eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

ZIENTZIA ETA TEKNOLOGIA FAKULTATEA
FACULTAD DE CIENCIA Y TECNOLOGÍA

Integration and resolution of differential equations in finite terms

Final Degree Dissertation
Degree in Mathematics

Eki González García

Supervisor:
Josu Sangroniz Gómez

Leioa, 19 June 2019

Contents

Introduction

When we are introduced to integrals in high school we learn some methods to find primitives of functions. We may try to use these methods to integrate very simple functions such as e^{x^2}, e^x/x or $(\sin x)/x$ failing once and again and wonder if we are doing something wrong and why we are unable to find the result. The reason is that this result "does not" exist, in the sense that there is not a "prettier" way to describe the function $\int e^{x^2}\mathrm{d}x$ than $\int e^{x^2}\mathrm{d}x$ itself. Certainly, it can be written as an infinite series, but it cannot be expressed as a combination of finitely many elementary functions (which we usually understand as radical, exponential and trigonometric functions and their inverses). Describing if an integral can be expressed in this way is what is known as the problem of integration in finite terms.

Similarly, once we learn various methods to solve differential equations, we may try to use them to solve simple equations like $Y'' - xY = 0$ with no success. Again the problem is that this equation "does not" have a solution in a similar sense as above. But now the impossibility is even stronger: the solution of the equation can not be given even if we allow also integral symbols in the final expression (notice that in this sense the previous problem would trivially have a solution). This problem is studied in differential Galois theory, an analogue of classical Galois theory, that studies solutions of homogenous linear differential equations instead of polynomial equations.

In order to be able to make more precise this problem we need to formalize the concepts, which will allow us to work on an abstract setting. This is done in Chapter 1, which introduces the basic notions of what we understand by a derivation and how it works in the context of an abstract ring or field. As said before, we will be working abstractly, but, if one wishes to go down to earth, the idea to bear in mind is that the field we are working on is the field of meromorphic functions under the usual derivation (that is, complex functions defined on a suitable connected open subset of $\mathbb{C}$ that can be expressed by Laurent series). One may wonder why we do not work with real functions, which seem a more natural setting, for example with the ring of infinitely differentiable functions, $C^\infty(\mathbb{R})$. The reason is somewhat implicit in its name, it is just a ring. Working with differential fields makes

the theory easier than with rings. Furthermore, and this is the real reason, it does not even have a field of fractions, because it is not an integral domain. Indeed, if

$$f(x) = \begin{cases} 0 & \text{if } x \leq 0 \\ e^{-1/x^2} & \text{if } x > 0, \end{cases} \quad g(x) = \begin{cases} e^{-1/x^2} & \text{if } x < 0 \\ 0 & \text{if } x \geq 0, \end{cases}$$

f and g are infinitely differentiable non-zero functions, but $fg \equiv 0$. Also, working over complex numbers simplifies the number of functions that we have to care about: trigonometric functions can be expressed by exponentials and their inverses by logarithms.

Chapter 2 studies the first problem, namely, the existence of elementary primitives. It does so by presenting Liouville's Theorem, which characterizes the functions that have elementary primitives. The rest of the chapters develop the main aspects of differential Galois theory. Chapter 3 goes over concepts of Algebraic Geometry that are needed for the theory, specifically it introduces and studies algebraic groups. Chapter 4 gives the basic notions of homogenous linear differential equations over differential fields; then Chapter 5 gives the fundamental theorem of differential Galois theory (which states a correspondence between intermediate differential fields and closed subgroups of the differential Galois group analogously as the fundamental theorem of classical Galois theory) and finally Chapter 6 gives the solvability theorem, which states that a homogenous linear differential equation has a solution in the sense above mentioned if and only if the connected component of its differential Galois group containing the identity element is solvable.

The main sources used for this dissertation are the article by Roselincht [5] for the part about Liouville's Theorem and the book by Crespo and Hajto [2] for differential Galois theory. Apart from a few results this dissertation is mostly self-contained and an effort has been made to introduce the necessary concepts in order to prove that the problems we have discussed do not have solutions. That being said, the prerequisites are notions in Algebra learnt in the Bachelor's Degree in Mathematics as well as basic notions in Topology for the part of Algebraic Geometry. Being familiar with Algebraic Geometry is recommendable but not crucial, since the necessary material is introduced in Chapter 3.

It is worth mentioning that this dissertation includes solved exercises in Appendix A. They provide some results needed to complete the theory as well as examples that illustrate the theoretical results. They are referenced whenever they are needed to prove the results of the theory.

Chapter 1

Basic definitions and results

1.1 Differential rings

Definition 1.1.1. Let A be a ring. A *derivation* in A is a map $\mathrm{d} : A \longrightarrow A$ that satisfies the following properties:

(i) $\mathrm{d}(a+b) = \mathrm{d}(a) + \mathrm{d}(b)\ \forall a, b \in A$;

(ii) $\mathrm{d}(ab) = \mathrm{d}(a)b + a\mathrm{d}(b)\ \forall a, b \in A$.

$\mathrm{d}(a)$ is called the *derivative* of a and a usual notation will be $a' = \mathrm{d}(a)$, as well as a'', a''', $\ldots$, $a^{(n)}$ for consecutive derivatives. We set $a^{(0)} = a$.

The map defined by $a' = 0$ for every a in A is always a derivation and it is called the *trivial derivation*.

Remark 1.1.1. Immediate properties:

(i) if A is a unitary ring $1' = 0$ (since $1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1' = 1' + 1'$), and therefore $n' = 0$ for all n in the prime subring of A.

(ii) Leibniz's rule: $(ab)^{(n)} = \displaystyle\sum_{i=0}^{n} \binom{n}{i} a^{(n-i)} b^{(i)}$ (by induction on n).

Proposition 1.1.1. *If A is an integral domain with a derivation $'$, then $'$ extends uniquely to its fraction field* $\mathrm{Fr}(A)$.

Proof. Let $b \in A - \{0\}$. Then if $'$ is an extension of the derivation to $\mathrm{Fr}(A)$,

$$0 = 1' = \left(b\frac{1}{b}\right)' = b'\frac{1}{b} + b\left(\frac{1}{b}\right)' \Rightarrow \left(\frac{1}{b}\right)' = -\frac{b'}{b^2}.$$

This formula implies uniqueness of the extension since, if $\frac{a}{b} \in \mathrm{Fr}(A)$, it must be

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

And this formula does in fact define a derivation: it can be easily checked that it is well-defined and that satisfies the two properties. □

Definition 1.1.2. A *differential ring* is a commutative and unitary ring endowed with a derivation. A *differential field* is a differential ring which is also a field.

Example 1.1.1. (i) Every commutative and unitary ring A is a differential ring with the trivial derivation.

Over $\mathbb{Z}$ and $\mathbb{Q}$ the trivial derivation is the only possible one (actually, this is true for all prime subrings and subfields).

(ii) The ring of infinitely differentiable functions $C^\infty(\mathbb{R})$, the ring of holomorphic functions on the complex plane and the field of meromorphic functions on the complex plane with the usual derivations are all differential rings (and the last one is a differential field). These examples also work if we consider only the functions defined, for example, in a connected open subset of $\mathbb{R}$ or $\mathbb{C}$.

(iii) If A is a differential field, the derivation of A can be extended to $A[X]$ by assigning to X' any element in $A[X]$ (the usual one being $X' = 1$). If K is a differential field, the same method for defining a derivation works for $K(X)$, $A[X_1, \ldots, X_n]$, $K(X_1, \ldots, X_n)$, $A[X_i, i \in I]$ and $K(X_i, i \in I)$, but it requires some more work to check.

(iv) As a particular case of the previous one, $\mathbb{Q}[\pi] \cong \mathbb{Q}[X]$ so, for example, $\mathbb{Q}[\pi]$ is a differential ring with the derivation defined by $\pi' = 1 + \frac{7\pi}{3}$.

(v) If A is a differential ring we can consider the *ring of differential polynomials in n variables*, which we denote $A[X_1, \ldots, X_n]'$ and means $A[X_1, \ldots, X_n, X_1', \ldots, X_n', \ldots]$ where $X_i^{(j)}$ are all indeterminates and $(X_i^{(j)})' = X_i^{(j+1)}$. If K is a field we can construct in the same way the *field of differential rational functions in n variables*, which we denote $K(X_1, \ldots, X_n)'$.

Definition 1.1.3. Let A be a differential ring. $a \in A$ is said to be a *constant* if $a' = 0$. The set of these elements is a subring of A called the *ring of constants* of A and is denoted C_A.

If K is a field so is C_K, and in this case it is called the *field of constants* of K.

Notice that, as mentioned before, C_A always contains the prime subring of A (and its prime subfield in case A is a field).

1.2 Differential homomorphisms and extensions

Definition 1.2.1. Let A be a differential ring and I an ideal of A. I is said to be a *differential ideal* if $a' \in I$ for all $a \in I$.

If A is a ring and I is a differential ideal of A then A/I is a differential ring with the derivation defined by $\overline{a}' = \overline{a'}$. It is well defined because $\overline{a} = \overline{b}$ is equivalent to $a - b \in I$ and then the fact that I is differential implies $a' - b' = (a-b)' \in I$, that is, $\overline{a'} = \overline{b'}$. It clearly satisfies the conditions to be a derivation.

Definition 1.2.2. Let A and B be differential rings. A homomorphism $f : A \longrightarrow B$ is called a *differential homomorphism* if it commutes with the derivation, that is, $f(a)' = f(a')$ for all $a \in A$. We refer to f as a *differential isomorphism* if it has an inverse, and as a *differential automorphism* if in addition $A = B$.

If A is a differential ring and I a differential ideal of A, the natural homomorphism $A \longrightarrow A/I$ is clearly a differential homomorphism.

Proposition 1.2.1. *Let $f : A \longrightarrow B$ be a differential homomorphism. Then* $\ker f$ *is a differential ideal,* $\mathrm{Im} f$ *is a differential ring and the isomorphism* $\overline{f} : A/\ker f \longrightarrow \mathrm{Im} f$ *(given by $\overline{f}(\overline{a}) = f(a)$) is a differential one.*

Proof. It is clear that $\ker f$ is a differential ideal since if $a \in \ker f$, $0 = 0' = f(a)' = f(a')$, that is, $a' \in \ker f$. Also the map $\overline{f}$ is a differential isomorphism because

$$\overline{f}(\overline{a}') = \overline{f}(\overline{a'}) = f(a') = f(a)' = \overline{f}(\overline{a})'.$$

□

Definition 1.2.3. An extension of rings $A \subseteq B$, where A and B are differential rings, is called a *differential extension of rings* if the derivation of B restricts to the one in A. Analogously a field extension L/K, where L and K are differential fields, is called a *differential extension of fields* if the derivation of L restricts to the one in K.

Example 1.2.1. Considering $\mathbb{Q}(X)$ with the usual derivation, $\mathbb{Q}(X,Y)/\mathbb{Q}(X)$ is a differential extension with the derivation ∂_X but it is not with the derivation ∂_Y (where ∂_X and ∂_Y denote the usual partial derivatives).

Example 1.2.2. (i) If $A \subseteq B$ is a differential extension of commutative rings and S is a subset of B we can consider the *differential A-algebra generated by S*, which we denote $A[S]'$ and means the A-algebra generated by the elements of S and their successive derivatives. In the same way we consider the *differential field generated by S*, $K(S)'$ where L/K is a differential extension of fields and $S \subseteq L$.

(ii) Let K be a differential field and A and B be K-algebras such that $K \subseteq A$ and $K \subseteq B$ are differential extensions. Define $\varphi : A \times B \longrightarrow A \otimes_K B$ as $\varphi(a,b) = a' \otimes b + a \otimes b'$. Some simple computations show

that it is biadditive and balanced, therefore it induces an additive homomorphism $' : A \otimes_K B \longrightarrow A \otimes_K B$, which is a derivation on the ring $A \otimes_K B$.

Theorem 1.2.2. *Let K be a differential field and L/K be a separable algebraic extension of fields. Then, the derivation of K extends uniquely to L. Moreover, every K-automorphism of L is a differential automorphism.*

Proof. Let d denote the derivation in K. Suppose first that L/K is a finite extension. Then, by the primitive element theorem, $L = K(\alpha)$ for some $\alpha \in L$. Let us first check uniqueness, if $m \in K[X]$ is the minimal polynomial of α over K, we can apply derivation to $m(\alpha) = 0$ and get $m^{(\mathrm{d})}(\alpha) + m'(\alpha)\mathrm{d}(\alpha) = 0$, where $m^{(\mathrm{d})}$ denotes the polynomial obtained differentiating the coefficients of m and m' is the usual derived polynomial. The fact that the extension is separable implies $m'(\alpha) \neq 0$ and therefore we get $\mathrm{d}(\alpha) = -m^{(\mathrm{d})}(\alpha)(m'(\alpha))^{-1}$.

For existence we recall that $L \cong K[X]/(m)$, so we can work in the ring of polynomials modulo m. The separability of L/K implies that m and m' are coprime so let $p, q \in K[X]$ such that $1 = mp + m'q$ (which implies $\overline{m'q} = \overline{1}$ in $K[X]/(m)$), and extend the derivation in K to $K[X]$ by letting $\mathrm{d}(X) := -m^{(\mathrm{d})}\, q$. Notice that in $K[X]/(m)$, $\overline{\mathrm{d}(X)} = -\overline{m^{(\mathrm{d})}}\ \overline{m'}^{\,-1}$. Now we just have to see that (m) is a differential ideal and that will imply that $K[X]/(m)$ is a differential ring with a derivation extending the one in K. To see that it is enough to check that $\mathrm{d}(m) \in (m)$, but

$$\begin{aligned} \mathrm{d}(m) &= m^{(\mathrm{d})} + m'\mathrm{d}(X) = m^{(\mathrm{d})} + m'(-m^{(\mathrm{d})}q) = \\ &= m^{(\mathrm{d})}(1 - m'q) = m^{(\mathrm{d})}mp \in (m). \end{aligned}$$

That concludes the finite case. For the general case notice that $L = \bigcup E$ where E runs over the subfields $K \subseteq E \subseteq L$ with $[E : K] < \infty$. The derivation in K extends uniquely to a derivation d_E of each E. Notice that if $\alpha \in L$ and $\alpha \in E, F$ with $[E : K], [F : K] < \infty$, then $\alpha \in EF$ and $[EF : K] < \infty$. So, since the derivation extends uniquely to EF, $\mathrm{d}(\alpha) := \mathrm{d}_E(\alpha) = \mathrm{d}_{EF}(\alpha) = \mathrm{d}_F(\alpha)$ is a well defined element and d is a derivation in L extending the derivation in K.

Let us now prove the last claim. Let σ be a K-automorphism of L and d be the derivation in L extending the one in K. Then it is routine to check that $\tilde{\mathrm{d}} = \sigma^{-1} \circ \mathrm{d} \circ \sigma$ is a derivation. Also, $\tilde{\mathrm{d}}$ extends the derivation in K so, by uniqueness, $\tilde{\mathrm{d}} = \sigma^{-1} \circ \mathrm{d} \circ \sigma = \mathrm{d}$, which implies $\mathrm{d} \circ \sigma = \sigma \circ \mathrm{d}$ (and this is the definition of being a differential homomorphism). □

Chapter 2

Elementary primitives and Liouville's Theorem

The goal of this chapter is to prove Liouville's Theorem, which characterizes the functions with elementary primitives. This will be done in an abstract setting, but the idea to bear in mind, if we want to come back to our original problem, is that we are working with the differential field of meromorphic functions (defined on a suitable connected open subset of the complex plane). For example, we could take as a base (differential) field $\mathbb{C}(z, e^{z^2})$ and we would like to know if $\int e^{z^2} dz$ (which is meromorphic) is an element of this field or some extension obtained by successively adjoining elementary functions.

Working with complex functions, apart from making the theory simpler because we can work with fields instead of with rings (notice that for instance $C^\infty(\mathbb{R})$ is not a suitable setting because it is not an integral domain), allows to write trigonometric functions in terms of exponentials and their inverses in terms of logarithms. So we only need to worry about these two types of functions (exponentials and logarithms).

The idea of Liouville's theorem can be appreciated when we integrate rational functions. We know that the result is the sum of a rational function and a linear combination of logarithms of rational functions (to be more precise, logarithms of linear polynomials). This is in fact the general behaviour: if $f \in K$ (with K a differential field of meromorphic functions containing $\mathbb{C}(z)$), then f has an elementary primitive if and only if $\int f$ is the sum of an element in K and a linear combination of logarithms of elements in K, that is, $\int f = g + c_1 \log f_1 + \cdots + c_n \log f_n$ with $g, f_1, \ldots, f_n \in K$ and $c_1, \ldots, c_n \in \mathbb{C}$. The bottom line is that if a function has an elementary primitive we know where to look for it and if no function here is a primitive of it, this function has no elementary primitive at all.

2.1 Preliminary lemmas

In this chapter we will use the *logarithmic derivative* defined for $u \neq 0$ as $u^* = u'/u$ some of its properties are shown in Exercise 6 and Exercise 7.

Now, the formal definition that we need is the following one:

Definition 2.1.1. Let K be a differential field. An *elementary extension* is a differential extension F/K with the same constants such that there exists a chain of differential fields $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = F$ where, for all $1 \leq i \leq n$, K_i/K_{i-1} is either algebraic or $K_i = K_{i-1}(t_i)$ (t_i transcendental over K_{i-1}) such that there exists $u_i \in K_{i-1}^{\times}$ with $t_i^* = u_i'$ (*exponential case*) or $t_i' = u_i^*$ (*logarithmic case*). We say that an element $\alpha \in K$ has an *elementary primitive* if there exists an elementary extension F/K such that $\alpha = v'$ for some $v \in F$.

Notice that in the logarithmic case, $t_i' \in K_{i-1}$. We will usually work with this more general condition and still refer to it as the logarithmic case and call it a *logarithmic extension*. In a similar way we will usually work with the exponential case as $t_i^* \in K_{i-1}$ and call it an *exponential extension*.

An important part of this definition that maybe needs some explanation is why we require the extension to have the same constants. This prevents situations such as $K = \mathbb{C}(x, e^x)$ and t transcendental over K with $t' = t$, which in the field of meromorphic functions would imply $t = ae^x$ for some $a \in \mathbb{C}$ and therefore $t \in K$. In some sense the "true" elementary function that we want to have is e^x, not t. This problem arises because this extension adds constants, namely te^{-x} is a constant.

Now we start working towards our main goal.

