UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Introduction to Differential Galois Theory

Autor: Pau Martínez Marín

Director: Dra. Maria Teresa Crespo Vicente
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 20 de juny de 2021

Abstract

Galois theory is one of the most beautiful areas of mathematics presented in undergraduate studies. Most of its success is due to the brilliant idea by the French mathematician Évariste Galois of associating a group to every algebraic equation in a way that its solvability can be studied through the language of group theory. Later on, this same idea was pursued by mathematicians Émile Picard and Ernest Vessiot in the field of linear differential equations. The resulting theory of linear differential equations mirrors in great part that of polynomial equations.

The purpose of this work is twofold. On the one hand, we are going to give an alternative definition of the Galois group associated with a polynomial equation and prove its equivalence with the usual definition. Although somewhat more laborious to deal with, this definition allows for a deeper intuition of what the Galois group is about. On the other hand, we want to study the extension of Galois theory applied to linear differential equations. We will develop the theory of differential algebra in a way that will enable us to translate the alternative definition of the Galois group of a polynomial given in the first section to that of a linear differential equation. We will also prove its equivalence with the usual definition for the differential Galois group. Finally, we will comment on some ways in which these ideas are used to tackle the representation of solutions to differential equations in terms of their coefficients.

Resum

La teoria de Galois és una de les àrees de les matemàtiques més boniques que es solen presentar durant els estudis de grau. Gran part del seu èxit és causada per la genial idea del matemàtic francès Évariste Galois d'associar un grup a cada equació algebraica de tal manera que la seva resolubilitat pugui ser estudiada a través del llenguatge de la teoria de grups. Més tard, aquesta mateixa idea va ser perseguida pels matemàtics Émile Picard i Ernest Vessiot en el camp de les equacions diferencials lineals. La teoria resultant d'equacions diferencial lineals és en gran part anàloga a la d'equacions polinòmiques.

El propòsit d'aquest treball és doble. Per una banda, donarem una definició alternativa del grup de Galois associat a una equació algebraica i en demostrarem la seva equivalència amb la definició usual. Tot i que lleugerament més laboriosa de construir, aquesta nova definició permet una intuïció més profunda sobre el que representa el grup de Galois. Per l'altre costat, volem estudiar l'extensió de la teoria de Galois aplicada al camp de les equacions diferencials lineals. Desenvoluparem la teoria de l'àlgebra diferencial de tal manera que traduirem la definició alternativa del grup de Galois donada a la primera secció a la corresponent noció en les equacions diferencials. També en demostrarem l'equivalència amb la definició habitual del grup de Galois diferencial. Finalment, comentarem en algunes de les maneres en què aquestes idees són útils en l'estudi de les representacions de solucions d'equacions diferencials en termes dels seus coeficients.

2010 Mathematics Subject Classification. 11R32, 12H05, 14L17

Acknowledgements

The realization of this work would have never been possible without the many people who have been around me during these six years of undergraduate studies. First and foremost, my most sincere gratitude goes towards my parents and my sister, who have been always beside me and have been supporting me during these years. I would also like to express my gratefulness towards the friends I have made during my studies for encouraging each other in pursuing our interests. I would also like to thank the professors and authors who share their knowledge with students, allowing us to learn in various aspects. Finally, this work would not have been possible without the contribution of Dra. Maria Teresa Crespo Vicente. Her ample knowledge of the field and her dedication to my studies have certainly been of great value.

Contents

Introduction

Galois theory is one of the most beautiful areas of mathematics presented in undergraduate studies. It gives one instance of a problem that can be given a complete solution while historically developing new and useful mathematical ideas. And most of its success is due to the brilliant idea by the French mathematician Évariste Galois of associating a group to every polynomial equation in a way that its solvability can be studied through the language of group theory.

The purpose of this work is twofold. On the one hand, we want to give an alternative insight into the Galois group of a polynomial equation. This is why we are going to build towards a different definition of the group associated with a polynomial. Although requiring somewhat more preliminary work to be done, in the opinion of the author it gives some extra insight on what symmetries do the solutions of the equation possess. On the other hand, we want to extend this definition to the also successful Galois theory of differential equations. After presenting the required basic notions of differential algebra, we are going to successfully give an analogous definition for the differential Galois group to the one we presented for polynomials and prove its equivalence with the usual one.

Before beginning with the discussion itself, it might be appropriate to comment briefly on the work and its intention. The idea at the core of this work, that is, the definition of the Galois group in terms of algebraic relations between the roots and of group action stabilizers, is one that I have had on standby for some time now. I found it interesting to pursue this line of thought when I was studying for the course in algebraic equations at the University of Barcelona. When I had to chose which subject I wanted to study during my final degree work, this one was the first that I wanted to try. Since at that moment it was only a sketch of a possible definition that might work in the same way as the Galois group, I did not think it likely that the definition was correct. I had never found it in the books and it was natural to think that it was either incorrect or, in the best possible case, right but totally uninteresting.

After the first weeks of investigation and after getting in touch with my advisor, Dra. Maria Teresa Crespo, it was beginning to be clear to me that these concepts might be right. After some more dedication, I was seeing that apart from being right, it was also interesting (to me, at least). That is because it gives another kind of insight into the symmetries of linear equations, which are somewhat hidden by the more modern (and more straightforward) definitions involving automorphisms. So it seemed possible to write my final degree work about it. Further, in order to expand the scope of the work and make it more suitable to the length and content of such a work, I began studying the differential Galois theory, with the hope of being able to extend my original definition about polynomials to the differential case too. In this sense, I was greatly satisfied when I was beginning to see that indeed this might be possible. Therefore, when I arrived at the part when I was able to define the Galois group of a differential equation by considering the differential relationships between its solutions, it was greatly satisfying to me. In what follows, I hope with my best wishes that my intention has been successfully translated to the work and that my enthusiasm is present in the following pages.

Structure of the work

In **Section 1** we are going to refresh the basic concepts from ring and field theory and the theory of algebraic equations. We do this to establish the notation used throughout the work and to make it somewhat more self-contained. Please, note that most of these concepts were given during the undergraduate courses in algebraic structures and algebraic equations, so we will try not to go too deep into them.

After this brief introduction, we proceed to the first central part of the work, where we give an alternative and maybe original definition of the Galois group for a polynomial in terms of the group of permutations. Giving this definition, with its correspondent motivation, and proving its equivalence with the usual one was one of the main goals and motivations for this work. Moreover, the great target of the second (and larger) part of the work will be to build the theory of differential algebra in order to give an analogous definition for the differential Galois group.

In **Section 2** we will give the basic definitions and ideas about differential algebra. We will try to make it clear that this is the appropriate structure in which we can study linear differential equations. We will also emphasize the parallelisms between this structure and the structure required for polynomial equations. Next, a precise (and intuitive) definition is given for the notion of a linear differential equation and its solutions. A first study of the space of solutions and their structure is conducted. We will finish with an important result about the dimension of the space of solutions.

In the more technical **Section 3**, a discussion about the analog of the splitting field for a differential equation is conducted. Most of the section is concerned with proving the existence and uniqueness of such extensions, called Picard-Vessiot extensions. Before diving into that, and following the general philosophy of the work, we will spend some time carefully motivating the direction we are going to take with the proof. This approach can seem rather tiring or cumbersome at times, but we will stick to it in compensation for the abundance of more straightforward texts in the topic (and in other topics as well).

After covering most of our fundamental and technical prerequisites, we can now in **Section 4** proceed with another central part of the work, defining the differential Galois group of a linear differential equation. Again, the definition that we are going to reach will not be the standard contemporary definition, but one based on the same ideas that led us towards our definition of the polynomial Galois group. After another brief space dedicated to building towards this definition, we reach a passage that mirrors in great part what we saw during the first section but stated in the framework of differential algebra. Although some of the proofs will look very similar to the ones given about polynomial Galois theory, we will not omit them. That is because the similarity and resemblance between both theories are not obvious, and the fact that some proofs could almost be translated verbatim should be highlighted more than skipped.

In order to finish the work somewhat nicely, we give in **Section 5** a short view about one of many ways in which this theory of differential Galois groups is successful. Without any intention to present the results originally and borrowing from the appropriate sources when required, we are going to present in a personal fashion the notions of solvability by quadratures and of solvability in elementary functions. This is not by any means a principal section of the work and it's here only to give some completeness to the narrative.

Finally, in the **Appendix** we will give the basic definitions and results from the theory of algebraic geometry in affine spaces. In order to have some background knowledge about algebraic groups, which as will be seen, play a key role in differential Galois theory, some basic notions had to be studied. The result of these inquiries are briefly presented in this appendix and will be referenced in some points throughout the work.

1 The Galois Group of a Polynomial Equation

In this section, we are going to summarize the main results from Galois theory of polynomial equations. One of the goals of the section is to present the ideas and results of the theory in such a way that they can be exported into differential Galois theory as straightforwardly as possible. Another goal of the section is to give an alternative definition of the Galois group associated with a given polynomial. This definition will hopefully give another kind of motivation and insight for the theory and is the one that we will try to bring into the context of differential algebra. Please note, however, that most of the results in this section are covered during the courses of either algebraic structures or algebraic equations in the bachelor's degree in mathematics at the University of Barcelona.

Let's begin by stating the problem that we are going to tackle in this first section. Since the differential equations that we are going to consider further on in this work are going to be defined over a field of characteristic zero, we can develop the theory of algebraic equations for this kind of fields.

Problem 1.1. Let K be a field of characteristic zero and let $K[X]$ be its ring of polynomials. We want to follow Evariste Galois' genius idea and try to associate to each polynomial in $K[X]$ a group in such a way that this group, called the Galois group of the polynomial, gives insight into its properties. This is going to be the main goal of this chapter, and in order to get there, we are going to prove some of the main results of the theory.

1.1 Algebra Preliminaries

1.1.1 Polynomials and results from the theory of fields

We will begin the section by defining the main object of study of this chapter, the polynomial. Unless otherwise stated, all rings are considered to be commutative and with unity. We will designate the additive and the multiplicative neutral elements by the symbols 0 and 1 respectively.

Definition 1.2. *Let R be a ring (commutative with unity). Let $R^{\mathbb{N}} = R \times R \times ...$ be the numerable cartesian product of copies of R. An element p of $R^{\mathbb{N}}$ is of the form $p = (p_0, p_1, ...)$. We can define two binary operations in $R^{\mathbb{N}}$ as follows.*

(i) For $p = (p_0, p_1, ...), q = (q_0, q_1, ...) \in R^{\mathbb{N}}$, define the addition of polynomials as $p + q = (p_0 + q_0, p_1 + q_1, ...)$.

(ii) For $p = (p_0, p_1, ...), q = (q_0, q_1, ...) \in R^{\mathbb{N}}$, define the multiplication of polynomials as $p \cdot q = (c_0, c_1, ...)$ where $c_k = \sum_{i=0}^{k} p_i q_{k-i}$ for each $k \in \mathbb{N}$.

For this product to be well-defined we require another condition, namely, that the number of non-zero coefficients in each polynomial is finite. If that's the case, we denote as X the polynomial $X = (0, 1, 0, ...) \in R^{\mathbb{N}}$ and realise that we can write every polynomial $p = (p_0, ..., p_n, 0, ...)$ with finitely many non zero coefficients as $p = p(X) = \sum_{k=0}^{n} p_k X^k$, where $p_k = (p_k, 0, ...)$ by a stretch of notation and with the product defined above. The set of elements of $R^{\mathbb{N}}$ with finitely many non-zero coefficients together with those two operations will be denoted by $R[X]$, and is easily seen to be also a commutative ring with unity.

Thus, we have seen that given a ring R we can construct from it a ring of polynomials, $R[X]$. In what follows, we are going to review some of the basic properties of this construction. One can immediately see that if the ring R is an integral domain, then $R[X]$ is also an integral domain. Thus, we can see that the properties of the ring $R[X]$ depend a lot on those of the base ring R. One case of special interest arises when R is a field, and this is the case that we will be studying deeply. Before diving into that, let us define what is the degree of a polynomial

Definition 1.3. *Let R be a ring and $R[X]$ its ring of polynomials. We define the degree of a polynomial as a map* $\deg : R[X] \to \mathbb{N} \cup \{-\infty\}$ *where for* $p = (p_0, ...,) \in R[X]$, $\deg p = \max\{n \in \mathbb{N} : p_n \neq 0\}$. *This is well defined by the definition of the polynomial ring. By convenience, we define the degree of the zero polynomial to be $-\infty$.*

One can prove a number of basic useful results about the degree of the sum and the product of polynomials. Namely, that $\deg(p+q) \leq \max\{\deg p, \deg, q\}$ and that $\deg(pq) = \deg p + \deg q$ provided R is an integral domain and getting into account the usual rules to operate with the symbol $-\infty$. One remarkable property about polynomials involving their degree is the division algorithm. While it still holds in rings in a somewhat weaker form, it's nicer to switch here from rings to fields. This has no consequence in our work, since all this presentation is aimed towards Galois Theory, which is always constructed over fields. Moreover, in order to avoid considerations that would take us in other directions, we are going to consider only fields of characteristic zero, i.e., fields where $1 + 1 + 1 + ... + 1 = n \cdot 1 \neq 0$ for all positive n. Then, when we consider the ring of polynomials over a field K, we automatically know that $K[X]$ is a commutative ring with unity and that it is an integral domain. $K[X]$ inherits some other properties from K, but we will present them further on. That said, let's resume our discussion.

Theorem 1.4. *Let K be a field and $p(X), q(X) \in K[X]$, $q(X) \neq 0$. Then, there exist unique $d(X), r(X) \in K[X]$ so that $p(X) = d(X)q(X) + r(X)$ with* $\deg r(X) < \deg q(X)$.

This remarkable property allows us to prove the very important fact that the ring of polynomials over a field is a principal ideal domain. Let us first refresh the definition.

Definition 1.5. *Let R be an integral domain. Then, R is a principal ideal domain if for every $I \subseteq R$ ideal, there exists $a \in I$ so that $I = (a) = \{ra \in R : r \in R\}$. An ideal of this kind is called a principal ideal.*

Proposition 1.6. *Let K be a field. Then, $K[X]$ is a principal ideal domain.*

Together with it, we have another very useful concept, namely that of the unique factorization domain. Let R be an integral domain. We will denote $R^{\times} = R \setminus \{0\}$ and $R^* = \{a \in R : \exists b \in R, ab = ba = 1\}$, and call R^* the set of units of R. Then:

Definition 1.7. *Let R be a ring and $a, b \in R$. We will say that a divides b, and denote it by $a|b$, if there exists some $c \in R$ so that $ac = b$.*

Then, we can define the notions of primality and irreducibility:

Definition 1.8. *Let R be a ring and $a \in R$. We will say that p is a prime element of R if $p \neq 0$, $p \notin R^*$ and for all $a, b \in R$ such that p divides ab, then either p divides a or p divides b.*

Definition 1.9. *Let R be a ring and $q \in R$. We will say that q is an irreducible element of R if $q \neq 0$, $q \notin R^*$ and $\forall a, b \in R$ such that $q = ab$, we have that either $a \in R^*$ or $b \in R^*$.*

We have the result that in an integral domain, every prime element is also irreducible. With these definitions, we can define the very important notion of a unique factorization domain.

Definition 1.10. *Let R be an integral domain. We will say that R is a unique factorization domain if for every $a \in R^{\times}$, there exist $a_1, ..., a_n \in R$, all of them irreducible, such that $a = a_1...a_n$ and such that if $b_1, ..., b_m \in R$ are also all irreducible and $a = b_1, ..., b_m$, we have that $n = m$ and that, reordering the indices, $a_i = \epsilon_i b_i$ for all $i = 1, ..., n$, where $\epsilon_i \in R^*$.*

A fundamental result of the theory of rings states that:

Theorem 1.11. *Let R be a principal ideal domain. Then, R is a unique factorization domain.*

This result is proved in every introductory algebra book and was studied in the undergraduate course Algebraic Structures. Since we have proven that for K a field, $K[X]$ is a principal ideal domain, we have the also fundamental corollary:

Corollary 1.12. *Let K be a field. Then, $K[X]$ is a unique factorization domain.*

With this result, let us reconduct our discussion to the area that interests us, that is, that of polynomial equations.

1.1.2 Roots and splitting fields

First of all, given a field K and its ring of polynomials $K[X]$, we can define the evaluation map for a given $p(X) = p_0 + p_1X + ... + p_nX^n \in K[X]$ as $\psi_p : K \longrightarrow K$, $\psi_p(a) = p_0 + p_1a + p_2a^2 + ... + p_na^n$. In order to avoid cumbersome notation, we will usually denote $\psi_p(a) \equiv p(a)$ when no confusion can arise. If $a \in K$ is such that $p(a) = 0$, we will say that a is a root of p in K.

We will now see that this simple step produces a whole new set of properties and interesting things to study. Basically, by defining an evaluation map for every polynomial, we have defined the idea of an algebraic equation and its solutions. Thus, if a is a root for the polynomial $p(X)$, we can equivalently say that a is a solution for the polynomial equation $p(X) = 0$.

Let's begin our exploration of this new set of ideas by seeing that the amount of solutions for a given algebraic equation is limited by its degree, i.e., by the degree of the polynomial.

Proposition 1.13. *Let K be a field and $p(X) \in K[X]$ a nonzero polynomial. Let $a \in K$ be a root of $p(X)$. Then, the polynomial $X - a$ divides $p(X)$.*

Proof. Since we have seen the division algorithm in the ring of polynomials over a field, let $q(X), r(X) \in K[X]$ be the unique polynomials such that $p(X) = q(X)(X - a) + r(X)$ with $\deg r < \deg(X - a) = 1$. But, since by evaluating the expression at a, we have that $0 = p(a) = q(a)(a - a) + r(a)$ and since r is a polynomial of degree less than 1, then necessarily $r(X) = 0$ and we have that $p(X) = q(X)(X - a)$, as wanted. □

As a corollary, we get that nonzero polynomials of degree less than 1 cannot have roots. If $p(X)$ is a polynomial and $a \in K$ is a root of p such that $(X-a)^m$ divides $p(X)$ for $m \geq 1$ and m is the greater integer with this property, we will say that a is a root of multiplicity m of p in K. A root of multiplicity one will be referred to as a simple root.

Proposition 1.14. *Let K be a field and $p(X) \in K[X]$ be a polynomial of degree n. Then, $p(X)$ has at most n roots in K, each root counted with its multiplicity.*

Proof. Let $p(X) \in K[X]$ be a polynomial of degree n and let $a_1, ..., a_r \in K$ be distinct roots of p, each of multiplicity m_i. Then, we have seen that $(X-a_i)^{m_i}$ divides $p(X)$. Since none of this factors divide each other, we have that $p(X) = q(X)(X-a_1)^{m_1} \cdot ... \cdot (X-a_r)^{m_r}$. Then, in particular, $m_1 + ... + m_r \leq n$, as we wanted to see. □

We turn now to study what happens when a polynomial has no roots. This is interesting because as we will see, we can always construct a field in which the polynomial does has a root. But prior to that, we must give some definitions about ideals.

Definition 1.15. *Let R be a ring and $I \subseteq R$ an ideal. We will say that I is a prime ideal if $\forall a, b \in R$ such that $ab \in I$, we have that either $a \in I$ or $b \in I$.*

Proposition 1.16. *Let R be a ring and $I \subseteq R$ a prime ideal. Then, the quotient ring R/I is an integral domain. The reciprocal is also true.*

Definition 1.17. *Let R be a ring and $I \subseteq R$ a proper ideal. We will say that I is a maximal ideal if $\forall J \subseteq R$ ideal so that $I \subseteq J$, we have that either $J = I$ or $J = M$.*

We also have the characterization of maximal ideals in terms of quotient rings.

Proposition 1.18. *Let R be a ring and $I \subseteq R$ a proper ideal. Then, I is a maximal ideal if and only if the quotient ring R/I is a field.*

With these two ideas, we can see that given a polynomial with no roots (of positive degree), we can always construct a field containing the original field where the polynomial does have a root.

Theorem 1.19. *Let K be a field and let $p(X) \in K[X]$ be a polynomial of positive degree with no roots in K, that is, $p(a) \neq 0 \, \forall a \in K$. Then, there exists a field $\bar{K}$ that contains K as a subfield so that $p(X)$ viewed as a polynomial in $\bar{K}[X]$ has a root.*

Proof. Let's assume without loss of generality that $p(X)$ is an irreducible element of the ring $K[X]$. Notice that if that's not the case, since $K[X]$ is a unique factorization domain, there has to be an irreducible factor of $p(X)$ that does not have a root. Thus, by proving the result for irreducible polynomials, we are proving the general statement too.

Let then $p(X)$ be irreducible and notice that then, the principal ideal generated by $p(X)$, (p), is a maximal ideal. Indeed, (p) is a proper ideal since $p(X)$ has positive degree, and hence it is nonzero and it does not contain a unit. Then, if $I \subseteq K[X]$ is an ideal that contains (p), being $K[X]$ a principal ideal domain, $I = (q)$ for some $q(X) \in K[X]$. But, $(p) \subseteq (q)$ implies that $p \in (q)$, so that $p(X) = r(X)q(X)$ for some $r(X) \in K[X]$. But then, being $p(X)$ irreducible, either $r(x)$ is a unit (and then $(q) = (p)$) or $q(X)$ is a unit, and $(q) = K[X]$). Thus, (p) is a maximal ideal and then $\bar{K} = K[X]/(p)$ is a field.

