(Preliminary) Lecture Notes

Algebraic Theory of Differential Equations

Michael Wibmer
February 25, 2021

Contents

Motivation

Can you solve the integral $\int e^{-x^2} dx$? You probably guess correctly that the answer is "no". (Maybe you have seen that integral before or maybe your guess is simply based on the psychology of introductions to mathematical texts.) But what exactly do we mean, when we say that this integral cannot be solved? And how can we actually *prove* that this integral cannot be solved? A crucial step towards answering these questions is to make precise the notion of solving (in elementary terms). This can most conveniently be done using extensions of *differential fields*. A differential field is a field K together with a *derivation*, i.e., a map $\delta\colon K \to K$ satisfying

$$\delta(f+g) = \delta(f) + \delta(g) \quad \text{and} \quad \delta(fg) = \delta(f)g + f\delta(g)$$

for all $f, g \in K$. Typical examples are the field $K = \mathbb{C}(x)$ of rational functions or the field of meromorphic functions on an open connected subset of $\mathbb{C}$, both equipped with the usual derivation $\delta = \frac{d}{dx}$. An *elementary function* is an element of an extension $L/\mathbb{C}(x)$ of differential fields such that $L = \mathbb{C}(x)(a_1, \ldots, a_n, b_1, \ldots, b_m)$, where $\delta(a_i) \in \mathbb{C}(x)$ and b_i is algebraic over $\mathbb{C}(x)(b_1, \ldots, b_{i-1})$ or $\frac{\delta(b_i)}{b_i} \in \mathbb{C}(x)(b_1, \ldots, b_{i-1})$. That is, an elementary function can be expressed using integrals of rational functions (e.g., we can use $\log(x) = \int \frac{1}{x} dx$), and iterations of taking roots of univariate polynomials (e.g., we can use $\sqrt{\frac{x}{1+x^2}}$) and exponentials of integrals (e.g., we can use $e^{\int \frac{1}{1+x^2} dx}$). For example, $e^{\int \sqrt[3]{\frac{x}{1+x^4}} dx} + 7e^{-x}\log(x)^5$ is an elementary function. However, as we will see, $\int e^{-x^2} dx$ is not an elementary function.

For solving a general homogeneous linear differential equation

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

say with rational function coefficients $a_i \in \mathbb{C}(x)$, an approach, similar to the above approach to solving integrals by elementary functions, can be taken. (Note that solving the integral $\int f dx$ is the same as solving the differential equation $y' = f$.) However, for the purpose of solving linear differential equations, it makes sense to replace the notion of an elementary function by the more general notion of a *Liouvillian function*. For example, if you ask your favorite computer algebra system to solve the differential equation $y'' + 2xy' = 0$, the answer $c_1 + c_2 \int e^{-x^2} dx$ seems perfectly acceptable. A function is Liouvillian if it belongs to a differential field extension L of $\mathbb{C}(x)$ such that $L = \mathbb{C}(x)(a_1, \ldots, a_n)$, where either

- a_i is algebraic over $\mathbb{C}(x)(a_1, \ldots, a_{i-1})$, or
- $\delta(a_i) \in \mathbb{C}(x)(a_1, \ldots, a_{i-1})$ ("a_i is an integral"), or
- $\frac{\delta(a_i)}{a_i} \in \mathbb{C}(x)(a_1, \ldots, a_{i-1})$ ("a_i is an exponential of an integral").

In the Galois theory of polynomials, a univariate polynomials is solvable (by radicals) if and only if its Galois group is solvable. A similar result holds in differential Galois theory. A linear differential equation is solvable in the sense that all its solutions are Liouvillian functions if and only if its *differential Galois group* is (virtually) solvable.

In contrast to the situation in polynomial Galois theory, the differential Galois group of a linear differential equation is usually not a finite group. However, it carries an additional structure that makes differential Galois groups much more accessible than arbitrary groups: The differential Galois group of a linear differential equation is an *algebraic group*. Roughly speaking, algebraic groups are subgroups of the general linear group GL_n that

can be defined by polynomials in the matrix entries, e.g., the special linear group SL_n or the orthogonal group O_n are algebraic groups. The theory of algebraic groups is very rich and powerful. Through the differential Galois correspondence this theory can be brought to bear on the study of the solutions of linear differential equations.

It turns out that many linear differential equations have no Liouvillian solutions. Therefore, finding explicit expressions for the solutions is often a futile goal that has to be abandoned. Instead, the central question becomes to describe the algebra of the solutions. Ideally, one hopes to be able to describe all algebraic relations among the solutions and their derivatives. In particular, the transcendence degree of the differential field generated by all solutions is an important invariant describing the complexity of the solutions. The algebraic relations among the solutions are governed by the differential Galois group. For example, the transcendence degree of the differential field generated by all solutions equals the dimension of the differential Galois group.

To be more concrete, let us consider Bessel's differential equation

$$x^2y'' + xy' + (x^2 - \alpha^2)y = 0,$$

where α is a complex parameter. It has two $\mathbb{C}$-linearly independent solutions, the Bessel functions $J_\alpha(x)$ and $Y_\alpha(x)$ of the first and second kind respectively. Any other solution is of the form $c_1J_\alpha(x) + c_2Y_\alpha(x)$, with $c_1, c_2 \in \mathbb{C}$. The differential field generated by all solutions is thus $L = \mathbb{C}(x)(J_\alpha(x), Y_\alpha(x), J'_\alpha(x), Y'_\alpha(x))$. What can we say about this differential field? E.g., what is the transcendence degree of $L/\mathbb{C}(x)$? Is is four or is there an algebraic relation among $J_\alpha(x), Y_\alpha(x), J'_\alpha(x), Y'_\alpha(x)$? It turns out that there is an algebraic relation, namely $J_\alpha(x)Y'_\alpha(x) - J'_\alpha(x)Y_\alpha(x) = \frac{2}{\pi x}$. So the transcendence degree is at most three, but is it exactly three? Are there any other algebraic relations? Knowing the differential Galois group is very helpful for answering this kind of questions. One can show that the differential Galois group of Bessel's equation is SL_2 if $\alpha - \frac{1}{2} \notin \mathbb{Z}$. The action of SL_2 on $L/\mathbb{C}(x)$ is given by sending the matrix $Y = \begin{pmatrix} J_\alpha(x) & Y_\alpha(x) \\ J'_\alpha(x) & Y'_\alpha(x) \end{pmatrix}$ to YC, for $C \in \mathrm{SL}_2(\mathbb{C})$. Note that $Y \mapsto YC$ defines an automorphism of the differential field L that fixes $\mathbb{C}(x)$. Conversely, one can show that any automorphism of the differential field L that fixes $\mathbb{C}(x)$, is of the form $Y \mapsto YC$ for a unique $C \in \mathrm{SL}_2(\mathbb{C})$. (This is what is meant, when we say that the differential Galois group of Bessel's equation is SL_2.)

Since SL_2 has dimension three, $L/\mathbb{C}(x)$ has transcendence degree three and the algebraic relation $J_\alpha(x)Y'_\alpha(x) - J'_\alpha(x)Y_\alpha(x) = \frac{2}{\pi x}$ is essentially the only algebraic relation among these four functions, i.e., any other algebraic relation is a consequences of this one. Moreover, since SL_2 is not solvable, we see that the Bessel functions $J_\alpha(x)$ and $Y_\alpha(x)$ are not Liouvillian functions. If $\alpha - \frac{1}{2} \in \mathbb{Z}$, the differential Galois group of Bessel's equation is the multiplicative group $\mathbb{G}_m = \mathrm{GL}_1$. As $\mathbb{G}_m$ is solvable and of dimension one, $L/\mathbb{C}(x)$ should have transcendence degree one and all solutions should be Liouvillian functions. Indeed, we have $L = \mathbb{C}(x)(\sqrt{x}e^{ix})$ and a $\mathbb{C}$-basis of the solution space is given by the Liouvillian functions $e^{\pm ix}\sum_{n=0}^{s} \frac{(s+n)!}{(s-n)!n!}(\pm i)^n 2^{-n} x^{-n-\frac{1}{2}}$, where $s = \alpha - \frac{1}{2}$ is assumed to be positive.

Historically, the questions surrounding "solving polynomial and differential equations" might have been the chief motivation for the development of Galois theory and differential Galois theory. However, contemporary differential Galois theory has many interesting open problems and connections to other mathematical areas that are not related to "solving". I hope to give you a glimpse at these topics during the course.

Conventions

All rings are assumed to be commutative and unital. The set of natural numbers contains zero, i.e., $\mathbb{N} = \{0, 1, 2, \ldots\}$. For a subset F of a ring R, we denote with (F) the ideal of R generated by F. The field of fractions of an integral domain R is denoted $\mathrm{Frac}(R)$.

Chapter 1

The basics of differential algebra

In this chapter we introduce the basic framework for the study of (ordinary) differential equations from an algebraic standpoint.

1.1 Differential rings and differential fields

Rings and fields are intimately connected with the study of the solutions of algebraic equations. In a similar vein, differential rings and differential fields are closely connected with the study of the solutions of differential equations. Just as commutative rings are the basic objects in commutative algebra, the basic objects in differential algebra are differential rings. Recall that, according to our conventions, all rings are commutative.

Definition 1.1.1. *Let R be a ring. A* derivation *on R is a map $\delta\colon R \to R$ satisfying $\delta(f+g) = \delta(f) + \delta(g)$ and the Leibnitz rule $\delta(fg) = \delta(f)g + f\delta(g)$ for all $f, g \in R$. A* differential ring*, or* δ-ring *for short, is a pair (R, δ) consisting of a ring R and a derivation δ on R. The* ring of constants *of a differential ring (R, δ) is $R^\delta = \{f \in R |\ \delta(f) = 0\}$.*

In case R is a field, (R, δ) is a called a *differential field* or *δ-field* for short. A morphism $\phi\colon (R, \delta) \to (R', \delta')$ between differential rings is a morphism $\phi\colon R \to R'$ of rings such that $\phi(\delta(f)) = \delta'(\phi(f))$ for all $f \in R$. In this situation we also call R' a *differential R-algebra* or an *R-δ-algebra* for short. A morphism of R-δ-algebras is a morphism of R-algebras that is a morphism of differential rings. Such morphism are sometimes also referred to as R-δ-morphisms. A *differential subring*, or *δ-subring* for short, of a δ-ring (R, δ) is a subring R' of R such that $\delta(R') \subseteq R'$. Then R', together with the map $\delta'\colon R' \to R',\ f' \mapsto \delta(f')$ is a differential ring. If (L, δ) is a differential field with a differential subring K that is a field, then (L, δ) is a *differential field extension* of (K, δ').

For brevity, we will often omit the derivation from the notation, e.g., we may to refer to R as a differential ring. Moreover, the same symbol δ is used to denote various different derivations. For example, if L/K is an extension of differential fields, we denote the derivation on L and the derivation on K with the same symbol δ.

Exercise 1.1.2. *Let (R, δ) be a differential ring. Show that R^δ is a subring of R. Moreover show that R^δ is a field in case (R, δ) is a field. (In this situation one usually speaks of the* field of constants*, rather than the ring of constants.)*

Example 1.1.3. Let I be an open interval in $\mathbb{R}$ (i.e., $I = (a, b)$, $I = (-\infty, b)$, $I = (a, +\infty)$ or $I = \mathbb{R}$ with $a, b \in \mathbb{R}$), then the ring $R = \mathcal{C}^\infty(I)$ of infinitely differentiable (=smooth) functions from I to $\mathbb{R}$ is a differential ring with derivation δ defined as usual, i.e.,

$$\delta(f)(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \tag{1.1}$$

for $f \in \mathcal{C}^\infty(I)$ and $x \in I$. Note that $R^\delta \simeq \mathbb{R}$ consists of the constant functions from I to $\mathbb{R}$ (hence the name constants!). If I' is an open interval in $\mathbb{R}$ such that $I' \subseteq I$, then the restriction map $\mathcal{C}^\infty(I) \to \mathcal{C}^\infty(I')$ is a morphism of differential rings. The ring of polynomial functions is a differential subring of $\mathcal{C}^\infty(\mathbb{R})$. Also for any fixed period $p > 0$, the subring of all p-periodic functions in $\mathcal{C}^\infty(\mathbb{R})$ is a differential subring.

Example 1.1.4. Let R be a ring and let $R[x]$ be the univariate polynomial ring over R. Since $\mathbb{R}[x]$ can be identified with the ring of polynomial function from $\mathbb{R}$ to $\mathbb{R}$, we see from Example 1.1.3 that $\mathbb{R}[x]$ is a differential ring with the "usual derivation" (1.1). Formula (1.1) does not make sense for an arbitrary ring R. However, the derivation $\delta\colon \mathbb{R}[x] \to \mathbb{R}[x]$ can also be described by

$$\delta(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1 \tag{1.2}$$

and this formula makes sense over arbitrary rings. We therefore define a map $\delta\colon R[x] \to R[x]$ by (1.2). It is straightforward to check that $\delta\colon R[x] \to R[x]$ is a derivation. This derivation is sometimes denoted with $\frac{d}{dx}$.

Example 1.1.5. Let k be a field and let $k((x)) = \{\sum_{n=m}^{\infty} a_n x^n |\ m \in \mathbb{Z},\ a_n \in k\}$ be the field of formal Laurent series over k. Then $k((x))$ is a differential field with derivation $\delta\colon k((x)) \to k((x))$ defined by

$$\delta\left(\sum_{n=m}^{\infty} a_n x^n\right) = \sum_{n=m}^{\infty} n a_n x^{n-1}.$$

Note that $k[x]$, with derivation defined as in Example 1.1.4, is a differential subring of $k((x))$. Again, this derivation is sometimes denoted with $\frac{d}{dx}$.

Exercise 1.1.6. *Find the field of constants of the differential field $k((x))$ with derivation defined as in Example 1.1.5.*

Example 1.1.7. Let R be any ring. Then $\delta\colon R \to R,\ f \mapsto 0$ is a derivation. The resulting differential ring (R, δ) is called a constant differential ring.

The following familiar rules also hold in our abstract algebraic setting:

Lemma 1.1.8. *Let (R, δ) be a differential ring and $f \in R$. Then*

(i) *$\delta(f^n) = nf^{n-1}\delta(f)$ for all $n \geq 1$ and*

(ii) *for $g \in R^\times$ we have $\delta(\frac{1}{g}) = \frac{-\delta(g)}{g^2}$ and more generally $\delta\left(\frac{f}{g}\right) = \frac{\delta(f)g - f\delta(g)}{g^2}$ (quotient rule).*

Proof. We prove (i) by induction on n. The case $n = 1$ is obvious. Using the induction hypothesis we compute

$$\delta(f^n) = \delta(ff^{n-1}) = \delta(f)f^{n-1} + f\delta(f^{n-1}) = \delta(f)f^{n-1} + f(n-1)f^{n-2}\delta(f) = nf^{n-1}\delta(f).$$

For (ii), note that $\delta(1) = \delta(1 \cdot 1) = \delta(1) \cdot 1 + 1 \cdot \delta(1) = 2\delta(1)$ and so $\delta(1) = 0$. Therefore $0 = \delta(1) = \delta(gg^{-1}) = \delta(g)g^{-1} + g\delta(g^{-1})$ and $\delta(g^{-1}) = \delta(g)g^{-2}$. In general,

$$\delta(fg^{-1}) = \delta(f)g^{-1} + f\delta(g^{-1}) = \delta(f)g^{-1} - f\delta(g)g^{-2} = (\delta(f)g - f\delta(g))g^{-2}.$$

□

Exercise 1.1.9. *Find all derivations $\delta\colon \mathbb{Q} \to \mathbb{Q}$.*

Exercise 1.1.10. *Let (R, δ) be a differential ring and let $R[x_1, \dots, x_n]$ be a polynomial ring over R, equipped with a derivation $\delta\colon R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ that extends $\delta\colon R \to R$. Show that*

(i) *$\delta(f) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}\, \delta(x_i) + f^{\delta}$ for all $f \in R[x_1, \dots, x_n]$, where $\frac{\partial f}{\partial x_i}$ is the formal derivative of f with respect to x_i and f^{δ} is the polynomial obtained from f by applying δ to the coefficients of f. (To be precise, $\frac{\partial f}{\partial x_i}$ is defined as in formula (1.2) with f considered as a univariate polynomial in the variable x_i.)*

(ii) *For any choice of $f_1, \dots, f_n \in R[x_1, \dots, x_n]$, there exists a unique derivation $\delta\colon R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ extending $\delta\colon R \to R$ with $\delta(x_1) = f_1, \dots, \delta(x_n) = f_n$.*

Exercise 1.1.11. *Let (R, δ) be a differential ring. Show that*

$$\delta^n(fg) = \sum_{k=0}^{n} \binom{n}{k} \delta^{n-k}(f)\delta^k(g)$$

for all $f, g \in R$.

Exercise 1.1.12. *Let (R, δ) be a differential ring and let $S \subseteq R$ be a multiplicatively closed subset. Show that there exists a unique derivation $\delta\colon S^{-1}R \to S^{-1}R$ such that the canonical map $R \to S^{-1}R$ is a morphism of differential rings. (In particular, if R is an integral domain, the derivation $\delta\colon R \to R$ extends uniquely to $\mathrm{Frac}(R)$, the field of fractions of R.*

As we will be working with tensor products a lot, it is important to understand how derivations and tensor products interact.

Lemma 1.1.13. *Let R be a δ-ring and let S and T be R-δ-algebras. Then there exists a unique derivation $\delta\colon S \otimes_R T \to S \otimes_R T$ such that the maps $S \to S \otimes_R T,\ s \mapsto s \otimes 1$ and $T \to S \otimes_R T,\ t \mapsto 1 \otimes t$ are morphisms of δ-rings. It is determined by*

$$\delta(s \otimes t) = \delta(s) \otimes t + s \otimes \delta(t)$$

for $s \in S$ and $t \in T$.