Definition 2.1.2. Let $K(t)/K$ be a transcendental extension of fields and let $R \in K(t)^{\times}$ and $b \in K$. If $R(t) = (t-b)^m P(t)/Q(t)$ with $P, Q \in K[t]$, $P(b), Q(b) \neq 0$, $m \in \mathbb{Z}$, then we write $\nu_b(R) = m$. If $\nu_b(R) < 0$ we say that b is a *pole* or R with *multiplicity* $-m \in \mathbb{N}$. A pole of multiplicity 1 is called *simple* and a pole of multiplicity greater than 1 is called *multiple*.

Proposition 2.1.1. *Let $K(t)/K$ be a transcendental extension of fields and let $R, S \in K(t)^{\times}$, $b \in K$. If $R + S \neq 0$ then $\nu_b(R+S) \geq \min\{\nu_b(R), \nu_b(S)\}$ and equality holds if $\nu_b(R) \neq \nu_b(S)$.*

Proof. Let $m_1 = \nu_b(R)$, $m_2 = \nu_b(S)$ and suppose $m_1 \leq m_2$. Then we can write $R = (t-b)^{m_1} P_1/Q_1$ and $S = (t-b)^{m_2} P_2/Q_2$ with $P_1, Q_1, P_2, Q_2 \in K[t]$, $P_1(b), Q_1(b), P_2(b), Q_2(b) \neq 0$, and then

$$R+S = (t-b)^{m_1}\Big(\frac{P_1}{Q_1} + (t-b)^{m_2-m_1}\frac{P_2}{Q_2}\Big) = (t-b)^{m_1}\frac{P_1\,Q_2 + (t-b)^{m_2-m_1}P_2\,Q_1}{Q_1\,Q_2}$$

where $(Q_1\,Q_2)(b) = Q_1(b)\,Q_2(b) \neq 0$.

Now, if $m_1 < m_2$ then

$$\big(P_1\,Q_2 + (t-b)^{m_2-m_1}P_2\,Q_1\big)(b) = P_1(b)\,Q_2(b) \neq 0,$$

so $\nu_b(R+S) = m_1 = \min\{\nu_b(R), \nu_b(S)\}$.

And if $m_1 = m_2$,

$$R + S = (t-b)^{m_1}\frac{P_1\,Q_2 + P_2\,Q_1}{Q_1\,Q_2} = (t-b)^{m_1}\frac{(t-b)^{m_3}P}{Q_1\,Q_2}$$

with $P \in K[t]$, $P(b) \neq 0$ and $m_3 \geq 0$, so $\nu_b(R+S) = m_1 + m_3 \geq \min\{\nu_b(R), \nu_b(S)\}$. □

Corollary 2.1.2. *If b is a simple pole of R and it is not a simple pole of S then $R + S \notin K[t]$.*

Proof. $\nu_b(R) = -1 \neq \nu_b(S)$, then $\nu_b(R+S) = \min\{-1, \nu_b(S)\} < 0$, which implies that $R+S$ is not a polynomial. □

Lemma 2.1.3. *Let $K(t)/K$ be a logarithmic or exponential transcendental differential extension of fields with the same constants,* $\mathrm{char}K = 0$ *and K algebraically closed. Let $R_1, \ldots, R_n \in K(t)$, $R_i \neq 0$ for all $1 \leq i \leq n$ and $c_1, \ldots, c_n \in K$ linearly independent over $\mathbb{Q}$. Then the poles of $\sum_{i=1}^n c_i R_i^*$ are all simple and are the zeros and poles of $R_1, \ldots, R_n$, excluding 0 in the exponential case. Furthermore, $\sum_{i=1}^n c_i R_i^*$ does not have poles only if $R_i \in K$ for all $1 \leq i \leq n$ in the logarithmic case or if $R_i = a_i t^{m_i}$ with $a_i \in K$, $m_i \in \mathbb{Z}$ for all $1 \leq i \leq n$ in the exponential case.*

Proof. Since K is algebraically closed we can write, for each $1 \leq i \leq n$, $R_i = a_i \prod_{j=1}^{d_i}(t-\alpha_{ij})^{m_{ij}}$ with $d_i \in \mathbb{N}\cup\{0\}$ and $m_{ij} \in \mathbb{Z}\backslash\{0\}, \alpha_{ij} \in K$ for all $1 \leq j \leq d_i$. As seen in Exercise 6,

$$\sum_{i=1}^n c_i R_i^* = \sum_{i=1}^n c_i a_i^* + \sum_{i=1}^n \sum_{j=1}^{d_i} c_i m_{ij}\frac{t' - \alpha_{ij}'}{t-\alpha_{ij}}. \tag{2.1}$$

Since $t' = c$ or $t' = ct$ with $c \in K$, it is clear that all the poles of $\sum_{i=1}^n c_i R_i^*$ are simple and they must be one of the α_{ij}'s, that is, a zero or a pole of some R_i. Notice that when grouping together the terms where α_{ij} repeats in (2.1), the resulting coefficient is a $\mathbb{Z}$-linear combination of the c_i's, and therefore non-zero.

Since $t \notin K$ and the constants are in K, $t - \alpha_{ij}$ is not a constant, that is, $0 \neq (t-\alpha_{ij})' = t' - \alpha_{ij}'$. Then, in the logarithmic case $t' = c \in K^\times$, so we

get $t' - \alpha'_{ij} = c - \alpha'_{ij} \in K^\times$ and each α_{ij} is a pole of $\sum_{i=1}^n c_i R_i^*$. Therefore it always has poles unless $R_i \in K$ for all $1 \leq i \leq n$. In the exponential case $t' = ct$ with $c \in K^\times$, so $(t' - \alpha'_{ij})/(t - \alpha_{ij}) = (ct - \alpha'_{ij})/(t - \alpha_{ij})$. If α_{ij} is not a pole there has to be cancellation in this last expression, whence $c\alpha_{ij} - \alpha'_{ij} = 0$; but if $\alpha_{ij} \neq 0$ this implies that $\alpha_{ij}^* = c = t^*$ and by Exercise 6, $t = k\alpha_{ij}$ with k constant, which gives that $t \in K$, a contradiction. Then $\alpha_{ij} = 0$ is the only case when it is not a pole of $\sum_{i=1}^n c_i R_i^*$. Therefore this function always has poles unless 0 is the only zero and pole of each R_i, that is, $R_i = a_i t_i^m$ with $a_i \in K$ and $m_i \in \mathbb{Z}$ for all $1 \leq i \leq n$.

□

Lemma 2.1.4. *Let $K(t)/K$ be a logarithmic or exponential transcendental differential extension of fields with the same constants,* $\mathrm{char} K = 0$ *and K algebraically closed. Let $S \in K(t)$, $S \neq 0$. Then the poles of S' are the poles of S and are all multiple ones except in the exponential case when 0 is a simple pole of S, in which case 0 is also a simple pole of S'. Also, if $S \in K[t]$ and $S' \in K$, then $S = dt + e$ with d constant and in fact in the exponential case $S \in K$.*

Proof. Let $b \in K$. Writing $S' = S\,S^*$ we get $\nu_b(S') = \nu_b(S) + \nu_b(S^*)$. Then, from Lemma 2.1.3, we know that in the exponential case, $b = 0$ it is not a pole or a zero of S^*, so $\nu_b(S') = \nu_b(S)$, whence $b = 0$ is a simple pole of S' if and only if it is a simple pole of S; otherwise, if b is a pole of S^* it must be a simple one and also a zero or a pole of S; if it is a zero then $\nu_b(S') = \nu_b(S) - 1 \geq 1 - 1 = 0$ (so it is not a pole of S') and if it is a pole $\nu_b(S') = \nu_b(S) - 1 \leq -1 - 1 = -2$ (so it is a multiple pole).

To prove the second claim let $S = b_m t^m + \cdots + b_0 \in K[t]$ and suppose $S' \in K$.

Then, in the logarithmic case with $t' = c \in K$,

$$\begin{aligned} S' &= b'_m t^m + \cdots + b'_0 + (m b_m t^{m-1} + \cdots + b_1)t' = \\ &= b'_m t^m + (b'_{m-1} + m b_m c)t^{m-1} + \cdots + (b'_0 + b_1 c) \in K \end{aligned}$$

and therefore $b'_m = b'_{m-1} + m b_m c = \cdots = b'_1 + b_2 c = 0$. Then if b_k is constant, $1 \leq k \leq m$, $(b_{k-1} + k b_k t)' = b'_{k-1} + k b_k c = 0$, that is, $b_{k-1} + k b_k t$ is constant, whence $b_k = 0$ and b_{k-1} is constant. Since b_m is constant we conclude that $b_m = \cdots = b_2 = 0$ and b_1 is constant.

In the exponential case, $t' = ct$ with $c \in K$ and

$$\begin{aligned} &S' = b'_m t^m + \cdots + b'_0 + (m b_m t^{m-1} + \cdots + b_1)t' = \\ &\quad = (b'_m + m b_m c)t^m + (b'_{m-1} + (m-1) b_{m-1} c)t^{m-1} + \cdots + (b'_1 + b_1 c)t + b'_0 \in K, \end{aligned}$$

which now gives $b'_k + k b_k c = 0$ for all $1 \leq k \leq m$. If $b_k \neq 0$ we can consider $b_k^* = -kc = (t^{-k})^*$, whence, by Exercise 6, $t^{-k} = a_k b_k$ with a_k a non-zero

constant. Thus $t^{-k} \in K$, which is impossible because t is transcendental over K. Therefore $b_k = 0$ for all $1 \leq k \leq m$, that is, $S = b_0 \in K$. □

Lemma 2.1.5. *Let $K(t)/K$ be a logarithmic or exponential transcendental differential extension of fields with the same constants,* char$K = 0$. *Let $R_1, \ldots, R_n, S \in K(t)$, $R_i \neq 0$ and $c_1, \ldots, c_n \in K$ constants which are linearly independent over $\mathbb{Q}$ such that $\sum_{i=1}^{n} c_i R_i^* + S' \in K$. Then in the logarithmic case $R_i \in K$ for all $1 \leq i \leq n$ and $S = dt + e$ with d constant and in the exponential case $R_i = a_i t^{m_i}$ with $a_i \in K$, $m_i \in \mathbb{Z}$ for all $1 \leq i \leq n$ and $S \in K$.*

Proof. Suppose first that K is algebraically closed. As seen in the previous two lemmas, if $b \in K$ is a pole of $\sum_{i=1}^{n} c_i R_i^*$ or S' it always has different multiplicities in one and the other (a pole of $\sum_{i=1}^{n} c_i R_i^*$ is always simple and a pole of S' is always multiple, except in the exponential case when $b = 0$, where it can be a simple pole of S' but in this case 0 cannot be a pole of $\sum_{i=1}^{n} c_i R_i^*$). In any case, by Proposition 2.1.1, it would be a pole of $\sum_{i=1}^{n} c_i R_i^* + S'$, which does not have any poles because it is in K.

Therefore $\sum_{i=1}^{n} c_i R_i^*$ and S' do not have poles at all and then Lemma 2.1.3 implies that in the logarithmic case $R_i \in K$ and in the exponential case $R_i = a_i t^{m_i}$ for all $1 \leq i \leq n$. In both cases it follows that $S' \in K$ and finally, by Lemma 2.1.4, $S = dt + e$ with d constant in the logarithmic case and $S \in K$ in the exponential case (notice that, as seen in Lemma 2.1.4, S and S' have the same poles, so the fact that S' does not have poles implies $S \in K[t]$).

Now, for a general field K, we apply the result in the algebraic closure of K, $\overline{K}$ (notice that $\overline{K}[t]$ and $\overline{K}$ have the same constants as seen in Exercise 2 (ii)) and see that this implies the claimed result. That is because $K(t) \cap \overline{K} = K$ and $R_1, \ldots, R_n, S$ are in $K(t)$. □

2.2 Liouville's Theorem

Theorem 2.2.1 (Liouville's Theorem)**.** *Let K be a differential field of characteristic 0 and $\alpha \in K$. Then α has an elementary primitive if and only if $\alpha = \sum_{i=1}^{n} c_i u_i^* + v'$ with $u_1, \ldots, u_n \in K^\times$, $v \in K$ and $c_1, \ldots, c_n \in K$ constants which are linearly independent over $\mathbb{Q}$.*

Proof. Let $\alpha \in K$ and suppose it has an elementary primitive, that is, there exists an elementary extension F/K associated to a chain of fields $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = F$, K_i/K_{i-1} algebraic or logarithmic or exponential transcendental extension, and $y \in F$ such that $y' = \alpha$. Let us see that, for all $1 \leq j \leq m$, if $\alpha = \sum_{i=1}^{n} c_i u_i^* + v'$ with $u_1, \ldots, u_n \in K_j^\times$, $v \in K_j$ and $c_1, \ldots, c_n \in K$ constants which are linearly independent over $\mathbb{Q}$,

then there exist $z_1, \ldots, z_r \in K_{j-1}^{\times}$, $w \in K_{j-1}$ and $d_1, \ldots, d_r \in K$ constants which are linearly independent over $\mathbb{Q}$ such that $\alpha = \sum_{i=1}^{r} d_i z_i^* + w'$ (and then just apply this iteratively in descending order to get the claimed result).

If K_j/K_{j-1} is algebraic, applying the trace map to the expression of α gives that $\alpha = \sum_{i=1}^{n}(c_i/d)z_i^* + w'$ with $z_i = N_{K_j/K_{j-1}}(u_i)$ for each $1 \leq i \leq n$ and $w = Tr_{K_j/K_{j-1}}(v)$ (which implies $z_i, w \in K_{j-1}$ for each $1 \leq i \leq n$) and $d \in \mathbb{N}$ (see Exercise 5 and Exercise 7).

If $K_j = K_{j-1}(t_j)$ with $t_j' = u^*$ for some $u \in K_{j-1}^{\times}$ then by Lemma 2.1.5 $u_i \in K_{j-1}$ for all $1 \leq i \leq n$ and $v = dt_j + e$ with $e \in K_{j-1}$ and d constant. This gives that $v' = dt_j' + e' = du^* + e'$ and then $\alpha = \sum_{i=1}^{n} c_i u_i^* + du^* + e'$. Now, if $c_1, \ldots, c_n, d$ are not linearly independent over $\mathbb{Q}$ this means that $d = (r_1/s_1)c_1 + \cdots + (r_n/s_n)c_n$ with $r_1/s_1, \ldots, r_n/s_n \in \mathbb{Q}$. In this case write, for $1 \leq i \leq n$, $z_i = u_i^{s_i} u^{r_i}$ and notice that $\alpha = \sum_{i=1}^{n}(c_i/s_i)z_i^* + e'$ where now $c_1/s_1, \ldots, c_n/s_n$ are linearly independent constants.

For the exponential case, if $K_j = K_{j-1}(t_j)$ with $t_j' = u't$ for some $u \in K_{j-1}^{\times}$ then by Lemma 2.1.5 $u_i = a_i t_j^{m_i}$ with $a_i \in K_{j-1}$, $m_i \in \mathbb{Z}$ for all $1 \leq i \leq n$ and $v \in K_{j-1}$. Since $u_i^* = (a_i t_j^{m_i})^* = a_i^* + m_i u'$, this gives that $\alpha = \sum_{i=1}^{n} c_i a_i^* + \sum_{i=1}^{n} m_i c_i u' + v'$. Finally, write $w = \sum_{i=1}^{n} m_i c_i u + v \in K_{j-1}$ to get $\alpha = \sum_{i=1}^{n} c_i a_i^* + w'$. This concludes all the cases.

For the converse let $\alpha = \sum_{i=1}^{n} c_i u_i^* + v'$ with $u_1, \ldots, u_n \in K^{\times}$, $v \in K$ and $c_1, \ldots, c_n \in K$ constants which are linearly independent over $\mathbb{Q}$, and let us see that it has an elementary primitive. For that let $K_0 = K$ and for $1 \leq i \leq n$ let $K_i = K_{i-1}$ if u_i^* has a primitive $t_i \in K_{i-1}$ and $K_i = K_{i-1}(t_i)$, t_i transcendental over K_{i-1} and $t_i' = u_i^*$ otherwise. Then K_n/K is an elementary extension with $w = \sum_{i=1}^{n} c_i t_i + v \in K_n$ satisfying $w' = \alpha$ (K_n and K have the same constants by Exercise 9). That is, α has an elementary primitive. □

2.3 Elementary primitives of $f(z)e^{g(z)}$

Let $f, g \in \mathbb{C}(z)$, $f \neq 0$, g non-constant, we want to study if $f(z)e^{g(z)}$ has an elementary primitive. For that purpose we first have to give a modified version of Lemma 2.1.5:

Lemma 2.3.1. *Let $K(t)/K$ be a logarithmic or exponential transcendental differential extension of fields with the same constants,* $\mathrm{char}K = 0$. *Let $R_1, \ldots, R_n, S \in K(t)$, $R_i \neq 0$ and $c_1, \ldots, c_n \in K$ constants which are linearly independent over $\mathbb{Q}$ such that $\sum_{i=1}^{n} c_i R_i^* + S' \in K[t]$. Then $S \in K[t]$ and in the logarithmic case $R_i \in K$ for all $1 \leq i \leq n$ with d constant while in the exponential case $R_i = a_i t^{m_i}$ with $a_i \in K$, $m_i \in \mathbb{Z}$ for all $1 \leq i \leq n$.*

Proof. It is the same as the proof of Lemma 2.1.5 but removing some parts of it. Notice that since we know that S' has no poles, $S \in K[t]$ by Lemma 2.1.4. □

Theorem 2.3.2. *Let $f, g \in \mathbb{C}(z)$, $f \neq 0$, g non-constant. Then $f(z)e^{g(z)}$ has elementary primitive if and only if there exists $a \in \mathbb{C}(z)$ such that $f = a' + ag'$.*

Proof. We consider the base field $\mathbb{C}(z,t)$, where $t = e^{g(z)}$. Notice that $t' = g't \in \mathbb{C}(z,t)$, so this is a differential field.

Let us first see that t is transcendental over $\mathbb{C}(z)$. Since $t^* = g' \in \mathbb{C}(z)$, if t were algebraic over $\mathbb{C}(z)$ Exercise 7 would imply that there exist $n \in \mathbb{N}$ and $h \in \mathbb{C}(z)$ such that $h^* = ng'$; but the poles of h^* are simple and the ones of g' are multiple, therefore h^* does not have poles and then, by Exercise 6, $h \in \mathbb{C}$ which further implies $g' = 0$, but this is a contradiction.