Let's now see that, in the first place, $\varphi : K \to \bar{K}$ given by $\varphi(a) = a + (p) \in K[X]/(p)$ is an injective ring homomorphism, so that we can see K as a subfield of $\bar{K}$. Then, notice that $p(X)$ as seen as an element of $\bar{K}[X]$ satisfies the equation:

$$p(X+(p)) = \sum_{k=0}^{n}(p_k+(p))(X+(p))^k = \sum_{k=0}^{n}(p_k+(p))(X^k+(p)) = \sum_{k=0}^{n}(p_kX^k+(p)) = 0+(p)$$

Then, this finishes the proof, sicne $\alpha \equiv X + (p) \in \bar{K}$ is a root of $p(X)$. □

This is a very important result. We have just proven that if a polynomial of degree greater than zero over a field has no roots, then we can construct a field containing the original field where the polynomial does have a root. From now on, we will call the construction where we have a field containing another one as a subfield a field extension. The previous result has the very important corollary:

Corollary 1.20. *Let K be a field and $p \in K[X]$ a polynomial of positive degree n. Then, there exists a field $\bar{K} \supseteq K$ where there exists $\alpha_1, ..., \alpha_n \in \bar{K}$ such that $p(X) = \epsilon(X - \alpha_1) \cdot ... \cdot (X - \alpha_n)$, with $\epsilon \in K$.*

The result is easily proven by induction using the previous theorem.

Definition 1.21. *Let K be a field and $p(X) \in K[X]$ a polynomial. If $\bar{K} \supseteq K$ is a field extension where $p(X) = \epsilon(X - \alpha_1) \cdot ... \cdot (X - \alpha_n)$ for some $\alpha_i \in \bar{K}$, $\epsilon \in K$ we will say that $p(X)$ splits into linear factors in $\bar{K}$. If, morover, $\bar{K}$ is such that $\forall \bar{K}' \subseteq K$ so that $p(X)$ also splits in linear factors in $\bar{K}'$, then $\bar{K} = \bar{K}'$, we will say that $\bar{K}$ is a splitting field for the polynomial $p(X)$.*

Before moving to the next section, let us talk about the idea of adjoining an element to a field. Let K be a field and $\bar{K}$ be a field that contains K as a subfield. Then, given $\alpha \in \bar{K}$ not on K, we can consider the smallest subfield of $\bar{K}$ that contains both K and α. Further, we define:

Definition 1.22. *Let $\bar{K} \supseteq K$ an extension of fields and $\alpha \in \bar{K}$. We define the field $K(\alpha)$ to be the minimal subfield of $\bar{K}$ containing K and α. Similarly, if $\alpha_1, ..., \alpha_n \in \bar{K}$, then we define the field $K(\alpha_1, ..., \alpha_n)$ to be the smallest subfield of $\bar{K}$ containing both K and the set $\{\alpha_1, ..., \alpha_n\}$.*

We don't want to delve much further into the theory of algebraic extensions. We will give the following definitions in order to state the next result.

Definition 1.23. *Let $\bar{K} \supseteq K$ be an extension of fields and $\alpha \in \bar{K}$. We will say that α is algebraic over K if there exists $p(X) \in K[X]$ so that $p(\alpha) = 0$. Otherwise, we are going to say that α is trascendental over K.*
If an extension $\bar{K} \supseteq K$ is such that $\forall \alpha \in \bar{K}$, α is algebraic over K, we are going to say that it is an algebraic extension.

There are a number of interesting results that come out of these definitions. The only result that we are going to use now is the following one.

Proposition 1.24. *Let K be a field and $p(X) \in K[X]$. Let $\bar{K} \supseteq K$ be a splitting field for $p(X)$ over K. Then, $\bar{K} = K(\alpha_1, ..., \alpha_n)$, where $\alpha_1, ..., \alpha_n \in \bar{K}$ are the roots of $p(X)$ in $\bar{K}$.*

So, we have seen that for any polynomial we are able to construct a splitting field and that the splitting field is precisely the field generated by its roots. With these ingredients, we can construct the Galois group for a polynomial.

1.2 The Galois Group

In this section, we are going to follow Galois' insight and associate a group to every polynomial in such a way that this association reflects some of the properties of the solutions of the polynomial equation. First of all, we are going to give a motivating example to see how we are going to proceed.

Example 1.25. Consider the field $\mathbb{Q}$ and the polynomial $p(X) = X^4 - 2X^2 + 10 \in \mathbb{Q}[X]$. This has not been an arbitrary choice, it has been chosen because we know its roots in the field $\mathbb{C}$. Those are $\pm\sqrt{1 \pm 3i}$. Let's label those four roots as $\alpha_1 = \sqrt{1+3i}$, $\alpha_2 = -\alpha_1$, $\alpha_3 = \sqrt{1-3i}$, $\alpha_4 = -\alpha_3$. There are, as we can easily see, some algebraic relations between those four roots. Some of them are:

$$\alpha_1 + \alpha_2 = 0, \qquad \alpha_3 + \alpha_4 = 0, \qquad \alpha_1^2 + \alpha_3^2 - 2 = 0 \tag{1.1}$$

In order to associate a group to $p(X)$ so that it translates some of the properties of the roots to the proprties of groups, that is, so that it encodes their symmetries, we can think along the following path. We can think of the group of permutations of 4 elements, $\mathcal{S}_4$, as a group acting upon the set of roots of $p(X)$ as $\forall \sigma \in \mathcal{S}_4$, $\alpha_i \mapsto \alpha_{\sigma(i)}$. Then, we can see that those elements of $\mathcal{S}_4$ that leave invariant the relations between the roots $\alpha_1, ..., \alpha_4$ are clearly representing a symmetry of those roots. In this example, we can see that for the permutation $\sigma = (1\,2)$ we clearly have that

$$\alpha_{\sigma(1)} + \alpha_{\sigma(2)} = 0, \qquad \alpha_{\sigma(3)} + \alpha_{\sigma(4)} = 0, \qquad \alpha_{\sigma(1)}^2 + \alpha_{\sigma(3)}^2 - 2 = 0$$

Further, we can see that the permutation $\tau = (1\,3\,2\,4)$ also preserves the above relations. Therefore, the group generated by the permutations σ and τ, $G = \langle \tau, \sigma \rangle$, will leave invariant those relations, since clearly the composition of two permutations with this property also has this property. This group is isomorphic to the dihedral group of order 8. It can be checked that no other elements of $\mathcal{S}_4$ preserve the above relations. We should prove also that every other algebraic relation with coefficients in the field of rational numbers between the roots is a combination of the above relations, but we are going to leave it here for now and simply say that if that is the case, the group $G \cong D_{2,4}$ is naturally associated to the polynomial $p(X) = X^4 - 2X^2 + 10$ since it encodes the symmetries between its roots.

The goal of the following section is to generalize this procedure to an arbitrary polynomial over an arbitrary field (of characteristic zero). To do so, we will have to define precisely what we mean by an algebraic relation between the roots and what is the group action we are considering. In return, we are going to get a definition for the Galois group of a polynomial that gives a different kind of insight into Galois theory. Further, as we are going to see, this way of thinking about Galois groups also generalizes to the case of linear differential equations, and this alone should be a good motivation to study it.

1.2.1 Properties about group actions and multivariate polynomials

In order to give a formal construction of the group associated with the polynomial and so to define the Galois group, we first need to refresh some properties of polynomial rings in multiple indeterminates and of group actions.

Definition 1.26. *Let R be a ring. The ring of polynomials in n indeterminates, $R[X_1, ..., X_n]$, is defined by induction as the ring of polynomials (of a single indeterminate) with coefficients in the ring $R[X_1, ..., X_{n-1}]$. That is, $R[X_1, ..., X_n] = R[X_1, ..., X_{n-1}][X]$*

There are a lot of interesting facts about the ring of polynomials in n indeterminates. However, we won't need them at the moment. Let's only keep in mind that the ring $K[X_1, ..., X_n]$, K a field, can be seen as a K-vector space that admits as a basis $\{X_1^{\alpha_1} \cdot ... \cdot X_n^{\alpha_n}\}_{\alpha_1,...,\alpha_n=0,1,...}$.

Now that we have defined the ring of multivariate polynomials, let's get some insight into why are we going to use them. Let K be a field and $p(X) \in K[X]$. Let $\bar{K}$ be a splitting field for $p(X)$ and $\alpha_1, ..., \alpha_n \in \bar{K}$ be its roots. Since we are going to consider the permutations of $\mathcal{S}_n$ that preserve the algebraic relations between the roots, we need first to identify those algebraic relations. Let's then consider the ring $K[X_1, ..., X_n]$ and the map ψ_p defined as

$$\psi_p : K[X_1, ..., X_n] \longrightarrow \bar{K}, \qquad \psi_p(q(X_1, ..., X_n)) = q(\alpha_1, ..., \alpha_n)$$

We can see that this is a well-defined map and that it is a ring homomorphism. In fact, it is an homomorphism of K-algebras, since we have defined it over the K-basis of multivariate polynomials as $\psi_p(X_1^{m_1} \cdot ... \cdot X_n^{m_n}) = \alpha_1^{m_1} \cdot ... \cdot \alpha_n^{m_n}$. We can then see that the kernel of this homomorphism, $\ker \psi_p$, contains every algebraic relation between the roots of the polynomial $p(X)$ over the field K. Notationally, we are going to refer to this kernel as $\ker_K \psi_p$ when the base field is not clear by the context.

Next, since we will end up considering the elements of a group acting on a set that leaves invariant certain relations, we will refresh some definitions and results about group actions and stabilizers.

Definition 1.27. *Let G be a group and X be a set. An action of the group G over the set X is a map $\rho : G \times X \longrightarrow X$ so that:*

(i) $\rho(g, \rho(h, x)) = \rho(gh, x)$, $\forall g, h \in G$, $\forall x \in X$

(ii) $\rho(1, x) = x$, $\forall x \in X$

Straight from the definition, we can see that given a group action $\rho : G \times X \longrightarrow X$ and an element $g \in G$, there is an induced bijection $\rho_g : X \longrightarrow X$ defined as $\rho_g(x) = \rho(g, x)$. This is indeed a bijection, since it is injective ($\rho_g(x) = \rho_g(y)$, then $\rho(g^{-1}, \rho_g(x)) = \rho(g^{-1}, \rho_g(y))$, and then $x = y$) and it is surjective (if $x \in X$, then $\rho_g(g^{-1}, x) = x$).

Another concept that we are going to use is that of a stabilizer:

Definition 1.28. *Let $\rho : G \times X \longrightarrow X$ be a group action and let $x \in X$. We define the stabilizer of x to be the subgroup of G that leaves invariant x. That is, $Stab_\rho x = \{g \in G : \rho(g, x) = x\}$. This is indeed a subgroup of G.*

In this same way, we can define the stabilizer of a subset of X if we think about the induced action of G upon $\mathcal{P}(X)$, defined as $\tilde{\rho}(g, S) = \{\rho(g, s) \in X : s \in S\} \in \mathcal{P}(X)$. Thus, we define:

Definition 1.29. *Let G be a group, X a set and $\rho : G \times X \longrightarrow X$ a group action. Let $\rho : G \times \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ the induced action of G upon the subsets of X. Let $S \subseteq X$. We define $Stab_\rho S \equiv Stab_{\tilde{\rho}} S$, so $Stab_\rho S = \{g \in G : \rho(g, s) \in S, \forall s \in S\}$.*

Being ρ_g a bijection of X, we can easily see that $\mathrm{Stab}_\rho S$ as defined above is indeed the same as $\mathrm{Stab}_{\tilde{\rho}} S$, since if $\tilde{\rho}(g, S) \subseteq S$, then $\tilde{\rho}(g, S) = S$. Let's now consider the action of the permutation group $\mathcal{S}_n$ upon the set of multivariate polynomials.

Observation 1.30. Let K be a field and $\rho : \mathcal{S}_n \times K[X_1, ..., X_n] \longrightarrow K[X_1, ..., X_n]$ the action defined $\forall \sigma \in \mathcal{S}_n$ as $\rho(\sigma, q(X_1, ..., X_n)) = q(X_{\sigma(1)}, ..., X_{\sigma(n)})$. This is a well-defined action, since the induced map is defined over the basis $\rho_\sigma(X_1^{\alpha_1} \cdot ... \cdot X_n^{\alpha_n}) = X_{\sigma(1)}^{\alpha_1} \cdot ... \cdot X_{\sigma(n)}^{\alpha_n}$ and this is a morphism of K-algebras.

Finally, let's take a look at a result about conjugacy classes that we are going to use in the next section. Remember that if $\rho : G \times X \longrightarrow X$ is a group action, $g \in G$, and $S \subseteq X$, then we denote $gS = \{\rho(g, s) \in X : s \in S\}$. Further, if $H \subseteq G$ is a subgroup, we denote its conjugate by g as $gHg^{-1} = \{ghg^{-1} \in G : h \in H\}$. Indeed, it is a subgroup of G. Then, the results that interest us are:

Proposition 1.31. *Let $\rho : G \times X \longrightarrow X$ be a group action, $S \subseteq X$ and $g \in G$. Then,* $\mathrm{Stab}_\rho(gS) = g\mathrm{Stab}_\rho(S)g^{-1}$.

Proposition 1.32. *Let G be a group and $H \subseteq G$ a subgroup. Then, $\forall g \in G$, $gHg^{-1} \cong H$.*

They were proven during the undergraduate course about algebraic structures.

1.2.2 The Galois group of a polynomial

We have now gathered all the ingredients we need in order to define the Galois group. We present the definition as follows.

Definition 1.33. *Let K be a field and $p(X) \in K[X]$. Let $\bar{K} \supseteq K$ a splitting field for $p(X)$ and $\alpha_1, ..., \alpha_n \in \bar{K}$ the roots of $p(X)$ in $\bar{K}$. Let $\psi_p : K[X_1, ..., X_n] \longrightarrow \bar{K}$, defined as $\psi_p(q(X_1, ..., X_n)) = q(\alpha_1, ..., \alpha_n)$, be the evaluation homomorphism defined above and $\rho : \mathcal{S} \times K[X_1, ..., X_n] \longrightarrow K[X_1, ..., X_n]$, defined as $\rho(g, q(X_1, ..., X_n)) = q(X_{\sigma(1)}, ..., X_{\sigma(n)})$, be the action defined above. Then, we define the Galois group of the polynomial $p(X)$ over the field K as the stabilizer of the kernel of the evaluation map by the permutation action, that is,*

$$\mathrm{Gal}_K\, p(X) = \mathrm{Stab}_\rho \ker \psi_p$$

We can clearly see that it puts together the ideas exposed in the motivating example. In this section, we are going to see that indeed it is the Galois group of the polynomial when defined in the usual way. From this definition, there arise a number of trivial but important results, such as:

Corollary 1.34. *Let $p(X) \in K[X]$ be a polynomial of degree $n \geq 1$. Then, the order of its Galois group satisifies $\#\mathrm{Gal}_K\, p(X) \leq n!$*

Corollary 1.35. *If $p(X) \in K[X]$ is such that it splits in K and all of its roots are simple, then its Galois group is the trivial group,* $\operatorname{Gal}_K p(X) = \{\mathrm{id}\} \subseteq \mathcal{S}_n$

Proof. Indeed, if there are $\alpha_1, ..., \alpha_n, \epsilon \in K$ such that $p(X) = \epsilon(X - \alpha_1) \cdot ... \cdot (X - \alpha_n)$, then we can see that $\forall i = 1, ..., n$, the polynomial $q_i(X_1, ..., X_n) = X_i - \alpha_i$ is an element of $\ker \psi_p \subseteq K[X_1, ..., X_n]$. But if $\sigma \in \operatorname{Gal}_K p(X)$, then in particular $\rho(\sigma, q_i)$ must belong to $\ker \psi_p$ for all $i = 1, ..., n$. But $\rho(\sigma, q_i) = X_{\sigma(i)} - \alpha_i \in \ker \psi_p$ if and only if $\sigma(i) = i$, $\forall i = 1, ..., n$. Thus, $\operatorname{Gal}_K p(X) = \{id\}$. □

Before proving that this definition coincides with the usual one, we must be sure that the object is well defined. Note that we have already checked that most of the objects involved in this definition are well defined, namely that the Galois group is indeed a group and that the action and homomorphism used are well defined. Thus, the only thing that we must check is that the definition is independent of arbitrary choices. The only arbitrary choice involved in the definition is that of the order of the roots. Then, we must check that if we rearrange the roots of the polynomial, thus changing the definition of the evaluation morphism ψ_p, we still get the same object.

Proposition 1.36. *Let K be a field, $p(X)$ a polynomial, $\bar{K}$ a splitting field for $p(X)$ and $\alpha_1, ..., \alpha_n$ its roots in that field. If $\beta_1, ..., \beta_n \in \bar{K}$ is a rearrangement of those roots, and $\psi_p, \tilde{\psi_p} : K[X_1, ..., X_n] \longrightarrow \bar{K}$ are the evaluation morphisms defined as $\psi_p(X_i) = \alpha_i$, $\tilde{\psi_p}(X_i) = \beta_i$, then* $\operatorname{Stab}_\rho \ker \psi_p \cong \operatorname{Stab}_\rho \ker \tilde{\psi_p}$.

Proof. If $\alpha_1, ..., \alpha_n$ and $\beta_1, ..., \beta_n$ are the same elements rearanged, then there exists $\sigma \in \mathcal{S}_n$ so that $\beta_i = \alpha_{\sigma(i)}$. Then, we can see that if $q(X_1, ..., X_n) \in \ker \tilde{\psi_p}$, then $\tilde{\psi_p}(q(X_1, ..., X_n)) = q(\beta_1, ..., \beta_n) = q(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(n)}) = \psi_p \circ \rho(\sigma, q(X_1, ..., X_n)) = 0$, and so $\sigma \ker \tilde{\psi_p} \subseteq \ker \psi_p$. Similarly, we can see that $\alpha_i = \beta_{\sigma^{-1}(i)}$, so that by the same argument, $\sigma^{-1} \ker \psi_p \subseteq \ker \tilde{\psi_p}$. Therefore, since $\sigma^{-1}(\sigma \ker \psi_p) = \ker \psi_p$, we get the chain of inclusions

$$\ker \tilde{\psi_p} = \sigma^{-1}\sigma \ker \tilde{\psi_p} \subseteq \sigma^{-1} \ker \psi_p \subseteq \ker \tilde{\psi_p}$$

And therefore, $\sigma \ker \psi_p = \ker \tilde{\psi_p}$. But by the previous result on group stabilizers (proposition 1.31), we have that $\operatorname{Stab}_\rho(\ker \tilde{\psi_p}) = \sigma^{-1}\operatorname{Stab}_\rho \ker \psi_p \sigma \cong \operatorname{Stab}_\rho \ker \psi_p$. □

Then, we have seen that indeed this object is well defined, in the sense that a rearrangement of the roots gives isomorphic Galois groups. We will now see that this definition is in fact equivalent to the one usually given in algebra textbooks and in the Algebraic Equations course. This definition uses the idea of a field automorphism of the splitting field of the polynomial that is the identity map when restricted to the base field.

Definition 1.37. *Let $\bar{K} \supseteq K$ be a field extension. A K-automorphism of $\bar{K}$ is a field homomorphism $\varphi : \bar{K} \longrightarrow \bar{K}$ such that $\varphi(a) = a, \forall a \in K$. We will denote the set of all K-automorphism by $\operatorname{Aut}_K \bar{K}$. It is a group toghether with the composition of field homomorphisms.*

Then, the usual definition of the Galois group is the following one:

Definition 1.38. *Let K be a field, $p(X) \in K[X]$ a polynomial and $\bar{K}$ a splitting field. Then, we define the Galois group of the polynomial $p(X)$ over K as $\operatorname{Gal}_K p(X) = \operatorname{Aut}_K \bar{K}$.*

We can see that this definition is simpler, cleaner, and requires fewer previous concepts to be defined in order to reach it. However, the opinion of the author of this text is that some of its intuition gets hidden behind this simplicity and although it is easier to work with, it hides the idea that the roots of a polynomial possess some kind of symmetry. The definition exposed in this work, although somewhat impractical to work with, clearly exposes the symmetries of a polynomial and therefore is, in a sense, more natural.

We now turn to the task of proving that indeed both definitions are equivalent, in the sense that both groups are isomorphic.

Theorem 1.39. *Let $p(X) \in K$ be a polynomial and $\bar{K}$ a splitting field for $p(X)$, where its roots are $\alpha_1, ..., \alpha_n$. Then, with the previous definitions,* $\mathrm{Stab}_\rho \ker \psi_p \cong \mathrm{Aut}_K \bar{K}$.