Proof. Define $\overline{\delta}\colon S \times T \to S \otimes_R T$ by $\overline{\delta}(s, t) = \delta(s) \otimes t + s \otimes \delta(t)$. Then $\overline{\delta}(s_1 + s_2, t) = \overline{\delta}(s_1, t) + \overline{\delta}(s_2, t)$ and $\overline{\delta}(s, t_1 + t_2) = \overline{\delta}(s, t_1) + \overline{\delta}(s, t_2)$ for $s, s_1, s_2 \in S$ and $t, t_1, t_2 \in T$. Moreover, for $r \in R$ we have

$$\begin{aligned}\overline{\delta}(rs, t) &= \delta(rs) \otimes t + rs \otimes \delta(t) = \delta(r)s \otimes t + r\delta(s) \otimes t + rs \otimes \delta(t) = \\ &= s \otimes \delta(r)t + s \otimes r\delta(t) + \delta(s) \otimes rt = s \otimes \delta(rt) + \delta(s) \otimes rt = \overline{\delta}(s, rt).\end{aligned}$$

Therefore, there exists a unique additive map $\delta\colon S \otimes_R T \to S \otimes_R T$ with $\delta(s \otimes t) =$

$\delta(s) \otimes t + s \otimes \delta(t)$ for $s \in S$ and $t \in T$. It remains to check the Leibniz rule. We have

$$\delta\left(\left(\sum_i s_i \otimes t_i\right) \cdot \left(\sum_j s'_j \otimes t'_j\right)\right) = \delta\left(\left(\sum_{i,j} s_i s'_j \otimes t_i t'_j\right)\right) =$$
$$= \sum_{i,j} \left(\delta(s_i s'_j) \otimes t_i t'_j + s_i s'_j \otimes \delta(t_i t'_j)\right) =$$
$$= \sum_{i,j} \left(\delta(s_i) s'_j \otimes t_i t'_j + s_i \delta(s'_j) \otimes t_i t'_j + s_i s'_j \otimes \delta(t_i) t'_j + s_i s'_j \otimes t_i \delta(t'_j)\right) =$$
$$= \sum_{i,j} \left(\delta(s_i) s'_j \otimes t_i t'_j + s_i s'_j \otimes \delta(t_i) t'_j\right) + \sum_{i,j} \left(s_i \delta(s'_j) \otimes t_i t'_j + s_i s'_j \otimes t_i \delta(t'_j)\right) =$$
$$= \left(\sum_i \left(\delta(s_i) \otimes t_i + s_i \otimes \delta(t_i)\right)\right) \cdot \left(\sum_j s'_j \otimes t'_j\right) + \left(\sum_i s_i \otimes t_i\right) \cdot \left(\sum_j \left(\delta(s'_j) \otimes t'_j + s'_j \otimes \delta(t'_j)\right)\right) =$$
$$= \delta\left(\sum_i s_i \otimes t_i\right) \cdot \left(\sum_j s'_j \otimes t'_j\right) + \left(\sum_i s_i \otimes t_i\right) \cdot \delta\left(\sum_j s'_j \otimes t'_j\right).$$

□

In the sequel we will always assume that the tensor product of differential algebras is equipped with the derivation as in Lemma 1.1.13.

Lemma 1.1.14. *Let K be a δ-field of characteristic zero and let L be an algebraic field extension. Then there exists a unique extension $\delta\colon L \to L$ of $\delta\colon K \to K$ to a derivation on L.*

Proof. It suffices to treat the case when $L = K(a)$ is a simple algebraic extension. Let $f \in K[x]$ be the minimal polynomial of a over K. Assume that $\delta\colon L \to L$ is an extension of $\delta\colon K \to K$. Applying δ to $f(a) = 0$ we find $0 = f^\delta(a) + f'(a)\delta(a)$, where $f^\delta \in K[x]$ is the polynomial obtained from f by applying δ to the coefficients and $f' = \frac{df}{dx} \in K[x]$ is the formal derivative of f with respect to x as in Example 1.1.4. Because K has characteristic zero, f' is non-zero and so also $f'(a)$ is non-zero because f' has degree smaller than f. Therefore $\delta(a) = -\frac{f^\delta(a)}{f'(a)}$. This proves the uniqueness.

For the existence, consider the derivation $\delta\colon K[x] \to K[x]$ that extends $\delta\colon K \to K$ and satisfies $\delta(x) = -f^\delta h$, where $h \in K[x]$ is such that $h(a) = f'(a)^{-1}$. Since $L \simeq K[x]/(f)$, it suffices to show that (f) is a δ-ideal. We have

$$\delta(f) = f^\delta + f'\delta(x) = f^\delta(1 - f'h).$$

Because $f'(a)h(a) = 1$, the polynomial f divides $1 - f'h$. Therefore $\delta(f) \in (f)$ and so $(f) \subseteq K[x]$ is a δ-ideal. □

Exercise 1.1.15. *Let K be a δ-field of characteristic zero. Then K^δ is relatively algebraically closed in K. I.e., if $a \in K$ is algebraic over K^δ, then $a \in K^\delta$.*

1.2 Differential ideals

The role of differential ideals in differential algebra is similar to the role of ideals in commutative algebra.

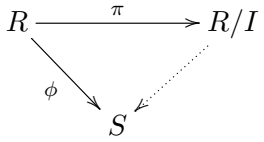
Definition 1.2.1. *A* differential ideal*, or* δ-ideal *for short of a* δ*-ring* (R, δ) *is an ideal* I *of* R *such that* $\delta(I) \subseteq I$*.*

For a δ-ideal I of a δ-ring R, the quotient R/I is naturally a δ-ring with derivation given by $\delta\colon R/I \to R/I,\ \overline{f} \mapsto \overline{\delta(f)}$. This map is well-defined because $f - g \in I$ implies $\delta(f) - \delta(g) = \delta(f-g) \in I$. Note that the canonical map $\pi\colon R \to R/I,\ f \mapsto \overline{f}$ is a morphism of δ-rings. The following proposition is a differential version of the isomorphism theorems for rings.

Proposition 1.2.2 (Isomorphism theorems for differential rings)**.** *Let* $\phi\colon R \to S$ *be a morphism of* δ*-rings and let* I *be a* δ*-ideal of* R*.*

(i) *The ideal* $\ker(\phi) \subseteq R$ *is a* δ*-ideal and* $\phi(R)$ *is a* δ*-subring of* S*. The map* $R/\ker(\phi) \to \phi(R),\ \overline{f} \mapsto \phi(f)$ *is an isomorphism of* δ*-rings.*

(ii) *There exists a morphism* $R/I \to S$ *of* δ*-rings such that*



commutes if and only if $I \subseteq \ker(\phi)$*. Moreover, in this case the map* $R/I \to S$ *is unique and given by* $\overline{f} \mapsto \phi(f)$*.*

(iii) *The map* $J \mapsto \pi(J)$ *is a bijection between the* δ*-ideals of* R *containing* I *and the* δ*-ideals of* R/I *with inverse* $J' \mapsto \pi^{-1}(J')$*.*

Proof. If we forget about the derivation, these statements are well-known. It is straightforward to check that all maps and constructions are compatible with δ. □

Recall that the radical $\sqrt{I}$ of an ideal I of a ring R is the ideal of R defined by

$$\sqrt{I} = \{f \in R |\ \exists\ n \geq 1 : f^n \in I\}.$$

Lemma 1.2.3. *Let* R *be a* δ*-ring containing* $\mathbb{Q}$ *(as a subring). If* $I \subseteq R$ *is a* δ*-ideal, then* $\sqrt{I}$ *is a* δ*-ideal.*

Proof. Let $f \in R$ be such that $f^n \in I$. We will show, by induction on $i = 1, \ldots, n$, that $f^{n-i}\delta(f)^{2i-1} \in I$. (Choosing $i = n$ then implies the lemma.)

For $i = 1$, the claim follows from $nf^{n-1}\delta(f) = \delta(f^n) \in I$ (Lemma 1.1.8 (i)) and the assumption that n can be inverted in R. Assume that $f^{n-(i-1)}\delta(f)^{2(i-1)-1} \in I$. Then

$$\delta(f^{n-i+1}\delta(f)^{2i-3}) = (n-i+1)f^{n-i}\delta(f)\delta(f)^{2i-3} + f^{n-i+1}(2i-3)\delta(f)^{2i-4}\delta^2(f) \in I.$$

After multiplying the above equation with $\delta(f)$, the second summand contains $f^{n-(i-1)}\delta(f)^{2(i-1)-1}$ as a factor and therefore belongs to I by the induction hypothesis. So we find that also $(n-i+1)f^{n-i}\delta(f)^{2i-1} \in I$. Since $n+i-1$ is invertible in R, we obtain $f^{n-i}\delta(f)^{2i-1} \in I$ as desired. □

☠ **1.2.4.** *Lemma 1.2.3 is not true without the assumption that* $\mathbb{Q} \subseteq R$*, even if* R *has characteristic zero. For example,* $I = (n, x^n) \subseteq \mathbb{Z}[x]$ *with* δ *as in Example 1.1.4 is a differential ideal for every* $n \geq 2$*. However,* $\sqrt{I}$ *is not a differential ideal because* $x \in \sqrt{I}$ *and* $\delta(x) = 1 \notin \sqrt{I}$*.*

We will need the following algebraic lemma. Recall that a ring R is reduced if $f^n = 0$ for $f \in R$ implies $f = 0$, or equivalently, the nilradical $\sqrt{0}$ of R equals (0).

Lemma 1.2.5. *Let R be a reduced ring. If $\mathfrak{p}$ is a minimal prime ideal of R and $f \in \mathfrak{p}$, then there exists a $g \in R \setminus \mathfrak{p}$ such that $fg = 0$.*

Proof. The prime ideals of $R_\mathfrak{p}$ are in bijection with the prime ideals contained in $\mathfrak{p}$ (Corollary A.1.4). Since $\mathfrak{p}$ is minimal, it follows that $R_\mathfrak{p}$ has only one prime ideal. Moreover, as R is reduced, also $R_\mathfrak{p}$ is reduced. A reduced ring with only one prime ideal is a field (Corollary A.1.6). So $\mathfrak{p}_\mathfrak{p}$ is the zero ideal of $R_\mathfrak{p}$. As $\frac{f}{1} \in \mathfrak{p}_\mathfrak{p}$, we see that $\frac{f}{1} = 0 \in R_\mathfrak{p}$. This means that $gf = 0$ for some $g \in R \setminus \mathfrak{p}$. □

Lemma 1.2.6. *Let (R, δ) be a differential ring containing $\mathbb{Q}$ and let $\mathfrak{p}$ be a minimal prime ideal of R. Then $\mathfrak{p}$ is a δ-ideal.*

Proof. We know from Lemma 1.2.3 that the nilradical $\sqrt{0}$ of R is a δ-ideal. Since every prime ideal of R contains $\sqrt{0}$, the minimal prime ideals of R are in bijection with the minimal prime ideals of $R/\sqrt{0}$. Using Proposition 1.2.2 (iii), we may replace R with $R/\sqrt{0}$. In other words, we can assume that R is reduced.

Let $f \in \mathfrak{p}$. By Lemma 1.2.5, there exists a $g \in R \setminus \mathfrak{p}$ such that $fg = 0$. In particular, f lies in the kernel $I = \{h \in R | \ \exists\ n \geq 1 : hg^n = 0\}$ of $R \to R_g$. Since this is a morphism of differential rings (Exercise 1.1.12), we see that I is a differential ideal. So $\delta(f) \in I$ and $\delta(f)g^n = 0 \in \mathfrak{p}$ for some $n \geq 1$. Since $g \notin \mathfrak{p}$, it follows that $\delta(f) \in \mathfrak{p}$ as desired. □

A *maximal δ-ideal* of a δ-ring R is a δ-ideal of R that is maximal in the set of all proper δ-ideal of R ordered by inclusion. In other words, a δ-ideal I of R is a maximal δ-ideal of R if $I \neq R$ and for any other δ-ideal J of R with $I \subseteq J$ and $J \neq R$ we have $J = I$.

☠ **1.2.7.** *A maximal δ-ideal need not be a maximal ideal.*

Corollary 1.2.8. *Let (R, δ) be a differential ring containing $\mathbb{Q}$. Then a maximal differential ideal of R is a prime ideal.*

Proof. Let I be a maximal δ-ideal of R and let $\mathfrak{p}$ be a minimal prime ideal of R/I. By Lemma 1.2.6, the ideal $\mathfrak{p}$ is a δ-ideal. Therefore, the inverse image $\mathfrak{p}' \subseteq R$ of $\mathfrak{p}$ under the map $R \to R/I$ is a prime δ-ideal containing I. The maximality of I implies $I = \mathfrak{p}'$. □

1.3 Differentially simple differential rings

Definition 1.3.1. *A δ-ring R is* δ-simple *if its only δ-ideals are the whole ring R and the zero ideal* (0).

A ring is a field if and only if its only ideals are the whole ring and the zero ideal. Therefore, one could argue that δ-simple δ-rings are a δ-analog of fields. In theory, it is easy to construct δ-simple δ-rings: Given any δ-ring R, by Zorn's lemma, there exists a maximal δ-ideal $\mathfrak{m}$ in R. By Proposition 1.2.2, the δ-ring $R/\mathfrak{m}$ is δ-simple. In practice, it is extremely difficult to carry out this construction explicitly. In fact, the following problem is a central problem in the Galois theory of differential equations: Given a δ-field K and $A \in K^{n \times n}$, consider the K-algebra $U = K\big[X_{ij}, \frac{1}{\det(X)} | \ 1 \leq i, j \leq n\big]$ as a K-δ-algebra via $\delta(X) = AX$. (Here X is an $n \times n$-matrix of indeterminates over K.) Can you find generators for a maximal δ-ideal of U?

Differentially simple δ-rings play a crucial role in the Galois theory of linear differential equations. In this section we establish their basic properties. These results may seem a bit technical at first, however, they are crucial for our further developments.

Example 1.3.2. Let k be a field of characteristic zero and let $k[x]$ the polynomial ring over k in the variable x, considered as a δ-ring as in Example 1.1.4. Then $k[x]$ is δ-simple. Indeed, any non-zero, proper ideal I of $k[x]$ is of the form $I = (f)$, where $f \in k[x] \setminus k$ is of minimal degree. Suppose $I = (f)$ is a δ-ideal. Then $\delta(f) \in I$ is an element of I of degree $\deg(f) - 1$. This contradicts the minimality of $\deg(f)$.

Over a field of positive characteristic p, the polynomial ring $k[x]$ is not δ-simple. For example, (x^p) is δ-ideal of $k[x]$.

Exercise 1.3.3. *Let k be a field of characteristic zero. Show that the ring $k[|x|]$ of formal power series over k (with derivation as in Example 1.1.5) is δ-simple.*

The following lemma provides some first properties of δ-simple δ-rings.

Lemma 1.3.4. *Let R be a δ-simple δ-ring. Then*

(i) *R^δ is a field.*

(ii) *If moreover R contains $\mathbb{Q}$, then R is an integral domain and*

(iii) $\mathrm{Frac}(R)^\delta = R^\delta$.

Proof. Let $c \in R^\delta$ be non-zero. As $\delta(dc) = \delta(d)c$ for $d \in R$, we see that $(c) \subseteq R$ is a δ-ideal. Since R is δ-simple, we have $1 \in (c)$, i.e., $c \in R^\times$. Applying δ to the formula $cc^{-1} - 1$, we find $c\delta(c^{-1}) = 0$. Therefore $\delta(c^{-1}) = 0$ and so $c^{-1} \in R^\delta$. Thus R^δ is a field.

In a δ-simple δ-ring the zero ideal is a maximal δ-ideal. So, by Corollary 1.2.8, the zero ideal is a prime ideal. This means that R is an integral domain.

For (iii), let $f, g \in R$, $g \neq 0$ such that $c = \frac{f}{g} \in \mathrm{Frac}(R)^\delta$. Then $\{h \in R |\ hc \in R\}$ is a differential ideal of R. Since it contain g, it is non-zero and so contains 1, i.e., $c \in R$. □

Lemma 1.3.5. *Let R be a δ-simple δ-ring and let S be an R-δ-algebra. Then R and S^δ are linearly disjoint over R^δ, i.e., the map $R \otimes_{R^\delta} S^\delta \to S$ is injective.*

Proof. It suffices to show that if $c_1, \ldots, c_n \in S^\delta$ are R^δ-linearly independent, then they are also R-linearly independent. Suppose, for a contradiction, that this is not the case and let $n \geq 2$ be minimal with the property that there exist $c_1, \ldots, c_n \in S^\delta$ that are R^δ-linearly independent but R-linearly dependent.

Set $I = \{f_1 \in R |\ f_1c_1 + \ldots + f_nc_n = 0\}$. Because the c_i are constant, I is a δ-ideal of R and from the minimality of n it follows that I is non-zero. Therefore $1 \in I$ and there exist $f_2, \ldots, f_n \in R$ such that

$$c_1 + f_2c_2 + \ldots + f_nc_n = 0. \tag{1.3}$$

Applying δ to (1.3) we find $\delta(f_2)c_2 + \ldots + \delta(f_n)c_n = 0$. But then the minimality of n implies $\delta(f_2) = \ldots = \delta(f_n) = 0$, i.e., $f_2, \ldots, f_n \in S^\delta$. This contradicts the assumption that $c_1, \ldots, c_n$ are S^δ-linearly independent. □

Exercise 1.3.6. *Let K be a δ-field of characteristic zero such that K^δ is algebraically closed. Let L/K be an extension of δ-field such that L is algebraic over K. Show that $L^\delta = K^\delta$.*

Lemma 1.3.7. *Let R be a δ-ring such that R^δ is a field and let D be an R^δ-algebra considered as a constant δ-ring. Then $(R \otimes_{R^\delta} D)^\delta \simeq D$.*

Proof. Let (d_i) be an R^δ-basis of D. Then any element f of $R \otimes_{R^\delta} D$ is uniquely of the form $f = \sum r_i \otimes d_i$ for some $r_i \in R$. If $f \in (R \otimes_{R^\delta} D)^\delta$, then $0 = \delta(f) = \sum \delta(r_i) \otimes d_i$. So $\delta(r_i) = 0$ for all i and therefore $f \in 1 \otimes D \subseteq R \otimes_{R^\delta} D$. □

In the sequel we will usually identify D with $(R \otimes_{R^\delta} D)^\delta$.

Proposition 1.3.8. *Let R be a δ-simple δ-ring and let D be an R^δ-algebra considered as a constant δ-ring. Then the map $I \mapsto R \otimes_{R^\delta} I$ is a bijection between the ideals of D and the δ-ideals of $R \otimes_{R^\delta} D$. The inverse is given by $J \mapsto J^\delta := \{f \in J |\ \delta(f) = 0\} = J \cap D$.*

Proof. Clearly $R \otimes_{R^\delta} I$ is a δ-ideal of $R \otimes_{R^\delta} D$ and $(R \otimes_{R^\delta} I)^\delta = I$ for every ideal I of D. It remains to show that $J = R \otimes_{R^\delta} (J \cap D)$ for every δ-ideal J of $R \otimes_{R^\delta} D$. By Lemma 1.3.5 applied to the R-δ-algebra $(R \otimes_{R^\delta} D)/J$, the map $R \otimes_{R^\delta} ((R \otimes_{R^\delta} D)/J)^\delta \to (R \otimes_{R^\delta} D)/J$ is injective. As $(R \otimes_{R^\delta} D)/R \otimes_{R^\delta} (J \cap D) \simeq R \otimes_{R^\delta} (D/J \cap D)$ embeds into $R \otimes_{R^\delta} ((R \otimes_{R^\delta} D)/J)^\delta$, it follows that the canonical map $(R \otimes_{R^\delta} D)/R \otimes_{R^\delta} (J \cap D) \to (R \otimes_{R^\delta} D)/J$ is injective. Therefore $J = R \otimes_{R^\delta} (J \cap D)$. □

From Proposition 1.3.8 we immediately obtain:

Corollary 1.3.9. *Let R be a δ-simple δ-ring and let D be a field extension of R^δ. Then $R \otimes_{R^\delta} D$ is δ-simple.* □

The following (algebraic version) of a theorem of Chevalley is a very important theorem in algebraic geometry (cf. Remark 1.3.11).