By Liouville's Theorem we get that ft has an elementary primitive (over $\mathbb{C}(z,t)$) if and only if

$$ft = \sum_{i=1}^{n} c_i u_i^* + v' \tag{2.2}$$

with $u_1, \ldots, u_n \in \mathbb{C}(z,t)^\times$, $v \in \mathbb{C}(z,t)$ and $c_1, \ldots, c_n \in \mathbb{C}$ constants which are linearly independent over $\mathbb{Q}$. Since $ft \in \mathbb{C}(z)[t]$, applying Lemma 2.3.1 to the exponential extension $\mathbb{C}(z)(t)/\mathbb{C}(z)$, we get that $v \in \mathbb{C}(z)[t]$ and $u_i = a_i t^{m_i}$ with $a_i \in \mathbb{C}(z)$, $m_i \in \mathbb{Z}$ for all $1 \leq i \leq n$. Writing $v = \sum_{j=0}^{m} b_j t^j$ with $b_1, \ldots, b_m \in \mathbb{C}(z)$, then $v' = \sum_{j=0}^{m} (b_j' + j b_j g') t^j$. Noticing that $\sum_{i=1}^{n} c_i u_i^* \in \mathbb{C}(z)$ (because $u_i^* = a_i^* + m_i g'$) we get from (2.2) that $f = b_1' + b_1 g'$. That is, $a = b_1$ is the element we are looking for.

For the converse, if $f = a' + ag'$ then fe^g has an elementary primitive, namely ae^g. □

We can now apply this Theorem to see that e^{z^2} and e^z/z do not have elementary primitives. This is done in Exercise 10.

Chapter 3

Linear algebraic groups

3.1 Affine varieties

Let K be a field and $I \subseteq K[X_1, \ldots, X_n]$. We denote $V(I)$ the set of points in K^n in which all the polynomials in I vanish. Notice that if J is the ideal generated by I then $V(I) = V(J)$, so we can assume that I is an ideal.

Definition 3.1.1. A subset of K^n of the form $V(I)$ is called an *affine variety*. The *Zariski topology* of K^n is the topology whose closed sets are the affine varieties.

Example 3.1.1. Clearly for any non-zero polynomial $f \in K[X]$, $V(f)$ is finite, so if $I \subseteq K[X]$ is a non-zero ideal then $V(I)$ is finite. Conversely, any finite subset, $S = \{x_1, \ldots, x_m\} \subseteq K$, is a variety ($S = V((X - x_1) \ldots (X - x_n))$). Hence, the Zariski topology of K is the cofinite topology.

If $S \subseteq K^n$ define $I(S)$ as the set of polynomials that vanish in every point of S. Notice that $I(S)$ is an ideal of $K[X_1, \ldots, X_n]$.

Proposition 3.1.1. *Let K be a field and $S \subseteq K^n$. Then $V(I(S)) = \overline{S}$ (that is, the Zariski closure of S).*

Proof. Clearly $V(I(S))$ is closed and $S \subseteq V(I(S))$, so $\overline{S} \subseteq V(I(S))$. For the converse suppose $S \subseteq V(J)$ for some ideal J and let us see that $V(I(S)) \subseteq V(J)$. Let $f \in J$, then $S \subseteq V(J)$ implies that $f(x) = 0$ for all $x \in S$, so $f \in I(S)$. Then $J \subseteq I(S)$ and therefore $V(J) \supseteq V(I(S))$. □

Definition 3.1.2. A topological space is a *Noetherian space* if for any descending chain of closed sets $Y_1 \supseteq Y_2 \supseteq \ldots$ there exists $r \geq 1$ such that $Y_i = Y_r$ for all $i \geq r$.

Closed subspaces of a Noetherian space are clearly Noetherian spaces.

Theorem 3.1.2. *K^n (and therefore any affine variety) is a Noetherian space.*

Proof. Let $S_1 \supseteq S_2 \supseteq \dots$ be a descending chain of closed sets. Then $I(S_1) \subseteq I(S_2) \subseteq \dots$ is an ascending chain of ideals of $K[X_1, \dots, X_n]$. Hilbert Basis Theorem states that this is a Noetherian ring and hence there exists $r \geq 1$ such that $I(S_i) = I(S_r)$ for all $i \geq r$. Therefore $V(I(S_i)) = V(I(S_r))$ for all $i \geq r$, but S_i are closed, so Proposition 3.1.1 implies that $S_i = S_r$ for all $i \geq r$. □

Definition 3.1.3. Let $S \subseteq K^n$ and $T \subseteq K^m$ be affine varieties. A *morphism of varieties* is a map $\varphi : S \longrightarrow T$ such that there exist $P_1, \dots, P_m \in K[X_1, \dots, X_n]$ polynomials that satisfy $\varphi(x) = (P_1(x), \dots, P_m(x))$ for all $x \in S$.

Theorem 3.1.3. *Morphisms of varieties are continuous maps (with respect to the Zariski topology).*

Proof. Let $V \subseteq K^n$ and $W \subseteq K^m$ ve affine varieties and $f : V \longrightarrow W$ be a morphism. Then f is given as $f = (F_1, \dots, F_m)$ with $F_1 \dots, F_m \in K[X_1, \dots, X_n]$.

If $S \subseteq W$ is a closed subset with $S = V(I)$ then

$$\begin{aligned} f^{-1}(S) &= \{x \in V \colon g(f(x)) = 0 \ \forall g \in I\} = \\ &= \{x \in V \colon g(F_1(x), \dots, F_m(x)) = 0 \ \forall g \in I\} = \\ &= V \cap V(g(F_1, \dots, F_m) \colon g \in I). \end{aligned}$$

So $f^{-1}(S)$ is closed in V and therefore f is a continuous map. □

Definition 3.1.4. Let X be a non-empty topological space. We say X is *irreducible* if whenever $X = X_1 \cup X_2$ with X_1 and X_2 closed sets, then either $X = X_1$ or $X = X_2$. A subset Y of a topological space is an *irreducible set* if it is irreducible with the subspace topology.

Notice that the continuous image of an irreducible variety is an irreducible variety.

If $X \subseteq K^n$ and $Y \subseteq K^m$ are affine varieties, $X \times Y \subseteq K^{n+m}$ is also an affine variety and then we consider over it the Zariski topology (which is different from the product topology).

Proposition 3.1.4. *If $X \subseteq K^n$ and $Y \subseteq K^m$ are irreducible sets then $X \times Y \subseteq K^{n+m}$ is an irreducible set.*

Proof. Suppose $X \times Y = C_1 \cup C_2$ with $C_1, C_2 \subseteq K^{n+m}$ closed. Then, for all $x \in X$, $\{x\} \times Y \subseteq C_1$ or $\{x\} \times Y \subseteq C_2$ (because Y is irreducible), so $X = X_1 \cup X_2$ with $X_i = \{x \in X \colon \{x\} \times Y \subseteq C_i\}$. If $C_1 = V(I_1)$, then

$X_1 = V(f_y \colon f \in I_1, y \in Y)$ where f_y is given by $f_y(x) = f(x,y)$, hence X_1 (and similarly X_2) is closed. Therefore $X = X_1$ or $X = X_2$, that is, $X \times Y = C_1$ or $X \times Y = C_2$. □

Theorem 3.1.5. *In a Noetherian space X, every non-empty closed subset Y can be expressed as a finite union of irreducible closed subsets Y_i, $Y = Y_1 \cup \cdots \cup Y_r$. If we require that $Y_i \not\supseteq Y_j$ for $i \neq j$, then Y_i are uniquely determined. They are called the* irreducible components *of Y and they are the maximal irreducible subsets of Y.*

Proof. Let $\mathcal{C}$ be the set of closed subsets of X that cannot be decomposed into a finite union of irreducible closed subsets. By way of contradiction assume $\mathcal{C}$ is non-empty.

If $C_1 \supseteq C_2 \supseteq \ldots$ is a descending chain in $\mathcal{C}$, then it is stationary because X is Noetherian. Thus, Zorn's Lemma implies that $\mathcal{C}$ has a minimal element Y. Since $Y \in \mathcal{C}$, Y is not irreducible (otherwise it would have a trivial decomposition), so there exist Y_1, Y_2 proper closed subsets of Y such that $Y = Y_1 \cup Y_2$. Since Y is minimal in $\mathcal{C}$ and $Y_1, Y_1 \subsetneq Y$ we get that Y_1 and Y_2 can be decomposed as a finite union of irreducible closed subsets. Therefore Y can also be decomposed (combining the decompositions of Y_1 and Y_2). This is a contradiction and that implies $\mathcal{C} = \emptyset$.

Assume that $Y = Y_1 \cup \cdots \cup Y_r$ and $Y = Y_1' \cup \cdots \cup Y_s'$ are two decompositions of Y satisfying the conditions. Then $Y_1' = Y \cap Y_1' = (Y_1 \cap Y_1') \cup \cdots \cup (Y_r \cap Y_1')$. Since Y_1' is irreducible $Y_1' = Y_1 \cap Y_1'$ (after reordering), so $Y_1' \subseteq Y_1$. Analogously $Y_1 \subseteq Y_j'$ for some j, so $Y_1' \subseteq Y_j'$ and this implies $j = 1$ and $Y_1' = Y_1$.

Let $Z = \overline{Y - Y_1}$ (Zariski closure) and let us see that $Z = Y_2 \cup \cdots \cup Y_r$. First notice that $Z = \overline{Y_2 - Y_1} \cup \cdots \cup \overline{Y_r - Y_1}$. Also, for all $2 \leq i \leq r$, $Y_i = (Y_i - Y_1) \cup (Y_i \cap Y_1)$ and since Y_i is closed, $Y_i = \overline{Y_i - Y_1} \cup \overline{Y_i \cap Y_1} = \overline{Y_i - Y_1} \cup (Y_i \cap Y_1)$. Now, Y_i being irreducible implies that $Y_i = \overline{Y_i - Y_1}$ or $Y_i = Y_i \cap Y_1$; the later contradicts $Y_i \not\subseteq Y_1$ and the former gives the result we wanted.

Similarly we have that $Z = Y_2' \cup \cdots \cup Y_s'$. So, arguing inductively, $r = s$ and $Y_i = Y_i'$ (after reordering) for all $1 \leq i \leq r$. Therefore the decomposition is unique.

In order to prove the last claim (that these Y_i are the maximal irreducible subsets of Y) let S be an irreducible subset of Y. Then $S = Y \cap S = (Y_1 \cap S) \cup \cdots \cup (Y_r \cap S)$. But S is irreducible, so $S = Y_i \cap S$ for some i and then $S \subseteq Y_i$. □

Proposition 3.1.6. *Let $S \subseteq K^n$ be an affine variety. Then S is irreducible if and only if $I(S)$ is a prime ideal.*

Proof. Let S be irreducible and let $fg \in I(S)$. Then $S \subseteq V(fg) = V(f) \cup V(g)$, so $S = (V(f) \cap S) \cup (V(g) \cap S)$ and this implies (without loss of generality) that $S = V(f) \cap S$. Then $S \subseteq V(f)$, that is, $f \in I(S)$.

For the converse assume S is not irreducible and let us prove that $I(S)$ is not a prime ideal. Write $S = S_1 \cup S_2$ with S_1 and S_2 closed proper subsets of S. Then for each $i \in \{1, 2\}$ there exists $f_i \in I(S_i) \backslash I(S)$ (since otherwise $S = V(I(S)) \subseteq V(I(S_i)) = S_i$). Now, for all $x \in S$, $x \in S_1$ or $x \in S_2$, so $f_1(x) = 0$ or $f_2(x) = 0$; in any case $(f_1 f_2)(x) = 0$. Thus $f_1 f_2 \in I(S)$ and therefore $I(S)$ is not a prime ideal. □

Corollary 3.1.7. *Let $f \in K[X_1, \ldots, X_n]$. Then $V(f)$ is an irreducible variety if and only if f is an irreducible polynomial.*

Definition 3.1.5. A subset of a topological space is called *locally closed* if it is the intersection of an open set with a closed set. A *constructible set* is a finite union of locally closed sets.

Example 3.1.2. Since the Zariski topology of K is the cofinite topology its constructible sets are finite and cofinite sets.

Theorem 3.1.8 (Chevalley theorem)**.** *Let $\varphi : X \longrightarrow Y$ be a morphism of varieties. Then φ maps constructible sets to constructible sets. In particular $\varphi(X)$ is constructible in Y.*

Proof. See [2, Theorem 2.2.21]. □

Example 3.1.3. If $\varphi : X \longrightarrow K$ is a morphism then $\varphi(X)$ is finite or cofinite.

3.2 Linear algebraic groups

Definition 3.2.1. A *linear algebraic group* (in the following an *algebraic group*) is a subgroup of $GL_n(K)$ (where K is a field), whose elements are the zeros of a set of polynomials $I \subseteq K[X_{11}, \ldots, X_{nn}]$.

Notice that an algebraic group G can be seen as contained in K^{n^2}, but it is not an affine variety because the condition $\det(x_{ij}) \neq 0$ is not a polynomial identity. However we can identify $GL_n(K)$ with the affine variety of K^{n^2+1}, $\{(x_{11}, \ldots, x_{nn}, y) \in K^{n^2+1} \colon \det(x_{ij})y - 1 = 0\}$ by means of the correspondence $(x_{ij}) \longmapsto (x_{11}, \ldots, x_{nn}, 1/\det(x_{ij}))$. In this way an algebraic group G is a closed subset of $GL_n(K) \subset K^{n^2+1}$. That is, G is an affine variety and we consider then its Zariski topology, with respect to which it

is a Noetherian space as seen in Theorem 3.1.2. The maps $G \times G \longrightarrow G$, $(x, y) \longmapsto xy$ and $G \longrightarrow G$, $x \longmapsto x^{-1}$ are then given by polynomials. (For inversion notice that if $(x_{ij}) \in G$ is identified with $(x_{11}, \ldots, x_{nn}, y) \in K^{n^2+1}$ then $(x_{ij})^{-1}$ is identified with $(y \operatorname{Ad}(x_{11}), \ldots, y \operatorname{Ad}(x_{nn}), \det(x_{ij}))$.)

Theorem 3.2.1. *Let G be an algebraic group. Then:*

(i) *the identity element belongs to a unique irreducible component of G, denoted G^0;*

(ii) *G^0 is a normal subgroup of G of finite index and its cosets are the irreducible components of G as well as the connected components of G;*

(iii) *every closed subgroup of G of finite index contains G^0;*

(iv) *each finite conjugacy class of G has at most $|G : G^0|$ elements.*

Proof. (i) Let $X_1, \ldots, X_m$ be the irreducible components of G that contain the identity element e. Define $\varphi : X_1 \times \cdots \times X_n \longrightarrow G$ as $\varphi(g_1, \ldots, g_n) = g_1 \ldots g_n$, which is continuous. Therefore, since $X_1 \times \cdots \times X_n$ is irreducible by Proposition 3.1.4, $X = \varphi(X_1 \times \cdots \times X_n)$ is also irreducible. Also $e = \varphi(e, \ldots, e) \in X$, so $X \subseteq X_{i_0}$ for some $i_0 \in \{1, \ldots, n\}$. But $\varphi(e, \ldots, e, g_i, e, \ldots, e) = g_i$, so $X_i \subseteq X \subseteq X_{i_0}$ for all $1 \leq i \leq n$, which implies $X_1 = \cdots = X_n$.

(ii) The maps $(g_1, g_2) \longmapsto g_1 g_2$ and $g \longmapsto g^{-1}$ are continuous and therefore $G^0 G^0$ and $(G^0)^{-1}$ are irreducible sets. Since they contain the identity, $G^0 G^0 \subseteq G^0$ and $(G^0)^{-1} \subseteq G^0$, which implies that G^0 is a subgroup of G. Similarly, for each $g \in G$, the map $h \longmapsto h^g$ is also continuous and then $(G^0)^g$ is an irreducible set that contains the identity, so $(G^0)^g \subseteq G^0$, which implies that G^0 is normal. Finally, for each $g \in G$, the map $x \longmapsto xg$ is a continuous map with inverse $x \longmapsto xg^{-1}$, so it maps irreducible components into irreducible components. That is, $G^0 g$ is an irreducible component of G for all $g \in G$. Since G is a Noetherian space it has finitely many irreducible components, so G^0 has finite index in G. Finally, since the irreducible components are cosets of G^0 they are disjoint and therefore they are also the connected components of G.

(iii) Let H be a closed subgroup of finite index. Assume first that $H \leqslant G^0$ and let $n = |G^0 : H|$. Then there exist $g_1, \ldots, g_n \in G^0$ such that $G^0 = \cup_{i=1}^n H g_i$; but $H g_i$ are closed (because H is closed) and G^0 is irreducible, so $G^0 = H g_{i_0}$ for some i_0 and, since it is a subgroup,

$G^0 = H$.

If $H \not\leqslant G^0$ consider $H \cap G^0$. It is a closed normal subgroup and

$$|G : H \cap G^0| = |G : H|\,|H : H \cap G^0|,$$

which by the second isomorphism theorem equals to

$$|G : H|\,|G^0H : G^0| \leq |G : H|\,|G : G^0| < \infty.$$

Now the previous paragraph implies $G^0 = H \cap G^0$, so $G^0 \subseteq H$.

(iv) Let $x \in G$ and $\{x_1 = x, x_2, \ldots, x_n\}$ be its conjugacy class (without repetitions). Define $f : G \longrightarrow G$, $f(g) = x^g$. It is a continuous map and $G = \cup_{i=1}^n f^{-1}(x_i)$. Also, for each i, $f^{-1}(x_i)$ is closed and, since there is a finite number of them, also open, which implies that G has at least n connected components. That is, $n \leq |G : G^0|$.

□

3.3 Solvability of algebraic groups

The aim of this section is to obtain a solvability condition for algebraic groups that will be needed in Theorem 6.1.3.

Definition 3.3.1. Let X be a topological space. We define the *dimension* of X, denoted $\dim X$, as the supremum of all integers n such that there exists a chain $Z_0 \subsetneq \cdots \subsetneq Z_n$ of irreducible closed subsets of X.

It is a well-known result that affine varieties have finite dimension (see [3, Corollary 9.5]). This implies that any non-empty family of irreducible varieties has a maximal element.