Proof. Supose for the sake of simplicity that all the roots are different to one another. Consider the group homomorphism given by $\varphi : \mathrm{Stab}_\rho \ker \psi_p \longrightarrow \mathrm{Aut}_K \bar{K}$, $\varphi(\sigma) \mapsto \varphi_\sigma$, where φ_σ is the K-automorphism of $\bar{K}$ given by $\varphi_\sigma(\alpha_i) = \alpha_{\sigma(i)}$ and $\varphi_\sigma(a) = a$, $\forall a \in K$. This is a well-defined group homomorphism, since $\varphi(\sigma\tau) = \varphi_\sigma \circ \varphi_\tau$. Further, φ_σ is a K-automorphism of $\bar{K}$, since it is a field homomorphism. Morover, it is an injective homomorphism, since if $\varphi_\sigma = \varphi_\tau$, then clearly $\sigma = \tau$.

The only thing left to prove it that φ is exhaustive. Let then be $\phi \in \mathrm{Aut}_K \bar{K}$. Since for every α_i we know that $\phi(\alpha_i)$ must be again a root of $p(x)$, let's define $\sigma \in \mathcal{S}_n$ so that $\phi(\alpha_i) = \alpha_{\sigma(i)}$. Now, we have to see that $\sigma \in \mathrm{Stab}_\rho \ker \psi_p$. But since ϕ is a K-automorphism of the field $\bar{K}$, if $q(X_1, ..., X_n)$ is an element of $\ker \psi_p$, we have that $\psi_p \circ \rho(\sigma, q) = q(\phi(\alpha_1), ..., \phi(\alpha_n)) = \phi(q(\alpha_1, ..., \alpha_n)) = \phi(0) = 0$. Since obviously $\phi = \varphi(\sigma)$ and we have seen that $\sigma \in \mathrm{Stab}_\rho \ker \psi_p$, we get that φ is exhaustive and therefore it is an isomorphism of groups. □

2 Differential Algebra

In this chapter, we are going to introduce the basic structure needed to study linear differential equations from an algebraic point of view, the differential field. Then, we will construct a theory as analogous as possible to the one constructed in the previous chapter, with the goal of defining in an analogous way an associated group to every linear differential equation.

2.1 Differential Rings

Let us begin by defining the structure in which we are going to develop the theory. All rings will be assumed to be with unity and of characteristic zero.

Definition 2.1. *Let R be a ring. A derivation in R is a map $\partial : R \longrightarrow R$ such that:*

(i) $\forall a, b \in R$, $\partial(a + b) = \partial(a) + \partial(b)$

(ii) $\forall a, b \in R$, $\partial(ab) = \partial(a)b + a\partial(b)$

A ring R together with a derivation $\partial : R \longrightarrow R$ will be called a differential ring (R, ∂).

We can easily see that a number of properties follow directly from this definition, such as:

Lemma 2.2. *Let (R, ∂) be a differential ring and $a \in R$. Then:*

(i) $\partial(1) = 0$

(ii) If $\partial(a)$ commutes with a, then $\partial(a^n) = na^{n-1}\partial(a)$ for all $n > 0$.

(iii) If $a \in R$ is an invertible element and $\partial(a)$ commutes with a, then $\partial(a^{-1}) = -a^{-2}\partial(a)$.

Proof. (i) is obvious, since $\partial(a) = \partial(1 \cdot a) = \partial(1)a + \partial(a)$ for any $a \in R$. (ii) can easily bee seen starting from $\partial(a^2) = \partial(a)a + a\partial(a) = 2\partial(a)$ and then using induction on the case $\partial(a^n) = \partial(a)a^{n-1} + a\partial(a^{n-1})$. FInally, (iii) comes from the fact that $\partial(1) = \partial(a^{-1}a) = \partial(a^{-1})a + a^{-1}\partial(a) = 0$. □

Unless otherwise stated, all rings are going to be commutative rings. We will denote a differential extension of rings as:

Definition 2.3. *Let (R, ∂), $(\bar{R}, \bar{\partial})$ be a differential rings so that $\bar{R} \supset R$ is a ring extension. Then, it is a differential extension if $\bar{\partial}_{|R} = \partial$. If $\bar{R}$, R are differential fields and $\bar{R} \supseteq R$ is a field extension, then it is a differential field extension if the same condition holds.*

Lemma 2.4. *Let (R, ∂) be a diferential integral domain and let $\mathcal{Q}(R)$ be the quotient field of R. Then, the derivation in R extends in a unique way to $\mathcal{Q}(R)$ so that $\mathcal{Q}(R) \supseteq R$ is a differential ring extension.*

Proof. From property (iii) of the previous lemma and since every non zero element $a \in \mathcal{Q}(R)$ is invertible, we know that $\tilde{\partial}(a^{-1}) = -\tilde{\partial}(a)a^{-2}$. Therefore, if $a \in R \subseteq \mathcal{Q}(R)$ and we want $(\mathcal{Q}, \tilde{\partial})$ to be a differential field that contains (R, ∂) as a differential subfield (i.e., $\tilde{\partial}_{|R} = \partial$), necessarily we must have that $\tilde{\partial}(a^{-1}) = -\partial(a)a^{-2}$ for every nonzero $a \in R$. □

In a way similar to that of ring theory, we can define a differential ideal as the kind of structure that allows us to construct quotients. Thus:

Definition 2.5. *Let (R, ∂) be a differential ring. A differential ideal of R is an ideal $I \subseteq R$ such that $\forall a \in I$, $\partial(a) \in I$.*

This is the extra condition needed in order to bring the differential ring structure to the quotient. Indeed, if (R, ∂) is a differential ring and $I \subseteq R$ is an ideal, we will only have that R/I is a differential ring (with the induced operations from R) if ∂ is well defined in the quotient. That is, if $\tilde{\partial} : R/I \longrightarrow R/I$ is a derivation. we demand that $\tilde{\partial}(a + I) = \partial(a) + I$. Thus, for this derivation to be well defined, we need that, since $a + I = (a + i) + I$, $i \in I$, then $\partial(a) - \partial(a + i) \in I$. That is, $\partial(i) \in I$, $\forall i \in I$. And that is precisely the structure of differential ideal that we have just defined.

Corollary 2.6. *Let (R, ∂) be a differential ring and $I \subseteq R$ a differential ideal. Then, R/I is a differential ring with the projected derivation $\partial(a + I) = \partial(a) + I$.*

We can present here some properties of differential ideals.

Definition 2.7. *Let (R, ∂) be a differential ring and $I \subseteq R$ a differential ideal. We will say that I is a maximal differential ideal if $\forall J \subseteq R$ differential ideal so that $I \subseteq J$, then either $J = R$ or $J = I$. Similarly, we will say that I is a prime differential ideal if it is a prime ideal.*

We can see that since a prime differential ideal is in particular a prime ideal, we have the same characterization as in the case of a prime ideal. Namely, $I \subseteq R$ is a prime ideal if and only if R/I is an integral domain. However, when talking about maximal differential ideals, we have to be more careful, since a maximal differential ideal need not be a maximal ideal. Indeed, we have the following property of maximal differential ideals, which is a key result that we are going to use further on.

Theorem 2.8. *Let (R, ∂) be a differential ring and $I \subseteq R$ a maximal differential ideal. Then, I is a prime ideal.*

Proof. This proof will follow that of [5](pp. 16). First of all, notice that if $R \supseteq K$ is a differential ring and $M \subseteq R$ is a differential maximal ideal, then R/M has no proper differential ideals. This is true, since the projection $\pi : R \longrightarrow R/M$ has the property that $\pi^{-1}(I)$ is a differential ideal of R containing M for every $I \subseteq R/M$ differential ideal. Therefore, $\pi^{-1}(I)$ must be either M (and then $I = (0) \subseteq R/M$) or R (and then $I = R/M$). Thus, we can from now on consider the ring R as having no proper differential ideals. The task is then to prove that if R has no proper differential ideals, then it is an integral domain.

In order to prove that, we can supose the existence of a zero divisor in R. Therefore, there are two nonzero elements $a, b \in R$ so that $ab = 0$. We are going to see that then, the differential ideal generated by a, that is, $\langle a \rangle = (a, \partial(a), \partial^2(a), ...)$, is a proper differential ideal or R. First of all, we have that since $\partial(ab) = \partial(a)b + a\partial(b) = 0$, we can multiply by b to get $\partial(a)b^2 + ab\partial(a) = \partial(a)b^2 = 0$. By induction, we can easily see that if $\partial^n(a)b^{n+1} = 0$, then deriving and multiplying by b we get:

$$\partial(\partial^n(a)b^{n+1})b = \partial^{n+1}(a)b^{n+2} + (n + 1)\partial^n(a)b^{n+1} = \partial^{n+1}(a)b^{n+2} = 0$$

Therefore, $\partial^n(a)b^{n+1} = 0$ for any two zero divisors a, b and for every n. Here, if $b^n \neq 0$ for every $n > 0$, we would get that $\partial^n(a)$ is a zero divisor for every n and therefore the differential ideal $\langle a \rangle$ is properly contained in R, since it only contains zero divisors (and therefore $\langle a \rangle \neq R$) and it $a \neq 0$ (and therefore $\langle a \rangle \neq (0)$). Thus, it must be that $b^n = 0$ for some $n > 0$. Now, since b was any zero divisor, we have proved that every zero divisor of R is nilpotent.

But now we are almost there, since being a nilpotent, we can choose n minimal so that $a^n = 0$. Therefore, we have that $\partial(a^n) = na^{n-1}\partial(a) = 0$ but $a^{n-1} \neq 0$ and $n \neq 0$, being K a subfield of zero characteristic of R. Therefore, $\partial(a)$ is again a zero divisor in R for every zero divisor a. Then, $\langle a \rangle$ is a differential ideal that only contains zero divisors and again that allows us to conclude that it is a proper differential ideal of R. Therefore, we have a contradiction with the initial assumption and it must be that R is an integral domain.

□

Before seeing some examples of differential rings, we define the idea of a differential homomorphism.

Definition 2.9. *Let $(R, \partial), (R', \partial')$ be differential rings. A map $\varphi : R \longrightarrow R'$ is a homomorphism of differential rings if it is a homomorphism of rings that commutes with the derivation. That is, such that $\varphi(\partial(a)) = \partial'(\varphi(a))$, $\forall a \in R$.*

We will take the chance now to see that a differential ring homomorphism can be extended in a unique way to the field of quotients.

Proposition 2.10. *Let $(A, \partial), (B, \partial')$ be differential integral domains and let $\varphi : A \longrightarrow B$ be a differential ring homomorphism. Then, there exists a unique differential field homomorphism $\tilde{\varphi} : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(B)$ so that $\tilde{\varphi}_{|A} = \varphi$.*

Proof. This is immediate, since we know from ring theory that φ extends in a unique way to the quotient field of R via $\tilde{\varphi}(a^{-1}) = \varphi(a)^{-1}$. We only have to check that this is indeed a differential field homomorphism provided that φ is. But trivially $\tilde{\varphi}(\partial(a)) = \varphi(\partial(a)) = \partial(\tilde{\varphi}(a))$ and $\tilde{\varphi}(\partial(a)^{-1}) = \varphi(\partial(a))^{-1} = (\partial(\varphi(a)))^{-1} = (\partial(\tilde{\varphi}(a)))^{-1}$ for every $a \in R$ nonzero. □

Example 2.11. Let us now see some examples of differential rings.

(i) Let R be a ring and define the trivial derivation on R as $\partial : R \longrightarrow R$ as $\partial(a) = 0$ for all $a \in R$. Then, (R, ∂) is a differential ring. Thus, any ring can be turned into a differential ring. Observe that since $\partial(1) = 0$, the only derivative that can be defined in the ring of integers $\mathbb{Z}$ or in the field of rationals $\mathbb{Q}$ is the trivial derivative.

(ii) Let (R, ∂) be a differential ring. We want to extend ∂ to its ring of polynomials $R[X]$ so that when restricted to R we have the same derivation as ∂. If that's the case, we can easily see that for every $p(X) = \sum_0^n p_k X^k$ and for every derivation $\tilde{\partial}$ in $K[X]$ so that $\tilde{\partial}_{|R} = \partial$, we will have $\tilde{\partial}(p(X) = \sum_0^n \partial(p_k)X^k + \sum_0^n kp_k X^{k-1}\tilde{\partial}(X)$. So the derivation in $K[X]$ is determined up to the choice of $\tilde{\partial}(X) \in K[X]$, which we can take arbitrarily.

(iii) Let (R, ∂) be a differential integral domain. By extending the previous construction to the field of fractions as in proposition 2.4, given the arbitrary choice of $\tilde{\partial}(X)$, we can see that $\mathcal{Q}(R[X]) = R(X)$ is a differential field.

(iv) Let $(\mathbb{Q}, \partial)$ be a differential field over the rationals, where ∂ must be the trivial derivative. Then consider the field of rational functions $\mathbb{Q}(X)$ and define $\partial(X) = 1$. Then, $(\mathbb{Q}(X), \partial)$ is a differential field and the derivative ∂ obeys the usual formal rules for differentiating rational functions.

(v) Let (K, ∂) be a differential field and let $A, B \supseteq K$ be K-algebras that are also differential ring extensions of K. Then, we can consider the ring given by the tensor product $A \otimes B$, which is again a K-algebra. We can extend the derivation ∂ to the tensor product by defining $\partial(a \otimes b) = \partial(a) \otimes b + a \otimes \partial(b)$ and extending by linearity. This is indeed a derivation since by definition the derivative of a sum is the sum of derivatives and the derivative of a product is $\partial((a \otimes b)(c \otimes d)) = \partial(a \otimes b)(c \otimes d) + (a \otimes b)\partial(c \otimes d)$, as can be seen expanding each term.

Finally, let us define some terminology.

Definition 2.12. *Let (R, ∂) be a differential ring and $c \in R$. We will say that c is a constant element of R if $\partial(c) = 0$. We will denote $C_R = \{c \in R : \partial(c) = 0\}$. It is a subring of R. If R is a field, then it also is a subfield.*

Definition 2.13. *Let $K \subseteq \bar{K}$ be a differential extension with derivation ∂. Then, $\alpha \in \bar{K}$ is primitive element of K if $\partial(\alpha) \in K$. Also, $\alpha \in \bar{K}$ is an exponential element of K if $\partial(\alpha)\alpha^{-1} \in K$.*

Definition 2.14. *Let (K, ∂) be a differential field and $R \supseteq K$ be a differential ring extension. We are going to say that R is finitely generated over K as a K-algebra if there exist $\alpha_1, ..., \alpha_n \in R$ so that $R = K[\alpha_1, ..., \alpha_n]$.*

2.2 The Linear Differential Equation

From now on, let (K, ∂) be a differential field of characteristic zero. In what follows, we are going to introduce the notion of a linear differential equation, mirroring as much as possible the ideas from the polynomial equations of the previous chapter. First of all, as an example, let us consider the intuitive idea of what a linear differential equation is, at least as they appear in real analysis or in physics.

Example 2.15. Consider the field of real numbers, $\mathbb{R}$. A linear homogeneous differential equation of order n with coefficients in $\mathbb{R}$ is given by a set of $n + 1$ elements of $\mathbb{R}$, like $\{a_0, ..., a_n\} \subseteq \mathbb{R}$, and is solved by a function $f(t) \in \mathcal{C}^n(\mathbb{R})$ that satisfies the relation $a_n \frac{d^n f}{dt^n} + ... + a_1 \frac{df}{dt} + a_0 f = 0$. We can also consider a set of functions $f_1, ..., f_n : \mathbb{R} \longrightarrow \mathbb{R}$ and the linear differential equation with those coefficients, which is going to be solved by a differentiable function $f(t) \in \mathcal{C}^n(\mathbb{R})$ that satisfies $f_n(t)\frac{d^n f}{dt^n} + ... + f_1(t)\frac{df}{dt} + f_0(t) f = 0$

This, however, is not the definition we are looking for. Notice how, in contrast with the polynomial case, there will be some important considerations to be taken with respect to the domains of definition of the coefficients and of the solutions. We know from the courses taken in real and complex analysis that the domains of definition play an important role in the solution of a differential equation. Those considerations we want to avoid in the algebraic study of differential equations since it is not clear how we can study them algebraically.

In order to solve this issue, we can work in a somewhat restricted domain and consider the differential equations as defined only over differential fields.

Example 2.16. Let (K, ∂) be a differential field. A linear homogeneous differential equation of order n will be given by an ordered set of $n+1$ elements $(a_0, ..., a_n) \subseteq K^{n+1}$ and will be solved by an element $b \in K$ if and only if $a_n\partial^n(b) + ... + a_1\partial(b) + a_0 b = 0$. If $\bar{K} \supseteq K$ is a differential field containing K as a differential subfield, we can view the $n+1$ elements defining the equation as elements of $\bar{K}$ and similarly say that an element α of $\bar{K}$ solves the equation if $a_n\partial^n(\alpha) + ... + a_1\partial(\alpha) + a_0\alpha = 0$. This way, we can find solutions in field extensions.

This definition looks much more like the one we would like to have. First of all, it is purely algebraic, in the sense that in order to talk about differential equations and their solutions we did not need to define any notion of continuity or of limit. Moreover, in the case where the differential field is for example $(\mathbb{R}(X), \frac{d}{dt})$, the definition agrees with the one used in analysis. Then, we can finally give the following definition:

Definition 2.17. *Let (K, ∂) be a differential field. A linear homogeneous differential equation of order n in K is an ordered $n+1$ tuple of elements $(a_0, ..., a_n) \in K^{n+1}$, with $a_n \neq 0$. An element $\alpha \in \bar{K}$, for some differential extension of K, is a solution for the equation if $a_n\partial^n(\alpha) + ... + a_1\partial(\alpha) + a_0\alpha = 0$.*

This is the formal definition of a linear homogeneous differential equation of order n. However, in order to have a greater analogy with the polynomial case, we might want to give further structure to those linear differential equations. In order to do so, we can define the ring of differential operators, which will work in much the same way as the ring of polynomials except for the fact that it won't be commutative, as we can expect.

Definition 2.18. *Let (K, ∂) be a differential field and consider the set $K^{\mathbb{N}} = K \times K \times ...$, the infinite numerable cartesian product of K. Its elements are of the form $a = (a_0, ..., a_n, ...) \in K^{\mathbb{N}}$. We can define two binary operations on $K^{\mathbb{N}}$ as follows.*

(i) $\forall a = (a_0, a_1, ...), b = (b_0, b_1, ...) \in K^{\mathbb{N}}$, we define its sum as $a + b = (a_0 + b_0, a_1 + b_1, ...) \in K^{\mathbb{N}}$.

In order to define the product, we need to work a bit more, since the product of linear differential operators won't in general be commutative.

(ii) Consider the elements $a = (0, ..., 0, a, 0, ...)$, $b = (0, ..., 0, b, 0, ...) \in K^{\mathbb{N}}$ with zeros everywhere except at the i-th and j-th coordinates respectively. Then, define its product as $a \cdot b = (0, ..., 0, c_j, 0, ..., 0, c_{i+j}, 0, ...)$ with zeros everywhere except at the j-th and $i+j$-th positions and with $c_j = a\partial^i(b)$, $c_{i+j} = ab$.

For this product to be well defined, we need again to restrict ourselves to the set of elements in $K^{\mathbb{N}}$ with finitely many nonzero elements, which we are going to denote as $K[d]$ and name as the ring of linear differential operators over K. Then, by defining the element $d = (0, 1, 0, ...) \in K[d]$ and denoting $\forall a \in K$, $a = (a, 0, ...)$, the product defined in (ii) can be written as $(ad^i) \cdot (bd^j) = a\partial^i(b)d^j + abd^{i+j}$. Then, we can write every element $L(d) \in K[d]$, $L(d) = (l_0, ..., l_n, 0, ...)$, as a polynomial in d, $L(d) = \sum_{k=0}^{n} l_k d^n$

Thus, much in the same way as with the polynomials in the previous section, we have represented (homogeneous) linear differential equations by a ring of polynomials. Before introducing the idea equivalent to the roots of those differential operators, let's give some results about the structure of this noncommutative ring. Note that we define the degree of a differential operator in an obvious way.

Proposition 2.19. *Let (K, ∂) be a differential field and let $K[d]$ be its ring of differential operators. Then, given $p(d), q(d) \in K[d]$, with $q(d) \neq 0$, there exist unique $a_R(d), r_R(d) \in K[d]$ and $a_L(d), r_L(d) \in K[d]$ so that $p(d) = q(d)a_R(d) + r_R(d)$, $p(d) = a_L(d)q(d) + r_L(d)$ and $\deg(r_R(d)), \deg(r_L(d)) < \deg(q(d))$.*

2.3 The Solutions of a Linear Differential Equation

Let us now follow our discussion of linear differential equations in the same way as we did with algebraic equations. In order to study the solutions of those equations, we defined the evaluation map of a polynomial. We are now going to do the same for differential equations.

Definition 2.20. *Let (R, ∂) be a differential ring and $L(d) \in R[d]$ a differential operator. We define the differential evaluation map of $L(d)$ as the map $\psi_L : K \longrightarrow K$ sending $\psi_L(\alpha) = \sum_{k=0}^{n} l_k \partial^k(\alpha)$. When there's no risk of confusion, we will denote $\psi_L(\alpha) = L(\alpha)$.*

For algebraic equations, we had that the evaluation map had no extra structure. In particular, it was not a ring homomorphism. For differential equations, however, the evaluation map does have an interesting structure when the differential ring is also a field. Remember that in that case, if (K, ∂) is a differential field and $C_K = \{c \in K : \partial(c) = 0\}$, then C_K is a subfield of K and we can view K as a C_K-vector space.