Theorem 1.3.10 (Chevalley)**.** *Let $R \subseteq S$ be an inclusion of integral domains such that S is finitely generated as an R-algebra and let s be a non-zero element of S. Then there exists a non-zero element $r \in R$ such that for every prime ideal $\mathfrak{p}$ of R with $r \notin \mathfrak{p}$ there exists a prime ideal $\mathfrak{P}$ of S with $s \notin \mathfrak{P}$ and $\mathfrak{P} \cap R = \mathfrak{p}$.*

Proof. We first assume that $S = R[a]$ is generated by a single element $a \in S$. We distinguish two cases:

First case: The element $a \in S \subseteq \mathrm{Frac}(S)$ is transcendental over $\mathrm{Frac}(R)$, so that we may identify S with a univariate polynomial ring $S = R[x]$ over R. Note that if $\mathfrak{p}$ is a prime ideal of R and $\mathfrak{P}$ denotes the ideal of $R[x]$ generated by $\mathfrak{p}$, then $R[x]/\mathfrak{P} \simeq (R/\mathfrak{p})[x]$. From this it follows that firstly, $\mathfrak{P}$ is a prime ideal of $R[x]$ with $\mathfrak{P} \cap R = \mathfrak{p}$ and secondly that if $r \in R$ is a non-zero coefficient of $s \in S$ when written as a polynomial in a, then $s \notin \mathfrak{P}$ if $r \notin \mathfrak{p}$. So we have found the sought for $r \in R$ in this case.

Second case: The element $a \in S \subseteq \mathrm{Frac}(S)$ is algebraic over $\mathrm{Frac}(R)$. Set $I = \{f \in R[x] |\ f(a) = 0\}$. Then $S \simeq R[x]/I$. Let $f \in I \setminus \{0\}$ be of minimal degree and let $r_1 \in R \setminus \{0\}$ be the leading coefficient of f. Let $g \in R[x]$ be such that $g(a) = s$. Note that, up to normalization, $f \in \mathrm{Frac}(R)[x]$ is the minimal polynomial of $a \in \mathrm{Frac}(S)$ over $\mathrm{Frac}(R)$. In particular, $f \in \mathrm{Frac}(R)[x]$ is irreducible. As $g(a) = s \neq 0$, we see that $g \notin (f) \subseteq \mathrm{Frac}(R)[x]$. So the greatest common divisor of f and g (as elements of $\mathrm{Frac}(R)[x]$) is 1, i.e., $1 \in (f, g) \subseteq \mathrm{Frac}(R)[x]$. This implies that there exists a non-zero $r_2 \in R$ with $r_2 = f_1 f + g_1 g$ for some $f_1, g_1 \in R[x]$.

We claim that $r = r_1 r_2$ does the trick. So let $\mathfrak{p}$ be an ideal of R with $r \notin \mathfrak{p}$. Let $k(\mathfrak{p}) = \mathrm{Frac}(R/\mathfrak{p})$ denote the residue field of $\mathfrak{p}$, Moreover, let $\overline{f} \in k(\mathfrak{p})[x]$ denote the image of f in $k(\mathfrak{p})[x]$ and let $\overline{I}$ denote the ideal of $k(\mathfrak{p})$ generated by the image of I in $k(\mathfrak{p})[x]$. We claim that $\overline{I} = (\overline{f}) \subseteq k(\mathfrak{p})[x]$. Clearly, $(\overline{f}) \subseteq \overline{I}$. For the converse inclusion, let $h \in I$ and let $\overline{h} \in k(\mathfrak{p})[x]$ denote the image of h in $k(\mathfrak{p})[x]$. Because $\deg(f) \leq \deg(h)$ we can write $r_1 h = af + b$ with $a, b \in R[x]$ and $\deg(b) < \deg(f)$. Because $h, f \in I$, also $b \in I$ and so $b = 0$ by the minimality of $\deg(f)$. Therefore $r_1 h = af$. Since $r_1 \notin \mathfrak{p}$ we see that $\overline{h} \in (\overline{f}) \subseteq k(\mathfrak{p})[x]$. So $\overline{I} = (\overline{f})$ as claimed.

It follows that $S \otimes_R k(\mathfrak{p}) = (R[x]/I) \otimes_R k(\mathfrak{p}) = k(\mathfrak{p})[x]/\overline{I} = k(\mathfrak{p})[x]/(\overline{f})$ is not the zero ring and therefore contains a prime ideal $\mathfrak{q}$. Let $\mathfrak{P} = \phi^{-1}(\mathfrak{q})$ be the inverse image of $\mathfrak{q}$ under the map $\phi\colon S \to S \otimes_R k(\mathfrak{p})$. Then $\mathfrak{P}$ is a prime ideal of S with $\mathfrak{P} \cap R = \mathfrak{p}$ because under ϕ, an

element of R either maps to zero, which is contained in $\mathfrak{q}$, or to a unit which is not contained in $\mathfrak{q}$. To finish the second case, it remains to show that $s \notin \mathfrak{P}$. Suppose $s \in \mathfrak{P}$, i.e., $\phi(s) \in \mathfrak{q}$. From $r_2 = f_1 f + g_1 g$ we obtain $r_2 = f_1(a)f(a) + g_1(a)g(a) = g_1(a)g(a) = g_1(a)s$. So $\phi(s) \in \mathfrak{q}$ implies $\phi(r_2) \in \mathfrak{q}$, i.e., $r_2 \in \mathfrak{P} \cap R = \mathfrak{p}$; a contradiction.

This proves the theorem in the case that S is generated as an R-algebra by a single element. From here it is a rather straightforward induction on the number of generators of S as an R-algebra. The base of the induction just having been established, assume that $S = R[a_1, \ldots, a_n]$. Applying the case $n = 1$ to the inclusion $R[a_1, \ldots, a_{n-1}] \subseteq R[a_1, \ldots, a_{n-1}][a_n]$, yields a non-zero $a \in R[a_1, \ldots, a_{n-1}]$ such that every prime ideal $\mathfrak{q}$ of $R[a_1, \ldots, a_{n-1}]$ with $a \notin \mathfrak{q}$ is of the form $\mathfrak{q} = \mathfrak{P} \cap R[a_1, \ldots, a_{n-1}]$ for some prime ideal $\mathfrak{P} \subseteq S = R[a_1, \ldots, a_n]$ with $s \notin \mathfrak{P}$. By induction, there exist a non-zero $r \in R$ such that for every prime ideal $\mathfrak{p}$ of R with $r \notin \mathfrak{p}$, there exists a prime ideal $\mathfrak{q}$ of $R[a_1, \ldots, a_{n-1}]$ with $a \notin \mathfrak{q}$ and $\mathfrak{q} \cap R = \mathfrak{p}$. Combining the last two sentences, we see that for every prime ideal $\mathfrak{p}$ of R with $r \notin \mathfrak{p}$ there exists a prime ideal $\mathfrak{P}$ of S with $s \notin \mathfrak{P}$ and $\mathfrak{P} \cap R = \mathfrak{p}$. □

Theorem 1.3.10 is most relevant in the case $s = 1$, in which the condition $s \notin \mathfrak{P}$ is vacuous. However, for the proof by induction it is important to allow a variable s.

Remark 1.3.11. *There is a more geometric interpretation of Theorem 1.3.10. For a ring R the set* $\mathrm{Spec}(R)$ *of all prime ideals of R can be considered as a topological space: A basis for the open sets of* $\mathrm{Spec}(R)$ *is given by the basic open sets $D(f) = \{\mathfrak{p} \in \mathrm{Spec}(R) |\ f \notin \mathfrak{p}\}$ for $f \in R$. The inclusion of rings $R \subseteq S$ induces a continuous map $\phi\colon \mathrm{Spec}(S) \to \mathrm{Spec}(R)$, $\mathfrak{P} \mapsto \mathfrak{P} \cap R$. With this language, the conclusion of Theorem 1.3.10 can be restated by saying that $\phi(D(s))$ contains the basic open subset $D(r)$. In particular, the image of ϕ contains a non-empty open subset.*

We now apply Chevalley's theorem to δ-simple δ-rings.

Proposition 1.3.12. *Let K be a δ-field of characteristic zero and let R be a δ-simple K-δ-algebra such that R is finitely generated as a K-algebra. Then R^δ is an algebraic field extension of K^δ.*

Proof. Suppose for a contradiction that $c \in R^\delta$ is transcendental over $k = K^\delta$. Since K and R^δ are linearly disjoint over K^δ (Lemma 1.3.5), it follows that c is transcendental over K, i.e., $K[c] \subseteq R$ is a polynomial ring. Applying Theorem 1.3.10 with $s = 1$ to the inclusion $K[c] \subseteq R$, yields a non-zero $f \in K[c]$ such that for every prime ideal $\mathfrak{p}$ of $K[c]$ with $f \notin \mathfrak{p}$ there exists a prime ideal $\mathfrak{P}$ of R with $\mathfrak{P} \cap K[c] = \mathfrak{p}$.

We claim that there exists a $d \in K^\delta$ such that $f \notin (c-d) \subseteq K[c]$. Note that $f \in (c-d)$ implies that $d \in K$ is a root of $f \in K[c]$. As f has only finitely many roots in K and K^δ is infinite (because K has characteristic zero) we see that there exists a $d \in K^\delta$ with $f \notin (c-d)$. As $c - d \in R^\delta$, the ideal of R generated by $c - d$ is a δ-ideal. Because R is δ-simple, this δ-ideal must equal R. On the other hand, by construction of f, for the prime ideal $\mathfrak{p} = (c-d)$ of $K[c]$, there exists a prime ideal $\mathfrak{P}$ of R with $\mathfrak{P} \cap K[c] = \mathfrak{p}$. Since $\mathfrak{P}$ contains the ideal of R generated by $c - d$ we obtain a contradiction. □

Chapter 2

Picard-Vessiot rings and Picard-Vessiot extensions

Throughout this chapter K denotes a differential field of characteristic zero.

In this chapter we begin our study of linear differential equations. Our primary goal is to understand the structure of the algebra generated by the solutions of a given linear differential equation.

2.1 Linear differential equations and systems

A homogeneous *n-th order linear differential equation* over K is an equation of the form

$$\delta^n(y) + a_{n-1}\delta^{n-1}(y) + \ldots + a_0 y = 0, \tag{2.1}$$

where $a_0, \ldots, a_{n-1} \in K$. Here y is considered to be a formal variable. A *solution* of (2.1) is an element f of some K-δ-algebra such that $\delta^n(f) + a_{n-1}\delta^{n-1}(f) + \ldots + a_0 f = 0$. One verifies immediately that for a given δ-field extension L/K the set of solutions of (2.1) is an L^δ-vector space. It is natural to wonder, what are the possible values for the dimension of this vector space? In analogy with the well known fact that a polynomial of degree n can have at most n roots (in any field containing the field of coefficients), one might expect that the dimension is bounded by n. As we will show, this is indeed the case. In fact, we will prove a more general result that applies to linear differential system. So we first discuss linear differential systems and then deduce the result for linear differential equations from the corresponding result for linear differential systems.

A homogeneous *linear differential system of order n* over K is a system of equations of the form

$$\begin{aligned}
\delta(y_1) &= A_{11}y_1 + A_{12}y_2 + \ldots + A_{1n}y_n \\
\delta(y_2) &= A_{21}y_1 + A_{2}2y_2 + \ldots + A_{2n}y_n \\
\vdots \quad &= \quad \vdots \qquad\qquad\qquad \vdots \\
\delta(y_n) &= A_{n1}y_1 + A_{n2}y_2 + \ldots + A_{nn}y_n,
\end{aligned}$$

where $A_{ij} \in K$ and $y_1, \ldots, y_n$ are formal variables. We will usually write such a system in the more compact form $\delta(y) = Ay$, where $A = (A_{ij})_{1\leq i,j\leq n} \in K^{n\times n}$ is the matrix of the differential system,

$$y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \quad \text{and } \delta(y) = \begin{pmatrix} \delta(y_1) \\ \vdots \\ \delta(y_n) \end{pmatrix}.$$

As a general matter of notation, if $B = (B_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \in R^{m\times n}$ is an $m\times n$-matrix with coefficients in a δ-ring R, then $\delta(B) = ((\delta(B_{ij}))_{\substack{1\le i\le m\\ 1\le j\le n}} \in R^{m\times n}$ is the matrix obtained by applying δ to the entries of B.

A *solution* to $\delta(y) = Ay$ is a vector $f = \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} \in R^n$, where R is some K-δ-algebra, such that $\delta(f) = Ay$. If L is a δ-field extension of K and $f, g \in L^n$ are solutions of $\delta(y) = Ay$, then $\delta(f+g) = \delta(f) + \delta(g) = Af + Ag = A(f+g)$. Moreover, if $c \in L^\delta$, then $\delta(cf) = c\delta(f) = cAf = A(cf)$. So the solutions of $\delta(y) = Ay$ in L^n are an L^δ-vector space. Again, it is natural to wonder, what are the possible values of the dimension of this vector space? The following lemma gives a partial answer.

Lemma 2.1.1. *Let $A \in K^{n\times n}$ and assume that $f_1, \dots, f_m \in K^n$ are K^δ-linearly independent solutions of $\delta(y) = Ay$. Then $f_1, \dots, f_m$ are K-linearly independent. In particular, $m \le n$.*

Proof. Suppose, for a contradiction, that there exist $\lambda_1, \dots, \lambda_m \in K$, not all equal to zero, such that

$$\lambda_1 f_1 + \dots + \lambda_m f_m = 0. \tag{2.2}$$

Without loss of generality, we can assume that $\lambda_1 = 1$ and that m is minimal, i.e., there is no non-trivial K-linear relation among $m-1$ elements taken from $\{f_1, \dots, f_m\}$. Applying δ to (2.2) yields

$$\begin{aligned} 0 &= \delta(\lambda_1)f_1 + \dots + \delta(\lambda_m)f_m + \lambda_1\delta(f_1) + \dots + \lambda_m\delta(f_m) = \\ &= \delta(\lambda_1)f_1 + \dots + \delta(\lambda_m)f_m + \lambda_1 Af_1 + \dots + \lambda_m Af_m = \\ &= \delta(\lambda_1)f_1 + \dots + \delta(\lambda_m)f_m + A(\lambda_1 f_1 + \dots \lambda_m f_m) = \\ &= \delta(\lambda_1)f_1 + \dots + \delta(\lambda_m)f_m = \delta(\lambda_2)f_2 + \dots + \delta(\lambda_m)f_m, \end{aligned}$$

because $\delta(c_1) = \delta(1) = 0$. This contradicts the minimality of m. □

Corollary 2.1.2. *Let $A \in K^{n\times n}$ and let L be a δ-field extension of K. Then the L^δ-vector space of solutions to $\delta(y) = Ay$ in L^n has dimension $\le n$.*

Proof. Apply Lemma 2.1.1 with $K = L$. □

To transfer the result of Corollary 2.1.2 from linear differential systems to linear differential equations, we associate to an n-th order linear differential equation

$$\delta^n(y) + a_{n-1}\delta^{n-1}(y) + \dots + a_0 y = 0 \tag{2.3}$$

over K, the n-th order linear differential system $\delta(y) = Ay$ over K, where

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}. \tag{2.4}$$

This matrix is called the *companion matrix* of (2.3). The connection is given by the fact that for a K-δ-algebra R, an element $f \in R$ is a solution of (2.3) if and only if

$$\begin{pmatrix} f \\ \delta(f) \\ \vdots \\ \delta^{n-1}(f) \end{pmatrix} \in R^n \tag{2.5}$$

is a solution of $\delta(y) = Ay$. Moreover, any solution of $\delta(y) = Ay$ is of the form (2.5). In particular, if L is a δ-field extension of K, then the map

$$f \mapsto \begin{pmatrix} f \\ \delta(f) \\ \vdots \\ \delta^{n-1}(f) \end{pmatrix}$$

is an isomorphism between the L^δ-vector space of solutions of (2.3) and the L^δ-vector space of solutions of $\delta(y) = Ay$. From Corollary 2.1.2 we therefor obtain:

Corollary 2.1.3. *Let L be a δ-field extension of K and $a_0, \ldots, a_{n-1} \in K$. Then the dimension of the L^δ-vector space of solutions of $\delta^n(y) + a_{n-1}\delta^{n-1}(y) + \ldots + a_0 y = 0$ in L is $\leq n$.* □

In the sequel we will be working with linear differential equations and linear differential systems. As explained above, the study of linear differential equations is more ore less subsumed in the study of linear differential systems. For notational and theoretical purposes systems are usually more convenient. However, for concrete examples, it is usually more natural to work with equations.

Given n solutions of an n-th order linear differential equation, according to Corollary 2.1.3, they are a basis of the solution space if and only if they are linearly independent. It is therefore desirable to have a simple method to test the linear independence (over constants). Such a method is provided by the Wronskian.

Definition 2.1.4. *Let $f_1, \ldots, f_n$ be elements of some δ-ring. The* Wronskian $\operatorname{wr}(f_1, \ldots, f_n)$ *of $f_1, \ldots, f_n$ is the determinant of the* Wronskian matrix

$$\operatorname{Wr}(f_1, \ldots, f_n) = \begin{pmatrix} f_1 & \cdots & f_n \\ \delta(f_1) & \cdots & \delta(f_n) \\ \vdots & & \vdots \\ \delta^{n-1}(f_1) & \cdots & \delta^{n-1}(f_n) \end{pmatrix} \in R^{n \times n}.$$

Lemma 2.1.5 (Wronskian lemma)**.** *Let $f_1, \ldots, f_n \in K$. Then $f_1, \ldots, f_n$ are K^δ-linearly independent if and only if* $\operatorname{wr}(f_1, \ldots, f_n) \neq 0$.