Lemma 3.3.1. *Let U and V be two open dense subsets of an algebraic group G. Then $G = UV$.*

Proof. Let $x \in G$. Since inversion in G is a homeomorphism, V^{-1} is also an open set, as well as its coset xV^{-1}. Therefore $xV^{-1} \cap U \neq \emptyset$, that is, there exist $u \in U$ and $v \in V$ such that $xv^{-1} = u$, which implies $x = uv \in UV$. □

Remark 3.3.1. If G is irreducible and $Y \subseteq G$ is a dense constructible set then $Y = \cup_{i=1}^n (U_i \cap C_i)$ with U_i and C_i (non-empty) open and closed sets respectively. Since G is irreducible and $G = \overline{Y} = \cup_{i=1}^n \overline{U_i \cap C_i}$ then $G = \overline{U_i \cap C_i}$ for some $1 \leq i \leq n$. But $\overline{U_i \cap C_i} \subseteq \overline{C_i} = C_i$ and $\overline{U_i \cap C_i} \subseteq \overline{U_i}$, so $G = C_i = \overline{U_i}$, hence U_i is dense in G and $U_i = U_i \cap C_i \subseteq Y$. Therefore the lemma is valid for U and V dense constructible sets.

Lemma 3.3.2. *Let G be an algebraic group and $f_i : X_i \longrightarrow G$, $i \in I$ a family of morphisms from irreducible varieties X_i to G such that $e \in Y_i = f_i(X_i)$ for all $i \in I$. If M is the subgroup generated by all Y_i then M is connected.*

Proof. For each $a = (a_1, \ldots, a_n)$ finite sequence in I define $Y_a := Y_{a_1} \ldots Y_{a_n}$, that is, the image of the morphism $\varphi_a : X_{a_1} \times \cdots \times X_{a_n} \longrightarrow G$ given by $\varphi_a(x_1, \ldots, x_n) = x_1 \ldots x_n$. Let us see that, for all a, $\overline{Y_a}$ is irreducible (hence connected): suppose $\overline{Y_a} = A \cup B$ with A and B closed sets, then $X_{a_1} \times \cdots \times X_{a_n} = \varphi^{-1}(Y_a) = \varphi^{-1}(A) \cup \varphi^{-1}(B)$; now, $\varphi^{-1}(A)$ and $\varphi^{-1}(B)$ are closed because φ is continuous and $X_{a_1} \times \cdots \times X_{a_n}$ is irreducible as it is a product of irreducible sets so (without loss of generality) $X_{a_1} \times \cdots \times X_{a_n} = \varphi^{-1}(A)$, this implies that $Y_a \subseteq A$ and therefore $\overline{Y_a} = A$ because A is closed.

Let a and b be two finite sequences in I and consider (a, b) the sequence obtained by juxtaposition of a and b. For each $x \in Y_a$ the map $y \longmapsto xy$ is a morphism from Y_b to $Y_{(a,b)}$, so, by continuity, sends $\overline{Y_b}$ to $\overline{Y_{(a,b)}}$, that is, $Y_a\overline{Y_b} \subseteq \overline{Y_{(a,b)}}$. Applying continuity again $\overline{Y_a}\,\overline{Y_b} \subseteq \overline{Y_{(a,b)}}$. Now let a such that $\overline{Y_a}$ is a maximal element in $\{\overline{Y_b} \colon b \text{ finite sequence in } I\}$. Then, for every b we get $\overline{Y_a} \subseteq \overline{Y_a}\,\overline{Y_b} \subseteq \overline{Y_{(a,b)}}$, so $\overline{Y_a}\,\overline{Y_b} = \overline{Y_a}$ and $Y_b \subseteq \overline{Y_a}$. Taking $b = a$ we get $\overline{Y_a}\,\overline{Y_a} = \overline{Y_a}$ and choosing b such that $Y_b = Y_a^{-1}$ (enlarging I if necessary to include the morphisms $x \longmapsto f_i(x)^{-1}$), $\overline{Y_a}\,\overline{Y_a}^{-1} = \overline{Y_a}$, this two facts imply that $\overline{Y_a}$ is a (closed) subgroup of G. Therefore $\overline{M} \subseteq \overline{Y_a}$ and then (since the other inclusion is clear from the definitions) $\overline{M} = \overline{Y_a}$. Hence $\overline{M}$ is connected.

Finally, since Y_a is constructible by Chevalley's Theorem 3.1.8, the remark after Lemma 3.3.1 implies $\overline{Y_a} = Y_aY_a \subseteq M$. So $M = \overline{M}$ is connected. □

Proposition 3.3.3. *Let A and B be subgroups of an algebraic group G. If A is closed and connected, then $[A, B]$ is connected. In particular $[G, G]$ is connected if G is connected.*

Proof. We have that A is a connected algebraic group so, since connected and irreducible components are the same by Theorem 3.2.1 (ii), A is an irreducible variety. For each $b \in B$ consider the morphism of varieties $f_b : A \longrightarrow G$ given by $f_b(a) = [a, b]$. Clearly $e = f_b(e) \subseteq f_b(A)$ for all $b \in B$ and the subgroup generated by all $f_b(A)$ is precisely $[A, B]$. Hence Lemma 3.3.2 implies the result. □

Lemma 3.3.4. *Let G be an algebraic group and H a closed normal subgroup of G such that G/H is abelian. If H^0 is solvable then G^0 is solvable.*

Proof. Since G/H is abelian then $[G, G] \subseteq H$ and hence $[G^0, G^0] \subseteq H$. By Proposition 3.3.3, $[G^0, G^0]$ is connected, so it must be contained in a connected component of H. That implies $[G^0, G^0] \subseteq H^0$ and therefore

$[G^0, G^0]$ is solvable (because H^0 is solvable by hypothesis), whence G^0 is solvable. □

3.4 Lie–Kolchin Theorem

Lemma 3.4.1. *Let K be an algebraically closed field and let M be a commuting set of $n \times n$ matrices over K. Then M is triangularizable.*

Proof. Let $V = K^n$ and consider M as a set of endomorphisms of V. Let $A \in M$ not a scalar matrix (notice that if M consists only of scalar matrices then we are done) and $\lambda \in K$ an eigenvalue of A (which exists because K is algebraically closed). Define $W = \ker(A - \lambda I)$ and notice that $0 \subsetneq W \subsetneq V$. If $B \in M$ and $w \in W$ then, since A commutes with B, $(A - \lambda I)(B(w)) = B((A - \lambda I)(w)) = 0$, so W is stable by the action of M. By induction there exists $v_1 \in V$ such that $\langle v_1 \rangle$ is stable by M. Then consider the action induced by M on $V/\langle v_1 \rangle$. By induction on n, there exists a basis $\overline{v_2}, \ldots, \overline{v_n}$ of $V/\langle v_1 \rangle$ such that $\langle \overline{v_2}, \ldots, \overline{v_i} \rangle$ is stable by the induced action of M for all $2 \leq i \leq n$. Then $v_1, \ldots, v_n$ is a basis of V such that $\langle v_1, \ldots, v_i \rangle$ is stable by the action of M for all $1 \leq i \leq n$. That is, such basis triangularizes M. □

Theorem 3.4.2 (Lie–Kolchin)**.** *Let K be an algebraically closed field and $G \leqslant GL_n(K)$ a connected solvable algebraic group. Then G is triangularizable.*

Proof. Let $V = K^n$ and consider G as endomorphisms of V. Assume that G is reducible (in the sense of representation theory), that is, that it has a non-trivial invariant subspace W of dimension m with $0 < m < n$ so that the elements of G can be written as

$$\begin{pmatrix} \varphi(x) & * \\ 0 & \psi(x) \end{pmatrix} \tag{3.1}$$

where $\varphi : GL_n(K) \longrightarrow GL_m(K)$ is induced by the restriction map $\varphi(x) = x_{|W}$ and $\psi : GL_n(K) \longrightarrow GL_{n-m}(K) \cong GL(V/W)$ is induced by the canonical projection $\psi(x)(v + W) = x(v) + W$. Now, $\varphi(G) \subseteq GL_m(K)$ is a connected (continuous image of a connected set) and solvable (homomorphic image of a solvable group) group, so by induction on n we get that $\varphi(G)$ is triangularizable. Analogously $\psi(G)$ is also triangularizable and therefore G is triangularizable. Hence, assume from now on that G is irreducible (in the sense of representation theory).

Consider $[G, G]$, which is connected by Proposition 3.3.3. Since G is solvable the derived series finishes at 1, so by induction assume $[G, G]$ is triangularizable. Let W be the subspace generated by the common eigenvectors of the matrices of $[G, G]$. Notice that $W \neq 0$ because it at least

contains the first vector of the basis in which $[G, G]$ has triangular form. Now, since $[G, G]$ is normal in G we have that, if $A \in G$, $B \in [G, G]$ and $v \in W$, then $A^{-1}BAv = \lambda v$ for some $\lambda \in K$, that is, $BAv = \lambda Av$. Therefore $Av \in W$, which implies that W is invariant by G and hence (since G is irreducible) $W = V$. That is, $[G, G]$ is in fact diagonalizable (thus, assume it is in diagonal form).

Since $[G, G]$ is normal, the conjugates of its elements are also diagonal matrices, so they are obtained permuting the eigenvalues. Therefore they have finite conjugacy classes and by Theorem 3.2.1 (iv) this classes have only one element (because as G is connected, $G = G^0$). Whence $[G, G] \subseteq Z(G)$. Let $A \in [G, G]$ and let $\lambda \in K$ be an eigenvalue of A, then the corresponding eigenspace, $\ker(A - \lambda I)$ is invariant by G (as seen in the proof of Lemma 3.4.1). Then $\ker(A - \lambda I) = V$ and hence $A = \lambda I$. That is, $[G, G]$ consists of scalar matrices. Also, since the matrices of $[G, G]$ have determinant 1 they have to be given by n-th roots of unity. This implies that $[G, G]$ is finite and then, since it is connected, $[G, G] = 1$. Therefore G is abelian and by Lemma 3.4.1 it is triangularizable. □

Chapter 4

Linear differential equations

In the sequel all rings and fields will be assumed to have characteristic zero.

4.1 Linear differential equations over differential fields

Definition 4.1.1. Let K be a differential field. A *homogenous linear differential equation* (of order n) is a expression of the form

$$Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_0 Y = 0$$

with $a_{n-1}, \ldots, a_0 \in K$. We will usually denote it by $\mathcal{L}(Y) = 0$. If L/K is a differential extension of fields, an element $y \in L$ is a *solution* of $\mathcal{L}(Y) = 0$ if it satisfies $\mathcal{L}(y) = 0$, that is,

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

Proposition 4.1.1. *Let L/K be a differential extension of fields and $\mathcal{L}(Y) = 0$ a homogenous linear differential equation over K. Then, the set of solutions of $\mathcal{L}(Y) = 0$ in L, is a vector space over the field of constants of L, C_L.*

A useful tool to obtain information about the dimension of this vector space is the following:

Definition 4.1.2. Let K be a differential field. The *wrońskian (determinant)* of $y_1, \ldots, y_n \in K$ is defined as

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

Proposition 4.1.2. *Let K be a differential field. Then $y_1, \dots, y_n \in K$ are linearly independent over C_K if and only if $W(y_1, \dots, y_n) \neq 0$.*

Proof. Suppose $\sum_{i=1}^{n} c_i y_i = 0$ with $c_1, \dots, c_n \in C_K$ not all of them zero. Then, differentiating successively, $\sum_{i=1}^{n} c_i y_i^{(k)} = 0$ for all k. That is, the columns of the wrońskian are linearly dependent and therefore $W(y_1, \dots, y_n) = 0$.

For the converse suppose $W(y_1, \dots, y_n) = 0$ and let

$$r = \min\{m \in \{1, \dots, n\} \colon W(y_1, \dots, y_m) = 0\}$$

(notice that we can assume $r \geq 2$ because otherwise $y_1 = 0$ and this case is trivial). Then there exist $c_1, \dots, c_r \in K$ not all zero such that

$$\sum_{i=1}^{r} c_i y_i^{(k)} = 0 \tag{4.1}$$

for each $0 \leq k \leq r-1$ and the proof would be finished if we prove that $c_1, \dots, c_r$ are constants. We can assume $c_r = 1$ and then, differentiating the k-th equation in (4.1) and subtracting from it the $(k+1)$-th one we get

$$0 = \Big(\sum_{i=1}^{r-1} c_i' y_i^{(k)} + \sum_{i=1}^{r} c_i y_i^{(k+1)}\Big) - \sum_{i=1}^{r} c_i y_i^{(k+1)} = \sum_{i=1}^{r-1} c_i' y_i^{(k)}$$

for each $0, \leq k \leq r-2$. That is, a linear combination of the columns of a matrix whose determinant, $W(y_1, \dots, y_{r-1})$, is non-zero (by minimality of r), is zero, which implies $c_1' = \cdots = c_{r-1}' = 0$. □

Notice that this proposition allows us to say "linearly independent over constants" without specifying the field, that is because the value of the wrońskian does not depend on the field.

Corollary 4.1.3. *The dimension over the field of constants of the vector space of solutions of a homogenous linear differential equation is at most the order of the equation.*

Proof. If $y_1, \dots, y_{n+1}$ are solutions of a homogenous linear differential equation of order n, then the last row of the wrońskian, $(y_1^{(n)}, \dots, y_{n+1}^{(n)})$, is a linear combination of the other ones and therefore $W(y_1, \dots, y_{n+1}) = 0$. This implies, by Proposition 4.1.2, that $y_1, \dots, y_{n+1}$ are linearly dependent over constants. □

4.2 Picard–Vessiot extensions: existence and uniqueness

In order to develop differential Galois theory we need an analogue to the splitting field of a polynomial used in classical Galois theory. This analogue is given in the following definition:

Definition 4.2.1. Let K be a differential field and $\mathcal{L}(Y) = 0$ a homogenous linear differential equation over K of order n. Then L/K is a *Picard–Vessiot extension* for $\mathcal{L}$ if it is a differential extension of fields with the same constants and $L = K(y_1, \dots, y_n)'$ with $y_1, \dots, y_n$ a fundamental system of solutions of $\mathcal{L}(Y) = 0$ (that is, n solutions linearly independent over constants).

In this definition we require the extension to have the same constants for the same reason as we did in Definition 2.1.1. With $K = \mathbb{C}(x, e^x)$ and the equation $Y' - Y = 0$ we could construct $L = K(t)'$ with t transcendental over K such that $t' = t$, which would add undesired solutions to the equation.

Let us first construct a set that has similar properties: let $\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_0 Y = 0$ be a homogenous linear differential equation over a differential field K and consider the ring of polynomials $K[Y_{ij},\ 0 \leq i \leq n-1,\ 1 \leq j \leq n]$. Extend to it the derivation of K by defining

$$\begin{aligned} Y'_{ij} &= Y_{i+1,j},\ 0 \leq i \leq n-2,\ 1 \leq j \leq n, \\ Y'_{n-1,j} &= -a_{n-1}Y_{n-1,j} - \cdots - a_0 Y_{0,j},\ 1 \leq j \leq n. \end{aligned}$$

Notice that then it is differentially generated over K by $Y_{0,1}, \dots, Y_{0,n}$ and these are solutions of $\mathcal{L}(Y) = 0$. Now let $W = \det(Y_{i,j}) = W(Y_{0,1}, \dots, Y_{0,n})$ and let $R := K[Y_{i,j}][W^{-1}]$. Then R is called the *full universal solution algebra* of $\mathcal{L}$ and the idea is to factor out R by an appropriate ideal in order to obtain an integral domain whose field of fractions will be a Picard–Vessiot extension of $\mathcal{L}$. Notice that W is invertible in R, which implies that it will be non-zero in any non-trivial quotient of R and therefore $Y_{0,1}, \dots, Y_{0,n}$ will keep linearly independent over constants.

Lemma 4.2.1. *Let R be a differential commutative ring and let I be a maximal element in the set of proper differential ideals of R. Then I is a prime ideal of R.*

Proof. Consider the quotient R/I and call it again R; now we have to prove that R is an integral domain under the assumption that R has no proper differential ideals. Let $a, b \in R$, $a, b \neq 0$, such that $ab = 0$. Then let us prove by induction on k that $a^{(k)}b^{k+1} = 0$ for all $k \in \mathbb{N} \cup \{0\}$ (notice that we already have the base case as $ab = 0$): assume that $a^{(k-1)}b^k = 0$ holds and then, differentiating and multiplying by b this equality we obtain

$0 = (a^{(k)}b^k + ka^{(k-1)}b^{k-1}b')b = a^{(k)}b^{k+1}$.

This implies that if no power of b is zero then a and all its derivatives are zero divisors. In this case we can consider J the ideal generated by a and its derivatives, which is then a differential ideal that only contains zero divisors, hence $J \subsetneq R$. But also $0 \neq a \in J$, which gives that J is a proper differential idea, and this is a contradiction. This implies that b is nilpotent.

Since b is an arbitrary zero divisor, every zero divisor in R is nilpotent. In particular we can consider $a^n = 0$ with n minimal; then $0 = (a^n)' = na^{n-1}a'$; since $na^{n-1} \neq 0$ this implies that a' is a zero divisor. Again, a is an arbitrary zero divisor, so the derivative of a zero divisor is a zero divisor. We get that a and all its derivatives are zero divisors, which gives a contradiction considering the ideal generated by them. We conclude that R has no zero divisors. □

Lemma 4.2.2. *Let K be an algebraically closed field and R a finitely generated K-algebra without zero divisors. If $b \in R\backslash K$, then $b - c$ is a unit for at most finitely many $c \in K$.*

Proof. Let $R = K[x_1, \ldots, x_n]$, $K[X_1, \ldots, X_n]$ the ring of polynomials and $\varphi : K[X_1, \ldots, X_n] \longrightarrow R$ the homomorphism of K-algebras given by $\varphi(P(X_1, \ldots, X_n)) = P(x_1, \ldots, x_n)$. Then $R \cong K[X_1, \ldots, X_n]/I$ where $I = \ker(\varphi)$ is a prime ideal of $K[X_1, \ldots, X_n]$. We assume this is in fact an equality.

Let $S = V(I) \subseteq K^n$, which is an irreducible affine variety because I is a prime ideal. Let $b = f + I$ with $f \in K[X_1, \ldots, X_n]$. By Chevalley Theorem 3.1.8, $f(S) \subseteq K$ is finite or cofinite. If it is finite then, since it is also irreducible because S is irreducible, $f(S) = \{c\}$ is a single point; but this implies $f - c \in I(S) = I$ and therefore $b = c + I \in K$, which is a contradiction.