Proposition 2.21. *Let (K, ∂) be a differential field and $L(d) \in K[d]$ a differential operator. Then, $\psi_L : K \longrightarrow K$ is a C_K-linear map between vector spaces over C_K. In particular, $\ker \psi_L$ is a vector subspace over C_K.*

Proof. Let $L(d) = \sum_{k=0}^{n} l_k d^k$ and let $\lambda, \mu \in C_K$ and $\alpha, \beta \in K$. Then, by the additivity property of the derivation, $\partial^k(\alpha + \beta) = \partial^k(\alpha) + \partial^k(\beta)$ and being λ, μ constants, we have that

$$\psi_L(\lambda\alpha + \mu\beta) = \sum_{k=0}^{n} l_k \partial^k(\lambda\alpha + \mu\beta) = \sum_{k=0}^{n} l_k(\lambda\partial^k(\alpha) + \mu\partial^k(\beta)) = \lambda\psi_L(\alpha) + \mu\psi_L(\beta)$$

Thus, ψ_L is a C_K-linear map and then $\ker \psi_L$ is a vector subspace of K over C_K. □

This is indeed a remarkable property. We have as a corollary that the sum of solutions and the product of a solution by a constant are again solutions. Further, we can now study the notions of linear independence over constants of the solutions. What more can we say about this vector space of solutions? This will be the main object of our study during the following sections. The symmetries that we will be pursuing with Galois theory are those exhibited by this vector space. Then, let's center our efforts in studying its properties with more detail.

We can start by asking about the dimension of the vector space of solutions. First of all, notice that if $L(d) = \sum_{k=0}^{n} l_k d^k$ and $\alpha \in \ker L$, then we can write the n-th derivative of α as a linear combination of the previous derivatives, $\partial^n(\alpha) = -\sum_{k=0}^{n-1} \frac{l_k}{l_n} \partial^k(\alpha)$. This is a property that we are going to exploit in the following proposition.

Definition 2.22. *Let (K, ∂) be a differential field. Let $\{\alpha_1, ..., \alpha_n\} \subseteq K$. We define the wronskian matrix of those elements as $W(\alpha_1, ..., \alpha_n) \in M_n(K)$,*

$$W(\alpha_1, ..., \alpha_n) = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \partial(\alpha_1) & \partial(\alpha_2) & \cdots & \partial(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \partial^{n-1}(\alpha_1) & \partial^{n-1}(\alpha_2) & \cdots & \partial^{n-1}(\alpha_n) \end{pmatrix}$$

That is, $W(\alpha_1, ..., \alpha_n) = (\partial^{i-1}(\alpha_j))_{i,j=1,...,n}$. Then, we define the wronskian determinant, or simply the wronskian, as $\det W(\alpha_1, ..., \alpha_n)$.

We can clearly see that the wronskian matrix encodes some information about linear dependence, since if $\alpha_1, ..., \alpha_n$ are linearly dependent elements over the field of constants, then the wronskian (determinant) vanishes. What is not so obvious at first sight is that the converse is also true. If the wronskian vanishes, then the n elements are linearly dependent over the field of constants.

Proposition 2.23. *Let (K, ∂) be a differential field, C_K its field of constants and $\alpha_1, ..., \alpha_n \in K$. Then, $\alpha_1, ..., \alpha_n$ are linearly dependent over C_K if and only if $\det W(\alpha_1, ..., \alpha_n) = 0$.*

Proof. For the first implication, we can obviously see that if $\alpha_1, ..., \alpha_n$ are linearly dependent over C_K, then its wronskian determinant is going to be zero since the linear dependence of the first row extends to the other ones.

For the converse implication, if $\det W(\alpha_1, ..., \alpha_n) = 0$, then there exist $\lambda_1, ..., \lambda_n \in K$ not all zero so that $\sum_k \lambda_k \partial^i \alpha_k = 0$, for $i = 0, ..., n-1$. We have to prove that all of them are constants. Without loss of generality, we can assume that all minors of the wronskian determinant of order $n-1$ are nonzero (if not, we can always study one of those minors). Now, the $k+1$-th equation given by the linear dependence of the $\alpha_1, ..., \alpha_n$ is $\sum_i \lambda_i \partial^{k+1} \alpha_i = 0$, while the derivative of the k-th equation is $\sum \partial(\lambda)_i \partial^k(\alpha_i) + \sum \lambda_i \partial^{k+1}(\alpha_i) = 0$. Combining those two equations for every $k = 0, ..., n-2$ we obtain $\sum \partial(\lambda_i)\partial^k(\alpha_i) = 0$. If we make the extra assumption that $\lambda_1 = 1$ (we can always do that), then we have $\sum_{i=2}^n \partial(\lambda_i)\partial^k(\alpha_i) = 0$ for $k = 0, ..., n-2$. But if $\partial(\lambda_1), ..., \partial(\lambda_n)$ are not all zero, then

$$\det W(\alpha_2, ..., \alpha_n) = \det \begin{pmatrix} \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \partial(\alpha_2) & \partial(\alpha_3) & \cdots & \partial(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \partial^{n-2}(\alpha_2) & \partial^{n-2}(\alpha_3) & \cdots & \partial^{n-2}(\alpha_n) \end{pmatrix} = 0$$

But this is a minor of order $n-1$ of the wronskian matrix, and by assumption it cannot be zero. Therefore, the coefficients $\partial(\lambda_2), ..., \partial(\lambda_n)$ must all be zero, and so $\lambda_i \in C_K$ for all $i = 1, ..., n$.

□

Then, as we were anticipating, we can see the following key consequence.

Corollary 2.24. *Let (K, ∂) be a differential field with field of constants C_K, $L(d) \in K[d]$ a linear operator of order n. Then, $\dim_{C_K} \ker L(d) \leq n$. That is, its solutions form a vector space of dimension at most n.*

Proof. Let $\alpha_1, ..., \alpha_{n+1} \in \ker L$ and lets proof that $W(\alpha_1, ..., \alpha_{n+1}) = 0$. But since the last row consists of the elements $\partial^n(\alpha_i)$ for $i = 1, ..., n+1$ and since $\partial^n(\alpha_i) = -\frac{1}{l_n}\sum_{k=0}^{n-1} l_k \partial^k(\alpha_i)$ we can easily see that the last row is indeed a linear combination of the previous n rows. Then, the wronskian determinant vanishes and given the previous proposition, $\alpha_1, ..., \alpha_{n+1}$ are C_K-linearly dependent. □

3 Picard-Vessiot Extensions

In this section, we are going to find the equivalent concept to the splitting field of a polynomial. We are going to see that given a differential field (with the restrictive assumption that its field of constants must be algebraically closed) and a linear differential operator of order n, we can always construct a differential extension of fields that contains n linearly independent solutions to the equation and that is minimal, in a sense that we are going to discuss below.

3.1 Motivating Examples

Our goal during this whole section is to prove that a linear differential equation of order n has exactly n linearly independent solutions over constants and to construct the field where these solutions are. In the following subsections, we are going to take a look at some simple examples in order to see in what direction we are going.
First of all, remember that in the case of polynomials, given a field K and an irreducible nonconstant polynomial $p(X) \in K[X]$, we had that $K[X]/\langle p(X)\rangle$ is a field and contains a root of $p(X)$. What is the analogue of this construction?

Example 3.1. Let (K, ∂) be a differential field and consider the linear differential operator $l(d) = d - c \in K[d]$. Remember that $l(\alpha) = \partial(\alpha) - c\alpha$. Suppose that $\forall \alpha \in K$, $\partial(\alpha)\alpha^{-1} \neq c$. Then, $l(\alpha) = 0$ has no solution in K.
Consider now the ring extension $K[X] \supseteq K$. We want to turn it into a differential ring in a way that $l(d)$ has a solution in it. The simplest way to do so is to turn $X \in K[X]$ into a solution, and since the extension of ∂ to $K[X]$ is determined up to the choice of $\partial(X)$, we can define $\partial(X) = cX$. Then, $(K[X], \partial)$ is a differential ring where $l(X) = 0$. Further, since $K[X]$ is an integral domain (since K is a field), we can consider its field of quotients $\mathcal{Q}(K[X]) = K(X)$ with the derivative again extended as $\partial(X) = cX$. Then, $K \subseteq K(X)$ is a differential field extension where $l(d) = 0$ has a solution. With this construction, we have adjoined an exponential element to K.

Example 3.2. Let us now consider the adjunction of an integral. Let (K, ∂) be a differential field and let $c \in K$ be so that $\forall \alpha \in K$, $\partial(\alpha) \neq c$. We want to find a differential extension for K where there exists a primitive element for c. One immediate way to do so is to consider as before the field of rational funcions $K(X)$ and extend the derivation ∂ as $\partial(X) = c$. Then, denoting $\alpha = X \in K(X)$, we have that $K(\alpha) \supseteq K$ is a differential field extension where c has a primitive element α.
Notice that in this construction, we have not defined a linear differential operator in $L[d]$ associated with the differential equation. In the way those objects have been defined, all operators in $K[d]$ represent homogeneous linear equations, and $\partial(x) = c$ is not an homogeneous equation. We can, however, turn this into a homogeneous equation by noticing that $c^{-1}\partial(\alpha) = 1$ for any α that solves it, and then $\partial(c^{-1}\partial(\alpha)) = 0$. Thus, α would be a solution for the second order homogeneous equation given by $l(d) = d^2 - \partial(c)c^{-1}d$.

We generalize this procedure in the following remark

Observation 3.3. Let (K, ∂) be a differential field and $l(d) \in K[d]$ be a linear differential operator. If $\alpha \in K$ is so that $l(\alpha) = 0$, then it is a solution for the homogeneous equation defined by $l(d)$. However, we can consider $c \in K$ and the nonhomogeneous equation $l(d) = c$. In order to make this equation suitable for the theory we have developed, we have to consider the homogenized operator $l_c(d)$ associated to the inhomogeneous equation $l(d) = c$, defined as $l_c(d) = d\partial(c^{-1})l(d)$. In this (noncommutative) factorization, we can easily see that any $\alpha \in K$ for which $l(\alpha) = c$ is a solution to $l_c(\alpha) = 0$. Since the order of $l_c(d)$ has increased by one, the upper bound on the dimension of its vector space of solutions has also increased by one. However, since $l(k) = l_0 k$, $\forall k \in C_K$, we can easily see that any constant of K will also be a solution to the nonhomogeneous equation. Then, the extra linearly independent element of the solution space can be associated with a constant being also a solution.

Finally, following the previous two examples (adjunction of an exponential and adjunction of an integral) we can see that we can construct a field extension containing a solution for a given linear differential equation.

Example 3.4. Let (K, ∂) be a differential field and $l(d) = \sum_{k=0}^{n} l_k d^k \in K[d]$ a linear differential operator. We can adjoin a solution of the homogeneous equation $l(d) = 0$ to the field K by considering the ring of polynomials in n indeterminates $K[X_0, ..., X_{n-1}]$ and by extending the derivative as $\partial(X_i) = X_{i+1}$ for $i < n-1$ and $\partial(X_{n-1}) = -\frac{1}{l_n}\sum_{k=0}^{n-1} l_k X_k$. Then, denoting $\alpha = X_0 \in K[X_0, ..., X_{n-1}]$, we can see that $l(\alpha) = 0$. Further, this ring of polynomials can be seen as $K[X_0, ..., X_{n-1}] = K[\alpha, \partial(\alpha), ..., \partial^{n-1}(\alpha)]$ and since it is an integral domain, we can consider its field of quotients $\mathcal{Q}(K[\alpha, \partial(\alpha), ..., \partial^{n-1}(\alpha)]) = K\langle\alpha\rangle$, the smallest differential field containing both K and α.

Notice that by repeating this procedure, we can adjoin any number of solutions linearly independent over K (and therefore, over C_K). In particular:

Observation 3.5. Following the notation of the previous example, with the differential operator $l(d) \in K[d]$ and the differential field extension $K\langle\alpha\rangle$, we can produce an extension containing both K and $K_1 = K\langle\alpha\rangle$ that adjoins a new solution. We simply consider the field of rational funcions $K_1(Y_0, ..., Y_{n-1})$ with the derivation defined previously as $\partial(Y_i) = Y_{i+1}$ for $i < n-1$ and $\partial(Y_{n-1}) = -\frac{1}{l_n}\sum_{k=0}^{n-1} l_k Y_k$. Denoting $\beta = Y_0$ we see again that $l(\beta) = 0$ and that $K_1(Y_0, ..., Y_{n-1}) = K_1\langle\beta\rangle = K\langle\alpha, \beta\rangle$, the smallest field containing both K and α, β. Notice how $K\langle\alpha, \beta\rangle = \mathcal{Q}(K[X_0, ..., X_{n-1}, Y_0, ..., Y_{n-1}])$ with the previously defined derivation. Morover, those solutions are linearly independent over K since $X, Y \in K\langle\alpha, \beta\rangle$ are trascendental elements over K.

Therefore, we arrive to the construction we were pursuing:

Corollary 3.6. *Let (K, ∂) be a differential field and $l(d) \in K[d]$ a linear differential operator given by $l(d) = \sum_{k=0}^{n} l_k d^k$. Then, for any integer m, there exists a differential field extension of K containing m solutions of the equation $l(d) = 0$ linearly independent over K.*

Proof. Consider the ring of polynomials in $m \cdot n$ indeterminates $K[X_{ij}]$ where $i = 1, ..., m$ and $j = 0, ..., n-1$. If we extend the derivation ∂ of K as $\partial(X_{ij}) = X_{i(j+1)}$ for all i and for $j < n-1$ and define $\partial(X_{i(n-1)}) = -\frac{1}{l_n}\sum_{k=0}^{n-1} l_k X_{ik}$, then, denoting $\alpha_i = X_{i0}$, we can see that $l(\alpha_i) = 0$ for all $i = 1, ..., m$. Since it is an integral domain, we can consider the differential field $K(X_{ij}) = K\langle\alpha_1, ..., \alpha_m\rangle$. This is a differential field extension of K that contains m solutions of $l(d)$ that are linearly independent over the field K, since the indeterminates are trascendental elements. □

Notice that this does not contradict the result in the previous chapter, where we saw that the solution space to a linear differential equation of order n has dimension at most n over the field of constants. This last part is crucial since in the previous examples we have been thinking about linear independence over the base field, but this is not, in general, the same as the field of constants of the extension. That is, if $\bar{K} = K\langle\alpha_1, ..., \alpha_m\rangle \supseteq K$ is the field extension considered above, while $\alpha_1, ..., \alpha_m$ are linearly independent over C_K (because they are over K, which contains C_K), they need not (and in fact, must not for $m > n$) be linearly independent over the field of constants of $\bar{K}$, $C_{\bar{K}}$. The whole thing rests upon the fact that in general $C_{\bar{K}} \neq C_K$. Consider the following observation.

Example 3.7. Let (K, ∂) be a field, $c \in K$ and $a \in K$ so that $\partial(a) = ca$. Then, $a \in K$ is a solution for the differential equation given by the operator $l(d) = d - c$ already considered above. If we consider again the field of rational functions $K(X)$ with the derivative $\partial(X) = cX$ and denote $\beta = X \in K(X)$, we have $K(X) = K\langle\beta\rangle = \bar{K}$ and we have adjoined a new solution, linearly independent over K and over C_K. However, since $l(d)$ is of order one, we know that $\ker_{C_{\bar{K}}} l(d)$ has dimension at most one over the field of constants of $\bar{K}$, $C_{\bar{K}}$. That means that $\alpha, \beta \in \bar{K}$ cannot be linearly independent over $C_{\bar{K}}$ and therefore that $C_{\bar{K}}$ cannot be equal to C_K.
Indeed, if we consider $\partial(\frac{\beta}{\alpha}) = \frac{\partial(\beta)\alpha - \beta\partial(\alpha)}{\alpha^2} = 0$ since $\partial(\beta)\alpha = c\beta\alpha = \beta\partial(\alpha)$, we get that $\lambda = \frac{\beta}{\alpha} \in C_{\bar{K}}$ is a constant. Further, $\lambda \notin K$ since $\beta = \lambda\alpha \notin K$. Therefore, λ is a constant in $C_{\bar{K}}$ that does not belong to C_K and then $C_{\bar{K}} \neq C_K$.

Therefore, before proceeding to the following section, we must highlight the following fact.

Proposition 3.8. *Let $L(d) \in K[d]$ be a linear differential operator of order n. Let $\bar{K}_1 \supseteq K$ be a differential extension where $L(d) = 0$ has n $C_{\bar{K}_1}$-linearly independent solutions $\alpha_1, ..., \alpha_n \in \bar{K}_1$. Let $K_1 = K\langle\alpha_1, ..., \alpha_n\rangle \subseteq \bar{K}_1$ with field of constants C_1. Let $\bar{K}_2 \supseteq \bar{K}_1$ be another extension containing the previous one where there are also n linearly independent solutions over its field of constants, $C_{\bar{K}_2}$, $\beta_1, ..., \beta_n \in \bar{K}_2$, and let $K_2 = K\langle\beta_1, ..., \beta_n\rangle \subseteq \bar{K}_2$ with field of constants C_2. Then, if they are so that $K_1 \subsetneq K_2$, then, $C_1 \subsetneq C_2$.*

Proof. First of all, we have $V_1 = \ker_{\bar{K}_1} L = \langle\alpha_1, ..., \alpha_n\rangle_{C_1}$ and $V_2 = \ker_{\bar{K}_2} L = \langle\beta_1, ..., \beta_n\rangle_{C_2}$, where the subscript C_1 and C_2 denotes that we are considering the vector space generated by those elements over those fields respectively. But since $\alpha_1, ..., \alpha_n$ are linearly independent over C_1, their wronskian determinant must be nonzero. And so, they will be linearly independent over C_2 as well. Therefore, $\langle\alpha_1, ..., \alpha_n\rangle_{C_2}$ is a C_2-vector space of dimension n contained in V_2 and so they are equal. But then, if $K_1 \subsetneq K_2$ we have that $V_1 \subsetneq V_2$, and since $V_1 = \langle\alpha_1, ..., \alpha_n\rangle_{C_1} \subsetneq \langle\alpha_1, ..., \alpha_n\rangle_{C_2} = V_2$, necessarily we must have that $C_1 \subsetneq C_2$. In particular, $C_2 \neq C_K$. □

Therefore, with this previous result, we can see that in order to find a minimal extension containing a full set of solutions for a differential equation, we must study the minimality of the field of constants. In particular, we can see that it has the following corollary.

Corollary 3.9. *Let (K, ∂) be a differential field, $L(d) \in K[d]$ a linear differential operator of order n and $\bar{K}$ a differential extension of K so that it contains n linearly independent solutions for $L(d) = 0$ over its field of constants $C_{\bar{K}}$ and is differentially generated by* *them. Let $\bar{K}$ also be so that $C_{\bar{K}} = C_K$. Then, if $\tilde{K} \supseteq K$ is a differential field extension so that $L(d) = 0$ also has a set of n linearly independent solutions over its constants that differentially generate it and $\tilde{K} \subseteq \bar{K}$, then $\tilde{K} = \bar{K}$.*

Proof. In the light of the previous result, if we had $\tilde{K} \subsetneq \bar{K}$, we would also have $C_{\tilde{K}} \subsetneq C_{\bar{K}}$. But since $C_K \subseteq C_{\tilde{K}} \subseteq C_{\bar{K}}$, we would have a contradiction. □

With these results, we have enough motivation to see what kind of analog to the splitting field of a polynomial we are looking for. We have also seen that the minimality of the field of constants will play a very important role.

3.2 Existence and Uniqueness of Picard-Vessiot Extensions

In the following discussion, we are going to see that given a differential field and a linear differential equation, we can always construct an extension where it has all of its solutions (meaning a set of linearly independent solutions over constants which size coincides with the order of the equation) and that we can do it in such a way that the construction is minimal. First of all, consider the following observation:

Observation 3.10. Let (K, ∂) be a differential field and $L(d) \in K[d]$ a linear differential operator of order n. If $\bar{K}$ is a differential extension that contains n-linearly independent over $C_{\bar{K}}$ solutions of $L(d) = 0$ (by the result on the wronskian, it cannot contain more than that) and those solutions are $\alpha_1, ..., \alpha_n \in \bar{K}$, then we can consider the smallest differential subfield contained in $\bar{K}$ that contains K as well as $\alpha_1, ..., \alpha_n$. We are going to denote this field as $K\langle\alpha_1, ..., \alpha_n\rangle$.

With this in mind, we can define what we mean by the minimal extension that contains a fundamental set of solutions to the linear equation. Consider, with the previous notation, a differential extension $\bar{K} \supseteq K$ containing n linearly independent solutions $\alpha_1, ..., \alpha_n \in \bar{K}$ so that:

(i) It is differentially generated by the solutions, i.e., $\bar{K} = K\langle\alpha_1, ..., \alpha_n\rangle$.

(ii) It has no new constants, i.e., $C_{\bar{K}} = C_K$.

Then, we can see that such an extension is minimal, in the following sense.