Proof. Assume that $f_1, \ldots, f_n$ are K^δ-linearly independent. Suppose, for a contradiction that $\operatorname{wr}(f_1, \ldots, f_n) = 0$. Then the rows of $\operatorname{Wr}(f_1, \ldots, f_n)$ are K-linearly dependent and so there exists a non-zero vector $a = (a_0, \ldots, a_{n-1}) \in K^n$ such that $a \operatorname{Wr}(f_1, \ldots, f_n) = 0$, i.e., every f_i is a solution of the linear differential equation $a_{n-1}\delta^{n-1}(y) + \ldots + a_0 y = 0$ of order at most $n-1$. It follows from Corollary 2.1.3 that $f_1, \ldots, f_n$ are K^δ-linearly dependent; a contradiction.

Assume that $\operatorname{wr}(f_1, \ldots, f_n) \neq 0$ and let $c_1, \ldots, c_n \in K^\delta$ be such that $c_1 f_1 + \ldots + c_n f_n = 0$. Then applying δ^i shows that also $c_1\delta^i(f_1) + \ldots + c_n\delta^i(f_n) = 0$. So the vector $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ lies in the nullspace of $\operatorname{Wr}(f_1, \ldots, f_n)$. As $\operatorname{wr}(f_1, \ldots, f_n) \neq 0$, the matrix $\operatorname{Wr}(f_1, \ldots, f_n)$ is invertible and so $c_1 = \ldots = c_n = 0$. □

Note that the condition $\operatorname{wr}(f_1, \ldots, f_n) \neq 0$ in Lemma 2.1.5 does not refer to K or K^δ. So it follows that if $f_1, \ldots, f_n \in K$ are K^δ-linearly independent, then $f_1, \ldots, f_n$ will also be L^δ-linearly independent, where L is any δ-field extension of K.

The following corollary summarizes the above results for linear differential equations.

Corollary 2.1.6. *Let $f_1, \ldots, f_n \in L$ be solutions of the n-th order linear differential equation*

$$\delta^n(y) + a_{n-1}\delta^{n-1}(y) + \ldots + a_0 y = 0 \tag{2.6}$$

over K in a δ-field extension L of K. Then the following statements are equivalent:

(i) *The elements $f_1, \ldots, f_n$ are a basis for the L^δ-vector space of solutions of (2.6).*

(ii) *The elements $f_1, \ldots, f_n$ are L^δ-linearly independent.*

(iii) $\mathrm{wr}(f_1, \ldots, f_n) \neq 0$.

Proof. The equivalence of (i) and (ii) follows from Corollary 2.1.3 and the equivalence of (ii) and (iii) follows from Lemma 2.1.5. □

We now return to linear differential systems. The following corollary follows from Lemma 2.1.1.

Corollary 2.1.7. *Let $\delta(y) = Ay$ be an n-th order linear differential system over K and let Y be an $n \times n$ matrix with coefficients in a δ-field extension L of K such that the columns of Y are solutions of $\delta(y) = Ay$. Then the following are equivalent:*

(i) *The columns of Y are a basis of the L^δ-vector space of solutions of $\delta(y) = Ay$ in L^n.*

(ii) *The columns of Y are L^δ-linearly independent.*

(iii) *The columns of Y are L-linearly independent.*

(iv) $Y \in \mathrm{GL}_n(L)$.

Definition 2.1.8. *Let $A \in K^{n\times n}$ and let R be a K-δ-algebra. A matrix $Y \in \mathrm{GL}_n(R)$ is a* fundamental solution matrix *for $\delta(y) = Ay$ if $\delta(Y) = AY$, i.e., the columns of Y are solutions of $\delta(y) = Ay$.*

The following simple lemma is fundamental for the development of differential Galois theory.

Lemma 2.1.9. *Let R be a K-δ-algebra and $A \in K^{n\times n}$. If $Y_1, Y_2 \in \mathrm{GL}_n(R)$ are fundamental solution matrices for $\delta(y) = Ay$, then there exists a (necessarily unique) matrix $C \in \mathrm{GL}_n(R^\delta)$ such $Y_2 = Y_1 C$.*

Proof. It suffices to show that $\delta(Y_1^{-1}Y_2)$ is the zero matrix. Take a moment to convince yourself that the Leibniz rule also holds for matrices, i.e., $\delta(B_1B_2) = \delta(B_1)B_2 + B_1\delta(B_2)$ for any two $n \times n$ matrices B_1, B_2 with coefficients in a δ-ring. It follows that $0 = \delta(I_n) = \delta(Y_1Y_1^{-1}) = \delta(Y_1)Y_1^{-1} + Y_1\delta(Y_1^{-1})$ so that $\delta(Y_1^{-1}) = -Y_1^{-1}\delta(Y_1)Y_1^{-1}$. Therefore

$$\delta(Y_1^{-1}Y_2) = \delta(Y_1^{-1})Y_2 + Y_1^{-1}\delta(Y_2) = -Y_1^{-1}AY_1Y_1^{-1}Y_2 + Y_1^{-1}AY_2 = 0$$

as desired. □

2.2 Picard-Vessiot rings and Picard-Vessiot extensions

In the previous section we have seen that for a linear differential system $\delta(y) = Ay$ of order n over K, the L^δ-vector space of solutions has dimension $\leq n$ for any δ-field extension L of K. It is natural to wonder if there always exists a δ-field extension L of K such that the dimension is exactly n? In other words, does there always exists a fundamental solution matrix in some δ-field extension of K? In the analytic context it is well-know that if $I \subseteq \mathbb{R}$ is open interval and $A(x)$ is an $n \times n$-matrix whose entries are continuous functions from I to $\mathbb{R}$, then the $\mathbb{R}$-vector space of C^1-functions $f\colon I \to \mathbb{R}^n$ that satisfy $f'(x) = A(x)f(x)$ has dimension n. It therefore seems natural to expect a similar result in our algebraic context. This question is somewhat similar to asking if for a given polynomial of degree n, there exists a field containing the coefficients in which the polynomial has n roots.

The answer is yes, and this is rather easy to see: Let $X = (X_{ij})_{1\leq i,j\leq n}$ be an $n \times n$-matrix of indeterminates over K. Define a derivation $\delta\colon K[X_{ij}|\ 1 \leq i, j \leq n] \to K[X_{ij}|\ 1 \leq i, j, \leq n]$ by $\delta(X) = AX$. By Exercise 1.1.10 there exists a unique such derivation extending $\delta\colon K \to K$. Moreover, by Exercise 1.1.12 this derivation uniquely extends to the field of fractions $L = K(X_{ij}|\ 1 \leq i, j \leq n)$ of $K[X_{ij}|\ 1 \leq i, j \leq n]$. Clearly, $X \in \mathrm{GL}_n(L)$ is a fundamental solution matrix for $\delta(y) = Ay$.

The solutions contained in the columns of X carry no interesting information. There are no algebraic relations among the entries of X. The structure of the field extension L of K is equally boring. In particular, it does not depend on A. (A more interesting question concerning the differential field L is, what is L^δ?) So, if, as explained in the beginning motivational section, our primary goal is to understand the algebraic relations among "the solutions" of $\delta(y) = Ay$, the solutions in L are clearly not "the right solutions".

The problem is that L is too big. For example, let us consider $K = \mathbb{C}(x)$ with the standard derivation $\delta = \frac{d}{dx}$. Then $\sqrt{x}$ is a solution of the first order system $\delta(y) = \frac{1}{2x}y$ and satisfies the algebraic relation $y^2 - x = 0$ over K. So we expect an extension of degree two, namely $\mathbb{C}(\sqrt{x})/\mathbb{C}(x)$ as the field generated by "the solutions", but the above construction gives a transcendental extension $L = \mathbb{C}(x)(X_{11})$ with $\delta(X_{11}) = \frac{1}{2x}X_{11}$. Note that $\mathbb{C}(\sqrt{x})^\delta = \mathbb{C} = \mathbb{C}(x)^\delta$ (Exercise 1.3.6) but L^δ is larger then $\mathbb{C}$. Indeed, because

$$\delta\left(\frac{X_{11}^2}{x}\right) = \frac{2X_{11}\frac{1}{2x}X_{11}x - X_{11}^2}{x^2} = 0,$$

we see that L contains the new constant $\frac{X_{11}^2}{x} \in L^\delta$. It turns out that the requirement of not having new constants is the appropriate condition to guarantee the uniqueness and a suitable minimality of "the differential field generated by the solutions".

Definition 2.2.1. *Let $A \in K^{n\times n}$. A* Picard-Vessiot extension *for $\delta(y) = Ay$ is a differential field extension L/K such that*

(i) *there exists $Y \in \mathrm{GL}_n(L)$ such that $\delta(Y) = AY$ and $L = K(Y_{ij}|\ 1 \leq i, j \leq n)$, i.e., L is generated, as a field extension of K, by the entries of Y and*

(ii) *$L^\delta = K^\delta$.*

The relevance of condition (ii) should become more transparent in the sequel. For now, we can think of it as saying that the elements of L are "reasonable functions". For example, for $K = \mathbb{C}(x)$ with the standard derivation $\delta = \frac{d}{dx}$, if we think of the elements of L as being functions of x, then condition (ii) simply says that if a function belonging to L has zero derivative, then it is a constant function.

The role of Picard-Vessiot extensions for linear differential systems in differential Galois theory is similar to the role of splitting fields for polynomials in classical Galois theory.

They are named after the French mathematicians Émil Picard and Ernest Vessiot that initiated differential Galois theory around the end of the 19th century. Vessiot was a student of Picard and their main motivation was to obtain, in analogy to classical Galois theory, a group theoretic characterization of when a linear differential equations is "solvable by quadratures" (cf. Chapter 5).

A somewhat different, but, as we will see, equivalent approach to finding "the minimal solution field" is through the algebraic relations. As above, consider an n-th order linear differential system $\delta(y) = Ay$ over K and let X be an $n \times n$-matrix of indeterminates over K. Let $U = K[X_{ij}, \frac{1}{\det(X)} | \ 1 \leq i, j \leq n]$ denote the localization of the polynomial ring $K[X_{ij} | \ 1 \leq i, j \leq n]$ at the multiplicatively closed set $\{1, \det(X), \det(X)^2, \ldots\}$. Define the structure of a K-δ-algebra on U by setting $\delta(X) = AX$. (By Exercises 1.1.10 and 1.1.12 the derivation on U is unique and well-defined.) We call the K-δ-algebra U the *universal solution algebra for* $\delta(y) = Ay$. This is justified by the following fact:

Exercise 2.2.2. *The matrix $X \in \mathrm{GL}_n(U)$ is a fundamental solution matrix for $\delta(y) = Ay$ and if R is any K-δ-algebra containing a fundamental solution matrix $Y \in \mathrm{GL}_n(R)$ for $\delta(y) = Ay$, then there exists a unique morphism $U \to R$ of K-δ-algebras that maps U to Y.*

So the possible algebraic relations that can be satisfied by the entries of a fundamental solution matrix for $\delta(y) = Ay$ correspond to the δ-ideals in U. Since we are interested in *all* algebraic relations a fundamental solution matrix may satisfy, it is natural to focus on the maximal δ-ideals of U. Note that for a maximal δ-ideal $\mathfrak{m}$ of U, the quotient $R = U/\mathfrak{m}$ is a δ-simple K-δ-algebra with a fundamental solution matrix $Y \in \mathrm{GL}_n(R)$ (namely the image of X) for $\delta(y) = Ay$ such that R is generated as a K-algebra by the entries of Y and $\frac{1}{\det(Y)}$. One of the miracles of differential Galois theory is that a different choice of the maximal δ-ideal in U yields essentially the same result. (See Exercise 2.2.21 for a precise statement.)

Definition 2.2.3. *Let $A \in K^{n \times n}$. A* Picard-Vessiot ring *for $\delta(y) = Ay$ is a δ-simple K-δ-algebra R such that*

(i) *there exists $Y \in \mathrm{GL}_n(R)$ with $\delta(Y) = AY$ and $R = K\big[Y_{ij}, \frac{1}{\det Y} | \ 1 \leq i, j \leq n\big]$, i.e., R is generated, as a K-algebra, by the entries of Y and the inverse of the determinant of Y and*

(ii) *$R^\delta = K^\delta$.*

It follows from Proposition 1.3.12 that condition (ii) in Definition 2.2.3 is automatically satisfied (i.e., can be omitted) if K^δ is an algebraically closed field. A Picard-Vessiot extension (respectively Picard-Vessiot ring) for a linear differential equation

$$\delta^n(y) + a_{n-1}\delta^{n-1}(y) + \ldots + a_0 y = 0 \tag{2.7}$$

over K is a Picard-Vessiot extension (respectively Picard-Vessiot ring) for the associated system $\delta(y) = Ay$ (as in (2.4)). Thus, a Picard-Vessiot extension for (2.7) is a δ-field extension L/K with $L^\delta = K^\delta$ such that there exist n K^δ-linearly independent solutions $y_1, \ldots, y_n \in L$ of (2.7) and

$$L = K\left(y_1, \ldots, y_n, \delta(y_1), \ldots, \delta(y_n), \ldots, \delta^{n-1}(y_1), \ldots, \delta^{n-1}(y_n)\right).$$

Similarly, a Picard-Vessiot ring for (2.7) is a δ-simple K-δ-algebra R with $R^\delta = K^\delta$ such that there exist n K^δ-linearly independent solution $y_1, \ldots, y_n \in R$ and

$$R = K\left[y_1, \ldots, y_n, \delta(y_1), \ldots, \delta(y_n), \ldots, \delta^{n-1}(y_1), \ldots, \delta^{n-1}(y_n), \tfrac{1}{\mathrm{wr}(y_1, \ldots, y_n)}\right].$$

Exercise 2.2.4. *Assume that K^δ is algebraically closed. Let L/K be a finite Galois extension (of fields). By Lemma 1.1.14 there exists a unique derivation on L extending the given derivation on K. Show that L/K is a Picard-Vessiot extension (and a Picard-Vessiotr ring).*

Exercise 2.2.5. *Can you find a Picard-Vessiot extension L/K such that L/K is a finite field extension but not Galois? Hint: To construct such an example K^δ should not be algebraically closed.*

To explain the relation between Picard-Vessiot rings and Picard-Vessiot extensions we need a preparatory lemma.

Lemma 2.2.6. *Let $A \in K^{n\times n}$ and let R be a K-δ-algebra such that $R = K[Y_{ij}, \frac{1}{\det(Y)} |\ 1 \leq i,j \leq n]$, where $Y \in \mathrm{GL}_n(R)$ satisfies $\delta(Y) = AY$. Assume that R is an integral domain with $\mathrm{Frac}(R)^\delta = K^\delta$. Furthermore, let S be a δ-simple K-δ-algebra such that $S = K[Z_{i,j}, \frac{1}{\det(Z)} |\ 1 \leq i,j \leq n]$, where $Z \in \mathrm{GL}_n(S)$ satisfies $\delta(Z) = AZ$. Then $(R \otimes_K S)^\delta$ is a finitely generated K^δ-algebra, indeed, $(R \otimes_K S)^\delta = K^\delta[C_{ij}, \frac{1}{\det(C)} |\ 1 \leq i,j \leq n]$, where $C = Y^{-1} \otimes Z = (\sum_{k=1}^n (Y^{-1})_{ik} \otimes Z_{kj})_{1\leq i,j\leq n} \in \mathrm{GL}_n((R \otimes_K S)^\delta)$. Moreover, the canonical map $\psi\colon R \otimes_{K^\delta} (R \otimes_K S)^\delta \to R \otimes_K S$ is an isomorphism.*

Proof. Note that $1 \otimes Z \in \mathrm{GL}_n(R \otimes_K S)$ and $Y \otimes 1 \in \mathrm{GL}_n(R \otimes_K S)$ are both fundamental solution matrices for $\delta(y) = Ay$. So, by Lemma 2.1.9, the matrix $C = (Y \otimes 1)^{-1}(1 \otimes Z) \in \mathrm{GL}_n(R \otimes_K S)$ has entries in $(R \otimes_K S)^\delta$. As $1 \otimes Z = (Y \otimes 1)C$ and the entries of Z and $\frac{1}{\det(Z)}$ generate S as a K-algebra, we see that ψ is surjective. Indeed, even the map

$$R \otimes_{K^\delta} K^\delta\big[C_{ij}, \tfrac{1}{\det(C)} |\ 1 \leq i,j \leq n\big] \to R \otimes_K S \tag{2.8}$$

is surjective. Consider the differential field $L = \mathrm{Frac}(R)$. By Lemma 1.3.5, the map $L \otimes_{L^\delta} (L \otimes_K S)^\delta \to L \otimes_K S$ is injective. Because $L^\delta = K^\delta$, we can interpret ψ as the restriction of this map. So ψ is injective and therefore an isomorphism as claimed.

Since also the map in (2.8) is an isomorphism, we obtain from Lemma 1.3.7 that $(R \otimes_K S)^\delta = K^\delta\big[C_{ij}, \frac{1}{\det(C)} |\ 1 \leq i,j \leq n\big]$. □

The following proposition explains the close connection between Picard-Vessiot extensions and Picard-Vessiot rings.

Proposition 2.2.7. *Let $A \in K^{n\times n}$. If R is a Picard-Vessiot ring for $\delta(y) = Ay$, then $\mathrm{Frac}(R)/K$ is a Picard-Vessiot extension for $\delta(y) = Ay$. Conversely, if L/K is a Picard-Vessiot extension for $\delta(y) = Ay$ with $Y \in \mathrm{GL}_n(L)$ such that $\delta(Y) = AY$ and $L = K(Y_{ij} |\ 1 \leq i,j \leq n)$, then $K[Y_{ij}, \frac{1}{\det(Y)} |\ 1 \leq i,j \leq n]$ is a Picard-Vessiot ring for $\delta(y) = Ay$.*

Proof. Assume that R is a Picard-Vessiot ring for $\delta(y) = Ay$ and let $Y \in \mathrm{GL}_n(R)$ be such that $\delta(Y) = AY$ and $R = K[Y_{ij}, \frac{1}{\det(Y)} |\ 1 \leq i,j \leq n]$. By Lemma 1.3.4 R is an integral domain with $\mathrm{Frac}(R)^\delta = R^\delta = K^\delta$. Since $\mathrm{Frac}(R) = K(Y_{ij} |\ 1 \leq i,j \leq n)$ we see that $\mathrm{Frac}(R)/K$ is a Picard-Vessiot extension for $\delta(y) = Ay$.

Assume that L/K is a Picard-Vessiot extension for $\delta(y) = Ay$ an let $Y \in \mathrm{GL}_n(L)$ be such that $\delta(Y) = AY$ and $L = K(Y_{ij} |\ 1 \leq i,j \leq n)$. Set $R = K[Y_{ij}, \frac{1}{\det(Y)} |\ 1 \leq i,j \leq n]$. We have to show that R is a Picard-Vessiot ring for $\delta(y) = Ay$. The only thing that really needs showing is that R is δ-simple. This, however, is a bit tricky.