So $f(S)$ is cofinite. For each $c \in f(S)$, $(f - c)(x_1, \ldots, x_n) = 0$ has a solution $x_c \in S$; that is, $f - c \in I(x_c)$ where $I(x_c)$ is a maximal ideal of $K[X_1, \ldots, X_n]$ that contains I. Therefore $b - c = (f - c) + I \in I(x_c)/I$ is not invertible because otherwise $I(x_c)$ should be the whole ring. □

Proposition 4.2.3. *Let K be a differential field with algebraically closed field of constants, and let $K \subseteq R$ be a differential extension of rings such that R is an integral domain finitely generated as a K-algebra. If R has no proper differential ideals and L is the field of fractions of R, then $C_L = C_K$.*

Proof. Assume there exists $b \in C_L\backslash C_K$. Let $b = p/q$ with $p, q \in R$, $q \neq 0$, and let J be the ideal of denominators of b, that is, $J = \{h \in R \colon hb \in R\}$. In fact J is a differential ideal because $hb \in R$ implies $h'b = (hb)' \in R$. Then $J = R$, because R has no proper differential ideals and $0 \neq q \in J$. Therefore

$1 \in J$ and $b = 1 \cdot b \in R$.

Now, it is enough to find $c \in C_K$ such that $b - c$ is not invertible in R, because then $(b-c)' = 0$ and $(b-c)R$ is a differential ideal different from R, so it has to be $\{0\}$ and then $b = c \in C_K$. Let $\overline{K}$ be the algebraic closure of K and consider $\overline{R} = R \otimes \overline{K}$. Then we can apply Lemma 4.2.2 to $b \otimes 1 \in \overline{R} \backslash \overline{K}$ (notice that Exercise 2 implies $C_{\overline{K}} = C_K$ and therefore $b \notin \overline{K}$) and, since C_K is infinite, we get that there exists $c \in C_K$ such that $b \otimes 1 - c \otimes 1 = (b-c) \otimes 1$ is not invertible in $\overline{R}$; hence, $b - c$ is not invertible in R. □

Proposition 4.2.4. *Let L_1/K, L_2/K be differential extensions of field with the same field of constants as K, C, such that C is algebraically closed and L_1 and L_2 are finitely generated as K-algebras. Then there exist a differential extension of fields with the same constants, L/K, and differential homomorphisms $\sigma_1 : L_1 \longrightarrow L$ and $\sigma_2 : L_2 \longrightarrow L$.*

Proof. $L_1 \otimes_K L_2$ is a finitely generated K-algebra and $K \subseteq L_1 \otimes_K L_2$ is a differential extension of rings with the natural derivation in $L_1 \otimes_K L_2$ (see Example 1.2.2 (ii)). Let I be a maximal differential ideal of $L_1 \otimes_K L_2$, which, by Lemma 4.2.1, is prime, and consider $R = (L_1 \otimes_K L_2)/I$. Let L be the field of fractions of R. By Proposition 4.2.3 $C_L = C$. Finally, consider $\sigma_i : L_i \longrightarrow L$ given by $\sigma_1(x) = x \otimes 1 + I$ and $\sigma_2(x) = 1 \otimes x + I$, which are differential homomorphisms. □

The following two corollaries give (respectively) uniqueness and existence of a Picard–Vessiot extension.

Corollary 4.2.5. *Let L_1/K, L_2/K be two Picard–Vessiot extensions for a homogenous linear differential equation $\mathcal{L}(Y) = 0$ over K and assume that the field of constants C is algebraically closed. Then there exists $\sigma : L_1 \longrightarrow L_2$ a differential K-isomorphism.*

Proof. Let L, σ_1 and σ_2 be the field and differential homomorphisms given by Proposition 4.2.4. Let $V_1 \subseteq L_1$, $V_2 \subseteq L_2$ and $V \subseteq L$ be the C-vector spaces of solutions of $\mathcal{L}(Y) = 0$ in L_1, L_2 and L respectively. Clearly $\sigma_1(V_1), \sigma_2(V_2) \subseteq V$. If $\mathcal{L}$ has order n then, by definition of Picard–Vessiot extension, $\dim(V_1) = n = \dim(V_2)$, and by Corollary 4.1.3 $\dim(V) \leq n$, hence (since σ_1 and σ_2 are injective) $\sigma_1(V_1) = V = \sigma_2(V_2)$. Now, $L_1 = K(V_1)'$, $L_2 = K(V_2)'$ and σ_1 and σ_2 are K-linear, this implies that $\sigma = \sigma_2^{-1} \circ \sigma_1 : L_1 \longrightarrow L_2$ is a differential K-isomorphism. □

Corollary 4.2.6. *Let K be a differential field with algebraically closed field of constants C and let $\mathcal{L}(Y) = 0$ be a homogenous linear differential equation over K. Let R be the full universal solution algebra for $\mathcal{L}$ and let P be a maximal differential ideal of R. Then P is a prime ideal and the field of fractions of R/P is a Picard–Vessiot extension of K for $\mathcal{L}$.*

Proof. By Lemma 4.2.1 P is a prime ideal, so R/P is an integral domain and we can consider its field of fractions L. R is differentially generated (as a K-algebra) by solutions of $\mathcal{L}(Y) = 0$ so L is differentially generated over K (as a field) by solutions of $\mathcal{L}(Y) = 0$, and these solutions are linearly independent over constants because the wrońskian is invertible in R (in particular this implies that it is non-zero in R/P and hence, non-zero in L). Finally, by Proposition 4.2.3, L has the same constants as K, so it is a Picard–Vessiot extension for $\mathcal{L}$. □

4.3 Two properties of Picard–Vessiot extensions

Theorem 4.3.1. *Let L/K be a Picard–Vessiot extension with algebraically closed field of constants and $K \subseteq F \subseteq L$ an intermediate differential field. Then every differential K-homomorphism $\sigma : F \longrightarrow L$ extends of a differential K-automorphism of L.*

Proof. Let $F_1 = \sigma(F)$, which is also an intermediate differential field of L/K and notice that $\sigma : F \longrightarrow F_1$ is a K-isomorphism. Clearly L/F and L/F_1 are Picard–Vessiot extensions of the same equation as L/K and hence (by uniqueness), we can assume one of them is the one constructed in Corollary 4.2.6. That is, we assume $L = \mathrm{Fr}(R/P)$ with $R = F[Y_{ij}, W^{-1}]$ the full universal solution algebra with respect to F and P a maximal differential ideal.

Let $R_1 = F_1[Y_{ij}, W^{-1}]$ be the full universal solution algebra with respect to F_1 and then extend σ in a natural way to a K-isomorphism $\widetilde{\sigma} : R \longrightarrow R_1$. Let $P_1 = \widetilde{\sigma}(P)$, which is then a maximal differential ideal of R_1. Consider the map from R/P to R_1/P_1 given by $x + P \longmapsto \widetilde{\sigma}(x) + P_1$, it is clearly an isomorphism and can be extended to the fields of fractions, so $\widehat{\sigma} : L = \mathrm{Fr}(R/P) \longrightarrow \mathrm{Fr}(R_1/P_1)$ is an isomorphism extending σ. Finally, $\mathrm{Fr}(R_1/P_1)$ is a Picard–Vessiot extension of F_1, so by uniqueness there exists an F_1-isomorphism $\varphi : \mathrm{Fr}(R_1/P_1) \longrightarrow L$; and then $\overline{\sigma} = \varphi \circ \widehat{\sigma}$ is a differential K-automorphism of L extending σ. □

Theorem 4.3.2. *Let L/K be a Picard–Vessiot extension with algebraically closed field of constants and let $x \in L \backslash K$. Then there exists a differential K-automorphism $\sigma : L \longrightarrow L$ such that $\sigma(x) \neq x$.*

Proof. Let us first give a more specific version of Proposition 4.2.4, namely, if we fix $x_1 \in L_1 \backslash K$ and $x_2 \in L_2 \backslash K$ then we can require $\sigma_1(x_1) \neq \sigma_2(x_2)$. To prove this let $z = x_1 \otimes 1 - 1 \otimes x_2 \in L_1 \otimes_K L_2$. Clearly $z \neq 0$ because $x_1, x_2 \notin K$; also z is not nilpotent because a tensor product of fields of characteristic zero can not have nilpotent elements (see [4, Theorem 1.18]). The problem now is that z might be a zero-divisor. Let $J = \cup_{i \geq 1} \mathrm{Ann}(z^i)$. It is a proper differential ideal of $L_1 \otimes_K L_2$ (indeed

$xz^i = 0$ implies $0 = (xz^{i+1})' = x'z^{i+1} + (i+1)xz^iz' = x'z^{i+1})$. Also $z \notin J$ (because it is not nilpotent). Then $\overline{0} \neq \overline{z} \in (L_1 \otimes_K L_2)/J$ and $\overline{z}$ is not a zero-divisor. Therefore we can consider the ring $R_1 = ((L_1 \otimes_K L_2)/J)[\overline{z}^{-1}]$ and I a maximal differential ideal of it. Let $R = R_1/I$. Since $\overline{z}$ is invertible in R_1 we get that $\overline{z} + I \neq 0$ in R and the rest of the proof of this part is analogous to the one of Proposition 4.2.4.

Now, apply this result to $L_1 = L_2 = L$ and $x_1 = x_2 = x$. We get F/K, a differential extension of fields with the same constants, and $\sigma_1, \sigma_2 : L \longrightarrow F$ differential homomorphisms with $\sigma_1(x) \neq \sigma_2(x)$. Finally, as $\sigma_1(L) = \sigma_2(L)$, $\sigma = \sigma_2^{-1} \circ \sigma_1$ is a K-automorphism of L with $\sigma(x) \neq x$. □

Chapter 5

Differential Galois theory

5.1 The Galois group of a Picard–Vessiot extension

Definition 5.1.1. Let L/K be a differential extension of fields. Then the *differential Galois group* of the extension is the group of differential K-automorphisms of L. It is denoted $\mathrm{Gal}(L/K)$.

Lemma 5.1.1. *Let L/K be a finitely generated extension of fields, $L = K(u_1, \ldots, u_n)$ and $\sigma : K[u_1, \ldots, u_n] \longrightarrow K[u_1, \ldots, u_n]$ a surjective homomorphism of K-algebras. Then σ is an isomorphism of K-algebras and therefore it can be extended to a K-automorphism of L.*

Proof. We need to prove that σ is injective. Let $u \in \ker \sigma$, $u \neq 0$. Suppose u is algebraic over K and let $m(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ be its minimal polynomial. Then $m(u) = 0$ and, applying σ, we get $0 = \sigma(u)^n + a_{n-1}\sigma(u)^{n-1} + \cdots + a_0 = a_0$, which contradicts m being an irreducible polynomial. Then u is transcendental over K.

Let $w_1, \ldots, w_k \in K[u_1, \ldots, u_n]$ be an algebraically independent set with k as large as possible (notice that k is at most the transcendence degree of L/K, which is finite). Since σ is surjective let $w_i = \sigma(v_i)$ with $v_i \in K[u_1, \ldots, u_n]$ for each $i \in \{1, \ldots, k\}$. By the maximality of k we get that $u, v_1, \ldots, v_k$ are not algebraically independent, that is, there exists $P \in K[X, X_1, \ldots, X_k]$, $P \neq 0$, such that $P(u, v_1, \ldots, v_k) = 0$. Choose this P such that $X \nmid P$ (this is possible because otherwise u would be a zero-divisor, but it is inside a field). Since u is transcendental over K, $P(u, X_1, \ldots, X_k) \neq 0$ and then (extending σ by $\sigma(X_i) = X_i$), $\sigma(P(u, X_1, \ldots, X_k)) = P(0, X_1, \ldots, X_k) \neq 0$ but $0 = \sigma(P(u, v_1, \ldots, v_k)) = P(0, w_1, \ldots, w_k)$, which contradicts that $w_1, \ldots, w_k$ are algebraically independent. We conclude that $\ker \sigma = 0$ and then σ is an isomorphism. □

Theorem 5.1.2. *The Galois group of a Picard–Vessiot extension is an algebraic group over the field of constants of the extension.*

Proof. Let $L = K(y_1, \dots, y_n)'$ where $y_1, \dots, y_n$ is a fundamental set of solutions of the homogenous linear differential equation. If $V = \langle y_1, \dots, y_n \rangle$ is the C_K-vector space of solutions of the equation, a differential K-automorphism of L, σ, can be seen as a linear automorphism of V (since it has to send solutions of the equation to solutions of the equation) and knowing how it acts on V is enough to know how it acts on L. So, σ can be described as $(\sigma(y_1), \dots, \sigma(y_n)) = (y_1, \dots, y_n)C$ where C is an invertible matrix of constants. We have to prove that such σ exists if and only if the entries of C satisfy a set of polynomial relations $S \subseteq C_K[X_{ij}, 1 \leq i, j \leq n]$.

Let $Z_1, \dots, Z_n$ be indeterminates and consider the diagram

$$\begin{array}{ccc} K[Z_1, \dots, Z_n]' & \xrightarrow{\varphi} & L \\ \Big\downarrow{\scriptstyle \psi} & & \\ L[X_{ij}, 1 \leq i, j \leq n] & \xrightarrow{\rho} & L \end{array}$$

where $X'_{ij} = 0$, $\varphi(Z_i) = y_i$, $(\psi(Z_1), \dots, \psi(Z_n)) = (y_1, \dots, y_n)(X_{ij})$ and $\rho(X_{ij}) = c_{ij}$ (with $C = (c_{ij})$ a given invertible matrix of constants). Let $\Gamma = \ker \varphi$. The set $\psi(\Gamma)$ consists of polynomials in the variables $\{X_{ij}\}$ with coefficients in L; we fix a C_K-basis $\{w_\alpha\}_{\alpha \in A}$ of L and consider the set of polynomials S that appear as coefficients of each w_α when writing the coefficients of polynomials in $\psi(\Gamma)$ in terms of this basis. It is clear that the entries of the matrix C satisfy the polynomial relations of S if and only if $\psi(\Gamma) \subseteq \ker \rho$.

It is now left to prove that there exists a differential K-automorphism σ of L such that $(\sigma(y_1), \dots, \sigma(y_n)) = (y_1, \dots, y_n)C$ if and only if $\psi(\Gamma) \subseteq \ker \rho$. If there exists such σ, the diagram is commutative (considering σ on the right, from top to bottom) and then $\rho(\psi(\Gamma)) = \sigma(\varphi(\Gamma)) = 0$, that is, $\psi(\Gamma) \subseteq \ker \rho$. Conversely, if $\psi(\Gamma) \subseteq \ker \rho$ we can factor $K[Z_1, \dots, Z_n]'$ by Γ and get a differential K-isomorphism $\overline{\varphi} : K[Z_1, \dots, Z_n]'/\Gamma \longrightarrow \operatorname{Im} \varphi = K[y_1, \dots, y_n]'$ given by $\overline{\varphi}(\overline{x}) = \varphi(x)$ and a differential K-homomorphism $\overline{\rho \circ \psi} : K[Z_1, \dots, Z_n]'/\Gamma \longrightarrow L$ given by $\overline{\rho \circ \psi}(\overline{x}) = \rho \circ \psi(x)$. With that we obtain a differential K-homomorphism $\sigma = \overline{\rho \circ \psi} \circ \overline{\varphi}^{-1} : K[y_1, \dots, y_n]' \longrightarrow K[y_1, \dots, y_n]'$, which is surjective because $(\sigma(y_1), \dots, \sigma(y_n)) = (y_1, \dots, y_n)C$. Therefore, by Lemma 5.1.1, σ can be extended to a differential K-automorphism of L. □

Example 5.1.1. Let K be a differential field and let $K(t)/K$ be a transcendental differential extension with the same constants.

(i) If $t' = a \in K^\times$ then 1 and t are solutions of $Y'' - (a'/a)Y' = 0$, linearly independent over constants and $K(1,t)' = K(t)$, so $K(t)/K$ is a Picard–Vessiot extension. If $\sigma \in \mathrm{Gal}(K(t)/K)$ then it can be described by the image of t (in general by the images of the solutions of the equation, but $\sigma(1) = 1$), which must be $\sigma(t) = bt + c$ with b and c constants. But also $a = \sigma(a) = (\sigma(t))' = ba$, so $b = 1$ and $\sigma(t) = t + c$. Conversely, for any constant c, $t \longmapsto t + c$ induces a K-automorphism of $K(t)$ which is differential. So

$$\mathrm{Gal}(K(t)/K) \cong \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} : c \in C_K \right\} \cong C_K.$$

(ii) If $t' = at$ with $a \in K$ then t is a solution of $Y' - aY = 0$ and $K(t)' = K(t)$, so $K(t)/K$ is a Picard–Vessiot extension. If $\sigma \in \mathrm{Gal}(K(t)/K)$, then it is given by $\sigma(t) = ct$ with c a constant (because $\sigma(t)^* = \sigma(t^*) = \sigma(a) = a = t^*$ and we can apply Exercise 6). Conversely, since t is transcendental over K, for any constant c the map $t \longmapsto ct$ induces a K-automorphism of $K(t)$ which is differential. So $\mathrm{Gal}(K(t)/K) \cong C_K^\times$.

5.2 The fundamental theorem of differential Galois theory

The fundamental theorem of differential Galois theory is analogous to the fundamental theorem of classical Galois theory. It gives a correspondence between the intermediate differential fields and the closed subgroups of the differential Galois group. This correspondence is given as follows: if L/K is a Picard–Vessiot extension and F is an intermediate differential field then L/F is also a Picard–Vessiot extension for the same equation and has differential Galois group $\mathrm{Gal}(L/F) = \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma_{|F} = \mathrm{id}_F\}$ and if H is a subgroup of $\mathrm{Gal}(L/K)$ we denote L^H the subfield of L fixed by H, that is, $L^H = \{x \in L \colon \sigma(x) = x, \forall \sigma \in H\}$ (which is in fact an intermediate differential field of L/K).