Proposition 3.11. *Let (K, ∂), $L(d) \in K[d]$ and $\bar{K}$ as above. If $\bar{K}' \subseteq \bar{K}$ is a differential extension of K so that it also contains n linearly independent solutions of $L(d) = 0$ over the field of constants of K, then $\bar{K}' = \bar{K}$.*

Proof. This is again a consequence of the previous corollary 3.9 □

Then, it follows that this is the definition that we are looking for.

Definition 3.12. *Let (K, ∂) be a differential field and $L(d) \in K[d]$ a linear differential operator of order n. Then, a differential extension $\bar{K} \supseteq K$ is a Picard-Vessiot extension for $L(d)$ over K if:*

(i) There exists $\{\alpha_1, ..., \alpha_n\} \subseteq \bar{K}$ linearly independent over $C_{\bar{K}}$ so that $L(\alpha_i) = 0$ for all $i = 1, ..., n$.

(ii) The field $\bar{K}$ is differentially generated over K by the solutions to the linear differential equation, $\bar{K} = K\langle \alpha_1, ..., \alpha_n \rangle$.

(iii) It adds no new constants, that is, $C_{\bar{K}} = C_K$.

3.2.1 Existence

We now turn to the task of proving that such extensions do exist for every differential operator over certain fields and that they are unique up to the isomorphism of differential fields. We have already seen in the previous section how the construction is going to be, that is, to construct a field where the operator has a given number of solutions we need only consider the ring of differential polynomials in that many indeterminates. In order to turn that into a Picard-Vessiot extension, we will need the following result, which comes from the theory of algebraic geometry.

Theorem 3.13. *Let (K, ∂) be a differential field and $R \supseteq K$ be a differential ring extension. Let R be an integral domain finitely generated as a K-algebra. Then, if R does not contain any proper differential ideal and if C_K is algebraically closed, the field extension $\mathcal{Q}(R)$ given by its field of quotients has C_K as the field of constants.*

We have not developed the tools needed in order to prove this result since it depends on a number of concepts from algebraic geometry. A proof for this result can be found in [4] (pp. 129). It is of capital importance due to the role played by the field of constants when looking for a minimal field extension, as was seen in 3.9. Indeed, thanks to this result we can see that if we construct a differential ring that contains the solutions to a given equation and without proper differential ideals, we will automatically have that it does not add constants. Further, thanks to proposition 2.8 from the previous chapter, we know that every maximal differential ideal is also a prime differential ideal. Therefore, if for a ring extension $R \supseteq K$ we take the quotient ring R/M, where M is a maximal differential ideal of R, we have that R/M is a differential integral domain (since M is a prime ideal) that is also without proper differential ideals, since M is a maximal differential ideal of R.

Let's then work towards our goal in a constructive manner.

Observation 3.14. Let (K, ∂) be a differential field (with C_K field of constants algebraically closed) and $L(d) \in K[d]$ a linear differential operator given by $L(d) = l_0 + l_1 d + ... + l_n d^n$. We know from the discussion of the previous section that $K[\partial^i X_j]$ with $i = 0, ..., n-1$ and $j = 1, ..., n$ is a differential ring and that $X_1, ..., X_n$ are n-linearly independent solutions over C_K, since we defined $l_n \partial^n(X_j) = -l_{n-1}\partial^{n-1}(X_j) + ... + l_0 X_j$. Morover, it is an integral domain and it is clearly generated differentially by the n independent solutions. One might therefore think that then $\mathcal{Q}(K[\partial^i X_j])$ is a Picard-Vessiot extension for L over K. But this fails to be true, since in general the field of constants of this field will contain new constants not in C_K.

In order to solve this problem and still thinking about $K[\partial^i X_j]$ as the first step towards a Picard-Vessiot extension, we can consider a maximal differential ideal $M \subseteq K[\partial^i X_j]$ and take the quotient $K[\partial^i X_j]/M$. From the previous results, we know that this is a differential integral domain and that it does not contain proper differential ideals. Therefore, $\mathcal{Q}(K[\partial^i X_j]/M)$ is a field extension of K that adds no new constants and that is generated by the solutions of $L(d)$. This, however, won't completely solve the problem either, since the linear independence of the solutions over C_K might be lost in the process.

Indeed, in $K[\partial^i X_j]$ we have that the wronskian determinant $w(X_1, ..., X_n)$ is clearly nonzero since it is a polynomial of positive degree. But if $M \subseteq K[\partial^i X_j]$ is a maximal ideal that contains $w(X_1, ..., X_n)$, then the wronskian of the solutions will be zero in the quotient ring. In order to solve that, we will localize the ring of polynomials in the inverse of the wronskian determinant. We will see how below.

Definition 3.15. *Let R be a ring that is an integral domain. A multiplicative system of R is a subgroup $S \subseteq R$ that is closed under the product of R. That is, $1 \in S$ and $\forall a, b \in S$, $ab \in S$. Then, the localization of R in S, denoted as $R[S^{-1}]$, is the ring of conjugacy classes of $R \times S$ given by the equivalence relation $(a, s) \sim (b, t)$ if and only if $at = bs$ and with operations defined in the same way as with the quotient field of an integral domain. The multiplicative group condition is required for the denominators to belong always to the set S.*

With this idea, we can consider instead of the ring of polynomials $K[\partial^i X_j]$, the localized ring of polynomials with respect to the multiplicative system of the powers of the wronskian, the set $W = \{w(X_1, ..., X_n)^k : k \in \mathbb{N}\}$. Then, the ring $K[\partial^i X_j][W^{-1}]$ has the property that for any maximal differential ideal M, the wronskian $w(X_1, ..., X_n) \notin M$, since it is now a unit of the ring. This is the last ingredient we need in order to prove the existence of Picard-Vessiot extensions.

Theorem 3.16. *Let $(K; \partial)$ be a differential field with algebraically closed field of constants C_K. Let $L(d) = l_n d^n + ... + l_0 \in K[d]$ be a linear differential operator of order n. Then, there exists a differential field $\bar{K}$ containing K as a subfield that is a Picard-Vessiot extension for $L(d)$ over K.*

Proof. We have already done most of the proof in parts, we only need now to join the pieces. First of all, consider the ring of differential polynomials given by $K[\partial^i X_j]$, $i = 0, ..., n-1$, $j = 1, ..., n$, with the derivation $l_n \partial^n(X_j) = -l_{n-1}\partial^{n-1}(X_j) - ... - X_j$. This is a differential integral domain that contains K as a subfield and that is generated by n C_K-linearly independent solutions of $L(d) = 0$. Now, consider the wronskian determiant $w(X_1, ..., X_n)$, which is nonzero, and consider the multiplicative system formed by its powers, $W \subseteq K[\partial^i X_j]$. If we now consider the localization $K[\partial^i X_j][W^{-1}]$ and a differential maximal ideal $M \subseteq K[\partial^i X_j][W^{-1}]$, we know that in particular, $w(X_1, ..., X_n) \notin M$, since it is an invertible element in the localized ring, and that M is also a prime ideal. Therefore, the quotient ring $K[\partial^i X_j][W^{-1}]/M$ is a differential integral domain which does not contain proper differential ideals. Therefore by the previous theorem 3.13 we get that $\bar{K} = \mathcal{Q}(K[\partial^i X_j][W^{-1}]/M)$ is a field that has the same field of constants as K. Morover, the classes of the elements $X_1, ..., X_n$ are clearly solutions to the equation $L(d) = 0$ viewed in this field and are linearly independent over C_K since $w(X_1, ..., X_n) \neq 0$. And finally, $\bar{K}$ is clearly generated over K by the classes of the solutions $X_1, ..., X_n$. Therefore, it is a Picard-Vessiot extension for $L(d)$ over K. □

Observation 3.17. As a remark on the previous proof, we see that the fact that the field $\mathcal{Q}(K[\partial^i X_j])$ is differentially generated over K by the elements $X_1, ..., X_n$ does not prevent $\bar{K}$ to also be generated over K by the classes of $X_1, ..., X_n$. The reason for this remark is that the notation $\bar{K} = K\langle X_1, ..., X_n\rangle$ is misleading since the field $\mathcal{Q}(K[\partial^i X_j])$ could also be denoted this way. One has to be careful when the field that contains this extension denoted as $K\langle X_1, ..., X_n\rangle$ is omitted.

3.2.2 Uniqueness

Having seen that Picard-Vessiot extensions always exist given that the field of constants is algebraically closed, we now turn to see whether they are unique. We want to see that if (K, ∂), $L(d) \in K[d]$ and $L_1, L_2 \supseteq K$ are Picard-Vessiot extensions for L over K, then they will be equal in a certain sense.

The main idea will be to see that Picard-Vessiot extensions are minimal in the sense that if they can be embedded in another extension, then they can be embedded in a unique way. Consider the following observation.

Observation 3.18. Let $L(d) \in K[d]$ be a differential operator and $\bar{K} = K\langle \alpha_1, ..., \alpha_n \rangle$ be a Picard-Vessiot extension for $L(d)$ over K with its solutions. Let $F \supseteq K$ be a differential extension that has the same field of constants as K. If there exists a differential K-morphism $\varphi : \bar{K} \longrightarrow F$, then $\varphi(\ker_{\bar{K}} L)$ is a C_K vector space of dimension n, since φ is an injective map (since it is in particular a field homomorphism) and then $\varphi(\alpha_1), ..., \varphi(\alpha_n)$ are linearly independent over C_K. But since $\varphi(\ker_{\bar{K}} L) \subseteq \ker_F L$ and $C_F = C_K$, then we must have that they are indeed equal. Then, if a K-morphism exists between a Picard-Vessiot extension and another extension that has the same constants, then it contains a fundamental set of solutions for $L(d) = 0$.

This is the key property that we are going to use in order to prove that Picard-Vessiot extensions are unique. Indeed, from the previous observation, we can prove the following result.

Corollary 3.19. *Let (K, ∂) be a differential field and $L(d) \in K[d]$. Let $\bar{K}_1, \bar{K}_2 \supseteq K$ be Picard-Vessiot extensions for L over K and let $\bar{K} \supseteq K$ be a field extension that adds no new constants. If there exist differential K-morphisms $\varphi_i : \bar{K}_i \longrightarrow \bar{K}$, for $i = 1, 2$, then $\varphi_1(\bar{K}_1) = \varphi_2(\bar{K}_2)$.*

Proof. This follows from the previous observation. Indeed, since φ_i is injective, commutes with the derivation and is the identity on K, we have that $\varphi_i(\ker_{\bar{K}_i} L)$ is a C_K vector space of dimension n. But since $\bar{K}$ has C_K as its field of constants and since $\ker_{\bar{K}} L$ has dimension at most n over C_K and since clearly $\varphi_i(\ker_{\bar{K}_i}) \subseteq \ker_{\bar{K}} L$, then we have that $\varphi_1(\ker_{\bar{K}_1} L) = \varphi_2(\ker_{\bar{K}_2} L) = \ker_{\bar{K}} L$. But then, since $\bar{K}_i = K\langle \ker_{\bar{K}_i} L \rangle$, we then have that $\varphi_1(\bar{K}_1) = \varphi_2(\bar{K}_2)$. □

Therefore, the only thing that we have to do in order to prove that Picard-Vessiot extensions are unique is to make sure that for any two Picard-Vessiot extensions for the same equation over the same field, we can always construct a differential extension that adds no new constants and embed them into it. If that's the case, then this last result will allow us to prove that there is a differential K-isomorphism between them. The first question is solved by the following observation.

Observation 3.20. We want to construct a differential field $\bar{K}$ containing K as a subfield, adding no new constants and so that any Picard-Vessiot extension of K for an operator $L(d) \in K[d]$ can be embedded into it. For the no-new-constants part, we would very much like to use our previous result 3.13. Then, we need an integral domain $R \supseteq K$ finitely generated as a K-algebra so that it has no proper differential ideals. Further, it needs to be big enough in order to contain a Picard-Vessiot extension for $L(d)$. Given two Picard-Vessiot extensions $\bar{K}_1, \bar{K}_2 \supseteq K$, our first idea would be to consider their tensor product $\bar{K}_1 \otimes \bar{K}_2$, where both extensions can be easily embedded. However, neither of those is finitely generated as a K-algebra (they are finitely generated differentially, but infinitely generated algebraically since they are fields).

In order to solve that issue, we can supose that one of the extensions has been constructed as in the existence theorem. Thus, $\bar{K}_1 = \mathcal{Q}(K[\partial^i X_j][W^{-1}]/I)$, where $R = K[\partial^i X_j][W^{-1}]/I$ is a differential integral domain finitely generated as a K-algebra. Then, we can consider the tensor product $R \otimes \bar{K}_2$. This is still not finitely generated as a K-algebra, but it is finitely generated as a $\bar{K}_2$-algebra. But this is good enough, since if $M \subseteq R \otimes \bar{K}_2$ is a differential maximal ideal, then $\bar{K} = \mathcal{Q}((R \otimes \bar{K}_2)/M)$ has the same field of constants as $\bar{K}_2$. But since $\bar{K}_2$ is a Picard-Vessiot extenision, it has the same field of constants as K.

Now, we can turn our efforts towards finding field homomorphisms from $\bar{K}_1, \bar{K}_2$ to this recently constructed extension $\bar{K}$. We do so in the following proof.

Proposition 3.21. *Let (K, ∂) be a differential field with algebraically closed field of constants C_K, $L(d) \in K[d]$ be a differential operator and $\bar{K}_1, \bar{K}_2 \supseteq K$ be two Picard-Vessiot extensions for it. Then, there exists a differential field extension $\bar{K} \supseteq K$ that adds no new constants and two field homomorphisms $\varphi_i : \bar{K}_i \longrightarrow \bar{K}$.*

Proof. Following the previous observation, let $\bar{K}_1$ be of the form $\bar{K}_1 = \mathcal{Q}(R)$ and let $\bar{K} = \mathcal{Q}((R \otimes \bar{K}_2)/M)$. Now, consider the injective differential ring homomorphism $\psi : R \longrightarrow R \otimes \bar{K}_2$ given by the obvious inclusion $\psi(a) = a \otimes 1$. We can project ψ into the quotient $\tilde{\psi} : R \longrightarrow (R \otimes \bar{K}_2)/M$ without losing injectivity, since the preimage $\psi^{-1}(M) \subseteq R$ is a differential ideal and if $\psi^{-1}(M) = R$, then $\psi(1) = 1 \otimes 1$ would be an element of M, which is a contradiction with the fact that M is a maximal differential ideal (and thus is a proper ideal). Then, $\psi^{-1}(M) = \{0\}$ and therefore $\tilde{\psi}$ is again injective.

Now, since it is an injective differential ring homomorphism, we can extend $\tilde{\psi} : R \longrightarrow (R \otimes \bar{K}_2)/M$ to their fields of fractions in a unique way, and define $\varphi_1 : \bar{K}_1 = \mathcal{Q}(R) \longrightarrow \bar{K} = \mathcal{Q}((R \otimes \bar{K}_2)/M)$ as this extension. This is a differential field homomorphism.

Finally, we can consider $\varphi_2 : \bar{K}_2 \longrightarrow \mathcal{Q}((R \otimes \bar{K}_2)/M)$ defined as $\varphi_2(a) = (1 \otimes a) + M$, which is injective since it is a field homomorphism. Morover, by their definition, φ_1, φ_2 are differential K-morphisms. □

We now are at last able to prove the uniqueness of Picard-Vessiot extensions:

Theorem 3.22. *Let (K, ∂) be a differential field with algebraically closed field of constants, $L(d) \in K[d]$ a differential linear operator and $\bar{K}_1, \bar{K}_2$ be two Picard-Vessiot extensions for L over K. Then, there exists a field K-isomorphism $\psi : \bar{K}_1 \longrightarrow \bar{K}_2$.*

Proof. Without loss of generality, we can assume $\bar{K}_1$ to be the Picard-Vessiot extension constructed in the existence proof, $\bar{K}_1 = \mathcal{Q}(R)$, where $R = K[\partial^i X_j][W^{-1}]/I$. Define $\bar{K} \supseteq K$ as $\bar{K} = R \otimes \bar{K}_2$ and consider the field K-morphisms $\varphi_i : \bar{K}_i \longrightarrow \bar{K}$ defined in the previous proposition. Then, by corollary 3.19, we have that $\varphi_1(\bar{K}_1) = \varphi_2(\bar{K}_2)$ and since they are field K-morphisms (and therefore, are injective), we get that $\varphi_2^{-1} \circ \varphi_1 : \bar{K}_1 \longrightarrow \bar{K}_2$ is a differential field K-isomorphism. □

4 The Galois Group of a Differential Equation

During this section, we are going to fulfill our objective of associating a group to every linear differential equation. The idea, due to Galois, will be to study the set of solutions to a given differential equation and its structure in order to encode information about its symmetries in the form of a group. Much in the same way as with algebraic equations, our intuition is going to take us to a different definition to the one usually given. We are going to prove, however, that both definitions give us the same object, the differential Galois group.

4.1 Motivating Examples

Let's begin with some examples in order to get an idea of how we are going to proceed. We have already seen some of those examples. We are now going to associate a group with their solutions.

Given a differential field (K, ∂) with algebraically closed field of constants C_K and a linear differential operator $L(d) \in K[d]$ of order n, we can consider a Picard-Vessiot extension $\bar{K}$ for it. Let $\alpha_1, ..., \alpha_n \in \bar{K}$ be a set of C_K-linarly independent solutions of $L(d) = 0$. Then, denoting $L : \bar{K} \longrightarrow \bar{K}$ the evaluation map by a stretch of notation, we can see that it is a C_K linear map and $\ker L(d) = \langle \alpha_1, ..., \alpha_n \rangle$ is a vector space over C_K of dimension n.

We want to associate a group with $L(d)$ so that it encodes the structure and symmetry of its space of solutions. To begin with, the structure of the space of solutions $\ker L(d)$ is that of a vector space and the group that encodes this information is the group of C_K linear automorphisms of $\ker L(d)$. But since these solutions belong to a differential field, they possess some extra structure that is not considered in the group of linear automorphisms. So, in a sense, the group of linear automorphisms is "too big"since all of its elements preserve the linear structure of $\ker L(d)$ but not all of them preserve its supplementary differential structure. In the following examples, we are going to consider the subgroup of those linear automorphisms that also preserve the differential structure of the solutions and call it the Galois group associated with the differential equation.

Example 4.1. Let (K, ∂) be a differential field with algebraically closed field of constants C_K and consider the linear differential operator $L(d) = d^2 - \partial(c)c^{-1}d \in K[d]$. We know from the preceding section that we can consider a Picard-Vessiot extension $\bar{K} \supseteq K$ for $L(d)$ where, if $\alpha, \beta \in \bar{K}$ are two linearly independent solutions over C_K (which is equal to $C_{\bar{K}}$), we can write as $\bar{K} = K\langle \alpha, \beta \rangle$. Since $1 \in K$ is a solution for $L(d) = 0$, we can pick $\beta = 1$ and then the other linarly independent solution can be picked so that $\partial(\alpha) = c$. Then, $\bar{K} = K\langle \alpha, 1 \rangle = K\langle \alpha \rangle$ is a Picard-Vessiot extension for $L(d)$ and $\ker L(d) = \langle \alpha, 1 \rangle \subseteq \bar{K}$ as a C_K-vector space.

Now, as said above, since the solutions of $L(d)$ have the structure of a vector space over C_K, our first idea to consider as the group that encodes the structure and symmetry of the solutions is the group of linear automorphisms of $\ker L(d)$, denoted as $\mathrm{Aut}_{C_K} \ker_{\bar{K}} L$. Once we have fixed a basis for the vector space, its linear automorphisms are in bijection with the group of invertible matrices $\mathbb{GL}_2(C_K)$ and in fact this is a group isomorphism. Then, if $\varphi : \ker L \longrightarrow \ker L$ is a linear isomorphism, its matrix $\Phi = (\varphi_{ij}) \in \mathbb{GL}_n(C_K)$ in the basis $\{\alpha, 1\}$ is given by the images

$$\varphi(\alpha) = \varphi_{11}\alpha + \varphi_{12}1 \qquad \varphi(1) = \varphi_{21}\alpha + \varphi_{22}1$$

The group $\mathbb{GL}_2(C_K)$ is in general too large for it to succesfuly give the information we want about the linear equation. In particular, we would like the images of the solutions to behave in the same way as the solutions themselves. By considering linear automorphisms, we already have by definition that the image of a solution is again a solutions to the same differential equation. In order to make the images behave in the same way differentially, we consider some particular relations which we want to be preserved. For example, since 1 is a constant, we demand $\varphi(1)$ to be again a constant. Morover, since $\partial(\alpha) = c\alpha$, we want its image to satisfy the same relation, $\partial(\varphi(\alpha)) = c\alpha$. Finally, we want $\varphi(1) = 1$ since 1 belongs to the field K and therefore it is not only a property of the differential equation but of the base field itself. With this three conditions we get:

(i) $\partial(\varphi(1)) = 0 : \ \partial(\varphi_{21}\alpha + \varphi_{22}1) = \varphi_{21}\partial(\alpha) = c\varphi_{21}\alpha = 0 \implies \varphi_{21} = 0$

(ii) $\partial(\varphi(\alpha)) = c\alpha : \ \varphi_{11}\partial(\alpha) = c\alpha \implies \varphi_{11} = 1$

(iii) $\varphi(1) = 1 : \ \varphi_{22} = 1$

Therefore, if we consider the elements of $\mathbb{GL}_2(C_K)$ that preserve those three relations, we are considering the invertible matrices over C_K of the form

$$\begin{pmatrix} 1 & \varphi \\ 0 & 1 \end{pmatrix}$$

Where $\varphi \in C_K$. The elements of this form are indeed a subgroup of $\mathbb{GL}_2(C_K)$. We should now proof that there are no more requirements to satisfy and that this group is indeed the one we were looking for, but for now we are going to stop here and associate to this operator the group:

$$G = \left\{ \begin{pmatrix} 1 & \varphi \\ 0 & 1 \end{pmatrix} \in \mathbb{GL}_2(C_K) : \ \varphi \in C_K \right\} \cong C_K^+$$

Which is indeed isomorphic to the additive subgroup of C_K.