Let S be a δ-simple K-δ-algebra such that there exists a $Z \in \mathrm{GL}_n(S)$ with $\delta(Z) = AZ$ and $S = K[Z_{ij}, \frac{1}{\det(Z)} |\ 1 \leq i,j \leq n]$, i.e., S is a quotient of the universal solutions algebra

U by a maximal δ-ideal. The idea is to show that S and R become isomorphic after extending the constants so that also R has to be δ-simple. By Lemma 2.2.6 the canonical map $R \otimes_{K^\delta} (R \otimes_K S)^\delta \to R \otimes_K S$ is an isomorphism. Let D be any field extension of K^δ such that there exists a morphism $(R \otimes_K S)^\delta \to D$ of K^δ-algebras (for example, D could be a quotient of $(R \otimes_K S)^\delta$ by a maximal ideal). We have a morphism

$$S \to R \otimes_K S \simeq R \otimes_{K^\delta} (R \otimes_K S)^\delta \to R \otimes_{K^\delta} D$$

of K-δ-algebras, where the first map is the inclusion into the second factor. This morphism extends to a morphism $\psi\colon S \otimes_{S^\delta} D \to R \otimes_{K^\delta} D$ of $K \otimes_{K^\delta} D$-δ-algebras by D-linearity. By Corollary 1.3.9 the δ-ring $S \otimes_{S^\delta} D$ is δ-simple, so ψ is injective. Since $Z \otimes 1 \in \mathrm{GL}_n(S \otimes_{S^\delta} D)$ is a fundamental solution matrix for $\delta(y) = Ay$, also $\psi(Z \otimes 1)$ is a fundamental solution matrix for $\delta(y) = Ay$. By Lemmas 2.1.9 and Lemma 1.3.7, there exists a matrix $C \in \mathrm{GL}_n(D) \subseteq \mathrm{GL}_n(R \otimes_{K^\delta} D)$ such that $Y \otimes 1 = \psi(Z \otimes 1)C$. In particular, the entries of $Y \otimes 1$ lie in the image of ψ. Since the entries of Y and $\frac{1}{\det(Y)}$ generate R as a K-δ-algebra, it follows that ψ is surjective. Thus ψ is an isomorphism. As $S \otimes_{S^\delta} D$ is δ-simple, also $R \otimes_{K^\delta} D$ is δ-simple. This implies that R is δ-simple, because $I \otimes_{K^\delta} D$ is a non-trivial δ-ideal of $R \otimes_{K^\delta} D$ for a non-trivial δ-ideal I of R. □

Proposition 2.2.7 shows in particular that for a given linear differential system $\delta(y) = Ay$ there exists a Picard-Vessiot extension if and only if there exists a Picard-Vessiot ring.

Theorem 2.2.8 (Existence of Picard-Vessiot extensions and Picard-Vessiot rings)**.** *Let $A \in K^{n\times n}$ and assume that K^δ is algebraically closed. Then there exists a Picard-Vessiot extension and a Picard-Vessiot ring for $\delta(y) = Ay$.*

Proof. Thanks to all our previous work this proof comes easy: As above, choose a maximal δ-ideal $\mathfrak{m}$ in the universal solution algebra $U = K[X_{ij}, \frac{1}{\det(X)} |\ 1 \le i, j \le n]$. Then $R = U/\mathfrak{m}$ is a δ-simple K-δ-algebra satisfying (i) of Definition 2.2.3. Since K^δ is algebraically closed, R also satisfies (ii) by Proposition 1.3.12. Thus R is a Picard-Vessiot ring for $\delta(y) = Ay$. By 2.2.7 the field of fractions $L = \mathrm{Frac}(R)$ of R is Picard-Vessiot extension for $\delta(y) = Ay$. □

Exercise 2.2.9. *Let $A \in K^{n\times}$. Show that there exists a finite field extension k' of $k = K^\delta$ such that there exists a Picard-Vessiot extension for $\delta(y) = Ay$ over $K' = K \otimes_k k'$. (Hint: To begin with, use Exercise 1.1.15 to show that $K' = K \otimes_k k'$ is a field for any algebraic field extension k' of k and that $K'^\delta = k'$.)*

The reader may wonder why we need both, the Picard-Vessiot extensions and the Picard-Vessiot rings? If the concepts are more or less equivalent, could we not make do with just one of them? The answer is that for some purposes Picard-Vessiot extensions are more useful (e.g., for the Galois correspondence) while for other purposes Picard-Vessiot rings (e.g., for defining the differential Galois group) are more practical.

Picard-Vessiot extensions often exist, even if K^δ is not algebraically closed. To discuss the case of constant linear differential systems let us recall the definition of the *matrix exponential*. Let k be a field of characteristic zero and $A \in k^{n\times n}$. We define

$$e^{Ax} = \sum_{i=0}^{\infty} A^i \tfrac{x^i}{i!} \in k[[x]]^{n\times n},$$

where A^0 is the $n \times n$ and identity matrix and $k[[x]]$ is the ring of formal power series over k. If $A, B \in k^{n\times n}$ with $AB = BA$, then one verifies, as in the case of the usual exponential function, that $e^{Ax}e^{Bx} = e^{(A+B)x}$. In particular, e^{Ax} is invertible and $(e^{Ax})^{-1} = e^{-Ax}$.

Proposition 2.2.10. *Assume that $K = k$ is a constant δ-field. Then, for every $A \in k^{n\times n}$ there exits a Picard-Vessiot extension of K for $\delta(y) = Ay$.*

Proof. Set

$$Y = e^{Ax} = \sum_{i=0}^{\infty} A^i \tfrac{x^i}{i!} \in k[[x]]^{n\times n} \subseteq k((x))^{n\times n}.$$

We consider $k((x))$ as a δ-field as in (Example 1.1.5). Then $\delta(Y) = AY$. As $k((x))^\delta = k$ (Exercise 1.1.6) and $Y \in \mathrm{GL}_n(k((x)))$. It is clear that $k(Y_{i,j}|\ 1 \le i, j \le n) \subseteq k((x))$ is a Picard-Vessiot extension for $\delta(y) = Ay$. □

The following proposition discusses another instance where Picard-Vessiot extensions always exist.

Proposition 2.2.11. *Let k be a field of characteristic zero and $K = k(x)$ with derivation $\delta = \frac{d}{dx}$. Let $A \in K^{n\times n}$. Then there exists a Picard-Vessiot extension of K for $\delta(y) = Ay$.*

Proof. We will use a basic property of the ring $k[[x]]$ of formal power series over k: The units in $k[[x]]$ are exactly the elements of the form $f = a_0 + a_1x + a_2x^2 + \ldots$ with $a_0 \neq 0$. (To see this, make an ansatz for f^{-1}.)

Let $a \in k$ be a regular point of $A \in k(x)^{n\times n}$, i.e., none of the denominators occurring in A vanishes at a. Let $k[[x-a]]$ denote the ring of formal power series over k in the variable $x - a$. Then $k[x] = k[x-a] \subseteq k[[x-a]]$. If $h \in k[x] = k[x-a]$ is a denominator occurring in one of the entries of A, then h is invertible in $k[[x-a]]$ because h does not vanish at a. Therefore $A \in k[[x-a]]^{n\times n}$. So we may write $A = \sum_{i=0}^{\infty} A_i(x-a)^i$, with $A_i \in k^{n\times n}$. We now make an ansatz

$$Y = \sum_{i=0}^{\infty} Y_i \frac{(x-a)^i}{i!} \in k[[x-a]]^{n\times n}$$

for a fundamental solution matrix Y for $\delta(y) = Ay$, where the $Y_i \in k^{n\times n}$ are still to be determined. We have

$$\delta(Y) = \sum_{i=0}^{\infty} Y_i \cdot i\ \frac{(x-a)^{i-1}}{i!} = \sum_{i=0}^{\infty} Y_{i+1} \frac{(x-a)^i}{i!}.$$

Comparing the coefficients with

$$AY = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} A_j Y_{i-j} \right) \frac{(x-a)^i}{i!},$$

yields the recurrence formula

$$Y_{i+1} = \sum_{j=0}^{i} A_j Y_{i-j} \tag{2.9}$$

for $i \in \mathbb{N}$. Thus we can choose Y_0 arbitrarily, say $Y_0 = I_n$ (the $n \times n$ identity matrix), and then all the other Y_i's are determined by (2.9). By construction, we have $\delta(Y) = AY$. To see that Y is invertible, note that the evaluation at a defines a morphism $k[[x-a]] \to k$, $f \mapsto f(a)$ of k-algebras. So $\det(Y)(a) = \det(Y(a)) = \det(Y_0) = 1$. Thus $Y \in \mathrm{GL}_n(k[[x-a]])$. The subfield $k(x)(Y_{ij}|\ 1 \le i, j \le n)$ of $k((x-a))$ generated by the entries of Y is a Picard-Vessiot extension for $\delta(y) = Ay$ because $k((x-a))^\delta = k$. (Here the derivation on $k((x-a))$ is $\frac{d}{d(x-a)}$, (as in Example 1.1.5) but note that $\frac{d}{d(x-a)} = \frac{d}{dx}$ on $k(x)$.)

□

Unfortunately, Picard-Vessiot extension do not always exist. This is illustrated in the following example.

Example 2.2.12 (Seidenberg)**.** We first construct the δ-field K. Let $\mathbb{R}[z_1, z_2]$ be the polynomial ring over $\mathbb{R}$ in two variables. Define a derivation δ on $\mathbb{R}[z_1, z_2]$ that is zero on $\mathbb{R}$ and satisfies $\delta(z_1) = z_2$ and $\delta(z_2) = -4z_1$ (cf. Exercise 1.1.10). Then $\delta(4z_1^2 + z_2^2 + 1) = 8z_1z_2 + 2z_2(-4z_1) = 0$ and so $(4z_1^2 + z_2^2 + 1) \subseteq \mathbb{R}[z_1, z_2]$ is a δ-ideal.

Note that $4z_1^2 + z_2^2 + 1$ is irreducible. In fact, $4z_1^2 + z_2^2 + 1$ is irreducible, even when considered as an element of $\mathbb{C}[z_1, z_2]$. To see this, suppose that $4z_1^2 + z_2^2 + 1 = fg$ is a non-trivial factorization in $\mathbb{C}[z_1, z_2]$. Then f and g must have degree 1, say $f = f_1z_1 + f_2z_2 + f_3$ and $g = g_1z_1 + g_2z_2 + g_3$ with $f_1, f_2, f_3, g_1, g_2, g_3 \in \mathbb{C}$. As all coefficients must be non-zero, we can assume $f_1 = 1$ and $g_1 = 4$. Then $fg = (z_1 + f_2z_2 + f_3)(4z_1 + g_2z_2 + g_3) = 4z_1^2 + f_2g_2z_2^2 + (g_2 + 4f_2)z_1z_2 + (4f_3 + g_3)z_1 + (f_2g_3 + f_3g_2)z_2 + f_3g_3$. From $f_2g_2 = 1$ and $g_2 + 4f_2 = 0$ it follows that $g_2^2 = -4$. Similarly, from $f_3g_3 = 1$ and $4f_3 + g_3 = 0$ it follows that $g_3^2 = -4$. Multiplying the equation $f_2g_3 + f_3g_2 = 0$ with g_2g_3 and using $f_2g_2 = 1,\ g_3f_3 = 1$ yields $g_3^2 + g_2^2 = 0$. But $g_3^2 + g_2^2 = -4 - 4 = -8$; a contradiction. Thus $4z_1^2 + z_2^2 + 1 \in \mathbb{C}[z_1, z_2]$ is irreducible.

Therefore $(4z_1^2 + z_2^2 + 1) \subseteq \mathbb{R}[z_1, z_2]$ is a prime ideal and $R = \mathbb{R}[z_1, z_2]/(4z_1^2 + z_2^2 + 1)$ is an integral domain. So we can consider the differential field $K = \mathrm{Frac}(R)$.

We will next show that $K^\delta = \mathbb{R}$. As a first step in this direction, we show that K^δ is algebraic over $\mathbb{R}$. Suppose, for a contradiction, that there exists a $c \in K^\delta$ that is transcendental over $\mathbb{R}$. Then K is algebraic over $\mathbb{R}(c)$. By Lemma 1.1.14 the unique derivation on K extending the trivial derivation on $\mathbb{R}(c)$ is trivial. This contradicts the fact that $\delta^2(z_1) = z_2$ and that the image of z_2 in K is non-zero. Therefore K^δ is algebraic over $\mathbb{R}$. So there are only two possibilities, either $K^\delta = \mathbb{R}$ or $K^\delta = \mathbb{C}$.

Suppose, for a contradiction, that $K^\delta = \mathbb{C}$. Then $K \otimes_{\mathbb{R}} \mathbb{C}$ contains $\mathbb{C} \otimes_R \mathbb{C}$. Since

$$\begin{aligned}\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{R}[x]/(x^2 + 1) \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[x]/(x^2 + 1) = \mathbb{C}[x]/((x + i)(x - i)) = \\ = \mathbb{C}[x]/(x + i) \times \mathbb{C}[x]/(x - i) = \mathbb{C} \times \mathbb{C}\end{aligned}$$

by the Chinese Remainder Theorem, we see that $K \otimes_{\mathbb{R}} \mathbb{C}$ is not an integral domain. On the other hand, $\mathbb{C}[z_1, z_2]/(4z_1^2 + z_2^2 + 1)$ is an integral domain because $4z_1^2 + z_2^2 + 1 \in \mathbb{C}[z_1, z_2]$ is irreducible. Note that $K \otimes_{\mathbb{R}} \mathbb{C}$ is isomorphic to the localization of $R \otimes_{\mathbb{R}} \mathbb{C}$ at $\{r \otimes 1 \in R \otimes_{\mathbb{R}} \mathbb{C} |\ r \in R \setminus \{0\}\}$. But $R \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[z_1, z_2]/(4z_1^2 + z_2^2 + 1)$ is an integral domain and any localization of an integral domain is an integral domain. Thus $K \otimes_{\mathbb{R}} \mathbb{C}$ is an integral domain; a contradiction.

So K is a δ-field with $K^\delta = \mathbb{R}$. We will show that there does not exist a Picard-Vessiot extension of K for $\delta^2(y) + y = 0$. In fact, we will show that any δ-field extension L of K that contains a non-zero solution of $\delta^2(y) + y = 0$ satisfies $K^\delta \subsetneq L^\delta$. If $\eta \in L$ is a non-zero solution of $\delta^2(y) + y = 0$, then

$$\delta\left(\frac{\delta(\eta)}{\eta}\right) = \frac{\delta^2(\eta)\eta - \delta(\eta)^2}{\eta^2} = -1 - \left(\frac{\delta(\eta)}{\eta}\right)^2.$$

So $u = \frac{\delta(\eta)}{\eta}$ satisfies $\delta(u) = -1 - u^2$. We have

$$\delta(1 + u^2) = 2u\delta(u) = -2u(1 + u^2) \tag{2.10}$$

and, if $a_1, a_2 \in K$ denote the images of z_1 and z_2 respectively, then

$$\begin{aligned}\delta(a_1 + a_2u - a_1u^2) = a_2 - 4a_1u + a_2(-1 - u^2) - a_2u^2 - a_12u(-1 - u^2) = \\ = -2a_1u - 2a_2u^2 + 2a_1u^3 = -2u(a_1 + a_2u + a_1u).\end{aligned} \tag{2.11}$$

If $1+u^2=0$, then $u=i$ or $-i$ and we are done since $i \in L^\delta \smallsetminus K^\delta$. So we may assume $1+u^2 \neq 0$. From equations (2.10) and (2.11) it follows that $c = \frac{a_1+a_2u-a_1u^2}{1+u^2} \in L^\delta$. If $c \notin K^\delta$ we are done. So we may assume $c \in K^\delta = \mathbb{R}$. Then

$$(-c-a_1)u^2 + a_2u + a_1 - c = 0.$$

Solving this equation for u, we find that $\sqrt{a_2^2 - 4(-c-a_1)(a_1-c)} \in K(u) \subseteq L$. But $a_2^2 - 4(-c-a_1)(a_1-c) = a_2^2 + 4(a_1^2 - c^2) = -1 - 4c^2 < 0$. Therefore $i \in L$ and so $i \in L^\delta \smallsetminus K^\delta$.

Exercise 2.2.13. *Let $f \in \mathbb{R}[z_1, z_2]$ be such that f is irreducible in $\mathbb{C}[z_1, z_2]$. Let δ be a derivation on $\mathbb{R}[z_1, z_2]$ such that $\delta(a) = 0$ for all $a \in \mathbb{R}$. Assume that (f) is a δ-ideal of $\mathbb{R}[z_1, z_2]$ such that the derivation on $\mathbb{R}[z_1, z_2]/(f)$ is non-trivial. Set $L = \mathrm{Frac}(\mathbb{R}[z_1, z_2]/(f))$. Show that $L^\delta = \mathbb{R}$.*

Having discussed the existence of Picard-Vessiot extensions, we now work towards their uniqueness. For this we will need a fundamental result from algebraic geometry.

Theorem 2.2.14 (Hilbert's Nullstellensatz (weak form))**.** *Let k be a field (of arbitrary characteristic) and let L be a field extension of k that is finitely generated as a k-algebra. Then L is a finite (algebraic) extension of k.*

Proof. We first show that L/k is algebraic. Suppose, for a contradiction, that there exist an element $a \in L$ that is transcendental over k. Applying Theorem 1.3.10 to the inclusion $k[a] \subseteq L$, yields an $f \in k[a]$ such that for every prime ideal $\mathfrak{p}$ of $k[a]$ with $f \notin k[a]$ there exists a prime ideal $\mathfrak{P}$ of L with $\mathfrak{P} \cap k[a] = \mathfrak{p}$. But as L is a field, the only prime ideal of L is $\mathfrak{P} = (0)$. Thus, to obtain a contradiction, it suffices to show that $k[a]$ contains a non-zero prime ideal $\mathfrak{p}$ with $f \notin \mathfrak{p}$. Let b be any element in the algebraic closure $\overline{k}$ of k, that is not a root of f. Then the kernel $\mathfrak{p}$ of the k-algebra morphism $k[a] \to \overline{k}$ determined by $a \mapsto b$ is a non-zero prime ideal of $k[a]$ with $f \notin \mathfrak{p}$. Thus L/k is algebraic. Because L/k is algebraic and finitely generated, it must be finite. □

The following two corollaries are alternative formulations of Hilbert's weak Nullstellensatz.