Lemma 5.2.1. *Let L/K be a differential extension of fields, $y_1, \ldots, y_n \in L$ and $g \in L[X_1, \ldots, X_n]'$ a differential polynomial. Let H and T be subgroups of $\mathrm{Gal}(L/K)$ such that $L^H = L^T$. Then $g(\sigma(y_1), \ldots, \sigma(y_n)) = 0$ for all $\sigma \in H$ if and only if $g(\sigma(y_1), \ldots, \sigma(y_n)) = 0$ for all $\sigma \in T$.*

Proof. By way of contradiction assume there exists $g \in L[X_1, \ldots, X_n]'$ such that $g(\sigma(y_1), \ldots, \sigma(y_n)) = 0$ for all $\sigma \in H$ but not for all $\sigma \in T$. Take this g with minimal number of non-zero monomials. We can assume that at least one coefficient of g is 1. Let $\tau \in H$ and consider the polynomial τg obtained by applying τ to the coefficients of g. Then, for each $\sigma \in H$, $(\tau g)(\sigma(y_1), \ldots, \sigma(y_n)) = \tau(g(\tau^{-1}\sigma(y_1), \ldots, \tau^{-1}\sigma(y_n))) = \tau(0) = 0$ (because

$\tau^{-1}\sigma \in H$). Hence we get that $(g-\tau g)(\sigma(y_1),\dots,\sigma(y_n)) = 0$ for each $\sigma \in H$ and $g-\tau g$ has less monomials than g (because the one with coefficient 1 in g vanishes), so, by the minimality assumption, $(g-\tau g)(\sigma(y_1),\dots,\sigma(y_n)) = 0$ for each $\sigma \in T$. If $g-\tau g$ was not identically zero we could find $a \in L$ such that $g - a(g-\tau g)$ had less monomials than g, but then $g - a(g - \tau g)(\sigma(y_1),\dots,\sigma(y_n))$ would be zero for all $\sigma \in H$ but not for all $\sigma \in T$, which would contradict minimality. So $g - \tau g = 0$, which means that the coefficients of g are fixed by τ. Since $\tau \in H$ was arbitrary we get that g has coefficients in $L^H = L^T$ and then, for any $\sigma \in T$, $g(\sigma(y_1),\dots,\sigma(y_n)) = (\sigma g)(\sigma(y_1),\dots,\sigma(y_n)) = \sigma(g(y_1,\dots,y_n)) = 0$, which is a contradiction and completes the proof. □

Theorem 5.2.2. *Let L/K be a Picard–Vessiot extension and H and T subgroups of* $\mathrm{Gal}(L/K)$ *such that $L^H = L^T$. Then $\overline{H} = \overline{T}$ (that is, they have the same Zariski closure).*

Proof. Since the Zariski closure of a set S is $\overline{S} = V(I(S))$, it is enough to prove that $I(H) = I(T)$. That is, we have to prove that if $f \in C[X_{ij}, 1 \leq i,j \leq n]$ is a polynomial (where C is the field of constants and n the order of the equation) that vanishes on H, then it also vanishes on T. Suppose $L = K(y_1,\dots,y_n)'$ and let

$$W = \begin{pmatrix} y_1 & \dots & y_n \\ y_1' & \dots & y_n' \\ \vdots & & \vdots \\ y_1^{(n-1)} & \dots & y_n^{(n-1)} \end{pmatrix}, \; B = \begin{pmatrix} X_1 & \dots & X_n \\ X_1' & \dots & X_n' \\ \vdots & & \vdots \\ X_1^{(n-1)} & \dots & X_n^{(n-1)} \end{pmatrix}$$

and $g(X_1,\dots,X_n) = f(W^{-1}B) \in L[X_1,\dots,X_n]'$, where $X_1,\dots,X_n$ are indeterminates (notice that W^{-1} is well-defined because the solutions are linearly independent over constants and therefore $\det(W)$ is the wrońskian). Then $g(\sigma(y_1),\dots,\sigma(y_n)) = 0$ for all $\sigma \in H$ (because after substitution of X_i by $\sigma(y_i)$, $W^{-1}B$ becomes the matrix defining σ), so, by Lemma 5.2.1, $g(\sigma(y_1),\dots,\sigma(y_n)) = 0$ for all $\sigma \in T$, which means that f vanishes in T. □

Theorem 5.2.3 (Fundamental theorem of differential Galois theory)**.** *Let L/K be a Picard–Vessiot extension with algebraically closed field of constants and differential Galois group $G = \mathrm{Gal}(L/K)$. Then the correspondences*

$$H \longmapsto L^H \;, \quad F \longmapsto \mathrm{Gal}(L/F)$$

define bijections between the Zariski closed subgroups $H \leqslant G$ and the intermediate differential fields $K \subseteq F \subseteq L$. Furthermore, if $H \leqslant G$ corresponds to $K \subseteq F \subseteq L$ by this correspondence then H is a normal subgroup of G if and only if F is G-invariant. In this case $G/H \cong \mathrm{Gal}(F/K)$.

Proof. If $K \subseteq F \subseteq L$ is an intermediate differential field then L/F is a Picard–Vessiot extension and $H = \mathrm{Gal}(L/F) \leqslant G$. Also, by Theorem 5.1.2, H and G are algebraic groups over the field of constants (which is the same for both) and hence H is closed in G. Let $K \subseteq F_1, F_2 \subseteq L$ be two intermediate differential subfileds such that $\mathrm{Gal}(L/F_1) = \mathrm{Gal}(L/F_2)$ and assume there exists $x \in F_2 \backslash F_1$. Then by Theorem 4.3.2 there exists $\sigma \in \mathrm{Gal}(L/F_1)$ such that $\sigma(x) \neq x$, a contradiction since $\sigma \in \mathrm{Gal}(L/F_2)$. Thus $F_2 \subseteq F_1$ and similarly $F_1 \subseteq F_2$. Now let H and T be closed subgroups of G such that $L^H = L^T$, then Theorem 5.2.2 implies $\overline{H} = \overline{T}$ and since they are closed this means that $H = T$. So the given maps are bijections.

Let H is a closed subgroup of G and $F = L^H$. Then $H = \mathrm{Gal}(L/F)$ and it is a normal subgroup if and only if for all $g \in G$, $h \in H$ and $x \in F$, $g^{-1}(h(g(x))) = x$, that is, $h(g(x)) = g(x)$, which means that $g(x) \in L^H = F$ and this is the definition of F being G-invariant. For the last claim let $\rho : G \longrightarrow \mathrm{Gal}(F/K)$ be the restriction homomorphism (that is, $\rho(\sigma) = \sigma_{|F}$), it is surjective by Theorem 4.3.1 and H is by definition its kernel. □

Observe that in the conditions of the theorem, if F/K is a Picard–Vessiot extension then F is G-invariant, and then the last part of the theorem applies. Conversely it is also true that if F is G-invariant then F/K is a Picard–Vessiot extension, but this is more difficult to prove (see [2, Proposition 6.3.5]). Fortunately for our purposes the following particular case is sufficient.

Theorem 5.2.4. *Let K be a differential algebraically closed field and $K(t)/K$ a transcendental differential extension with the same field of constants and $t' = at$ with $a \in K$. Then for every intermediate differential field $K \subseteq E \subseteq K(t)$, E/K is a Picard–Vessiot extension.*

Proof. Let $K \subsetneq E \subseteq K(t)$ be an intermediate differential field. By Exercise 8 (ii), $t^n \in E$ for some $n \in \mathbb{N}$ and then $K(t^n) \subseteq E \subseteq K(t)$. By the classical Galois theory, $E = K(t^d)$ for some $d|n$ and t^d is a solution of the differential equation $Y' - adY = 0$, hence E/K is a Picard–Vessiot extension. □

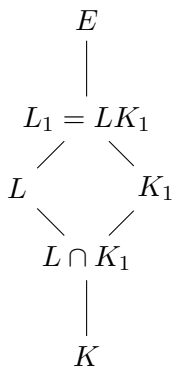
Chapter 6

Solvability of linear differential equations by quadratures

The aim of this chapter is to prove the analogue of the theorem in classical Galois theory about solvability by radicals of polynomial equations. Here we characterize when a linear differential equation over a differential field is solvable by quadratures. This means that we allow algebraic extensions, exponentials and integrals (notice that logarithms are also allowed since they can be represented as integrals). This type of solutions are the elements of what we will define as *generalized Liouville extensions*.

6.1 Solvability Theorem

Lemma 6.1.1. *Let E/K be a differential extension and $K \subseteq K_1, L \subseteq E$ with L/K a Picard–Vessiot extension. Let $L_1 = LK_1$, suppose that L_1 and L have the same field of constants C and that it is algebraically closed. Then L_1/K_1 es a Picard–Vessiot extension and its differential Galois group is isomorphic to the differential Galois group of $L/L \cap K_1$.*



Proof. If $L = K(y_1, \ldots, y_n)'$ then $L_1 = K_1(y_1, \ldots, y_n)'$, so L_1/K_1 is a Picard–Vessiot extension for the same homogenous linear differential equation as L/K. Thus we consider its differential Galois group $G = \mathrm{Gal}(L_1/K_1)$. If $\sigma \in G$ then $\sigma(L) = L$ because L_1 and L have the same constants (which implies that the space of solutions is the same for both fields). Then we can consider the restriction homomorphism $\rho : G \longrightarrow \mathrm{Gal}(L/K)$, which is injective because if $\sigma \in \ker \rho$ this means that σ fixes K_1 and L, so it also fixes $K_1 L = L_1$, that is, $\sigma = \mathrm{id}_{L_1} = 1_G$. So $G \cong H = \mathrm{Im}\rho$. Also, when thought as Zariski closed subsets of $\mathrm{GL}_n(C)$, $H = G$ and therefore H is a closed subgroup of $\mathrm{Gal}(L/K)$. By the Fundamental Theorem 5.2.3, $H = \mathrm{Gal}(L/L^H)$. Clearly $L^H \supseteq L \cap K_1$; conversely, if $x \in L \backslash (L \cap K_1)$, by Theorem 4.3.2 there exists $\sigma \in \mathrm{Gal}(L_1/K_1)$ such that $\sigma(x) \neq x$ and then $\rho(\sigma)(x) \neq x$, so $x \notin L^H$ and this completes the proof. □

Definition 6.1.1. Let M/K be a differential extension of fields with the same constants. We say it is a *Liouville extension* if there exists a chain of differential subfields $K = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ where, for each $1 \leq i \leq n$, $M_i = M_{i-1}(t_i)$ with $t_i' \in M_{i-1}$ or $t_i'/t_i = u_i$ with $u_i \in M_{i-1}$.

Lemma 6.1.2. *Let L/K be a Picard–Vessiot extension with algebraically closed field of constants. If there exist elements $u_1, \ldots, u_n \in L$ such that for each $\sigma \in \mathrm{Gal}(L/K)$ and $1 \leq j \leq n$*

$$\sigma(u_j) = a_{1j}u_1 + \cdots + a_{jj}u_j \tag{6.1}$$

with a_{ij} constants in L, then $K(u_1, \ldots, u_n)'$ is a Liouville extension of K.

Proof. Assume $u_1 \neq 0$ (otherwise it could be omitted) and let us prove the claim by induction on n (notice that the beginning of the proof will also serve as the base case for the induction). The first equation in (6.1) is $\sigma(u_1) = a_{11}u_1$, differentiating we obtain $\sigma(u_1') = a_{11}u_1'$ and dividing this equation by the previous one gives $\sigma(u_1'/u_1) = u_1'/u_1$. This holds for every σ, so $u_1'/u_1 \in L^{\mathrm{Gal}(L/K)} = K$, that is, $K(u_1)' = K(u_1)$ and it is a Liouville extension of K. Now divide every other equation in (6.1) by $\sigma(u_1) = a_{11}u_1$ to obtain

$$\sigma\left(\frac{u_j}{u_1}\right) = \frac{a_{1j}}{a_{11}} + \frac{a_{2j}}{a_{11}}\frac{u_2}{u_1} + \cdots + \frac{a_{jj}}{a_{11}}\frac{u_j}{u_1}$$

and differentiate to achieve

$$\sigma\left(\left(\frac{u_j}{u_1}\right)'\right) = \frac{a_{2j}}{a_{11}}\left(\frac{u_2}{u_1}\right)' + \cdots + \frac{a_{jj}}{a_{11}}\left(\frac{u_j}{u_1}\right)',$$

which is a set of equations with the same form as (6.1) but with one equation less. Thus, the inductive hypothesis implies that $M = K(u_1)((u_2/u_1)', \ldots, (u_n/u_1)')'$ is a Liouville extension of $K(u_1)$, but then $K(u_1, \ldots, u_n)' = M(t_2, \ldots, t_n)$ with $t_i = u_i/u_1$ and $t_i' = (u_i/u_1)' \in M$, so it is a Liouville

extension of M. Thus all intermediate extensions in $K \subseteq K(u_1) \subseteq M \subseteq K(u_1 \ldots, u_n)'$ are Liouville extensions, whereas $K(u_1 \ldots, u_n)'/K$ is a Liouville extension too. □

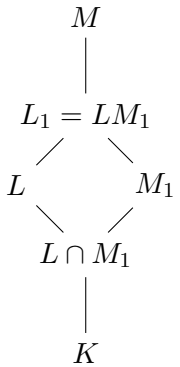
Definition 6.1.2. Let M/K be a differential extension of fields with the same constants. We say it is a *generalized Liouville extension* if there exists a chain of differential subfields $K = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ where, for each $1 \leq i \leq n$, $M_i = M_{i-1}(t_i)$ and M_i/M_{i-1} is algebraic or $t_i' \in M_{i-1}$ or $t_i' = u_i t_i$ with $u_i \in M_{i-1}$.

Theorem 6.1.3. *Let L/K be a Picard–Vessiot extension with algebraically closed field of constants. Then, the following are equivalent:*

(i) *there exists a generalized Liouville extension M/K with the same constants such that $L \subseteq M$;*

(ii) *the identity component G^0 of the differential Galois group $G = \mathrm{Gal}(L/K)$ is solvable.*

Proof. (i)⇒(ii): Let M/K be a generalized Liouville extension with the same constants such that $L \subseteq M$ and let $K = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ where, for each $1 \leq i \leq n$, $M_i = M_{i-1}(t_i)$ and M_i/M_{i-1} is algebraic or $t_i' \in M_{i-1}$ or $t_i' = u_i t_i$ with $u_i \in M_{i-1}$. Let us prove that the identity component G^0 of the differential Galois group $G = \mathrm{Gal}(L/K)$ is solvable by induction on n. Let $L_1 = LM_1 \subseteq M$. By Lemma 6.1.1, L_1/M_1 is a Picard–Vessiot extension and $\mathrm{Gal}(L_1/M_1) \cong \mathrm{Gal}(L/L \cap M_1) = H$. By the inductive hypothesis (since M/M_1 is a generalized Liouville extension with a chain of length one unit less) H^0 is solvable.



If M_1/K is algebraic it is also finite and then $L \cap M_1/K$ is finite. Exercise 11 (i) implies that $|G : H|$ is finite and then Theorem 3.2.1 (iii) implies $G^0 = H^0$ (so solvable). So suppose $M_1 = K(t)$ is transcendental and $t' \in K$ or $t' = at$ with $a \in K$ (so, as seen in Example 5.1.1, M_1/K is a Picard–Vessiot extension with abelian differential Galois group). If $t' \in K$ then

Exercise 8 (i) implies that $L \cap M_1 = K$ or $L \cap M_1 = M_1$ (so $L \cap M_1/K$ is a Picard–Vessiot extension) and if $t' = at$ with $a \in K$ then Theorem 5.2.4 implies that $L \cap M_1/K$ is a Picard–Vessiot extension. Therefore, the Fundamental Theorem 5.2.3 implies that H is a normal subgroup of G and that (seeing $L \cap M_1$ as a differential intermediate subfield first of L/K and then of M_1/K) $G/H \cong \mathrm{Gal}(L \cap M_1/K) \cong \mathrm{Gal}(M_1/K)/\mathrm{Gal}(M_1/L \cap M_1)$, so G/H is abelian. Finally, Lemma 3.3.4 implies that G^0 is solvable.

(ii)⇒(i): Consider $F = L^{G^0}$. Theorem 3.2.1 (ii) implies that G^0 has finite index in G, so Exercise 11 (ii) implies that F/K is a finite extension (hence algebraic). On the other hand L/F is a Picard–Vessiot extension and by the Fundamental Theorem 5.2.3 $\mathrm{Gal}(L/F) = G^0$. Since G^0 is by hypothesis solvable we can apply Lie–Kolchin Theorem 3.4.2 to get that it is triangularizable. Then we can apply Lemma 6.1.2 to obtain that L/F is a Liouville extension and therefore L/K is a generalized Liouville extension. □

6.2 Airy equation

Consider the Airy equation over $\mathbb{C}(x)$, $Y'' - xY = 0$, we will see that it cannot be solved by quadratures. It is known that it has two linearly independent solutions in the field of meromorphic functions in $\mathbb{C}$, so consider a Picard–Vessiot extension of it, L, inside this field. Let $G \subseteq \mathrm{GL}_2(\mathbb{C})$ be its differential Galois group.

Suppose that G^0 is solvable. Then Lie–Kolchin Theorem 3.4.2 implies that there exists a non-zero solution of the equation y such that for all $\sigma \in G^0$, $\sigma(y) = cy$ for some $c \in \mathbb{C}$. Then $\sigma(y') = cy'$ and hence $\sigma(y'/y) = y'/y$, that is, $y'/y = a \in L^{G^0}$, or equivalently $y' = ay$. It is known that the solutions of the Airy equation have infinitely many simple zeros (see [1, Theorem 1]), so this equality implies that $a = y^*$ has infinitely many poles (because a zero of y which is not a zero of y' must be a pole of a). But also G^0 has finite index in G, so Exercise 11 (ii) implies that a is algebraic over $\mathbb{C}(x)$ and this is impossible. Indeed, otherwise there would exist $p_n, \ldots, p_0 \in \mathbb{C}[x]$, $p_n \neq 0$, such that $p_n a^n + \cdots + p_0 = 0$, so every pole of a must be a zero of p_n (if $b \in \mathbb{C}$ is a pole of a of order m it is a pole of order km of a^k for all k, if it is not a zero of p_n then it is a pole of $p_n a^n$ of order nm and of order $\leq km < nm$ of $p_k a^k$ for all $0 \leq k \leq n-1$, so $p_n a^n \neq -p_{n-1}a^{n-1} - \cdots - p_0$) and hence p_n should be a polynomial with infinitely many zeros. Thus G^0 is not solvable. So, by Theorem 6.1.3, there does not exist a generalized Liouville extension $M/\mathbb{C}(x)$ such that $L \subseteq M$. Finally, Exercise 15 implies that the Airy equation does not have any solution in any generalized Liouville extension of $\mathbb{C}(x)$.

Let us now focus on finding G. Exercise 13 implies that the wrońskian of the equation w is a constant, that is, $w \in \mathbb{C}$. Therefore $G = \mathrm{Gal}(L/\mathbb{C}(x)) = \mathrm{Gal}(L/\mathbb{C}(x,w))$, so Exercise 14 implies that $G = G \cap SL_2(\mathbb{C})$, that is, $G \subseteq SL_2(\mathbb{C})$. Then G^0 is a non-solvable connected algebraic subgroup of $SL_2(\mathbb{C})$ and it is known that then it cannot be proper (see [2, Theorem 4.6.1]), so $G^0 = SL_2(\mathbb{C})$. Hence $G = SL_2(\mathbb{C})$.

Appendix A

Solved exercises

Exercise 1. Show that if F/K is an algebraic non-separable extension a derivation of K may not extend to a derivation of F or it might extend in more than one way.

