicheskim Gruppam, 1988.

[15] F. Murnaghan, *Linear Algebraic Groups.* Clay Mathematics Proceedings, Volume 4, 2005.

[16] J. J. Kovacic, *An Algorithm for Solving Second Order Linear Homogeneous Differential Equations.* J. Symbolic Computation (1986) 2, 3-43.

[17] C. J. Smith, *A Discussion and Implementation of Kovacic's Algorithm for Ordinary Differential Equations.* Research Report CS-84-35, University of Waterloo, 1984.

[18] P. B. Acosta-Humánez and D. Blázquez-Sanz, *Non-Integrability of some Hamiltonians with Rational Potentials.* American Institute of Mathematical Sciences, Discrete and Continuous Dynamical Systems, Volume 10, Number 2 & 3, 2008.

[19] H. Żołądek, *Two Remarks about Picard-Vessiot Extensions and Elementary Functions.* Colloquium Mathematicum, Volume 84/85, 2000.

[20] P. Goetz, *Why certain integrals are "impossible".* Talk, Sonoma State University, 2009.

[21] T. Dyckerhoff, *Tutorial on Differential Galois Theory.* Talk, GTEM Workshop on Constructive Galois Theory, 2008.