Corollary 2.2.15. *Let k be a field and let R be a finitely generated k-algebra. If $\mathfrak{m}$ is a maximal ideal in R, then $R/\mathfrak{m}$ is a finite field extension of k. In particular, there exists a morphism of k-algebras from R into a finite field extension of k.*

Proof. Because $\mathfrak{m}$ is maximal, the quotient $L = R/\mathfrak{m}$ is a field and so Theorem 2.2.14 applies. □

The following more classical reformulation explains the naming "Nullstellensatz":

Corollary 2.2.16. *Let $F \subseteq k[y_1, \ldots, y_n]$ be a set of polynomials such that $1 \notin (F) \subseteq k[y_1, \ldots, y_n]$. Then the system of algebraic equations $F = 0$ has a solution in a finite field extension of k.*

Proof. Since $1 \notin (F)$, there exists a maximal ideal $\mathfrak{m}$ of $k[y_1, \ldots, y_n]$ containing F. By Corollary 2.2.15 the quotient $k[y_1, \ldots, y_n]/\mathfrak{m}$ is a finite field extension of k. The images of the variables $y_1, \ldots, y_n$ in $k[y_1, \ldots, y_n]/\mathfrak{m}$ are a solution of $F = 0$. □

We are now prepared to tackle the uniqueness of Picard-Vessiot extensions.

Theorem 2.2.17 (Uniqueness of Picard-Vessiot extensions and Picard-Vessiot rings)**.** *Let $A \in K^{n\times n}$ and let R_1 and R_2 be two Picard-Vessiot rings for $\delta(y) = Ay$. Then there exists a finite field extension k' of $k = K^\delta$ such that $R_1 \otimes_k k'$ and $R_2 \otimes_k k'$ are isomorphic. In particular, if K^δ is algebraically closed, then R_1 and R_2 are isomorphic. Similarly, if K^δ is algebraically closed, and L_1/K and L_2/K are Picard-Vessiot extensions for $\delta(y) = Ay$, then L_1/K and L_2/K are isomorphic.*

Proof. The argument here is quite similar to the proof of Proposition 2.2.7. By Lemma 2.2.6 we know that $R_1 \otimes_K R_2 = R_1 \otimes_k (R_1 \otimes_K R_2)^\delta$ and that the k-algebra $(R_1 \otimes_K R_2)^\delta$ is finitely generated. By Corollary 2.2.15 there exists a finite field extension k' of k and a morphism $(R_1 \otimes_K R_2)^\delta \to k'$ of k-algebras. The morphism

$$R_2 \to R_1 \otimes_K R_2 = R_1 \otimes_k (R_1 \otimes_K R_2)^\delta \to R_1 \otimes_k k'$$

extends k'-linearly to a morphism $R_1 \otimes_k k' \to R_2 \otimes_k k'$. Because R_1 and therefore also $R_1 \otimes_k k'$ (Corollary 1.3.9) is δ-simple, this morphism is injective. An argument involving fundamental solution matrices (as in the proof of Proposition 2.2.7) shows that this map is also surjective and therefore an isomorphism.

For $i = 1, 2$ let L_i/K be Picard-Vessiot extensions with $Y_i \in \mathrm{GL}_n(L_i)$ such that $\delta(Y_i) = AY_i$ and the entries of Y_i generated L_i as a field extension of K. By Proposition 2.2.7 the K-algebra R_i generated by the entries of Y_i and $\frac{1}{\det(Y_i)}$ is a Picard-Vessiot ring for $\delta(y) = Ay$. Assuming that K^δ is algebraically closed, we know from the above that R_1 and R_2 are isomorphic as K-δ-algebras. This isomorphism extends to the quotient fields, yielding an isomorphism of δ-field extensions between L_1/K and L_2/K. □

Similarly to the existence, if K^δ is not algebraically closed, the uniqueness can fail. This is illustrated in the following example.

Example 2.2.18. We define a derivation δ on the polynomial ring $\mathbb{R}[z_1, z_2]$ by setting $\delta(\lambda) = 0$ for $\lambda \in \mathbb{R}$, $\delta(z_1) = z_2$ and $\delta(z_2) = -z_1$. Set $f_1 = z_1^2 + z_2^2 + 1$ and $f_2 = z_1^2 + z_2^2 - 1$. As

$$\delta(z_1^2 + z_2^2 \pm 1) = 2z_1\delta(z_1) + 2z_2\delta(z_2) = 2z_1z_2 + 2z_2(-z_1) = 0,$$

we see that $I_1 = (f_1)$ and $I_2 = (f_2)$ are δ-ideals of $\mathbb{R}[z_1, z_2]$ and so $R_i = \mathbb{R}[z_1, z_2]/(f_i)$ is an $\mathbb{R}$-δ-algebra ($i = 1, 2$). We claim that R_i is a Picard-Vessiot ring (over $\mathbb{R}$) for $\delta^2(y) + y = 0$. We will show that R_1 is Picard-Vessiot ring. The proof for R_2 is practically identical. It is straight forward to check that $f_1 \in \mathbb{C}[z_1, z_2]$ is irreducible (cf. Example 2.2.12). Therefore R_1 is an integral domain. Let L_1 be its field of fractions.

Let $y_1, y_2 \in L_1$ denote the images of z_1, z_2 respectively. Then y_1, y_2 are $\mathbb{R}$-linearly independent solutions of $\delta^2(y) + y = 0$, e.g., because $\mathrm{wr}(y_1, y_2) = -y_1^2 - y_2^2 = 1 \neq 0$. Thus it suffices to show that $L_1^\delta = \mathbb{R}$. However, this follows from Exercise 2.2.13.

Thus R_1 and R_2 are Picard-Vessiot rings (over $\mathbb{R}$) for $\delta^2(y) + y = 0$. To see that they are not isomorphic, it suffices to show that they are not isomorphism as $\mathbb{R}$-algebras. But note that $f_1 = 0$ has not solution in $\mathbb{R}$ whereas $f_2 = 0$ does have solutions in $\mathbb{R}$. In other words, there exists a morphism $R_2 \to \mathbb{R}$ of $\mathbb{R}$-algebras, but there does not exist a morphism $R_1 \to \mathbb{R}$ of $\mathbb{R}$-algebras. Thus R_1 and R_2 cannot be isomorphic.

Exercise 2.2.19. *Let $A \in K^{n\times}$. Let R_1 and R_2 be Picard-Vessiot rings for $\delta(y) = Ay$. Show that there exists a finite field extension k' of k and a $K \otimes_k k'$-δ-isomorphism $R_1 \otimes_k k' \simeq R_2 \otimes_k k'$. Find such a k' and isomorphism for the Picard-Vessiot rings R_1, R_2 in Example 2.2.18.*

Remark 2.2.20. *If there exists a Picard-Vessiot extension L/K for $\delta(y) = Ay$, then the set of all isomorphism classes of all Picard-Vessiot extensions for $\delta(y) = Ay$ is in bijection with $H^1(K^\delta, G)$, where G is the differential Galois group of L/K. (This is just a side remark, so don't worry if you do not understand it.)*

Exercise 2.2.21. *Assume that $k = K^\delta$ is algebraically closed. Let $A \in K^{n\times n}$ and consider the universal solution algebra $U = K\big[X_{ij}, \frac{1}{\det(X)} |\ 1 \leq i, j \leq n\big]$ for $\delta(y) = Ay$. Let $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be two maximal δ-ideals in U. Show that there exists a matrix $C \in \mathrm{GL}_n(k)$ such that $\mathfrak{m}_2 = \{p(XC) |\ p \in \mathfrak{m}_1\}$.*

2.3 Relation with the classical theory of differential equations

In the classical (analytic) approach to ordinary differential equations one is usually concerned with an explicit system

$$y'(x) = f(x, y(x)),$$

where $y(x) = \begin{pmatrix} y_1(x) \\ \vdots \\ y_n(x) \end{pmatrix}$ and $f\colon U \to \mathbb{R}^n$, for some open subset U of $\mathbb{R}^{n+1}$. For linear differential systems one has $f(x, y_1, \ldots, y_n) = A(x) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, where $A(x)$ is an $n \times n$ matrix whose entries $A_{ij}\colon I \to \mathbb{R}$ are functions on some open interval $I \subseteq \mathbb{R}$. The main existence and uniqueness result asserts that if the A_{ij}'s are continuous, then the initial value problem

$$y'(x) = A(x)y(x),\ y(x_0) = y_0$$

has a unique solution $y \in C^1(I, \mathbb{R}^n)$ for any $x_0 \in I$ and $y_0 \in \mathbb{R}^n$. This immediately implies that the $\mathbb{R}$-vector space of solutions of $y'(x) = A(x)y(x)$ in $C^1(I, \mathbb{R}^n)$ has dimension n. You should have seen these results in your class "Gewöhnliche Differentialgleichungen" but if you would like a reference you can see Theorem 3.9 in [Tes12].

So what is the connection between the analytic approach and our algebraic approach? In this regard, maybe the most pressing question is "What is K in the analytic approach?" This question does not really have a universal answer but depends on the context, or more precisely on the coefficients A_{ij}. For example, for constant differential systems, i.e., if $A(x) \in \mathbb{R}^{n\times n}$ does not depend on x, then the most natural choice for the base differential field K would be $K = \mathbb{R}$ with the trivial derivation $\delta = 0$. On the other hand, if all the $A_{ij}\colon I \to \mathbb{R}$ are rational functions, i.e., of the form $x \mapsto \frac{f(x)}{g(x)}$, for polynomials f, g with $g(x) \neq 0$ for all $x \in I$, then, a natural choice for (K, δ) would be $K = \mathbb{R}(x)$, the field of rational functions in the variable x, with derivation $\delta = \frac{d}{dx}$. In general, one might wish to choose K as "the smallest differential field containing all the coefficients A_{ij} of A". This does not quite make sense, for example, if the A_{ij}'s are not differentiable, they can't really belong to any differential ring or field. Also, the ring $C^\infty(I, \mathbb{R})$ contains zero-divisors, so if, e.g., $A_{11}(x)A_{12}(x) = 0$ for all $x \in I$ but A_{11} and A_{12} are not the zero-function, there cannot exist a field containing all A_{ij}'s. In practice, such examples rarely arise. In fact, if you look at the literature, you'll find that most examples of practical relevance have rational function coefficients. A particular nice class of functions to consider is the class $\mathrm{An}(I, \mathbb{R})$ of *real analytic* functions $f\colon I \to \mathbb{R}$. Recall that a function $f \in C^\infty(I, \mathbb{R})$ is *real*

analytic if for every $x_0 \in I$ the Taylor series $T(x,f) = \sum_{i=0}^{\infty} \frac{f^{(i)}(x_0)}{i!}(x-x_0)^i$ converges to $f(x)$ for all x in an open neighborhood of x_0. Note that $\mathrm{An}(I,\mathbb{R})$ equipped with the usual derivation $\frac{d}{dx}$ is a differential ring and that the map $\mathrm{An}(I,\mathbb{R}) \to \mathbb{R}[[x-x_0]]$ that associates to every $f \in \mathrm{An}(I,\mathbb{R})$ its Taylor series is injective. In particular, $\mathrm{An}(I,\mathbb{R})$ is an integral domain and so its field of fractions is naturally a differential field. If we equip $\mathbb{R}[[x-x_0]]$ with a derivation δ as in Example 1.1.5, then $\mathrm{An}(I,\mathbb{R}) \to \mathbb{R}[[x-x_0]]$ is in fact an embedding of differential rings and so $\mathrm{Frac}(\mathrm{An}(I,\mathbb{R}))$ embeds into $\mathbb{R}((x-x_0))$. As $\mathbb{R}((x-x_0))^\delta = \mathbb{R}$ it follows that also $\mathrm{Frac}(\mathrm{An}(I,\mathbb{R}))^\delta = \mathbb{R}$.

Assume now that all coefficients A_{ij} are real analytic functions on I. As the intersection of a family of δ-subfields of $\mathrm{Frac}(\mathrm{An}(I,\mathbb{R}))$ containing $\mathbb{R}$ and all the A_{ij}'s is a δ-subfield containing $\mathbb{R}$ and all the A_{ij}'s, there exists a smallest δ-subfield of $\mathrm{Frac}(\mathrm{An}(I,\mathbb{R}))$ containing $\mathbb{R}$ and all the A_{ij}'s. This δ-subfield of $\mathrm{Frac}(\mathrm{An}(I,\mathbb{R}))$ is a natural choice for the base differential field K.

If all the coefficients A_{ij} are real analytic functions on I, then also the solutions to $y'(x) = A(x)y(x)$ are real analytic functions on I. In particular, there exists a fundamental solution matrix $Y \in \mathrm{GL}_n(\mathrm{An}(I,\mathbb{R}))$ for $y'(x) = A(x)y(x)$. (This result is sometimes referred to as the Cauchy-Kowalevski theorem). Since $\mathrm{Frac}(\mathrm{An}(I,\mathbb{R}))^\delta = \mathbb{R}$, the subfield L of $\mathrm{Frac}(\mathrm{An}(I,\mathbb{R}))$ generated over K by the entries of Y is a Picard-Vessiot extension of K. Note that L can also be described as the subfield of $\mathrm{Frac}(\mathrm{An}(I,\mathbb{R}))$ generated over K by all the solutions of $y'(x) = A(x)y(x)$.

Example 2.3.1. Consider the linear differential equation $\delta^2(y) + y = 0$ over $K = \mathbb{R}$ with the trivial derivation. The functions $\cos(x)$, $\sin(x) \in \mathrm{An}(\mathbb{R},\mathbb{R})$ are a basis for the $\mathbb{R}$-vector space of solutions in $\mathrm{An}(\mathbb{R},\mathbb{R})$. By the above discussion, it is clear that $L = \mathbb{R}(\cos(x),\sin(x)) \subseteq \mathrm{Frac}(\mathrm{An}(\mathbb{R},\mathbb{R}))$ is a Picard-Vessiot extension for $\delta^2(y) + y = 0$. Moreover, $R = \mathbb{R}[\cos(x),\sin(x)]$ is a Picard-Vessiot ring for $\delta^2(y) + y = 0$. Note that

$$\mathrm{An}(\mathbb{R},\mathbb{R}) \subseteq \mathrm{An}(I,\mathbb{R}) \subseteq \mathbb{R}[[x]]$$

for any open interval I in $\mathbb{R}$ containing 0. So it really does not matter if we consider $\mathbb{R}[\cos(x),\sin(x)]$ inside $\mathrm{An}(\mathbb{R},\mathbb{R})$ or directly inside $\mathbb{R}[[x]]$.

We have seen in Section 2.2 that Picard-Vessiot rings and extensions are somewhat better behaved over algebraically closed fields of constants. Also complex analytic functions are better behaved than real analytic functions. Indeed, a basic result in complex analysis is that a complex valued function on an open subset of $\mathbb{C}$ is holomorphic (i.e., complex differentiable) if and only if it is analytic. Also, recall that for an open connected subset Ω of $\mathbb{C}$ the ring of holomorphic (=analytic) functions is an integral domain with field of fractions the field of meromorphic functions $\mathcal{M}(\Omega)$ on Ω. Recall that a function is meromorphic, if around every point it can be represented by a convergent Laurant series (only finitely many negative exponents allowed). Note that if $x_0 \in \Omega_1 \subseteq \Omega_2$, then

$$\mathcal{M}(\Omega_1) \subseteq \mathcal{M}(\Omega_2) \subseteq \mathbb{C}((x-x_0))$$

and these are inclusions of differential fields. Consider a linear differential system $y'(x) = A(x)y(x)$, where the A_{ij}'s are holomorphic functions on some open connected subset. Then the same arguments and results as in the case of real analytic functions discussed above apply.

Let us look in more detail at the special case of rational functions. So consider a linear differential system $y'(x) = A(x)y(x)$ with $A(x) \in \mathbb{C}(x)^{n\times n}$. We fix our base differential field K as $K = \mathbb{C}(x)$ with derivation $\frac{d}{dx}$. Chosse $x_0 \in \mathbb{C}$ such that x_0 is not a pole of any of the entries of $A(x)$. Then there exists an $\varepsilon > 0$ such that all entries A_{ij} of A are

holomorphic on the open disk $B(x_0, \varepsilon) = \{x \in \mathbb{C} |\ |x - x_0| < \varepsilon\}$. Moreover, there exists a fundamental solution matrix Y for $y'(x) = A(x)y(x)$ whose entries Y_{ij} are holomorphic functions on $\Omega = B(x_0, \varepsilon)$. Thus the field extension $L = K(Y_{ij} |\ 1 \leq i, j \leq n) \subseteq \mathcal{M}(\Omega)$ of $K = \mathbb{C}(x)$ is a Picard-Vessiot extension for $y'(x) = A(x)y(x)$. Therefore also $R = K[Y_{ij}, \frac{1}{\det(Y)} |\ 1 \leq i, j \leq n] \subseteq \mathcal{M}(\Omega)$ is a Picard-Vessiot ring for $y'(x) = A(x)y(x)$.

One of the miracles of differential Galois theory is that this Picard-Vessiot ring can also be constructed in a completely different algebraic fashion that, a priori, does not seem to be related to holomorphic functions: Consider the universal solution algebra $U = K\big[X_{ij}, \frac{1}{\det(X)} |\ 1 \leq i, j \leq n\big]$ with derivation $\delta(X) = AX$ and choose any maximal differential ideal $\mathfrak{m}$ of U. Then, it follows from Theorem 2.2.17 that $U/\mathfrak{m}$ is isomorphic to R.

2.4 Infinite Picard-Vessiot extensions

Modern Galois theory is mainly concerned with actions of absolute Galois groups (i.e., the Galois group of the separable algebraic closure) on certain geometric objects, rather than with the Galois groups of polynomials. Knowing the Galois group of one specific polynomial $f \in \mathbb{Q}[x]$ only tells you something about the solutions of that specific polynomial and so, unless that polynomial is for some reason particularly interesting, knowing its Galois group is maybe not so interesting either, since that does not really tell you much about $\mathbb{Q}$ or $\overline{\mathbb{Q}}$. However, knowing (what ever that means) the absolute Galois group of $\mathbb{Q}$ would be a significant achievement towards a better understanding of the arithmetic of $\mathbb{Q}$.

The situation in differential Galois theory is similar. Surely, there is an interest in obtaining a better understanding of the algebraic properties of solutions of certain explicit linear differential equations. But what can be said about *all* solutions to *all* linear differential equations over K? Is there a differential analog of the absolute Galois group, i.e., is there an absolute differential Galois group of K that governs all the differential Galois groups of linear differential systems over K?

We will see that the answer is "yes". To describe the differential analog of the algebraic closure we need to allow families of linear differential systems and not just a single differential system in the definition of Picard-Vessiot extensions. Note that the algebraic closure of a field k can be defined as the splitting field of the family of all polynomials over k. We will follow a similar approach here.