Solution. Let $K = \mathbb{F}_2(X^2)$, $F = \mathbb{F}_2(X)$. In F, $(X^2)' = 2XX' = 0$ for any derivation $'$. Now a derivation in K can be defined by giving $(X^2)'$ any arbitrary value in K, for example:

- $(X^2)' = 1$ in K. This is impossible in F, so this derivation does not extend to F.
- $(X^2)' = 0$ in K. This is always true in F, so $X' = 0$ and $X' = 1$ define two possible extensions to F.

□

Exercise 2. Let F/K be an algebraic, separable, differential extension.

(i) Show that the field of constants of F is the set of the elements in F that are algebraic over the field of constants of K. Is this true if the extension is not separable?

(ii) Conclude that if $K(t)/K$ is a differential extension extension with the same constants and t is a transcendental element over K, then $F(t)$ and F also have the same constants.

Solution. (i) Let $\alpha \in F$ be algebraic over C_K, and let $m \in C_K[X]$ be its minimal polynomial. Then $\alpha' = -m^{(\mathrm{d})}(\alpha)/m'(\alpha)$, but $m^{(\mathrm{d})} = 0$, so $\alpha \in C_F$.

For the converse let $\alpha \in F \backslash K$ be a constant and $m \in K[X]$ its minimal polynomial, then $m'(\alpha) \neq 0$ and $\alpha' = -m^{(\mathrm{d})}(\alpha)/m'(\alpha) = 0$, so $m^{(\mathrm{d})}(\alpha) = 0$. Also, m is monic, which implies $\deg(m^{(\mathrm{d})}) < \deg(m)$ and therefore $m^{(\mathrm{d})} = 0$ (because m is the minimal polynomial of α and $m^{(\mathrm{d})}(\alpha) = 0$). This implies that the coefficients of m are constants, that is, $m \in C_K[X]$ and therefore

α is algebraic over C_K.

This is not true if F/K is not separable: for example $\mathbb{F}_2(X)/\mathbb{F}_2(X^2)$, $'$ defined by $X' = 1$. $(X^2)'$ must be 0 as seen in the previous exercise, so all the elements in $\mathbb{F}_2(X^2)$ are constants but X is algebraic over $\mathbb{F}_2(X^2)$ and it is not a constant.

(ii) $C_F \subseteq C_{F(t)}$ is trivial, so let us see the other inclusion. For that let $f \in C_{F(t)}$ and suppose $f \notin F$ (if $f \in F$ then clearly $f \in C_F$). Since $F(t)/K(t)$ is an algebraic, separable, differential extension then, by (i), $f \in C_{F(t)}$ if and only if f is algebraic over $C_{K(t)} = C_K \subseteq K$, and the elements in $F(t)$ that are algebraic over K are precisely the ones in F, so $f \in F$, which is a contradiction. □

Exercise 3. Let K be a field of characteristic 0 and consider the differential field $K(t)$, where the elements of K are constants, t is transcendental over K and $t' = 1$. Show that the field of constants of $K(t)$ is K. What is the field of constants of $K(t)$ if the characteristic of K is positive?

Solution. Let $p/q \in K(t)$ with $p, q \in K[t]$ coprime (and $q \neq 0$). Then $(p/q)' = (p'q - pq')/q^2 = 0$ if and only if

$$p'q - pq' = 0. \tag{A.1}$$

If $q' \neq 0$ then (A.1) implies $p/q = p'/q'$, but $\deg p' < \deg p$ and $\deg q' < \deg q$, so this contradicts p and q coprime. Therefore $q' = 0$ and (A.1) leaves us with $p'q = 0$, which implies $p' = 0$ (because $q \neq 0$). So, p/q is constant if and only if $p' = q' = 0$. In characteristic 0 this happens if and only if $p, q \in K$, which happens if and only if $p/q \in K$.

If char $K = n > 0$ then $p' = q' = 0$ if and only if there exist $p_1, q_1 \in K[t]$ such that $p(t) = p_1(t^n), q(t) = q_1(t^n)$. So $C_{K[t]} = \{p(t^n) \colon p \in K[t]\}$. □

Exercise 4. If K is a field we consider the usual derivation in the ring of formal power series $K[[x]]$ and the ring homomorphism $e : K[[x]] \longrightarrow K$ given by $e(\sum_{n=0}^{\infty} a_n x^n) = a_0$. Let R be a commutative differential ring and $\sigma : R \longrightarrow K$ a ring homomorphism. Show that if the characteristic of K is zero there exists a unique differential homomorphism $T_\sigma : R \longrightarrow K[[x]]$ such that $e \circ T_\sigma = \sigma$.

Solution. Let $r \in R$ and denote by $r_0, r_1, \cdots \in K$ the coefficients of $T_\sigma(r)$,

that is, $T_\sigma(r) = \sum_{n=0}^{\infty} r_n x^n$. Then:

$$\begin{aligned}
\sigma(r) &= e(T_\sigma(r)) = e\left(\sum_{n=0}^{\infty} r_n x^n\right) = r_0 \Rightarrow r_0 = \sigma(r) \\
\sigma(r') &= e(T_\sigma(r')) = e(T_\sigma(r)') = e\left(\sum_{n=1}^{\infty} n\, r_n x^{n-1}\right) = r_1 \Rightarrow r_1 = \sigma(r') \\
&\vdots \\
\sigma(r^{(k)}) &= e(T_\sigma(r^{(k)})) = e(T_\sigma(r)^{(k)}) = \\
&= e\left(\sum_{n=k}^{\infty} n(n-1)\dots(n-k+1)\, r_n x^{n-k}\right) = k!\, r_k \Rightarrow r_k = \frac{\sigma(r')}{k!}
\end{aligned}$$

So, this gives uniqueness as

$$T_\sigma(r) = \sum_{n=0}^{\infty} \frac{\sigma(r^{(n)})}{n!} x^n.$$

Let us now see that this in fact defines a differential homomorphism:

$$T_\sigma(1) = \sum_{n=0}^{\infty} \frac{\sigma(1^{(n)})}{n!} x^n = 1 + \sum_{n=1}^{\infty} \frac{\sigma(0)}{n!} x^n = 1$$

$$\begin{aligned}
T_\sigma(r_1 + r_2) &= \sum_{n=0}^{\infty} \frac{\sigma((r_1+r_2)^{(n)})}{n!} x^n = \sum_{n=0}^{\infty} \frac{\sigma(r_1^{(n)} + r_2^{(n)})}{n!} x^n = \\
&= \sum_{n=0}^{\infty} \frac{\sigma(r_1^{(n)}) + \sigma(r_2^{(n)})}{n!} x^n = \sum_{n=0}^{\infty} \frac{\sigma(r_1)^{(n)} + \sigma(r_2)^{(n)}}{n!} x^n = \\
&= \sum_{n=0}^{\infty} \frac{\sigma(r_1)^{(n)}}{n!} x^n + \sum_{n=0}^{\infty} \frac{\sigma(r_2)^{(n)}}{n!} x^n = T_\sigma(r_1) + T_\sigma(r_2)
\end{aligned}$$

$$T_\sigma(r_1\, r_2) = \sum_{n=0}^{\infty} \frac{\sigma((r_1\, r_2)^{(n)})}{n!} x^n = \sum_{n=0}^{\infty} \frac{\sigma(\sum_{k=0}^{n} \binom{n}{k} r_1^{(k)} r_2^{(n-k)})}{n!} x^n =$$
$$= \sum_{n=0}^{\infty} \frac{\sum_{k=0}^{n} \binom{n}{k} \sigma(r_1^{(k)}) \sigma(r_2^{(n-k)})}{n!} x^n =$$
$$= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{n!}{k!\,(n-k)!\,n!} \sigma(r_1^{(k)}) \sigma(r_2^{(n-k)}) x^n =$$
$$= \left(\sum_{n=0}^{\infty} \frac{\sigma(r_1)^{(n)}}{n!} x^n \right) \left(\sum_{m=0}^{\infty} \frac{\sigma(r_2)^{(m)}}{m!} x^m \right) = T_\sigma(r_1) T_\sigma(r_2)$$

$$T_\sigma(r)' = \left(\sum_{n=0}^{\infty} \frac{\sigma(r^{(n)})}{n!} x^n \right)' = \sum_{n=1}^{\infty} \frac{\sigma(r^{(n)})}{n!} n\, x^{n-1} = \sum_{n=1}^{\infty} \frac{\sigma(r^{(n)})}{(n-1)!} x^{n-1} =$$
$$= \sum_{n=0}^{\infty} \frac{\sigma(r^{(n+1)})}{n!} x^n = T_\sigma(r')$$

□

Exercise 5. (i) Let F/K be a differential algebraic extension with char $K = 0$. Show that if $u \in K$ and $u = v'$ for some $v \in F$, then in fact $u = w'$ for some $w \in K$ (that is, if u has a primitive in F, then it has a primitive in K). Conclude that if K and F have the same constants, $v \in K$. (Hint. Apply the trace map of the appropriate extension to the equality $u = v'$.)

(ii) Apply (i) to show that the functions $\log x$ and $\arctan x$ are transcendental.

Solution. (i) Let $L = K(v)$, N the normal closure of L over K and $[L : K] = n$. Then there exist n distinct K-homomorphisms $\tau_1, \ldots, \tau_n$ from L to N and the map $x \longmapsto Tr_{L/K}(x) = \sum_{i=i}^{n} \tau_i(x)$ is a group homomorphism from $(L, +)$ to $(K, +)$. Also, by Theorem 1.2.2, $\tau_1, \ldots, \tau_n$ are differential. So, we have:

$$Tr_{L/K}(u) = \sum_{i=i}^{n} \tau_i(u) = \sum_{i=i}^{n} u = n\, u$$
$$Tr_{L/K}(v') = \sum_{i=i}^{n} \tau_i(v') = \sum_{i=i}^{n} \tau_i(v)' = \Big(\sum_{i=i}^{n} \tau_i(v) \Big)' = Tr_{L/K}(v)'$$

and $u = v'$, so $u = w'$ with

$$w = \frac{1}{n}\, Tr_{L/K}(v) \in K.$$

If K and F have the same constants then $v' - w' = (v - w)' = 0$, so $v - w \in C_F = C_K \subseteq K$, which implies $v \in K$.

(ii) $(\log x)' = 1/x$ and $(\arctan x)' = 1/(1 + x^2)$ are both in $K(x)$ so, if the functions where algebraic, (i) would imply that they are in $K(x)$, which is not true. □

Exercise 6. Let K be a differential field. We define the *logarithmic derivative* of an element $u \in K$, $u \neq 0$, as $u^* = u'/u$. Show that $(uv)^* = u^* + v^*$ and $(u^{-1})^* = -u^*$ for any $u, v \in K^*$. Conclude that $(u^m)^* = mu^*$ for any integer m. Show that $u^* = v^*$ if and only if $u = cv$ for some non-zero constant $c \in K$. If $t, a, a_1, \ldots, a_r \in K, a \neq 0, t \neq a_i$, and $m_1, \ldots, m_r$ are integers, what is the logarithmic derivative of $u = a(t-a_1)^{m_1} \ldots (t-a_r)^{m_r}$?

Solution.

$$(uv)^* = \frac{u'v + uv'}{uv} = \frac{u'}{u} + \frac{v'}{v} = u^* + v^*$$

and

$$(u^{-1})^* = -\frac{u^{-2}u'}{u^{-1}} = -\frac{u'}{u} = -u^*.$$

The general case can be easily proven by induction: if $m = 0$, then $(u^0)^* = 1^* = 1'/1 = 0$, and now, for $m > 0$,

$$(u^m)^* = u^* + (u^{m-1})^* = u^* + (m-1)u^* = mu^*$$

and

$$(u^{-m})^* = (u^{-1})^* + (u^{-(m-1)})^* = -u^* - (m-1)u^* = -mu^*.$$

Now, $u^* = v^*$ if and only if $0 = (u/v)(u^* - v^*) = (u'v - uv')/v^2 = (u/v)'$, that is, if and only if $u/v = c$ is a constant (which is non-zero because u is non-zero).

Using these properties we can compute the required logarithmic derivative as:

$$\begin{aligned}(a(t-a_1)^{m_1} \ldots (t-a_r)^{m_r})^* &= a^* + ((t-a_1)^{m_1})^* + \cdots + ((t-a_r)^{m_r})^* = \\ &= a^* + m_1 (t-a_1)^* + \cdots + m_r (t-a_r)^* = \\ &= \frac{a'}{a} + m_1 \frac{t' - a_1'}{t - a_1} + \cdots + m_r \frac{t' - a_r'}{t - a_r}.\end{aligned}$$

□

Exercise 7. Show that the result in Exercise 5 (i) is still true if we replace the derivative $'$ by the logarithmic derivative * and if we just require w^* to be a multiple of u. (Hint. Use the trace and the norm maps of the appropriate extension as in Exercise 5.)

Solution. Using the same notation as in Exercise 5, that $x \longmapsto N_{L/K}(x) = \prod_{i=1}^{n} \tau_i(x)$ is a group homomorphism from $(L^*, \cdot)$ to $(K^*, \cdot)$ and that $\tau_i(x^*) = \tau_i(x'/x) = \tau_i(x')/\tau_i(x) = \tau_i(x)'/\tau_i(x) = \tau_i(x)^*$, we get:

$$Tr_{L/K}(u) = \sum_{i=i}^{n} \tau_i(u) = \sum_{i=i}^{n} u = n\,u$$
$$Tr_{L/K}(v^*) = \sum_{i=i}^{n} \tau_i(v^*) = \sum_{i=i}^{n} \tau_i(v)^* = \Big(\prod_{i=i}^{n} \tau_i(v)\Big)^* = N_{L/K}(v)^*$$

so nu has a logarithmic primitive

$$w = N_{L/K}(v) \in K^*.$$

If K and F have the same constants then $nv^* - w^* = (v^n/w)^* = 0$, so $v^n/w \in C_F = C_K \subseteq K$, which implies $v^n \in K$.

□

Exercise 8. Let $K(t)/K$ be a transcendental differential extension of fields of characteristic 0 with the same constants.

(i) Show that if $t' \in K$ there does not exist any proper intermediate differential subfield. Is this true in positive characteristic?

(ii) Show that if $t^* \in K$ and E is an intermediate differential subfield then $t^n \in E$ for some $n \in \mathbb{N}$.

Solution. (i) Let E be a differential field, $K \subsetneq E \subseteq K(t)$. Suppose $K(t)/E$ is algebraic, then, since $t' \in K \subset E$ and $C_{K(t)} = C_E$, Exercise 5 implies $t \in E$ and then $E = K(t)$. Let us see that in fact $K(t)/E$ is algebraic: let $f(t) = p(t)/q(t) \in E \backslash K$, $p(T), q(T) \in K[T]$, $q(t) \neq 0$, then $m(T) = q(T)f(t) - p(T) \in E[T]$ is a non-zero polynomial and $m(t) = 0$, which implies that t is algebraic over E.

This is not true if char $K = p$, because $K(t^p)$ is a proper intermediate field and $(t^p)' = 0$, so it is in fact a differential field.

(ii) With the same argument as before, since $K(t)/E$ is algebraic we get by Exercise 7 that $t^n \in E$ for some $n \in \mathbb{N}$.

□

Exercise 9. Let $K(t)/K$ be an extension of differential fields of characteristic 0 and suppose that $t' = u \in K$. Assume that u has no primitive in K. Notice that, by Exercise 5, t is transcendental over K.

(i) Prove that if $p(t) \in K[t]$ is a constant, then $p(t) = p_0 \in K$. (Hint. Show that if p has positive degree, $p(t)' = 0$ implies that u has a primitive in K.)

(ii) Prove that $K(t)$ and K have the same constants. (Suppose $p(t)/q(t)$ is a constant, where p and q are coprime polynomials and q is monic. Show that $q(t)|q(t)'$ and then apply (i) to conclude that $q(t) = 1$ and $p(t)$ is a constant in K.)

(iii) Conclude that if K is a differential field of characteristic 0 and $u_1, \ldots, u_n \in K$, there exists a differential extension F/K with the same constants such that the elements u_i have primitives in F.

(iv) Prove that the same results are true if $t^* = u \in K$, assuming that no multiple of u has logarithmic primitive in K.

Solution. (i) Suppose $p(t) = p_n t^n + \cdots + p_0$ with $n \geq 1$ and $p_n \neq 0$, then $p(t)' = p_n' t^n + (p_{n-1}' + n p_n u) t^{n-1} + \cdots + (p_0' + p_1 u)$. So, if $p(t)' = 0$ then p_n is a constant and $p_{n-1}' + p_n u = 0$, which implies $u = (-p_{n-1}/p_n)'$, a contradiction.

(ii) Suppose $p(t)/q(t) \in K$ with p and q coprime and q monic, is a constant. Then $p(t)'q(t) = p(t)q(t)'$, this implies that $q(t)|q(t)'$ but, since q is monic, q has strictly higher degree than $q(t)'$ and therefore q has degree 0 (so, since it is monic, $q(t) = 1$). Finally $p(t)/q(t) = p(t)$ is constant, so, applying (i), $p(t)$ is a constant in K.

(iii) Let $F_0 = K$. Then, for all $1 \leq i \leq n$, if u_i has a primitive in F_{i-1} let $F_i = F_{i-1}$, else let $F_i = F_{i-1}(t_1)$ with $t_i' = u_i$. By (ii) F_i and F_{i-1} have the same constants for all $1 \leq i \leq n$, so $F := F_n$ and K also have the same constants. It is clear that F/K is a differential extension and that every u_i has a primitive in F.

(iv) Let us follow a similar process as before. If $p(t)' = 0$ then $p_n' + n p_n u = 0$, so $-nu = p_n^*$; thus $p(t) = p_0 \in K$. If $q(t) = t^n + q_{n-1} t^{n-1} + \cdots + q_0$ and $q(t)|q(t)'$ then (looking at the leading coefficient) $q(t)' = (n-k)uq(t)$, so, for all $0 \leq k \leq n-1$, $q_k' = nuq_k$ which implies $q_k = 0$ (otherwise $(n-k)u = q_k^*$); hence $q(t) = t^n$. Then $(p(t)/q(t))' = (p(t)' - nup(t))/t^n = 0$ implies that $p_k' + (k-n)up_k = 0$ for every p_k coefficient of p. Again this implies that $p_k = 0$ for all $k \neq n$, so $p(t)/q(t) = p_n \in K$.