Before studying the general case, let's do another example.

Example 4.2. This time, let's consider the real field $\mathbb{R}$ with the trivial derivation and extend it to the field of real rational functions $\mathbb{R}(X)$ with $\partial(X) = 1$. Consider $L(d) \in \mathbb{R}(X)[d]$ given by $L(d) = d^2 + 1$. We know from elementary calculus that the real funcions $\cos x, \sin x : \mathbb{R} \longrightarrow \mathbb{R}$ are linearly independent solutions for this equation, and thus $\mathbb{R}(X)\{\sin x, \cos x\}$ is a Picard-Vessiot extension for the operator $L(d)$ over the field $\mathbb{R}(X)$. Therefore, $\ker L = \langle \sin x, \cos x \rangle$ since we know that it has to be a vector space over $\mathbb{R} = C_{\mathbb{R}(X)}$ of dimension 2.
Following the previous example, we are going to define its Galois group as the group of real linear automorphisms that also preserve its differential structure. Let $\varphi \in \mathrm{Aut}_{\mathbb{R}}(\ker L)$ and let $(\varphi_{ij}) \in \mathbb{GL}_2(\mathbb{R})$ be its matrix in the basis $\sin x, \cos x$. Then,

$$\varphi(\sin x) = \varphi_{11} \sin x + \varphi_{12} \cos x \qquad \varphi(\cos x) = \varphi_{21} \sin x + \varphi_{22} \cos x$$

What differential relations do we want φ to preserve? First of all, the relations $\partial(\sin x) = \cos x$ and $\partial(\cos x) = -\sin x$ must remain valid when changing $\sin x$, $\cos x$ by its images under φ. Then, we also want the relation $\cos^2 x + \sin^2 x = 1$ to be preserved under φ, that is, we want $\varphi(\sin x)^2 + \varphi(\cos x)^2 = 1$. By imposing this conditions we get the following restrictions upon the coefficients of (φ_{ij}):

(i) $\partial(\varphi(\sin x)) = \varphi(\cos x) : \varphi_{11}\cos x - \varphi_{12}\sin x = \varphi_{21}\sin x + \varphi_{22}\cos x \implies \varphi_{11} = \varphi_{22}, \varphi_{12} = -\varphi_{21}$.

(ii) $\varphi(\sin x)^2 + \varphi(\cos x)^2 = 1 : (\varphi_{11}\sin x + \varphi_{12}\cos x)^2 + (\varphi_{21}\sin x + \varphi_{22})^2 = 1 \implies \varphi_{11}^2 + \varphi_{12}^2 = 1$.

Again, it remains to be seen that every other differential relation between the solutions of $L(d)$ has already been taken into account with those two relations. Then, the group associated to the equation $L(d) = d^2 + 1 = 0$ over the field $\mathbb{R}(X)$ is:

$$G = \left\{ \begin{pmatrix} \lambda & \mu \\ -\mu & \lambda \end{pmatrix} \in \mathbb{GL}_2(\mathbb{R}) : \lambda^2 + \mu^2 = 1 \right\} = \mathbb{SO}_2(\mathbb{R})$$

4.2 The Differential Galois Group

During the following discussion, we are going to construct the Galois group associated with a given linear differential equation. As we have seen in the previous examples, we will define it as the subgroup of the group of linear automorphisms that preserve the differential relations between the solutions of the equation. Moreover, we are going to closely follow the same construction studied in the context of polynomial equations.

Let's begin by defining what we understand as a differential relation.

Definition 4.3. *Let (K, ∂) be a differential field. We define the ring of differential polynomials over K as the ring of polynomials in a countable number of indeterminates $K[X_0, ..., X_n, ...]$ together with the derivation given by $\partial(X_i) = X_{i+1}$. This is a well-defined differential ring since we have extended the derivation to every indeterminate. We are going to denote it by $K\{X\}$. An element of $K\{X\}$ will be denoted by $p\{X\} \in K\{X\}$, remembering that in fact $p\{X\} = p(X, \partial X, ...)$.*
In a similar way, we can define the ring of diffrential polynomials in several indeterminates as the ring of polynomials $K[X_{ij}]$ with $j = 1, ..., n$ and $i = 0, ...$ together with the derivation given by $\partial(X_{ij}) = X_{i(j+1)}$. We are going to denote it by $K\{X_1, ..., X_n\}$. An element of this differential ring will be denoted by $p\{X_1, ..., X_n\}$.

Now that we have defined the set where differential relations are going to be, we define the following map:

Definition 4.4. *Let (K, ∂) be a differential field and $K\{X_1, ..., X_n\}$ the ring of polynomials in n differential indeterminates. Let $L(d) \in K[d]$ be a differential operator and $\bar{K} = K\langle \alpha_1, ..., \alpha_n \rangle$ a Picard-Vessiot extension, where $\alpha_1, .., \alpha_n$ are linearly independent solutions of $L(d) = 0$ over the field of constants. We define the map*
$\psi_\alpha : K\{X_1, ..., X_n\} \longrightarrow \bar{K}$ as $\psi_\alpha(p\{X_1, ..., X_n\}) = p\{\alpha_1, ..., \alpha_n\}$. It is a differential ring homomorphism. Then, we are going to say that the differential polynomial $p\{X_1, ..., X_n\}$ represents a differential relation between solutions if $p\{X_1, ..., X_n\} \in \ker_K \psi_\alpha$.

Notice that the previously defined map is indeed a ring homomorphism, since $K\{X_1, ..., X_n\} = K[X_{ij}]$ is in particular a K-vector space that admits $\{\Pi_{ij} X_{ij}^{m_{ij}}\}$ as a basis and we have defined $\psi_\alpha(\Pi_{ij} X_{ij}^{m_{ij}}) = \Pi_{ij} \partial^i(\alpha_j)^{m_{ij}}$. Therefore, since it is also compatible with the product in $K[X_{ij}]$, it is also a morphism of K-algebras. Further, it is indeed a differential ring homomorphism. Thus, $\ker \psi_\alpha$ is a differential ideal of $K\{X_1, ..., X_n\}$. We are not going to use this property by now, but let us note that it allows the following result:

Corollary 4.5. *Let $L(d) \in K[d]$ be a differential operator over K and let $\bar{K} = K\langle \alpha_1, ..., \alpha_n \rangle \supseteq K$ be a Picard-Vessiot extension for L. Let $\psi_\alpha : K\langle X_1, ..., X_n \rangle \longrightarrow \bar{K}$ be the ring homomorphism defined above and $\ker_K \psi_\alpha$ its kernel. Then, $\bar{K} \cong \mathcal{Q}(K\langle X_1, ..., X_n \rangle / \ker_K \psi_\alpha)$.*

Proof. This is a simple application of the isomorphism theorem for rings. Since $\ker_K \psi_\alpha$ is an ideal of the ring of differential polynomials, we have that $K\langle X_1, ..., X_n \rangle / \ker_K \psi_\alpha \cong \mathrm{Im}_K(\psi_\alpha)$. But $\ker_K \psi_\alpha$ is a prime ideal, since $\bar{K}$ is a field. Therefore, the quotient is an integral domain. Morover, it is a differential integral domain, since $\ker_K \psi_\alpha$ is clearly a differential ideal. Therefore, $\mathcal{Q}(K\langle X_1, ..., X_n \rangle / \ker_K \psi_\alpha) \cong \mathcal{Q}(\mathrm{Im}(\psi_\alpha)) \subseteq \bar{K}$ is a differential field. But since it contains a full set of solutions for $L(d) = 0$ and $\bar{K}$ is a Picard-Vessiot extension, we must have the isomorphism $\mathcal{Q}(K\langle X_1, ..., X_n \rangle / \ker_K \psi_\alpha) \cong \bar{K}$. □

Following the notation of the previous definition, the object we are interested in studying is precisely $\ker L \subseteq \bar{K}$, which as we have already seen is a C_K-vector space. The linear structure of this space is reflected by its group of linear automorphisms, $\mathrm{Aut}_{C_K} \ker L$. Once a basis has been fixed for the vector space, we can identify every linear automorphism with an element of $\mathbb{GL}_n(C_K)$, its associated matrix. As we have already seen, we are going to find a subgroup of $\mathrm{Aut}_{C_K} \ker L$ (or, once a basis has been fixed, a subgroup of $\mathbb{GL}_n(C_K)$) that preserves the differential relations between the solutions. In order to do so, we define the following group action:

Definition 4.6. *Let (K, ∂) be a differential field and $L(d) \in K[d]$ be a linear differential operator. Let $\bar{K} = K\langle \alpha_1, ..., \alpha_n \rangle$ be a Picard-Vessiot extension for $L(d)$ with its basis of solutions. Consider the ring $K\{X_1, ..., X_n\}$ of differential polynomials. We define the group action of $\mathbb{GL}_n(C_K)$ over the differential polynomials as*

$$\rho : \mathbb{GL}_n(C_K) \times K\{X_1, ..., X_n\} \longrightarrow K\{X_1, ..., X_n\}, \qquad \rho((\lambda_{rs}), \partial^j X_i) = \sum_k \lambda_{kj} \partial^j X_k$$

This action is well defined and it can be seen as the action of $\mathrm{Aut}_{C_K} \ker L$ over the polynomials once its basis has been fixed.

That the action is well defined is easily seen. In fact, much more than that, since for every $\Lambda = (\lambda_{rs}) \in \mathbb{GL}_n(C_K)$, the induced map $\rho_\Lambda(p) = \rho(\Lambda, p)$ is in fact a ring homomorphism. Since the monomials $\Pi_{i,j}(\partial^i X_j)^{m_{i,j}}$ are generators for $K\{X_1, ..., X_n\}$ as a K-algebra, the action is defined so that $\rho_\lambda(\Pi_{i,j}(\partial^i X_j)^{m_{i,j}}) = \Pi_{i,j}(\sum_k \lambda_{kj} \partial^i X_k)^{m_{i,j}}$.

With these definitions, and with the same idea that worked for algebraic equations in the first chapter of this work, we are going to define the Galois group of a differential linear equation as:

Definition 4.7. *Let (K, ∂) be a differential field, $L(d) \in K[d]$ a linear differential equation, $\bar{K} = K\langle \alpha_1, ..., \alpha_n \rangle$ a Picard-Vessiot extension for $L(d)$ generated by a basis of solutions. Let $\psi_\alpha : K\{X_1, ..., X_n\} \longrightarrow \bar{K}$ be the evaluation map defined as $\psi_\alpha(p\{X_1, ..., X_n\}) = p\{\alpha_1, ..., \alpha_n\}$. Let $\rho : \mathbb{GL}_n(C_K) \times K\{X_1, ..., X_n\} \longrightarrow K\{X_1, ..., X_n\}$ be the group action defined above. Then, we define the Galois group of $L(d)$ over K as*

$$\mathrm{Gal}_K L = \mathrm{Stab}_\rho \ker_K \psi_\alpha$$

This is the definition we have been working towards during all this work. It naturally captures the symmetries of the space of solutions by considering the group of morphisms that preserve them.

We now turn to see that it is in fact well defined. The only thing that we have to check is that there are no arbitrary choices involved. We can see that in the previous definition we did make an arbitrary choice, that is, we fixed a basis for the vector space of solutions. In order to prove that different choices of basis give the same Galois group, we begin by the following observation:

Observation 4.8. Let (K, ∂) be a differential field with algebraically closed field of constants, $L(d) \in K[d]$ be a differential operator and let $\bar{K} \supseteq K$ be a Picard-Vessiot extension for L over K. Let $\{\alpha_1, ..., \alpha_n\}, \{\beta_1, ..., \beta_n\} \supseteq \ker_K L$ be basis for the vector space of solutions, with their respective evaluation morphisms $\psi_\alpha, \psi_\beta : K\{X_1, ..., X_n\} \longrightarrow \bar{K}$. What is the relation between $\ker_K \psi_\alpha$ and $\ker_K \psi_\beta$? First of all, notice that we can consider the change of basis matrix $\Lambda = (\lambda_{ij}) \in \mathbb{GL}_n(C_K)$ as $\alpha_i = \sum_j \lambda_{ij}\beta_j$. Now, if $p\{X_1, ..., X_n\} \in \ker_K \psi_\alpha$, we have that $\psi_\alpha(p\{X_1, ..., X_n\}) = p\{\alpha_1, ..., \alpha_n\} = 0$. But, using the change of basis matrix, we can write $p\{\alpha_1, ..., \alpha_n\} = p\{\sum_k \lambda_{1k}\beta_k, ..., \sum_k \lambda_{nk}\beta_k\} = \psi_\beta \circ \rho(\Lambda, p) = 0$.

Remember that given the group action ρ, an element $\Lambda \in \mathbb{GL}_n(C_K)$ and a subset $S \subseteq K\{X_1, ..., X_n\}$, we can consider the set $\Lambda S = \{\rho(\Lambda, p) : p \in S\}$. Thus, we can see that

$$\Lambda \ker_K \psi_\alpha = \{\rho(\Lambda, p) : p \in \ker_K \psi_\alpha\} \subseteq \ker_K \psi_\beta$$

Using a similar argument and taking into account that the reciprocal change of basis matrix from α to β is just the inverse matrix Λ^{-1}, we can see that

$$(\Lambda^{-1}) \ker_K \psi_\beta \subseteq \ker_K \psi_\alpha$$

Therefore, since $\Lambda^{-1}\Lambda \ker_K \psi_\alpha = \ker_K \psi_\alpha$ and since group actions respect inclusions, we have the following chain of inclusions:

$$\ker_K \psi_\beta = \Lambda(\Lambda^{-1} \ker_K \psi_\beta) \subseteq \Lambda \ker_K \psi_\alpha \subseteq \ker_K \psi_\beta$$

Allowing us to conclude that $\Lambda \ker_K \psi_\alpha = \ker_K \psi_\beta$. Thus, we can easily prove the result we were looking for.

Corollary 4.9. *Let (K, ∂), $L(d) \in K[d]$ be as before and let $\bar{K} \subseteq K$ be a Picard-Vessiot extension for $L(d)$ over K. Let $\ker_K L$ be the C_K-vectror space of solutions of $L(d) = 0$ in $\bar{K}$ and let $\{\alpha_1, ..., \alpha_n\}, \{\beta_1, ..., \beta_n\} \subseteq \ker_K L$ be two basis for it. Then, with the evaluation morphisms $\psi_\alpha, \psi_\beta : K\{X_1, ..., X_n\} \longrightarrow \bar{K}$ defined accordingly, we have that* $\mathrm{Stab}_\rho \ker_K \psi_\alpha \cong \mathrm{Stab}_\rho \ker_K \psi_\beta$

Proof. Let $\Lambda = (\lambda_{ij}) \in \mathbb{GL}_n(C_K)$ be the change of basis matrix so that $\alpha_i = \sum_j \lambda_{ij}\beta_j$. Then, by the previous observation, we know that $\ker_K \psi_\beta = \Lambda \ker_K \psi_\alpha$. But by the properties of group actions and stabilizers reviewed in Section 1 we know that $\mathrm{Stab}_\rho \ker_K \psi_\beta = \mathrm{Stab}_\rho(\Lambda \ker_K \psi_\alpha) = \Lambda(\mathrm{Stab}_\rho \ker_K \psi_\alpha)\Lambda^{-1} \cong \mathrm{Stab}_\rho \ker_K \psi_\alpha$, since conjugate subgroups are isomorphic. □

Another important fact about the differential Galois group is that it is a linear algebraic group. The theory of algebraic groups is briefly developed in the appendix to this work.

Proposition 4.10. *With the previous notation, if $L(d) \in K[d]$ is a linear operator over a differential field with algebraically closed constants, then* $\mathrm{Gal}_K L$ *is a closed subgroup of* $\mathbb{GL}_n(C_K)$ *under the Zariski Topology of the affine space* K^{n^2+1}.

Proof. According to the theory of affine varieties developed in the appendix, we have to see that there exists a finite set of polynomials $f_1, ..., f_m \in K[X_{11}, ..., X_{nn}]$ so that $\mathrm{Gal}_K L = \{(\lambda_{11}, ..., \lambda_{nn}) \in \mathbb{GL}_n(C_K) : f_i(\lambda_{11}, ..., \lambda_{nn}) = 0,\ i = 1, ..., m\}$. In order to find them, let's consider a basis $\{\alpha_1, ..., \alpha\}$ for $\ker_K L \subseteq \bar{K}$, where $\bar{K}$ is a Picard-Vessiot extension for L over K. Then, if $\psi_\alpha : K\{X_1, ..., X_n\} \longrightarrow \bar{K}$ is the evaluation morphism defined above, we can consider $\ker_K \psi_\alpha$. This is an ideal of the ring of polynomials in n^2 indeterminates $K\{X_1, ..., X_n\}$ and by the Hilbert basis theorem (see appendix), there exist a finite number of polynomials so that $\ker_n \psi_\alpha = \langle f_1(X_{11}, ..., X_{nn}), ..., f_m(X_{11}, ..., X_{nn})\rangle$. Now, for each one of those, if $\Lambda = (\lambda_{ij}) \in \mathrm{Gal}_K L$, we know that $\psi_\alpha(\rho(\Lambda, f_i)) = 0$. Therefore, expanding it out, we can write that $f_l(\sum_k \lambda_{jk}\partial^i\alpha_k) = \sum_r f_r^{(l)}(\lambda_{11}, ..., \lambda_{nn})\psi_\alpha g_r\{X_1, ..., X_n\} = 0$, where $f_r^{(l)}(\lambda_{11}, ..., \lambda_{nn})$ are the coefficients for the polynomial $f_l(\sum_k \lambda_{jk}\partial^i\alpha_k)$ when expanded and written in terms of a finite set of differential polynomials $g_r\{X_1, ..., X_n\}$ not depending on the λ_{ij}. Since each one of those coefficients has to be identically zero for the whole polynomial to be zero, we then have that

$$f_r^{(l)}(\lambda_{11}, ..., \lambda_{nn}) = 0,\ r = 1, ..., r_l,\ l = 1, ..., m$$

is a finite set of polynomials that is zero when evaluated on the elements of the matrix Λ, for every such matrix in the Galois group. Conversely, it is a rather long but easy calculation to see that if $\Lambda = (\lambda_{ij}) \in \mathbb{GL}_n(C_K)$ satisfies $f_r^{(l)}(\lambda_{11}, ..., \lambda_{nn}) = 0$ for every r, l, then $f_l(\sum_k \lambda_{jk}\partial^i\alpha_k) = 0$ for every f_l generating $\ker_K \psi_\alpha$, and therefore by definition $\Lambda \in \mathrm{Gal}_K L$. □

Having seen that the Galois group is a well-defined object and that it has by construction the properties that we expect it to have, we can now prove that this definition coincides with the usual definition of the differential Galois group. We begin by giving this usual definition:

Definition 4.11. *Let (K, ∂) be a differential field with an algebraically closed field of constants. Let $L(d) \in K[d]$ be a linear differential operator and let $\bar{K} \supseteq K$ be a Picard-Vessiot extension for L over K. Then, the differential Galois group of $L(d)$ over K is defined to be the group of differential K-automorphisms of the field $\bar{K}$, that is,* $\mathrm{Aut}_K\bar{K}$.

First of all, we can see that $\mathrm{Aut}_K\bar{K}$ can be embedded in the general linear group $\mathbb{GL}_n(C_K)$, where n is the order of the differential operator $L(d)$.

Proposition 4.12. *Let (K, ∂), $L(d) \in K[d]$, $\bar{K}$ be as above and let $\mathrm{Aut}_K\bar{K}$ be its differential Galois group. Then, there exists an injective group homomorphism $\mathrm{Aut}_K\bar{K} \hookrightarrow \mathbb{GL}_n(C_K)$*

Proof. Let $\alpha_1, ..., \alpha_n \in \bar{K}$ be a basis for $\ker_{\bar{K}} L$. Then, $\bar{K} = K\langle\alpha_1, ..., \alpha_n\rangle$ and if $\varphi \in \mathrm{Aut}_K\bar{K}$, then it is completely determined by the images $\varphi(\alpha_i)$ for $i = 1, ..., n$. Since $\varphi(\alpha_i) \in \ker_{\bar{K}} L$, we can write it in terms of the basis $\alpha_1, ..., \alpha_n$ and so for every $\varphi \in \mathrm{Aut}_K\bar{K}$ we have a set of n^2 constants $\lambda_{ij}(\varphi) \in C_K$, $i, j = 1, ..., n$, so that $\varphi(\alpha_i) = \lambda_{i1}(\varphi)\alpha_1 + ... + \lambda_{in}(\varphi)\alpha_n$.