We consider a family $\mathcal{F} = (\delta(y) = A_i y)_{i \in I}$ of linear differential systems over K. Here I is an arbitrary index set and $A_i \in K^{n_i \times n_i}$ for some $n_i \geq 1$. The length of the vector y of variables may of course depend of i but we allow ourselves the little abuse of notation to not indicate this dependence explicitly.

Most of the definitions and results we discussed earlier for a single linear differential system generalize to the context of families of linear differential systems in a rather straight forward manner.

Definition 2.4.1. *A δ-field extension L/K is a* Picard-Vessiot extension for the family $\mathcal{F} = (\delta(y) = A_i y)_{i \in I}$ *if*

(i) *for every $i \in I$ there exists a matrix $Y_i \in \mathrm{GL}_n(L)$ such that $\delta(Y_i) = AY_i$ and L is generated as a field extension of K be the entries of all Y_i's and*

(ii) *$L^\delta = K^\delta$.*

Definition 2.4.2. *A δ-simple K-δ-algebra is a* Picard-Vessiot ring for the family $\mathcal{F} = (\delta(y) = A_i y)_{i \in I}$ *if*

(i) *for every $i \in I$ there exists a matrix $Y_i \in \mathrm{GL}_n(R)$ such that $\delta(Y_i) = AY_i$ and R is generated as a K-algebra by the entries of all Y_i's and $\frac{1}{\det(Y_i)}$ and*

(ii) $R^\delta = K^\delta$.

Similarly to Proposition 2.2.7 we have:

Proposition 2.4.3. *If R is a Picard-Vessiot ring for $\mathcal{F} = (\delta(y) = A_i y)_{i \in I}$, then $\mathrm{Frac}(R)/K$ is Picard-Vessiot extension for $\mathcal{F}$. Conversely, if L/K is a Picard-Vessiot extension for $\mathcal{F}$, and the matrices Y_i are as in (i) of Definition 2.4.1, then the K-algebra R generated by the entries of all Y_i's and $\frac{1}{\det(Y_i)}$ is a Picard-Vessiot ring for $\mathcal{F}$.*

Proof. The first claim is clear from Lemma 1.3.4. For the second claim it suffices to show that R (defined as in the proposition) is δ-simple. Suppose, for a contradiction, that J is a non-trivial δ-ideal of R and let $f \in J$ be a non-zero element. Then there are $i_1, \dots, i_m \in I$ such that f lies in the K-algebra S generated by the entries of $Y_{i_1}, \dots, Y_{i_m}$ and $\frac{1}{\det(Y_{i_1})}, \dots, \frac{1}{\det(Y_{i_m})}$. Note that

$$Y = \begin{pmatrix} Y_{i_1} & & & \\ & Y_{i_2} & & \\ & & \ddots & \\ & & & Y_{i_m} \end{pmatrix}$$

is a fundamental solution matrix for $\delta(y) = Ay$ where

$$A = \begin{pmatrix} A_{i_1} & & & \\ & A_{i_2} & & \\ & & \ddots & \\ & & & A_{i_m} \end{pmatrix}.$$

Moreover, $\mathrm{Frac}(S) \subseteq L$ and so $\mathrm{Frac}(S)^\delta = K^\delta$. It therefore follows form Propostion 2.2.7 that S is a Picard-Vessiot ring for $\delta(y) = Ay$. In particular, S is δ-simple. But the δ-ideal $S \cap J$ of S contains f; a contradiction. □

Generalizing Theorem 2.2.8 we have:

Theorem 2.4.4 (Existence of infinite Picard-Vessiot extensions)**.** *Assume that K^δ is algebraically closed. Let $\mathcal{F}$ be a family of linear differential systems over K. Then there exists a Picard-Vessiot extension (and therefore also a Picard-Vessiot ring) for $\mathcal{F}$.*

Proof. Consider the set (cf. Remark 2.4.5) $\mathcal{S}$ of all pairs $(\mathcal{G}, M)$, where $\mathcal{G}$ is a subfamily of $\mathcal{F}$ and M/K is a Picard-Vessiot extension for $\mathcal{G}$. We define a partial order on $\mathcal{S}$ by $(\mathcal{G}_1, M_1) \leq (\mathcal{G}_2, M_2)$ if $\mathcal{G}_1 \subseteq \mathcal{G}_2$ and $M_1 \subseteq M_2$. If $(\mathcal{G}_i, M_i)_{i \in I}$ is any chain in $\mathcal{S}$, then also $(\cup \mathcal{G}_i, \cup M_i)$ belongs to $\mathcal{S}$. Therefore, Zorn's lemma yields the existence of a maximal element $(\mathcal{G}, M)$ in $\mathcal{S}$. We claim that $\mathcal{G} = \mathcal{F}$ (so that M is the sought for Picard-Vessiot extension for $\mathcal{F}$). Suppose that $\mathcal{G} \subsetneq \mathcal{F}$ and let $\delta(y) = Ay$ be an element from $\mathcal{F}$ that does not belong to $\mathcal{G}$. By Theorem 2.2.8 there exists a Picard-Vessiot extension M'/M for $\delta(y) = Ay$. But then M'/K is a Picard-Vessiot extension for the family containing $\mathcal{G}$ and $\delta(y) = Ay$. As $M \subseteq M'$, this contradicts the maximality of $(\mathcal{G}, M)$. □

Remark 2.4.5. *The above proof is not entirely rigorous. The problem is that $\mathcal{S}$ is not a set (but a proper class). This could be avoided by restricting the M's to be δ-subfields of a "sufficiently large" δ-field extension of K or by assuming that all M's belong to a*

"sufficiently large" set $\mathcal{M}$ of δ-field extension of K. For example, $\mathcal{M}$ could be a set (!) of δ-field extension of K such that every δ-field extension of K of cardinality at most $|K|$ is isomorphic to an element of $\mathcal{M}$. Alternatively, one could also use transfinite induction, but I did not want to bother talking about ordinals in case people are not familiar with that.

Theorem 2.4.6 (Uniqueness of infinite Picard-Vessiot extensions)**.** *Assume that K^δ is algebraically closed. Let L/K and L'/K be Picard-Vessiot extensions for a family $\mathcal{F}$ of linear differential systems over K. Then L/K and L'/K are isomorphic δ-field extensions of K. Similarly, any two Picard-Vessiot rings for $\mathcal{F}$ are isomorphic as K-δ-algebras.*

Proof. It suffices to treat the case of Picard-Vessiot extensions. For a subfamily $\mathcal{G}$ of $\mathcal{F}$ let $L_\mathcal{G}$ and $L'_\mathcal{G}$ denote the subfield of L and L' respectively generated by all the entries of fundamental solution matrices for linear differential systems in $\mathcal{G}$. Note that $L_\mathcal{G}/K$ and $L'_\mathcal{G}/K$ are Picard-Vessiot extensions for $\mathcal{G}$.

Let $\mathcal{S}$ be the set of all pairs $(\mathcal{G}, \phi)$, where $\mathcal{G}$ is a subfamily of $\mathcal{F}$ and $\phi\colon L_\mathcal{G} \to L'_\mathcal{G}$ is a K-δ-isomorphism. We can define a partial order on $\mathcal{S}$ by $(\mathcal{G}_1, \phi_1)) \leq (\mathcal{G}_2, \phi_2)$ if and only if $\mathcal{G}_1$ is contained in $\mathcal{G}_2$ and ϕ_2 extends ϕ_1. For any chain $(\mathcal{G}_i, \phi_i)_{i\in I}$ in $\mathcal{S}$ there exists an upper bound $(\mathcal{G}, \phi) \in \mathcal{S}$. Indeed we can choose $\mathcal{G} = \cup_{i\in I}\mathcal{G}_i$ and $\phi\colon L_\mathcal{G} \to L'_\mathcal{G}$ defined by $\phi(a) = \phi_i(a)$ for $a \in L_{\mathcal{G}_i}$.

By Zorn's lemma there exists a maximal element $(\mathcal{G}, \phi)$ in $\mathcal{S}$. It suffices to show that $\mathcal{G} = \mathcal{F}$ because then ϕ is the desired isomorphism. Suppose $\mathcal{G}$ is properly contained in $\mathcal{F}$. Let $\delta(y) = Ay$ be a linear differential system in $\mathcal{F}$ that is not in $\mathcal{G}$ and let $\mathcal{G}_1$ be the family consisting of $\mathcal{F}$ and $\delta(y) = Ay$. Then $L_{\mathcal{G}_1}/L_\mathcal{G}$ and $L'_{\mathcal{G}_1}/L'_\mathcal{G}$ are Picard-Vessiot extensions for $\delta(y) = Ay$. Because $L'_\mathcal{G}$ and $L_\mathcal{G}$ are isomorphic (via ϕ), it follows from Theorem 2.2.17 that also $L_{\mathcal{G}_1}$ and $L'_{\mathcal{G}_2}$ are isomorphic via an isomorphism extending ϕ. This contradicts the maximality of $(\mathcal{G}, \phi)$. □

Definition 2.4.7. *Assume that K^δ is algebraically closed. The Picard-Vessiot extension $\widetilde{K}/K$ for the family of all linear differential systems over K is called the* linear closure of *K.*

2.5 Differentially finite elements

From a Picard-Vessiot ring R for a linear differential system $\delta(y) = Ay$, we can (by Proposition 2.2.7) construct a Picard-Vessiot extension L/K for $\delta(y) = Ay$ by passing to the field of fractions $L = \mathrm{Frac}(R)$. In particular, we can pass from R to L without any reference to the differential system $\delta(y) = Ay$. The other way around, the situation seems a bit different. To construct a Picard-Vessiot ring R from a Picard-Vessiot extension L/K we need to choose a fundamental solution matrix $Y \in \mathrm{GL}_n(L)$. One easily sees that (given A) the K-δ-algebra $R = K\big[Y_{ij}, \frac{1}{\det(Y)} |\ 1 \leq i, j \leq n\big]$ does not depend on the choice of Y. However, it seems perceivable that R depends on A: Clearly, a Picard-Vessiot extension for $\delta(y) = Ay$ can also be a Picard-Vessiot extension for $\delta(y) = By$, where $B \in K^{m\times m}$ does not need to have the same dimension as A. For example, K/K is a Picard-Vessiot extension for every linear differential system that has a fundamental solution matrix in K. If $Y \in \mathrm{GL}_n(L)$ is such that $\delta(Y) = AY$ and $Z \in \mathrm{GL}_m(L)$ is such that $\delta(Z) = BZ$, it is a priori, unclear if $K\big[Y_{ij}, \frac{1}{\det(Y)} |\ 1 \leq i, j \leq n\big] = K\big[Z_{ij}, \frac{1}{\det(Z)} |\ 1 \leq i, j \leq m\big]$. However, in this section we will show that this is indeed the case using differentially finite elements.

Definition 2.5.1. *Let R be a K-δ-algebra. An element $a \in R$ is called* differentially finite*, or* δ-finite *for short, over K if it satisfies a non-trivial linear differential over K. Equivalently, the K-vector space generated by $a, \delta(a), \delta^2(a), \ldots$ is finite dimensional.*

One can think of δ-finite elements as being analogous to algebraic or integral elements in classical algebra. Note that $a \in R$ is δ-finite over K if and only if there exists a finite dimension K-subspace V of R such that $\delta(V) \subseteq V$. We will use this characterization of δ-finite elements in what follows.

Example 2.5.2. Let R be a K-δ-algebra, $A \in K^{n\times n}$. Assume $f = \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} \in R^n$ is a solution of $\delta(y) = Ay$. Then every f_i is δ-finite over K. Indeed, from $\delta(f) = Af$ it follows that the K-subspace of R generated by $f_1, \ldots, f_n$ is δ-finite.

Lemma 2.5.3. *Let R be a K-δ-algebra. Then the set of elements of R that are δ-finite over K form a K-δ-subalgebra of R.*

Proof. Let $f_1, f_2 \in R$ and for $i = 1, 2$ let V_i be a finite dimensional K-subspace of R with $f_i \in V_i$ and $\delta(V_i) \subseteq V_i$. Then $V_1 + V_2$ is a finite dimensional δ-stable K-subspace of R with $f_1 + f_2 \in V_1 + V_2$. So $f_1 + f_2$ is δ-finite over K. For $\lambda \in K$, we have $\lambda f_1 \in V_1$. So also λf_1 is δ-finite. The K-subspace V_1V_2 generated by all elements of the form h_1h_2 with $h_1 \in V_1$ and $h_2 \in V_2$ is δ-stable (use the Leibniz rule) and contains f_1f_2. This shows that the δ-finite elements are a K-subalgebra. Since $\delta(f_1) \in V_1$ they are K-δ-subalgebra. □

The following proposition characterizes the elements of a Picard-Vessiot extension that are contained in "the" Picard-Vessiot ring.

Proposition 2.5.4. *Let L/K be a Picard-Vessiot extension for a family $\mathcal{F} = (\delta(y) = A_iy)_{i\in I}$ of linear differential systems over K. Let R be the K-subalgebra of L generated by the entries of all Y_i's and $\frac{1}{\det(Y_i)}$, where $Y_i \in \mathrm{GL}_n(L)$ satisfies $\delta(Y_i) = AY_i$. Then R consists exactly of the elements of L that are δ-finite over K. In particular, R does not depend on the choice of $\mathcal{F}$ (only on L).*

Proof. Let $R' \subseteq L$ denote the set of all elements of L that are δ-finite over K. We know from Lemma 2.5.3 that R is a K-δ-subalgebra of L. By Example 2.5.2 the entries of all Y_i's lie in R'. If $Y \in \mathrm{GL}_n(L)$ satisfied $\delta(Y) = AY$ with $A \in K^{n\times n}$, then (as in the proof of Lemma 2.1.9)

$$\delta(Y^{-1}) = -Y^{-1}\delta(Y)Y^{-1} - Y^{-1}AYY^{-1} = -Y^{-1}A.$$

This shows that the K-subspace of L generated by the entries of Y^{-1} is stable under δ. Therefore $\frac{1}{\det(Y)} = \det(Y^{-1})$ is δ-finite by Lemma 2.5.3. So $R \subseteq R'$.

Assume that $f \in R'$ and let V be a finite dimensional K-subspace of L such that $f \in V$ and $\delta(V) \subseteq V$. Set $I = \{r \in R |\ rV \subseteq R\}$. One easily checks that I is a δ-ideal of R. Because V is finite dimensional, I is non-zero. As R is δ-simple we have $1 \in I$. But then $f \in V \subseteq R$. Thus $R = R'$ as claimed. □

Exercise 2.5.5. *Show that $\frac{1}{\log(x)}$ is not δ-finite over $(\mathbb{R}(x), \frac{d}{dx})$.*

Chapter 3

The differential Galois group

In this chapter we introduce the protagonist of this course: The differential Galois group of a linear differential equation. We also present some first example computations.

3.1 Algebraic groups and group schemes

As we will see in Section 3.2, the Galois group of a linear differential system is not just a plain group; it is a so-called *algebraic group*. Roughly speaking, algebraic groups are groups that can be described by algebraic equations in finitely many variables, e.g., the special linear group SL_n is described by the equation $\det(X) - 1 = 0$, where X is an $n \times n$ matrix of indeterminates. Group schemes are a generalization of algebraic groups, allowing for infinitely many variables. Group schemes occur as the Galois groups of infinite families of linear differential systems. For example, the absolute differential Galois group of a differential field is a group scheme.

In this section we introduce algebraic groups and group schemes and we discuss some of their basic properties. A more detailed study of algebraic groups is postponed to the later sections.

Throughout Section 3.1 k denotes an arbitrary field. Contrary to the previous chapter we do not assume that k has characteristic zero. This field k will be our "base field"; meaning, that the algebraic equations describing our algebraic groups will have coefficients in k. Examples of algebraic groups are easy to come by. For example, the general linear groups GL_n, the special linear groups SL_n, the orthogonal groups O_n, or the groups μ_n of n-th roots of unity, are algebraic groups. Note that in $k = \mathbb{Q}$ or $k = \mathbb{R}$, there are only two roots of unity (1 and -1), whereas in $k = \mathbb{C}$ there are exactly n n-th roots of unity. So, if we restrict ourselves to solutions of $x^n - 1 = 0$ in k only, we might miss out on some roots of unity and obtain somewhat undesirable results, e.g., a group of 4-th roots of unity that only has two elements (rather than the expected 4). In positive characteristic, the situation can be even more degenerate: In a field k of characteristic $p > 0$, the only p-th root of unity is 1, because $x^p - 1 = (x-1)^p$ in characteristic p. Note, however, that a k-algebra T might well contain non-trivial p-th roots of unity. For example, the image of $1 + x$ in $T = k[x]/(x^p)$ is a p-th root of unit. Moreover, for any k-algebra, the set $\mu_p(T) = \{g \in T |\ g^p = 1\}$ of p-th roots of unity in T is a group under multiplication.

Similarly, for any k-algebra T, we have groups $\mathrm{GL}_n(T) = \{g \in T^{n\times n} |\ \det(g) \in T^\times\}$, $\mathrm{SL}_n(T) = \{g \in T^{n\times n} |\ \det(g) = 1\}$, $\mathrm{O}_n(T) = \{g \in T^{n\times n} |\ gg^T = g^T g = I_n\}$. If $\psi\colon T \to T'$ is a morphism of k-algebras, we obtain an induced morphism of group $\mathrm{GL}_n(T) \to \mathrm{GL}_n(T')$ by applying ψ to the matrix entries. The identity map $T \to T$ induces the identity map

$\mathrm{GL}_n(T) \to \mathrm{GL}_n(T')$ and if $T \to T'$, $T' \to T''$ are two morphisms of k-algebras, then the map $\mathrm{GL}_n(T) \to \mathrm{GL}_n(T'')$ induced by the composition $T \to T' \to T''$ is the composition $\mathrm{GL}_n(T) \to \mathrm{GL}_n(T') \to \mathrm{GL}_n(T'')$. These two observations can be summarized by saying that GL_n is a functor from the category of k-algebras to the category of groups. For the other examples (i.e., for $\mathrm{SL}_n, \mathrm{O}_n$ or μ_n instead of GL_n) everything works the same way.

The algebraic groups, which we are about to define, will be functors from the category of k-algebras to the category of groups. But not any such functor is an algebraic group. The algebraic groups are exactly those functors that can be described by algebraic equations (in finitely many variables). In case you are not familiar with the notions "category" and "functor", take a look at Appendix A.2.

Definition 3.1.1. *A (covariant) functor X from the category of k-algebras to the category of sets is called* representable*, if it is isomorphic to the functor $T \rightsquigarrow \mathrm{Hom}(S,T)$ for some k-algebra T. In this case, we also say that X* is represented by *S or that S represents X.*

Here $\mathrm{Hom}(S,T)$ denotes the set of k-algebra morphisms from S to T. The functor $T \rightsquigarrow \mathrm{Hom}(S,T)$ is defined on morphism as follows: If $\psi\colon T \to T'$ is a morphism of k-algebras, then $\mathrm{Hom}(S,T) \to \mathrm{Hom}(S,T')$, $\varphi \mapsto \psi\varphi$. The following lemma gives a precise meaning to the idea of describing a functor by algebraic equations.