□

Exercise 10. Show that if g and h are polynomials, $\int \frac{e^g}{h}$ cannot be expressed in elementary terms unless g is constant or g is linear and h is constant. (Hint. Otherwise $1/h = a' + ag'$ for some non-zero rational function a. If a is a polynomial, h is constant and g is linear. A pole of a of multiplicity m is a zero of h of multiplicity $m+1$. If $a = p/q$, write $1/h = a' + ag'$ as a polynomial identity and compare degrees.)

Solution. If e^g/h has an elementary primitive then Theorem 2.3.2 implies that

$$1/h = a' + ag' \tag{A.2}$$

for some $a \in \mathbb{C}(x)$. If a is a polynomial then $a' + ag'$ is a polynomial, so h is constant and then $\deg(a' + ag') = 0$. But, if $g' \neq 0$, $\deg(a' + ag') = \deg(ag')$ (because a' has smaller degree than a) and then $0 = \deg(ag') = \deg(a) + \deg(g')$ implies $\deg(a) = \deg(g') = 0$, so g is linear.

If $b \in \mathbb{C}$ is a pole of a of multiplicity m then it is easy to see that it is a pole of a' of multiplicity $m+1$ and therefore, by (A.2), a pole of $1/h$ of multiplicity $m+1$ (that is, a zero of h of multiplicity $m+1$). Now, writing $a = p/q$ with p, q coprime polynomials, (A.2) gives

$$q^2 = (p'q - pq' + pqg')h. \tag{A.3}$$

It is clear that $\deg(pq) > p'q - pq'$ so, if $g' \neq 0$, (A.3) gives $\deg(q^2) = \deg(pqg'h)$ and this implies $\deg(q) = \deg(p) + \deg(g') + \deg(h) \geq \deg(h)$. But every zero of q (that is, a pole of a) is a zero of h with higher multiplicity, which gives $\deg(q) < \deg(h)$, a contradiction. □

Exercise 11. Let F/K be any extension of fields and G a group of K-automorphisms of F.

(i) Show that if $K \subseteq E \subseteq F$ and E/K is finite, then the subgroup H of E-automorphisms in G has finite index. (Hint. There are only finitely many K-homomorphisms $E \longrightarrow F$, so there exist finitely many $\sigma_1, \ldots, \sigma_n \in G$ such that any $\sigma \in G$ restricts to E as one of them.)

(ii) Show that if $H \leqslant G$ is a subgroup of finite index, F^H/F^G is a finite extension. (Hint. Let $n = |G : H|$ and take $n+1$ elements $u_1, \ldots, u_{n+1} \in F^H$. If G is the disjoint union of the cosets $\sigma_i H$, $1 \leq i \leq n$, there exist $\lambda_1, \ldots, \lambda_{n+1} \in F$ not all zero such that

$$\lambda_1 \sigma_i(u_1) + \cdots + \lambda_{n+1}\sigma_i(u_{n+1}) = 0,\ 1 \leq i \leq n.$$

Assume without loss of generality that $\lambda_1, \ldots, \lambda_{k-1} \neq 0$, $\lambda_k = 1$, $\lambda_i = 0, i > k$ with k as small as possible. Notice that the same relations hold with $\lambda_1, \ldots, \lambda_{n+1}$ replaced by $\sigma_j(\lambda_1), \ldots, \sigma_j(\lambda_{n+1})$. Conclude that $\lambda_i \in F^G$ for all i.)

Solution. (i) If E/K is a finite extension then there only exist at most $[E : K]$ K-homomorphisms $E \longrightarrow F$ for any field $F \supseteq E$ (the maximum being attained if $F \supseteq N$ with N the normal closure of E/K, and in fact this homomorphisms go from E to N). So there exist $\sigma_1, \ldots, \sigma_n \in G$ such that for any $\sigma \in G$, $\sigma_{|E} = \sigma_i$ for some $1 \leq i \leq n$. Then $\sigma_{|E}^{-1}\sigma_i$ is an E-automorphism of F, that is, $\sigma_{|E}^{-1}\sigma_i \in H$. This implies $\sigma H = \sigma_i H$, hence $G = \cup_{i=1}^n \sigma_i H$.

(ii) Suppose $H \leqslant G$ with $n = |G : H| < \infty$, so that $G = \cup_{i=1}^n \sigma_i H$. Take any $u_1, \ldots, u_{n+1} \in F^H$. Consider

$$\lambda_1 \sigma_i(u_1) + \cdots + \lambda_{n+1}\sigma_i(u_{n+1}) = 0,\ 1 \leq i \leq n,$$

which is a homogenous system of n linear equations and $n+1$ unknowns, so it has a solution with $\lambda_1 \ldots, \lambda_{n+1}$ not all zero. Assume, after reordering of the u_i if necessary, that $\lambda_1, \ldots, \lambda_{k-1} \neq 0$, $\lambda_k = 1$, $\lambda_i = 0$, $i > k$ with k as small as possible. Now take $\sigma \in G$ and apply it to each equation, then, for all $1 \leq i \leq n$, $\sum_{j=1}^{n+1} \sigma(\lambda_j)\,(\sigma\sigma_i)(u_j) = 0$. Notice that $\sigma\sigma_i = \sigma_{i'}\tau$ for some $1 \leq i' \leq n$, $\tau \in H$ and then $(\sigma\sigma_i)(u_j) = \sigma_{i'}(u_i)$. So $\sigma(\lambda_1), \ldots, \sigma(\lambda_n)$ is another solution of the system of equations which also satisfies $\sigma(\lambda_1), \ldots, \sigma(\lambda_{k-1}) \neq 0$, $\sigma(\lambda_k) = 1$, $\sigma(\lambda_i) = 0$, $i > k$. Therefore $\lambda_1 - \sigma(\lambda_1), \ldots, \lambda_n - \sigma(\lambda_n)$ is a solution of the system of equations with $\lambda_i - \sigma(\lambda_i) = 0$, $i \geq k$; this contradicts the minimality of k unless $\lambda_i - \sigma(\lambda_i) = 0$ for all $1 \leq i \leq n$. This implies $\lambda_1, \ldots, \lambda_n \in F^G$. In conclusion, any $u_1, \ldots, n_{n+1} \in F^H$ are linearly dependent over F^G (considering the equation in the system with $\sigma_i = \mathrm{id}$), which implies that F^H has dimension less than $n+1$ as an F^G-vector space, or equivalently, $[F^H : F^G] < n + 1 < \infty$.

□

Exercise 12. Consider a homogenous linear differential equation over $\mathbb{C}$ with constant coefficients:

$$Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y = 0,\ a_i \in \mathbb{C}.$$

(i) Show that if all the roots $\lambda_1, \ldots, \lambda_n$ of the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ are simple, the Picard–Vessiot extension of the equation over $\mathbb{C}$ is $\mathbb{C}(e^{\lambda_1 x}, \ldots, e^{\lambda_n x})$. What happens if the polynomial has mutiple roots?

(ii) Show that the Galois group of the differential equation is abelian.

(iii) Describe as an algebraic subgroup of $GL_3(\mathbb{C})$ the Galois group of the differential equation $4Y''' - 8Y'' - 3Y' + 9Y = 0$. Is it connected?

Solution. (i) For each λ_i it is easy to check that $e^{\lambda_i x}$ is a solution of the equation and these are linearly independent, so $\mathbb{C}(e^{\lambda_1 x}, \dots, e^{\lambda_n x})'$ is a Picard–Vessiot of the equation. But $e^{\lambda_i x} = \lambda_i e^{\lambda_i x} \in \mathbb{C}(e^{\lambda_i x})$, so $\mathbb{C}(e^{\lambda_1 x}, \dots, e^{\lambda_n x})' = \mathbb{C}(e^{\lambda_1 x}, \dots, e^{\lambda_n x})$.

If the roots $\lambda_1, \dots, \lambda_k$ of the polynomial have multiplicities $m_1, \dots, m_k$ respectively ($m_1 + \cdots + m_k = n$), then $e^{\lambda_1 x}, xe^{\lambda_1 x}, \dots, x^{m_1} e^{\lambda_1 x}, \dots, x^{m_k} e^{\lambda_k x}$ are n solutions of the equation linearly independent over constants. Therefore $\mathbb{C}(e^{\lambda_1 x}, xe^{\lambda_1 x}, \dots, x^{m_1} e^{\lambda_1 x}, \dots, x^{m_k} e^{\lambda_k x})' = \mathbb{C}(x, e^{\lambda_1 x}, \dots, e^{\lambda_k x})$ is a Picard–Vessiot extension of the equation.

(ii) Let G be the differential Galois group of the extension. If λ_i is a root of the polynomial then, in particular, $e^{\lambda_i x}$ is a solution of $Y' - \lambda_i Y = 0$ so, if $\sigma \in G$, $\sigma(e^{\lambda_i x})$ has to be a solution of the same equation. That is $\sigma(e^{\lambda_i x}) = ce^{\lambda_i x}$ for some $c \in \mathbb{C}$, $c \neq 0$. If the polynomial has multiple roots we also need to analyse $\sigma(x)$, similarly as before, $\sigma(x)' = \sigma(x') = \sigma(1) = 1$, so it must be $\sigma(x) = x + d$ for some $d \in \mathbb{C}$. Now let $\sigma, \tau \in G$, it is enough to check that they commute in an arbitrary generator $x^k e^{\lambda_i x}$. Suppose $\sigma(e^{\lambda_i x}) = c_1 e^{\lambda_i x}$, $\sigma(x) = x + d_1$, $\tau(e^{\lambda_i x}) = c_2 e^{\lambda_i x}$, $\tau(x) = x + d_2$ with $c_1, c_2, d_1, d_2 \in \mathbb{C}$, then

$$\begin{aligned}(\tau\sigma)(x^k e^{\lambda_i x}) = (\tau\sigma)(x)^k (\tau\sigma)(e^{\lambda_i x}) = \tau(x + d_1)^k \tau(c_1 e^{\lambda_i x}) = \\ = (x + d_1 + d_2)^k (c_1 c_2 e^{\lambda_i x}),\end{aligned}$$

which is clearly equal to $(\sigma\tau)(x^k e^{\lambda_i x})$. Whence G is abelian.

(iii) Let's first find the solutions of the equation, $4X^3 - 8X^2 - 3X + 9 = (x + 1)(2x - 3)^2$, so $e^{-x}, e^{3x/2}, xe^{3x/2}$ are solutions of the equation linearly independent over $\mathbb{C}$. Therefore $\mathbb{C}(x, e^{-x}, e^{3x/2}) = \mathbb{C}(x, e^{x/2})$ is a Picard–Vessiot of the equation. Then, if G is the differential Galois group of the extension, an element $\sigma \in G$ is characterized by the values $\sigma(x)$ and $\sigma(e^{x/2})$, as discussed in (ii) these have to be $\sigma(x) = x + a$ and $\sigma(e^{x/2}) = be^{x/2}$ with $a, b \in \mathbb{C}$, $b \neq 0$. Also, a map σ defined by a choice of a and b as $\sigma(x) = x + a$ and $\sigma(e^{x/2}) = be^{x/2}$ defines an automorphism, that is because x and $e^{x/2}$ are algebraically independent as well as $x + a$ and $be^{x/2}$; which is in fact a differential automorphism, since it is enough to check that it commutes with the derivation when applied to the generators. Then

$$\begin{aligned}\sigma(e^{-x}) &= \sigma(e^{x/2})^{-2} = b^{-2} e^{-x} \\ \sigma(e^{3x/2}) &= \sigma(e^{x/2})^3 = b^3 e^{3x/2} \\ \sigma(xe^{3x/2}) &= \sigma(x)\sigma(e^{x/2})^3 = (x + a) b^3 e^{3x/2}.\end{aligned}$$

Hence, when written in the basis $\{e^{-x}, e^{\frac{3x}{2}}, xe^{3x/2}\}$,

$$G = \left\{ \begin{pmatrix} b^{-2} & 0 & 0 \\ 0 & b^3 & ab^3 \\ 0 & 0 & b^3 \end{pmatrix} : a, b \in \mathbb{C}, b \neq 0 \right\}.$$

In fact $G \cong \mathbb{C} \times \mathbb{C}^\times$, so it is connected. □

Exercise 13. Compute w', where w is the wrońskian of n solutions of a homogenous linear differential equation of order n. When is w a non-zero constant? (Hint. Use the definition of determinant.)

Solution. Let $Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_0 Y = 0$ be the homogenous linear differential equation and $y_1, \ldots, y_n$ its solutions. Then

$$w = \begin{vmatrix} y_1 & \cdots & y_n \\ y_1' & \cdots & y_n' \\ \vdots & & \vdots \\ y_1^{(n-1)} & \cdots & y_n^{(n-1)} \end{vmatrix} = \sum_{\sigma \in \Sigma_n} \epsilon(\sigma) \prod_{k=0}^{n-1} y_{\sigma(k+1)}^{(k)}$$

and therefore

$$w' = \sum_{\sigma \in \Sigma_n} \epsilon(\sigma) \sum_{j=0}^{n-1} y_{\sigma(j+1)}^{(j+1)} \prod_{\substack{k=0 \\ k \neq j}}^{n-1} y_{\sigma(k+1)}^{(k)} = \sum_{j=0}^{n-1} \sum_{\sigma \in \Sigma_n} \epsilon(\sigma) y_{\sigma(j+1)}^{(j+1)} \prod_{\substack{k=0 \\ k \neq j}}^{n-1} y_{\sigma(k+1)}^{(k)} =$$

$$= \sum_{j=0}^{n-1} \begin{vmatrix} y_1 & \cdots & y_n \\ y_1' & \cdots & y_n' \\ \vdots & & \vdots \\ y_1^{(j-1)} & \cdots & y_n^{(j-1)} \\ y_1^{(j+1)} & \cdots & y_n^{(j+1)} \\ y_1^{(j+1)} & \cdots & y_n^{(j+1)} \\ \vdots & & \vdots \\ y_1^{(n-1)} & \cdots & y_n^{(n-1)} \end{vmatrix} = \begin{vmatrix} y_1 & \cdots & y_n \\ y_1' & \cdots & y_n' \\ \vdots & & \vdots \\ y_1^{(n-2)} & \cdots & y_n^{(n-2)} \\ y_1^{(n)} & \cdots & y_n^{(n)} \end{vmatrix} =$$

$$= \begin{vmatrix} y_1 & \cdots & y_n \\ y_1' & \cdots & y_n' \\ \vdots & & \vdots \\ y_1^{(n-2)} & \cdots & y_n^{(n-2)} \\ -a_{n-1}y_1^{(n-1)} - \cdots - a_0 y_1 & \cdots & -a_{n-1}y_n^{(n-1)} - \cdots - a_0 y_n \end{vmatrix} =$$

$$= -\sum_{j=0}^{n-1} a_j \begin{vmatrix} y_1 & \cdots & y_n \\ y_1' & \cdots & y_n' \\ \vdots & & \vdots \\ y_1^{(n-2)} & \cdots & y_n^{(n-2)} \\ y_1^{(j)} & \cdots & y_n^{(j)} \end{vmatrix} = -a_{n-1} \begin{vmatrix} y_1 & \cdots & y_n \\ y_1' & \cdots & y_n' \\ \vdots & & \vdots \\ y_1^{(n-2)} & \cdots & y_n^{(n-2)} \\ y_1^{(n-1)} & \cdots & y_n^{(n-1)} \end{vmatrix} = -a_{n-1} w.$$

Hence, w is a non-zero constant when $a_{n-1} = 0$ and $y_1, \dots, y_n$ are linearly independent over constants. □

Exercise 14. Show that if L/K is the Picard–Vessiot extension of a homogenous linear differential equation with wrońskian w and Galois group $G \subseteq GL_n(C)$, the subgroup corresponding to the differential subfield $K(w)$ under the Galois correspondence is $G \cap SL_n(C)$. (Hint. If $\sigma \in G$, what is the relation between $\sigma(w)$ and w?)

Solution. Let H be the required subgroup, that is, $H = \mathrm{Gal}(L/K(w))$. By definition $H = \{\sigma \in G\colon \sigma(w) = w\}$. Now, if $w = W(y_1, \dots, y_n)$ and $\sigma = (a_{ij}) \in G$, then $\sigma(w) = W(\sigma(y_1), \dots, \sigma(y_n))$. But $(\sigma(y_1)^{(j)}, \dots, \sigma(y_n)^{(j)}) = (y_1^{(j)}, \dots, y_n^{(j)})(a_{ij})$ for all $0 \le j \le n-1$, so $W(\sigma(y_1), \dots, \sigma(y_n)) = w \det(a_{ij}) = w \det \sigma$. Finally, $H = \{\sigma \in G\colon \det \sigma = 1\} = G \cap SL_n(C)$. □

Exercise 15. Show that if a second order homogenous linear differential equation has a solution in some (generalized) Liouville extension, then all the solutions can be found in an extension of the same type. (Hint. Consider the wrońskian and notice that any (non-homogeneous) first order linear differential equation can be solved by quadratures.)

Solution. Let K be the base field, $L = K(y_1, y_2)/K$ a Picard–Vessiot extension of the equation and assume $y_1 \in M$ with M/K a (generalized) Liouville extension. Consider $w = W(y_1, y_2) = y_1 y_2' - y_1' y_2$ and let $M_1 = M(w)$ (recall that by Exercise 13 $w' = -a_1 w$ with $a_1 \in K$). Then M_1/K is a (generalized) Liouville extension.

It is left to prove that $Y' + aY = b$ with $a, b \in M_1$ has a solution in a Liouville extension of M_1. Indeed consider $M_2 = M_1(t_2)$ with $t_2' = -a t_2$ and $M_3 = M_2(t_3)$ with $t_3' = b/t_2$; then M_3/M_1 is a Liouville extension and $y = t_2 t_3 \in M_3$ is a solution of $Y' + aY = b$:

$$y' = t_2' t_3 + t_2 t_3' = -a t_2 t_3 + t_2 b/t_2 = -ay + b.$$

(Notice that Exercise 9 implies that this process does not add new constants.) □

Bibliography

[1] Steven B. Bank and Ilpo Laine. On the oscillation theory of $f''+Af = 0$ where A is entire. *Transactions of the American Mathematical Society* **273**(1) 350-363, 1982.

[2] Teresa Crespo and Zbigniew Hajto. Algebraic groups and differential Galois theory. Graduate Studies in Mathematics volume 122. American Mathematical Society, Providence, Rhode Island, 2011.

[3] James S. Milne. Algebraic geometry (v5.20), 2009. Available at `www.jmilne.org/math/`.

[4] James S. Milne. Algebraic number theory (v3.03), 2011. Available at `www.jmilne.org/math/`.

[5] Maxwell Rosenlicht. Liouville's theorem on functions with elementary integrals. *Pacific Journal of Mathematics* **24**(1) 153-161, 1968.