Then, we define the map $\Phi_\alpha : \mathrm{Aut}_K\bar{K} \longrightarrow \mathbb{GL}_n(C_K)$ as $\Phi_\alpha(\varphi) = (\lambda_{ij}(\varphi))_{i,j=1,...,n} \in \mathbb{GL}_n(C_K)$. It is a group homomorphism, since the image of the identity map is the identity matrix and the image of the composition of K-automotphisms is the product of their matrices. Indeed, if $\Phi_\alpha(\varphi) = (\lambda_{ij})$, $\Phi_\alpha(\psi) = (\mu_{ij})$, we have that $\varphi \circ \psi(\alpha_i) = \varphi(\sum_j \mu_{ij}\alpha_j) = \sum_j \mu_{ij}\varphi(\alpha_j) = \sum_k(\sum_j \mu_{ij}\lambda_{jk})\alpha_k$ and therefore $\Phi_\alpha(\varphi \circ \psi) = (\sum_j \mu_{ij}\lambda_{jk})_{i,k=1,...,n} \in$

$\mathbb{GL}_n(C_K)$. In particular, the image of the inverse of a K-automorphism is the inverse matrix. Finally, Φ_α is obviously injective.

□

We are going to use this result to prove the conclusion that we were very much looking forward to.

Theorem 4.13. *Let (K,∂), $L(d) \in K[d]$, $\bar{K} \supseteq K$ be as before, $\alpha_1, ..., \alpha_n \in \bar{K}$ be a basis for the vector space of solutions of $L(d) = 0$ and $\mathrm{Stab}_\rho \ker \psi_\alpha$, $\mathrm{Aut}_K \bar{K}$ be defined as above. Then, $\mathrm{Stab}_\rho \ker \psi_\alpha \cong \mathrm{Aut}_K \bar{K}$.*

Proof. Using our previous result, what we are going to prove is that given a basis $\alpha_1, ..., \alpha_n \in \bar{K}$ for the C_K-vector space of solutions of $L(d)$, the groups $\mathrm{Im}\Phi_\alpha$ and $\mathrm{Stab}_\rho \ker_K \psi_\alpha$ are in fact equal. Then, being Φ_α injective, we are going to have the desired isomorphism $\mathrm{Aut}_K \bar{K} \cong \mathrm{Stab}_\rho \ker_K \psi_\alpha$.

Let then $\Lambda = (\lambda_{ij}) \in \Phi_\alpha(\mathrm{Aut}_K \bar{K}) \subseteq \mathbb{GL}_n(C_K)$ and let $\varphi \in \mathrm{Aut}_K \bar{K}$ be its preimage. Then, if $p\{X_1, ..., X_n\} \in \ker_K \psi_\alpha$, we clearly have that $\psi_\alpha \circ \rho(\Lambda, p) = p\{\varphi(\alpha_1), ..., \varphi(\alpha_n)\} = \varphi \circ \psi_\alpha(p\{X_1, ..., X_n\}) = 0$, being φ a K-differential automorphism. Therefore, $\Lambda \in \mathrm{Stab}_\rho \ker_K \psi_\alpha$.

In order to prove that $\mathrm{Stab}_\rho \ker_K \psi_\alpha \subseteq \mathrm{Im}\Phi_\alpha(\mathrm{Aut}_K \bar{K})$, let $\Lambda = (\lambda_{ij}) \in \mathrm{Stab}_\rho \ker_K \psi_\alpha$ and let's define a differential K-automorphism of $\bar{K}$ that has Λ as its image under Φ_α. Consider the map $\psi = \psi_\alpha \circ \Lambda : K\{X_1, ..., X_n\} \longrightarrow \bar{K}$, which is a differential ring homomorphism. Then, since $\ker \psi_\alpha \subseteq \ker(\psi_\alpha \circ \Lambda)$, being $\Lambda \in \mathrm{Stab}_\rho \ker \psi_\alpha$, we can define it in the quotient ring $K\{X_1, ..., X_n\}/\ker \psi_\alpha$ and therefore, we can get a differential field K-isomorphism $\tilde{\psi} : \mathcal{Q}(K\{X_1, ..., X_n\}) \longrightarrow \mathrm{Im}\tilde{\psi} \subseteq \bar{K}$. But by corollary 4.5, we have a differential K-isomorphism $\bar{K} \cong \mathcal{Q}(K\{X_1, ..., X_n\}/\ker \psi_\alpha)$. Combining this two, we have a differential K-isomorphism $\varphi : \bar{K} \cong \mathcal{Q}(K\{X_1, ..., X_n\}/\ker \psi_\alpha) \cong \mathrm{Im}\tilde{\psi}$.

We only have to see that $\mathrm{Im}\tilde{\psi} = \bar{K}$, since its injectivity is given by the fact that it is a field homomorphism. Morover, it is surjective since $\mathrm{Im}(\tilde{\psi})$ contains a full set of solutions for $L(d)$ and $\bar{K}$ is a minimal differential field with this property. Therefore, $\varphi : \bar{K} \longrightarrow \bar{K}$ is a differential K-automorphism. Also, by construction of $\tilde{\psi}$ and of the isomorphism of corollary 4.5, it is clear that $\Phi_\alpha(\varphi) = \Lambda$, finishing our proof.

□

4.3 Some examples

Before finishing this section, let us comment on some basic examples for the Galois group of a differential equation. First of all, we can consider the simplest examples of a linear differential equation, already commented. During this section, let (K, ∂) be a differential field with an algebraically closed field of fractions.

Example 4.14. Let's consider the differential operator $L(d) = d - \lambda \in K[d]$, with $\lambda \neq 0$. Let $\bar{K} = K\langle\alpha\rangle \supseteq K$ be a Picard-Vessiot extension for it. This corresponds to the adjunction of an exponential, since $L(\alpha) = \partial(\alpha) - \lambda\alpha = 0$. Then, we can consider its Galois group $\mathrm{Gal}_K L$, which is going to be a closed subgroup of $\mathbb{GL}_1(C_K) \cong C_K^*$, the multiplicative group of C_K. This particular subgroup will be determined by the differential relationships between the solution α an the field K.

Since for every $p\{X\} \in K\{X\}$, $\psi_\alpha(p\{X\}) \in K[\alpha]$, we only have to study whether there are any polynomials in $K[X]$ which evaluate to zero at α. We will not enter into too much detail, but if there are no such polynomials (i.e, if α is trascendental over K), then $\ker \psi_\alpha$ consists only of homogeneous polynomials in $K\{X\}$, and clearly for every $\mu \in C_K^*$, $p\{\mu X\} = \mu^k p\{X\}$ for some $k >$ and therefore $\psi_\alpha \circ \rho(\mu, p\{X\}) = 0$. Then, $\mathrm{Gal}_K L = C_K^*$.

Otherwise, if α is not trascendental over K, then we can consider the minimal polynomial of α over K, $\mathrm{Irr}_K\alpha(X) \in K\{X\}$. It clearly belongs to $\ker \psi_\alpha$. As is shown in [5] (pp. 22), by seeing that the derivative of $\mathrm{Irr}_K\alpha(X)$ evaluated at α divides $\mathrm{Irr}_K\alpha(X)$, we get that $\alpha^k \in K$ for some $k > 0$. Therefore, since if $\mu \in \mathrm{Gal}_K L$, then in particular $\psi_\alpha \circ \rho(\mu, X^k - c) = \mu^k \alpha^k - c = 0$, then $\mu^k = 1$ and it has to be a k-th root of unity in C_K^*. Therefore, $\mathrm{Gal}_K L \cong C_K$ is a finite cyclic subgroup of C_K^*.

Example 4.15. The next simple equation corresponds to the inhomogeneous first-order linear equation, $L(d) = d \in K[d]$, which we want to be solved when $L(\alpha) = a \in K$. As we saw in the begining of this chapter, we can turn this inhomogeneous problem into an homogeneous one by defining $L_a(d) = d^2 - a^{-1}\partial(a)d$. We then can consider a Picard-Vessiot extension for it $\bar{K} = K\langle 1, \alpha \rangle$, where α is a solution for the inhomogeneous equation. Then, its Galois group $\mathrm{Gal}_K(L_a)$ is going to be a subgroup of $\mathbb{GL}_2(C_K)$. As we saw in example 4.1, if $\Lambda = (\lambda_{ij}) \in \mathbb{GL}_2(C_K)$, then it is of the form:

$$\Lambda \in \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in \mathbb{GL}_2(C_K) : \, c \in C_K \right\} \cong C^+$$

Which is clearly an element of the additive subgroup of C_K. Since we can easily see that for every $c \in C_K$, the element $\Lambda_c \in \mathbb{GL}_2(C_K)$ given by $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ gives the differential K-auromorphism defined by $\varphi_c(\alpha) = \alpha + c$, which is clearly an element of the Galois group. Therefore, $\mathrm{Gal}_K L \cong C^+$.

Example 4.16. Finally, let's consider an example of order two. Let (K, ∂) be a differential field with an algebraically closed field of constants and consider the differential operator $L(d) = d^2 + 1$. In the field of real rational functions, we recognize it as the operator having the trigonometric functions sin and cos as solutions. In the field K, however, being C_K algebraically closed, we know that -1 is a square. That is, $-1 = \lambda^2$ for some $\lambda \in C_K$.

In that case, we can give the following two non equivalent factorizations $L(d) = L_-(d)L_+(d)$ and $L(d) = L_+(d)L_-(d)$, where $L_-(d) = d - \lambda$ and $L_+(d) = d + \lambda$. If $\bar{K} = K\langle \alpha, \beta \rangle$ is a Picard-Vessiot extension for $L(d)$ over K, we can chose them so that $L_+(\alpha) = 0$ and $L_-(\beta) = 0$. We can see that they are linearly independent over C_K, because if $\alpha + \mu\beta = 0$ with some nonzero $\mu \in C_K$, then differenciating we get $-\lambda\alpha + \mu\lambda\beta = 0$, and combining it with $\lambda\alpha + \mu\lambda\beta = 0$ we would end up with $\alpha, \beta = 0$. (We can also consider an alternative argument, where $K_1 = K\langle \alpha \rangle$ is a Picard-Vessiot extension for $L_+(d)$ and $K_2 = K\langle \beta \rangle$ is a Picard-Vessiot extension for $L_-(d)$. Then, we can see that $K_1, K_2 \subseteq \bar{K}$)

To calculate it differential Galois group, which is going to be a subgroup of $\mathbb{GL}_2(C_K)$, we can see that since the relations $\partial(\alpha) = -\lambda\alpha$ and $\partial(\beta) = \lambda\beta$ have to be preserved, then:

$$\mathrm{Gal}_K L \subseteq \left\{ \begin{pmatrix} \mu & 0 \\ 0 & \nu \end{pmatrix} \in \mathbb{GL}_2(C_K) : \, \mu, \nu \neq 0 \right\} \cong C^* \times C^*$$

We can then determine $\mathrm{Gal}_K L$ by using our previous considerations about the Galois group of the operators $L_+(d)$ and $L_-(d)$.

5 Liouville Extensions and Elementary Functions

In this section, and with the only intention to give some extra completeness to this work and to indicate some of the ways in which this theory can be useful, we will present some concepts that derive from those already developed. Those are the notion of a Liouville extension and its relationship with closed-form formulas and the idea of integration and elementary functions. We are going to expose and develop the results concerning those two ideas. However, we will not prove the results involved in this part of the work and refer the reader to appropriate references.

5.1 Liouville Extensions

In this section, we are going to study the most immediate analogue to solvable extensions in the case of a polynomial equation. Remember that, as was seen during the undergraduate course in Galois theory, a solvable equation was defined as follows:

Definition 5.1. *Let K be a field and $p(X) \in K[X]$ of degree n. Let $\bar{K} = K(\alpha_1, ..., \alpha_n)$ be a splitting field for $p(X)$. Then, we will say that $p(X)$ is a solvable by radicals equation if there exists a field $\tilde{K} \supseteq \bar{K}$, a chain of intermediate subfields $K_0 = K \subseteq K_1 \subseteq ... \subseteq K_m = \tilde{K}$, elements $\beta_1, ..., \beta_m \in \tilde{K}$ and strictly positive integers $n_1, ..., n_m > 0$ so that:*

(i) $K_i = K_{i-1}(\beta_i)$ *and therefore* $\tilde{K} = K(\beta_1, ..., \beta_m)$.

(ii) $\beta_i^{n_i} \in K_{i-1}$. *That is,* β_i *is obtained extracting a radical from* K_{i-1}.

We can clearly see that this definition encapsulates the notion of expressing the root of a polynomial in terms of the basic algebraic operations, $+, -, \cdot, \div, \sqrt[n]{\cdot}$. Indeed, if a polynomial is solvable by radicals, then its roots can be expressed doing a finite number of algebraic operations with elements of the base field K. Then, there is the important result of Galois:

Theorem 5.2. *Let K be a field of characteristic zero and $p(X) \in K[X]$. Then, $p(X)$ is solvable by radicals if and only if $\mathrm{Gal}_K p(X)$ is a solvable group.*

This alone should justify the approach of Galois theory to the study of polynomial equations. That's why it seems natural to look for a similar result in the theory of linear differential equations. And indeed, that's precisely the result we are studying in this section. First of all, we should address the question of what is the differential analogue of extracting a root? Since, in the previous section, we saw that linear differential equations of order one give either exponentials (homogeneous case) or primitives (nonhomogeneous case), it is natural to think of those as the basic field extensions of differential algebra. Then, having seen that the differential analogues of a root extraction are primitives and exponentials of primitives, we can define a similar type of differential field extensions to the solvable ones in polynomial equations. First of all, we give the definition of an element expressible by quadratures:

Definition 5.3. *Let (K, ∂) be a differential field and $\bar{K} \supseteq K$ be a differential field extension. An element $\alpha \in \bar{K}$ is expressible by quadratures over K if there exists a chain of differential subfields $K = K_0 \subseteq K_1 \subseteq ... \subseteq K_n$ so that $\alpha \in K_n$ and there exist $\alpha_1, ...\alpha_n \in K_n$ so that $K_i = K_{i-1}\langle\alpha_i\rangle$ and α_i is either an algebraic element, a primitive or the exponential of a primitive over K_{i-1}.*

This definition can be followed by the more general definition of a Liouville extension:

Definition 5.4. *Let (K, ∂) be a differential field and $\bar{K} \supseteq K$ be a differential extension. We are going to say that $\bar{K}$ is a Liouville extension if there exist intermediate fields $K_0 = K \subseteq K_1 \subseteq ... \subseteq K_n = \bar{K}$ and elements $\alpha_1, ..., \alpha_n \in \bar{K}$ so that $K_{i+1} = K_i\langle\alpha_i\rangle$ and either $\partial(\alpha_i) \in K_i$, or $\partial(\alpha_i)/\alpha_i \in K_i$, or α_i is algebraic over K_i.*

We can easily see the following corollary:

Corollary 5.5. *If $\bar{K} \supseteq K$ is a Liouville extension and $\alpha \in \bar{K}$, then α is expressible by quadratures over K.*

Thus, the concept of a Liouville extension and of an element expressible in quadratures are analogous concepts to a radical extension and an element expressible by radicals in the theory of polynomial equations. We could, however, consider another kind of analogous ideas, and indeed we are going to do so in the next section.

We would very much want to find a characterization of this new notion of solvability in terms of the Galois group of the differential equation. And indeed, that's the case. The differential counterpart of Galois' theorem relating the solvability of a differential equation with its Galois group is the following:

Theorem 5.6. *Let (K, ∂) be a differential field with algebraically closed field of constants, $L(d) \in K[d]$ a differential operator and $\bar{K}$ a Picard-Vessiot extension for $L(d)$. Then, $L(d)$ is solvable in closed form if and only if its differential Galois group,* $\mathrm{Gal}_K L$ *is so that its identity component,* $(\mathrm{Gal}_K L)^0$*, is a solvable group (as an algebraic group).*

Observation 5.7. We can see that in contrast to polynomial Galois theory, here what is required to be solvable is the identity component of the differential Galois group. As can be seen in [11] (pp. 98), there is a stronger notion of representability by quadratures which excludes the possibility of extracting roots. In this context, the notion of quadrature that we have defined above is usually referred to as "solvable by generalized quadratures". Then, if we define an element as representable in quadratures if it can be expressed using only primitives and exponentials of primitives, then the above result would indeed relate this representability with the solvability of the whole differential Galois group, not only of its identity component.

We will not go deeper into these results in this work. Let us, however, comment on some examples. Appropriate bibliography will be referenced in each case.

Example 5.8. Let $\mathbb{C}$ be the field of complex numbers and consider the differential field of rational functions $(\mathbb{C}(X), \partial)$, where ∂ is the trivial derivation in $\mathbb{C}$ extended to $\mathbb{C}(X)$ as $\partial(X) = 1$. We can consider the Airy equation in $\mathbb{C}(X)$, given by the differential operator $L_A(d) = d^2 - X \in \mathbb{C}(X)[d]$. We can then consider $\mathbb{C}(X)\langle\alpha, \beta\rangle \supseteq \mathbb{C}(X)$ a Picard-Vessiot extension for $L_A(d)$, where α, β are two $\mathbb{C}$-linearly independent solutions. Following the development as in A. Magid [13] (pp. 56), J. Hubbard [8] (pp. 16), we can see that the differential Galois group of the Airy operator is $\mathrm{Gal}_{\mathbb{C}(X)} L_A = \mathbb{SL}_2(\mathbb{C})$. Further, those references show that the connected component of this Galois group is the whole group and that it is not a solvable group. Therefore, by our previous results, the solutions to the Airy equation are not representable by quadratures over the field of complex rational functions.

The second example can be found in [10] (pp. 417).

Example 5.9. Let again $(\mathbb{C}(X), \partial)$ be the differential field of rational complex functions and consider the Bessel operator $L_\nu = d^2 + \frac{1}{X}d + (1 - \frac{\nu^2}{X^2})$, where $\nu \in \mathbb{C}$. Following the calculations in [10], one can see that for the case where $\nu - \frac{1}{2} \notin \mathbb{Z}$, then $\mathrm{Gal}_{\mathbb{C}(X)} L_\nu = \mathbb{SL}_2(\mathbb{C})$ which by the previous example is not solvable and neither is its identity component. Then, the solutions to the Bessel differential equation are not expressible by quadratures over the field of rational functions with complex coefficients when 2ν is not an integer, as is well known in physics.

5.2 Integration in Terms of Elementary Functions

To finish our work, let us give another application of the differential Galois theory. Continuing with our interest in what kind of relation do the solutions of an equation have with respect to the coefficients of the equation, we are going to introduce the idea of elementary functions. For the following definitions, we are going to follow the text of J. Murphy, [15] (pp. 13).

Definition 5.10. *Let (K, ∂) be a differential field and $\bar{K} \supseteq K$ a differential field extension. Let $\alpha \in \bar{K}$. Then, it is elementary over K one of the following holds:*

(i) α is algebraic over K.

(ii) α is a logarithm over K. That is, there exists $\beta \in K$ nonzero so that $\partial(\alpha) = \frac{\partial(\beta)}{\beta}$.

(iii) α is an exponential over K. That is, there exists $\beta \in K$ nonzero so that $\frac{\partial(\alpha)}{\alpha} = \partial(\beta)$.

This is not enough in order to introduce the idea of an elementary function. Over the field $\mathbb{C}(X)$ we would like our elementary functions to be the above elements together with compositions among them. According to the above definition, $\log X$ would be elementary over $\mathbb{C}(X)$ in some differential extension that contains it, but $\log\log(X)$ would not. Neither would X^X be elementary, since it can be written as $X^{X \log X}$ and it satisfies none of the above criteria. Then, it is clear that we have to take compositions into account in order to have a satisfactory notion of elementary functions. Then, we give the following definition:

Definition 5.11. *Let (K, ∂) be a differential field and $\bar{K} \supseteq K$ be a differential field extension. Then, $\bar{K}$ is a field of elementary functions over K if there exists a chain of differential field extensions $K_0 = 0 \subseteq K_1 \subseteq ... \subseteq K_n = \bar{K}$ and elements $\beta_1, ..., \beta_n \in \bar{K}$ so that $K_i = K_{i-1}\langle\beta_i\rangle$ and β_i is elementary over K_{i-1}.*

With this definition, previous examples such as $\log\log X$ or X^X are now elementary functions over $\mathbb{C}(X)$, since we can consider the chain $\mathbb{C}(X) \subseteq \mathbb{C}(X)\langle\alpha\rangle \subseteq \mathbb{C}(X)\langle\alpha, \beta\rangle$, where $\partial(\alpha) = \frac{1}{X}$ and $\partial(\beta) = \frac{\partial(\alpha)}{\alpha}$, giving $\beta = \log\log X$, where each α and β is a logarithm in the previous field.

We then arrive at the following necessity condition for a differential field extension to be elementary over a certain field. This result is due to A. Magid, and the corresponding proof can be found in [13] (pp. 82).

Theorem 5.12. *Let C be an algebraically closed field and consider the differential field $(C(X), \partial)$ of rational functions with trivial derivation in C and $\partial(X) = 1$. Let $L(d) \in K[d]$ be a linear differential operator and $\bar{C} \supseteq C(X)$ be a Picard-Vessiot extension for $L(d)$ over*

$C(X)$. If there exists a field of elementary functions E over $C(X)$ so that $C(X) \subseteq \bar{C} \subseteq E$, then the identity component of $\mathrm{Gal}_{C(X)}L$ *is an abelian group.*

For the sake of completeness, we are going to borrow the following argument from A. Magid [13](pp. 82) to give an example of the case where the solution to a differential equation is not expressible in terms of elementary functions.

Example 5.13. Let $(\mathbb{C}(X), \partial)$ be the field of rational functions with complex coeficients as defined before. Then, if in some extension $\tilde{\mathbb{C}}$ of $\mathbb{C}(X)$ there's an element $\alpha \in \tilde{\mathbb{C}}$ so that $\partial(\alpha) = \exp(-X^2)$ (i.e., $\alpha = \int e^{-x^2}$), then α is not contained in an elementary field of functions over $\mathbb{C}(X)$. Therefore, there is no combination of logarithms, exponentials, algebraic elements and arithmetic operations we can do in $C(X)$ in order to get an expression for α.

A proof for this can be found in A. Magid [13] (pp. 81, 82) , and rests upon the fact that we can consider the linear differential operator $L(d) = d^2 + 2x \in \mathbb{C}(X)[d]$. Then, we can consider a Picard-Vessiot extension $\tilde{\mathbb{C}} \subseteq \mathbb{C}(X)$ for it so that $\tilde{\mathbb{C}} = \mathbb{C}(X)\langle 1, \alpha \rangle$, where α is a primitive of $\exp(-X^2)$. Then, the argument follows until it is shown that $\mathrm{Gal}_{\mathbb{C}(X)}(L) \cong \mathbb{GL}_2(\mathbb{C})^+ \rtimes \mathbb{GL}_2(\mathbb{C})^*$ and that its identity component is not an abelian group. Hence, by the above theorem, there's no field of elementary functions containing both 1 and α, and since 1 is cleary elementary, α is not an elementary function over $\mathbb{C}(X)$.

6 Conclusions

During the course of this work, we have introduced another way of thinking about the known topic of Galois theory. We have also seen how this slightly different approach also works for the Galois theory of differential equations. In doing so, we have developed the advanced machinery of differential algebra and exposed it in the clearest way possible. And finally, we have given some hints of what is all of this useful for.

Overall, I think that this project works in various ways. Firstly, the narrative (or the guiding plot) of the work has worked out pretty well. The brief but complete first section about algebraic equations contains most of the ideas that have been, later on, developed in great length in the context of differential algebra. Therefore, this structure has been useful to highlight the great analogy existent between those two parts of the work. Moreover, the somewhat original parts of the work, which include both definitions of the Galois group (algebraic and differential) as well as the results that follow from them, are in a way parallels too. This further manifests the success of these ideas, in that they can be extended without much modification to the differential case.

Secondly, with respect to the contents of the work themselves, I consider it a great thing that those original ideas (or faintly original, without the intention of overemphasizing it) have worked out well. Indeed, as was said during the introduction, I was not at all sure that this investigation was going to allow me to carry out my own ideas. Therefore having established that those ideas, although insightful but not necessarily useful, are indeed correct, and having proved some results from them, is in my opinion a greater success than I was expecting.

Finally, with respect to the theory studied in order to progress with the work, I have found it a highly satisfying theory in mathematics. Algebraic Galois theory is beautiful for its complete solution to an interesting mathematical problem. Therefore, seeing that its ideas can also be extended to the field of linear differential equations greatly enhances the beauty of the original theory too. Besides, I have found the study of concepts usually within the field of analysis through the lens of algebra a very interesting instance of what can be done by combining the ideas we have gathered during our undergraduate studies.

A Affine Varieties and Algebraic Groups

In this section, we are going to study some basic notions of affine varieties and algebraic geometry. Let's begin by defining:

Definition A.1. *Let K be a field. Define the affine n dimensional space over K as $K^n = K \times ... \times K$. Consider also the set of multivariate polynomials over K, $K[X_1, ..., X_n]$. An affine variety in K^n is a subset $A \subseteq K^n$ so that there exist a finite subset $\{p_1, ..., p_m\} \subseteq K[X_1, ..., X_n]$ that is zero precisely on the set of points of A. That is, $A = \{a \in K^n : p_i(a) = 0, \forall i_1, ..., m\}$.*

Here, we must recall the great result by Hilbert:

Theorem A.2. *Let K be a field. Then, every ideal of $K[X_1, ..., X_n]$ is finitely generated.*

Then, with this result, we have that for every ideal $I \subseteq K[X_1, ..., X_n]$ we can consider the affine variety $\mathcal{V}(I)$ defined as the set of zeroes of a finite set of generators of I. This affine variety is well defined and is independent of the choice of generators.

Definition A.3. *Let K be a field. Then, $\mathcal{I}(K[X_1, ..., X_n])$ denotes the set of ideals of $K[X_1, ..., X_n]$ and $\mathcal{V}(K^n)$ denotes the set of affine varieties of K^n.*

An important fact is the following one:

Proposition A.4. *Let K be a field, K^n its affine n-space. Then*

(i) $\emptyset, K^n \in \mathcal{V}(K^n)$.

(ii) If $A, B \in \mathcal{V}(K^n)$, then $A \cup B \in \mathcal{V}(K^n)$.

(iii) If $\{A_i\}_i \subseteq \mathcal{V}(K^n)$ is an arbitrary indexed subset of $\mathcal{V}(K^n)$, then $\cap_i A_i \in \mathcal{V}(K^n)$.

Thus, $\mathcal{V}(K^n)$ are the closed sets of a topology for K^n, called the Zariski topology.

The proof is straightforward and is based upon the following mappings between the sets of ideals of $K[X_1, ..., X_n]$ and the set of varieties of K^n.

Lemma A.5. *With this definition, we can define the map $\psi_{\mathcal{V}} : \mathcal{I}(K[X_1, ..., X_n]) \longrightarrow \mathcal{V}(K^n)$ associating to each ideal its affine variety. This map reverses inclusions, ie., if $I \subseteq J \in \mathcal{I}(K[X_1, ..., X_n])$, then $\psi_{\mathcal{V}}(J) \subseteq \psi_{\mathcal{V}}(I)$.*

This map is not injective, since for example $\psi_{\mathcal{V}}(\langle X \rangle) = \psi_{\mathcal{V}}(\langle X^2 \rangle)$. It is, however, exhaustive, since for every affine variety $X \in \mathcal{V}(K^n)$, there are some $f_1, ..., f_m \in K[X_1, ..., X_n]$ so that $\psi_{\mathcal{V}}(\langle f_1, ..., f_m \rangle) = X$. We are going to study this later.

In that same way, given a set $S \subseteq K^n$, we can consider the set of polynomials that are zero on S. That is, we can consider the set $\mathcal{I}(S) = \{p \in K[X_1, ..., X_n] : p(a) = 0, \forall a \in S\}$. It is clearly an ideal. Thus, we can also consider the following map $\psi_{\mathcal{I}} : \mathcal{V}(K^n) \longrightarrow \mathcal{I}(K[X_1, ..., X_n])$ that associates to every affine variety the ideal of polynomials that are zero on it. It also reverses inclusions in the same sense as $\psi_{\mathcal{V}}$. However, this map fails to be exhaustive, since if K is not algebraically closed, there are nontrivial ideals of $K[X_1, ..., X_n]$ that cannot be reached by $\psi_{\mathcal{I}}$. For the sake of simplicity, when the meaning is clear by the context, we are going to denote $\psi_{\mathcal{V}}(J) = \mathcal{V}(J)$ and $\psi_{\mathcal{I}}(X) = \mathcal{I}(X)$.

We would like $\psi_{\mathcal{I}}$ and $\psi_{\mathcal{V}}$ to be inverses of each other. This problem is solved by the theorem known as Hilbert's Nullstellensatz. Remember first that given a ring R and an ideal $I \subseteq R$, it's radical is given by $\sqrt{I} = \{a \in R : a^n \in I \, \text{for some} \, n \geq 0\}$. It is also an ideal. An ideal is called radical if it is equal to its radical.

Theorem A.6. *Let K be an algebraically closed field. Then:*

(i) If $M \subseteq K[X_1, ..., X_n]$ is a maximal ideal, then there exists $p = (p_1, ..., p_n) \in K^n$ so that $M = \langle X_1 - p_1, ..., X_n - p_n \rangle$.

(ii) If $I \subseteq K[X_1, ..., X_n]$ is a proper ideal, then $\mathcal{V}(I) \neq \emptyset$. That is, multivariate polynomial equations always have solution.

(iii) If $I \subseteq K[X_1, ..., X_n]$ is an ideal, then $\mathcal{I} \circ \mathcal{V}(I) = \sqrt{I}$

With this important result, we can see that $\psi_{\mathcal{I}}$ is exhaustive when K is algebraically closed and that $\psi_{\mathcal{V}}$ is injective when restricted to the set of radical ideals of $K[X_1, ..., X_n]$. Thus, we have seen that:

Corollary A.7. *Let K be an algebraically closed field. Then, there is a bijection ψ : $\sqrt{\mathcal{I}}(K[X_1, ..., X_n]) \longrightarrow \mathcal{V}(K^n)$.*

Indeed, the bijection is given by $\psi = \psi_{\mathcal{V}}$ and $\psi^{-1} = \psi_{\mathcal{I}}$. We can see from this result and from Hilbert's Nullstellensatz that through the bijective correspondence between radical ideals of $K[X_1, ..., X_n]$ and affine varieties of K^n, maximal ideals correspond to points in K^n and prime ideals correspond to irreducible closed sets of K^n under the Zariski topology.

Let's now define what are the maps between affine varieties that preserve their structure.

Definition A.8. *Let K be an algebraically closed field and $X \subseteq K^n$, $Y \subseteq K^m$ affine varieties. A map $\phi : X \longrightarrow Y$ is a morphism of affine varieties if there exist polynomials $p_1, ..., p_m \in K[X_1, ..., X_n]$ so that $\varphi(k_1, ..., k_n) = (p_1(k_1, ..., k_n), ..., p_m(k_1, ..., k_n)) \in Y$.*

As an example, we can see that:

Example A.9. Let K be an algebraically closed field and $X \subseteq Y \subseteq K^n$ be affine varieties. Then, the inclusion map $\phi : X \hookrightarrow Y$ given by $\phi(x_1, ..., x_n) = (x_1, ..., x_n)$ is a morphism of affine varieties.

Before proceeding with the next example, we are going to define the notion of the product of varieties.

Definition A.10. *Let K be an algebraically closed field and $X \subseteq K^n$, $Y \subseteq K^m$ affine varieties. Let $\mathcal{I}(X) = \langle p_1, ..., p_r \rangle \subseteq K[X_1, ..., X_n]$ and $\mathcal{I}(Y) = \langle q_1, ..., q_s \rangle \subseteq K[X_1, ..., X_m]$. If we now consider the ring $K[X_1, ..., X_n, Y_1, ..., Y_m]$, we can view the previous polynomial rings as subrings of this one, and so consider $p_1, ..., p_r, q_1, ..., q_s \in K[X_1, ..., X_n, Y_1, ..., Y_m]$. Then, we define the affine variety product of X and Y as $X \times Y = \mathcal{V}(\langle p_1, ..., p_r, q_1, ..., q_m \rangle)$.*

Example A.11. Let K be a field and $X \subseteq K^n$, $Y \subseteq K^m$ be affine varieties. The projection maps $\pi_X, \pi_Y : X \times Y \longrightarrow X, Y$ are morphisms of affine varieties.

We now have all the ingredients we need in order to define what a linear algebraic group over an affine space is.

Definition A.12. *Let K be an algebraically closed field and $G \subseteq K^n$ an affine variety that has also a group structure, i.e, a product $* : G \times G \longrightarrow G$, a neutral element $e \in G$ and an inverse function $\mathrm{i} : G \longrightarrow G$ satisfying the group axioms. Then, G is a linear algebraic group if the product $*$ and the inverse function i are morphisms of affine varieties (when considering $G \times G$ as the product variety) and if $e : G \longrightarrow G$ giving the neutral element is also a morphism of affine varieties.*

Example A.13. As an example, we can consider $\mathbb{C}$ and the complex affine n-space $\mathbb{C}^n$. Then, the set $A = \{(z, 0, ..., 0) \in \mathbb{C}^n : z \in \mathbb{C}\}$ is a linear algebraic group. In the first place, A is indeed an affine variety, since it is the variety defined as the set of zeroes of the polyniomials $p_2(X_1, ..., X_n) = X_2, ..., p_n(X_1, ..., X_n) = X_n$. Then, the map $\mathrm{i}(X_1, ..., X_n) = (-X_1, 0, ..., 0)$ and the map $e(X_1, ..., X_n) = (0, ..., 0)$ are morphisms of affine varieties corresponding to the additive operations of the group A. Further, the map $+(X_1, ..., X_n, Y_1, ..., Y_n) = (X_1 + Y_1, 0, ..., 0)$ is a morphism too. Therefore, $A \subseteq \mathbb{C}^n$ is a linear algebraic group.

We are now in the position to see how the group of invertible matrices over a given field is indeed an algebraic group, thus giving sense to its name: the general linear algebraic group. Let K be an algebraically closed field and let $\mathbb{GL}_n(K) \subseteq M_{n\times n}(K)$ be the group of invertible n by n square matrices with coefficients in K, together with matrix multiplication.

Observation A.14. Let K be a field and $\mathbb{GL}_n(K)$ the group of invertible square matrices over K of dimension n described above. Since we want to see it as an algebraic group, we first have to embed it in an affine space. The obvious impulse would be to see it as a subset of K^{n^2}. This, however, won't work, since we would have $\mathbb{GL}_n(K) = \{(\lambda_{11}, ..., \lambda_{nn}) \in K^{n^2} : \det(\lambda_{ij}) \neq 0\}$, but this is the complementary of the set $\{(\lambda_{11}, ..., \lambda_{nn}) \in K^{n^2} : \det(\lambda_{ij}) = 0\}$ which is a closed set in the Zariski topology, being the set of zeroes of a polynomial (the determinant). Then, $\mathbb{GL}_n(K)$ is not a closed set in K^{n^2} and therefore it is not an affine variety in K^{n^2}.

From this observation, we can see that our next guess is indeed the correct one.

Proposition A.15. *Let K be an algebraically closed field and let $\mathbb{GL}_n(K)$ be the group of invertible n by n matrices over K. Then, it is a linear algebraic group in the affine space K^{n^2+1}.*

Proof. In order to turn $\mathbb{GL}_n(K)$ into an affine variety of K^{n^2+1} we need it to be closed in the Zariski topology. That is, it has to be the set where some polynomials are zero. Since the defining property of an invertible matrix is that its determinant is nonzero, we can see that $\mathbb{GL}_n(K) = \{(\lambda_{11}, ..., \lambda_{nn}, \lambda) \in K^{n^2+1} : \det(\lambda_{ij})\lambda - 1 = 0\}$ is a good embedding of the invertible matrices, in the sense that it is a closed subset under the Zariski topology.

In order to see that it is a linear algebraic group, we need to see that the group operations are morphisms of affine varieties. We can, in a rather cumbersome and long way, see that the inverse matrix is given by polynomials on each component, while the neutral element (the identity matrix) is obviously given by a morphism. Further, matrix multiplication is also given by polynomials. Then, we get that the general linear group over K is indeed a linear algebraic group. □

Straight from the definition, we can see the following result.

Lemma A.16. *Let K be a field and $G \subseteq K^n$ a linear algebraic group. Then, every subgroup of G that is closed under the Zariski topology is again a linear algebraic group.*

This allows us to give some examples of linear algebraic groups as closed subgroups of the general linear group.

Example A.17. Let K be a field and let $\mathbb{GL}_n(K) \subseteq K^{n^2+1}$ be the general linear group over K. The following subgroups are also linear algebraic groups:

(i) The group of upper triangular matrices, $\mathbb{T}_n(K) = \{(\lambda_{11}, ..., \lambda_{nn}, \lambda) \in \mathbb{GL}_n(K) : \lambda_{ij} = 0, \forall i > j\}$.

(ii) The group of diagonal matrices, $\mathbb{D}_n(K) = \{(\lambda_{11}, ..., \lambda_{nn}, \lambda) \in \mathbb{GL}_n(K) : \lambda_{ij} = 0, \forall i \neq j\}$.

(iii) The special linear group, $\mathbb{SL}_n(K) = \{(\lambda_{11}, ..., \lambda_{nn}, \lambda) \in \mathbb{GL}_n(K) : \lambda = 1\}$.

We can see that those are indeed closed subsets of K^{n^2+1}, since we have described them as the zero sets of extra polynomials.

Finally, before ending this appendix about affine varieties and algebraic groups, we are going to give the notions of connectedness and solvability of an algebraic group. As we are going to see, they are relevant in the context of the Lie-Kolchin theorem.

Definition A.18. *Let K be an algebraically closed field and K^n its affine n-space. Let $X \subseteq K^n$ be an affine variety of K^n. Then, X is connected if it is a connected topological space under the induced Zariski topology. That is, X is connected if and only if for all $A, B \subseteq X$ affine varieties of K^n so that $X = A \cup B$ and $A \cap B = \emptyset$, then either $A = \emptyset$ or $B = \emptyset$.*

With this notion of connectedness, we can define the identity component of an algebraic group.

Definition A.19. *Let K be an algebraically closed field and $G \in \mathcal{V}(K^n)$ be an algebraic group. Then, the identity component of G, denoted as G^0, is the connected subgroup of G that contains the identity element.*

We can also give an notion of solvability restricted to the context of algebraic groups.

Definition A.20. *Let K be an algebraically closed field and $G \in \mathcal{V}(K^n)$ be an algebraic group. Then, G is solvable as an algebraic group if there is a chain of algebraic subgroups $G_0 = \{i\} \subseteq G_1 \subseteq ... \subseteq G_n = G$ so that G_i is a normal subgroup of G_{i+1} for every $i = 0, ..., n-1$ and so that the quotient groups G_i/G_{i-1} are all abelian.*

Then, we can present the celebrated theorem due to Sophus Lie and Ellis Kolchin. A proof can be found in [5] (pp. 69).

Theorem A.21. *If $G \subseteq \mathbb{GL}_n(K)$ is a connected and solvable subgroup of the general linear group over the algebraically closed field K for $n > 1$, then G is conjugate to a triangular subgroup of $\mathbb{GL}_n(K)$.*

Bibliography

[1] Bronstein, M: *Symbolic Integration I.* Algorithms and Computations in Mathematics, vol 1, Springer, 2004.

[2] Claramunt, J; Ara, P: *Differential Galois Theory, Groups of Symmetries in Differential Equations.* Universitat Autònoma de Barcelona, Treball Final de Grau, 2014.

[3] Conrad, B: *Impossibility Theorems for Elementary Integration.* 2005

[4] Crespo, T; Hajto, Z: *Algebraic Groups and Differential Galois Theory.* Graduate Studies in Mathematics, Volume 122. American Mathematics Society, 2010.

[5] Crespo, T; Hajto, Z: *Introduction to Differential Galois Theory.* Cracow University of Technology Press, Cracow, 2007.

[6] Goldstein, L. J: *Abstract Algebra: A First Course.* Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1973.

[7] Hartshorne, R: *Algebraic Geometry.* Graduate Texts in Mathematics, Springer-Verlag New York, 1977.

[8] Hubbard, J. H; Lundell, B: *A First Look at Differential Algebra.* The American Mathematical Monthly, Vol 2018, pp 245-261, 2011.

[9] Kaplansky, I: *An Introduction to Differential Algebra.* Hermann, 1957.

[10] Kolchin, E. R: *Differential Algebra and Algebraic Groups.* Pure and Applied Mathematics, vol. 54, Academic Press, New York, 1973.

[11] Khovanskii, A: *Topological Galois Theory.* Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg, 2014.

[12] Khovanskii, A; Alekseev, V.B: *Abel's Theorem in Problems and Solutions. Appendix by A. Khovanskii: Solvability of equations by explicit formulae (Liouville's theory, differential Galois theory, and topological obstructions).* Springer Netherlands, 2004.

[13] Magid, A: *Lectures on Differential Galois Theory.* American Mathematical Society, University Lectures Series, vol 7, 1994.

[14] Morales Ruiz, J. J: *Differential Galois Theory and Non-Integrability of Hamiltonian Systems.* Modern Birkhäuser Classics, Birkhäuser Basel, 1999.

[15] Murphy, J: *Differential Galois Theory.* UChicago 2010 REU, University of Chicago, 2010.

[16] van der Put, M; Singer, M. F: *Galois Theory of Linear Differential Equations.* Grundlehren der mathematischen Wissenschaften, 328. Springer-Verlag Berlin Heidelberg, 2003.

[17] Singer, M. F: *Introduction to the Galois Theory of Linear Differential Equations.* arXiv:abs/0712.4124, 2007.

[18] Sutherland, A: *18.782 Introduction to Arithmetic Geometry.* Fall 2013. Massachusetts Institute of Technology: MIT OpenCourseWare, https://ocw.mit.edu, 2013.