Lemma 3.1.2. *Let $F \subseteq k[x_1,\dots,x_n]$ be a set of polynomials in the variables $x_1,\dots,x_n$. For a k-algebra T, set $\mathbb{V}_T(F) = \{a \in T^n |\ f(a) = 0\ \forall\ f \in F\}$. Then the functor $T \rightsquigarrow \mathbb{V}_T(F)$ is representable. Indeed, it is represented by the finitely generated k-algebra $S = k[x_1,\dots,x_n]/(F)$.*

Conversely, a functor from the category of k-algebras to the category of sets, that is represented by a finitely generated k-algebra, is isomorphic to a functor of the form $T \rightsquigarrow \mathbb{V}_T(F)$ for a suitable n and $F \subseteq k[x_1,\dots,x_n]$.

Proof. Set $S = k[x_1,\dots,x_n]/(F)$ and let $\overline{x_1},\dots,\overline{x_n}$ denote the images of $x_1,\dots,x_n$ in S. If $\psi\colon S \to T$ is a morphism of k-algebras, then $(\psi(\overline{x_1}),\dots,\psi(\overline{x_n})) \in \mathbb{V}_T(F)$. Conversely, if $(a_1,\dots,a_n) \in \mathbb{V}_T(F)$, there exists a unique morphism $\psi\colon S \to T$ with $(\psi(\overline{x_1}),\dots,\psi(\overline{x_n}) = (a_1,\dots,a_n)$. Thus $\mathrm{Hom}(S,T) \to \mathbb{V}_T(F)$, $\psi \to (\psi(\overline{x_1}),\dots,\psi(\overline{x_n}))$ is a bijection. It is straightforward to check that for any morphism $T_1 \to T_2$ of k-algebras, the diagram

$$\begin{array}{ccc} \mathrm{Hom}(S,T_1) & \longrightarrow & \mathbb{V}_{T_1}(F) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(S,T_2) & \longrightarrow & \mathbb{V}_{T_2}(F) \end{array}$$

commutes. So, the functors $T \rightsquigarrow \mathrm{Hom}(S,T)$ and $T \rightsquigarrow \mathbb{V}_T(F)$ are isomorphic, i.e, S represents $T \rightsquigarrow \mathbb{V}_T(F)$.

To prove the second claim of the lemma, it suffices to show that the functor $T \rightsquigarrow \mathrm{Hom}(S,T)$ is isomorphic to some $T \rightsquigarrow \mathbb{V}_F(T)$. Because S is a finitely generated k-algebra, it can be written as $S = k[x_1,\dots,x_n]/(F)$ for some $n \geq 1$ and $F \subseteq k[x_1,\dots,x_n]$. Then, by the above, the functors $T \rightsquigarrow \mathrm{Hom}(S,T)$ and $T \rightsquigarrow \mathbb{V}_T(F)$ are isomorphic. □

Exercise 3.1.3. *Formulate and proof a variant of Lemma 3.1.2 for infinitely many variables. I.e., the finite set $x_1,\dots,x_n$ of variables in Lemma 3.1.2 should be replaced by an arbitrary set of variables.*

Definition 3.1.4. *A functor from the category of k-algebras to the category of groups is an* affine group scheme *(over k) if it is representable (when considered as a functor to the category of sets). An affine group scheme is an* affine algebraic group *(over k) if it can be represented by a finitely generated k-algebra.*

It will occasionally be useful to consider functors that can be described by algebraic equations but that do not necessarily have a group structure. We therefore make the following definition.

Definition 3.1.5. *A functor from the category of k-algebras to the category of sets is an* affine scheme *(over k) if it is representable. An affine scheme is* of finite type *(over k) if it can be represented by a finitely generated k-algebra.*

So the affine algebraic groups are exactly the affine group schemes that are of finite type. Since all schemes and algebraic groups in this course will be affine, we shall henceforth drop the adjective "affine". Let X be a scheme. A rather basic question that we need to address is the uniqueness of a k-algebra representing X. This is best understood in the general context of representable functor: Let ??

Lemma 3.1.6 (Yoneda lemma)**.**

Definition 3.1.7. *Let X be a scheme over k and assume we are given an isomorphism $X \simeq \mathrm{Sp}(k[X])$, where $k[X]$ is some k-algebra. The* universal element x_{univ} *of X is the element of $X(k[X])$ that corresponds to the identity map* $\mathrm{id}\colon k[X] \to k[X]$ *under the bijection $X(k[X]) \simeq \mathrm{Sp}(k[X])(k[X]) = \mathrm{Hom}(k[X], k[X])$.*

Remark 3.1.8. *Let $\phi\colon X \to Y$ be a morphism of schemes over k. Let $k[X]$ and $k[Y]$ be k-algebras with $X \simeq \mathrm{Sp}(k[X])$ and $Y \simeq \mathrm{Sp}(k[Y])$. According to the proof of ??, the dual map $\phi^*\colon k[Y] \to k[X]$ of ϕ is the image of x_{univ} under*

$$X(k[X]) \xrightarrow{\phi_{k[X]}??} Y(k[X]) \simeq \mathrm{Sp}(k[Y])(k[X]) = \mathrm{Hom}(k[Y], k[X]).$$

3.2 The definition of the differential Galois group

From now to the end of this chapter K is a differential field of characteristic zero and $k = K^\delta$ is its field of constants.

Definition 3.2.1. *Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R. The* differential Galois group *$G(L/K)$ of L/K is the functor from the category of k-algebras to the category of groups given by $G(L/K)(T) = \mathrm{Aut}(R \otimes_k T/K \otimes_k T)$, where T is considered to be a constant δ-ring and the automorphisms are understood to be differential automorphisms.*

So, an element τ of $G(L/K)(T)$ is, by definition, a $K \otimes_k T$-δ-isomorphism $\tau\colon R \otimes_k T \to R \otimes_k T$. On morphisms $G(L/K)$ is given by change. In detail, if $T \to T'$ is a morphism of k-algebras, we have a morphism $G(L/K)(T) \to G(L/K)(T')$ of groups that sends $\tau \in G(L/K)(T)$ to the map

$$R \otimes_k T' = (R \otimes_k T) \otimes_T T' \xrightarrow{\tau \otimes T'} (R \otimes_k T) \otimes_T T' = R \otimes_k T'.$$

If $\mathcal{F}$ is a family of linear differential systems over K, e.g., a single differential system $\delta(y) = Ay$ and $k = K^\delta$ is algebraically closed, then there exists a unique Picard-Vessiot extension L/K for $\mathcal{F}$ (Theorems 2.4.4 and 2.4.6). In this situation, the differential Galois group of L/K is also called the *differential Galois group of $\mathcal{F}$*.

☠ **3.2.2.** *If k is not algebraically closed, it does not make sense to speak of* the *differential Galois group of a family of linear differential systems over K. See ??*

Definition 3.2.3. *Assume that k is algebraically closed. The* absolute differential Galois group *of K is the differential Galois group of the linear closure of K.*

In other words, the absolute differential Galois group of K is the Galois group of the family of all linear differential systems over K.

☠ **3.2.4.** *If k is not algebraically closed, it does not make sense to speak of the absolute differential Galois group of K.*

Our first call of duty is to show that $G(L/K)$ is a group scheme. To this end we need a little preparation.

Proposition 3.2.5. *Let R/K be a Picard-Vessiot ring. Then the canonical map*

$$R \otimes_k (R \otimes_K R)^\delta \to R \otimes_K R$$

is an isomorphism.

Proof. Note that if R is of finite type, then this is a special case of Lemma 2.2.6. Since R is a union of Picard-Vessiot rings of finite type (??) this implies the proposition. □

Lemma 3.2.6. *Let R/K be a Picard-Vessiot ring and let T be a k-algebra. Then every $K \otimes_k T$-δ-morphism $R \otimes_k T \to R \otimes_k T$ is an isomorphism.*

Proof. Let $\tau\colon R \otimes_k T \to R \otimes_k T$ be a $K \otimes_k T$-δ-morphism. Then $\ker(\tau)$ is a δ-ideal of $R \otimes_k T$. Because $R \otimes_k T$ is δ-simple (Corollary 1.3.9), it follows that $\ker(\tau) = 0$. So τ is injective.

Since R is the union of Picard-Vessiot rings of finite type (Remark ??) we may assume that R is of finite type. Let $A \in K^{n\times n}$ be such that R is a Picard-Vessiot ring for $\delta(y) = Ay$. Let $Y \in \mathrm{GL}_n(R)$ be such that $\delta(Y) = AY$ and $R = K\big[Y_{ij}, \frac{1}{\det(Y)} \mid 1 \le i, j \le n\big]$. Then $\tau(Y)\,\mathrm{GL}_n(R \otimes_k T)$ and $Y \otimes 1 \in \mathrm{GL}_n(R \otimes_k T)$ are fundamental solution matrices for $\delta(y) = Ay$. By Lemmas 2.1.9 and 1.3.7, there exists a matrix $C \in \mathrm{GL}_n(T)$ such that $\tau(Y) = (Y \otimes 1)(1 \otimes C)$. From this it follows that the entries of Y and $\frac{1}{\det(Y)}$ lie in the image of τ. Since these elements generate $R \otimes_k T$ as a $K \otimes_k T$-algebra, it follows that τ is surjective. □

Lemma 3.2.7. *Let R be a K-δ-algebra with $R^\delta = k$. Let T_1 and T_2 be k-algebras considered as constant δ-rings. Then the canonical map from the set $\mathrm{Hom}(T_1, T_2)$ of k-algebra morphisms $T_1 \to T_2$ to the set $\mathrm{Hom}_R(R \otimes_k T_1, R \otimes_k T_2)$ of R-δ-morphisms $R \otimes_k T_1 \to R \otimes_k T_2$ is bijective.*

Proof. It suffices to describe the inverse. By Lemma 1.3.7 we have $(R \otimes_k T_1)^\delta = T_1$ and $(R \otimes_k T_2)^\delta = T_2$. So every R-δ-morphism $R \otimes_k T_1 \to R \otimes_k T_2$ restricts to a morphism $T_1 \to T_2$ of k-algebras. □

We are now prepared to show that the differential Galois group of a Picard-Vessiot extension is a group scheme.

Proposition 3.2.8. *Let L/K be a Picard-Vessiot extension. Then the differential Galois group $G(L/K)$ of L/K is a group scheme (over k). In fact, $G(L/K)$ is represented by $(R \otimes_k R)^\delta$, where R is the Picard-Vessiot ring of L/K.*

Proof. Set $G = G(L/K)$ and $k[G] = (R \otimes_K R)^\delta$. We have the following chain of identifications, where the second equality uses Lemma 3.2.6, the fifth equality uses Proposition 3.2.5 and the last equality uses Lemma 3.2.7:

$$\begin{aligned} G(T) &= \mathrm{Aut}(R \otimes_k T / K \otimes_k T) = \mathrm{Hom}_{K \otimes_k T}(R \otimes_k T, R \otimes_k T) = \mathrm{Hom}_K(R, R \otimes_k T) \\ &= \mathrm{Hom}_R(R \otimes_K R, R \otimes_k T) = \mathrm{Hom}_R(R \otimes_k k[G], R \otimes_k T) = \mathrm{Hom}(k[G], T). \end{aligned} \tag{3.1}$$

It is straightforward to check that the above identifications are functorial in T. Therefore G is represented by $k[G]$. □

Important notational convention: Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and differential Galois group $G = G(L/K)$. By Proposition 3.2.8 the functor G is a group scheme that is represented by $(R \otimes_K R)^\delta$. It therefore makes sense to set $k[G] = (R \otimes_K R)^\delta$. By Proposition 3.2.5 the canonical map $R \otimes_k k[G] \to R \otimes_K R$ is an isomorphism. Therefore, in the sequel, we will usually identify $R \otimes_K R$ with $R \otimes_k k[G]$. Note that there is no easy explicit description of the inverse of the canonical map $R \otimes_k k[G] \to R \otimes_K R$. We denote with the letter ρ the map

$$\rho \colon R \to R \otimes_K R = R \otimes_k k[G]$$

derived from the inclusion $R \to R \otimes_K R,\ a \mapsto 1 \otimes a$ of R into the second factor.

In the sequel we will usually identify $G = G(L/K)$ with $\mathrm{Sp}(k[G])$ as in Proposition 3.2.8. It is important to understand how exactly this identification works. So let us go through the identification of $G(T)$ with $\mathrm{Hom}(k[G], T)$ made in (3.1) explicitly. Given a $K \otimes_k T$-δ-automorphism $\tau \colon R \otimes_k T \to R \otimes_k T$, the corresponding element $g \in \mathrm{Hom}(k[G], T)$ is the restriction of $R \otimes_K R \to R \otimes_k T,\ a \otimes b \mapsto a\tau(b \otimes 1)$ to $k[G] \subseteq R \otimes_K R$. Conversely, given an element $g \in \mathrm{Hom}(k[G], T)$, the corresponding $K \otimes_k T$-δ-automorphism $\tau \colon R \otimes_k T \to R \otimes_k T$ is the T-linear extension of the map $R \xrightarrow{\rho} R \otimes_k k[G] \xrightarrow{R \otimes g} R \otimes_k T$. In particular, we have the following:

Remark 3.2.9. *Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and differential Galois group $G = G(L/K)$. The universal element g_{univ} of G (in the sense of Definition 3.1.7) is the $k[G]$-linear extension of ρ, i.e.,*

$$g_{\mathrm{univ}} \colon R \otimes_k k[G] \to R \otimes_k k[G],\ r \otimes f \mapsto \rho(r) f.$$

We call g_{univ} the universal automorphism *of R.*

Let L/K be a Picard-Vessiot extension for a family $\mathcal{F} = (\delta(y) = A_i y)_{i \in I}$ of linear differential systems over K. Let R be the Picard-Vessiot ring of L/K and let $Y_i \in \mathrm{GL}_{n_i}(L)$ be such that $\delta(Y_i) = A_i Y_i$ for all $i \in I$. For a k-algebra T and an element $g \in G(T) = G(L/K)(T)$ the matrix $g(Y_i \otimes 1) \in \mathrm{GL}_{n_i}(R \otimes_k T)$ is also a fundamental solution matrix for $\delta(y) = A_i y$ and therefore (Lemma 2.1.9) there exist unique $C_i(g) \in \mathrm{GL}_{n_i}((R \otimes_k T)^\delta) = \mathrm{GL}_{n_i}(T)$ (Lemma 1.3.7) such that $g(Y_i \otimes 1) = Y_i \otimes C_i(g)$.

Lemma 3.2.10. *The assignment $g \mapsto \prod_{i \in I} C_i(g)$ defines a closed embedding $\phi \colon G \to \prod_{i \in I} \mathrm{GL}_{n_i}$ of group schemes. In particular, for a linear differential system $\delta(y) = Ay$ with $A \in K^{n \times n}$, the choice of fundamental solution matrix $Y \in \mathrm{GL}_n(L)$, determines a closed embedding of $G = G(L/K)$ into GL_n.*

Proof. Because R is generated by the entries of all Y_i's and $\frac{1}{\det(Y_i)}$, an element $g \in G(T)$ is uniquely determined by the $C_i(g)$'s, i.e., $G(T) \to \prod_{i \in I} \mathrm{GL}_{n_i}(T)$ is injective. It is straight forward to check that ϕ is a morphism of group schemes.

To see that ϕ is a closed embedding, we have to show that $\phi^*\colon ??k\big[X_i, \frac{1}{\det(X_i)} \mid i \in I\big] \to k[G]$ is surjective. To find ϕ^*, we need to find $\phi(g_{\text{univ}})$ (Remark 3.1.8). Since $G_{\text{univ}}(Y_i \otimes 1) = 1 \otimes Y_i \in \mathrm{GL}_n(R \otimes_K R) = \mathrm{GL}_n(R \otimes_k k[G])$ and we see that $C_i(g_{\text{univ}}) = (Y_i \otimes 1)^{-1}(1 \otimes Y_i) = Y_i^{-1} \otimes Y_i \in \mathrm{GL}_n(k[G])$. Therefore, ϕ^* is determined by $\phi^*(X_i) = Y_i^{-1} \otimes Y_i$. So show that ϕ^* is surjective, it thus suffices to show that the k-subalgebra S of $(R \otimes_K R)^\delta = k[G]$ generated by all entries of all $Y_i^{-1} \otimes Y_i$'s and the inverse of $\det(Y_i^{-1} \otimes Y_i)$ is in fact all of $k[G]$. The map $R \otimes_k S \to R \otimes_K R$ is surjective because $1 \otimes Y_i = (Y_i \otimes 1)(Y_i^{-1} \otimes Y_i)$. So $R \otimes_k S = R \otimes_K R = R \otimes_k k[G]$ and so $S = k[G]$ by Lemma 1.3.7. □

Exercise 3.2.11. *Show that a different choice of the fundamental matrices Y_i leads to a conjugate ??*

Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and differential Galois group G. By ?? the k-algebra $k[G] \subseteq R \otimes_K R$ acquires the structure of Hopf algebra. It will be helpful to know what this Hopf algebra structure looks like. It can be described as the restriction of certain maps on $R \otimes_K R$.

Note that

$$R \otimes_K R \otimes_K R = R \otimes_K R \otimes_k k[G] = R \otimes_k k[G] \otimes_k k[G]$$

and therefore $(R \otimes_K R \otimes_K R)^\delta = k[G] \otimes_k k[G]$ be Lemma 1.3.7.

Lemma 3.2.12. *Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and differential Galois group G. Then the comultiplication $k[G] \to k[G] \otimes_k k[G]$ of the Hopf-algebra $k[G] = (R \otimes_K R)^\delta$ is the restriction of the map $R \otimes_K R \to R \otimes_K R \otimes_K R,\ a \otimes b \mapsto a \otimes 1 \otimes b$ to the constants.*

Proof. To find the dual of the multiplication $G \times G \to G$, we need to plug the generic point of $G \times G$ into the definition of the multiplication (Remark 3.1.8). The generic point of $G \times G$ is of the form $(g_{1,\text{univ}}, g_{2,\text{univ}}) \in G(T) \times G(T) = (G \times G)(T)$, where $T = k[G] \otimes_k k[G]$. Here $g_{1,\text{univ}}$ is the T-linear extension of $R \xrightarrow{\rho} R \otimes_k k[G] \to R \otimes_k k[G] \otimes_k k[G]$, where the second map is $r \otimes f \mapsto r \otimes f \otimes 1$. Similarly, $g_{2,\text{univ}}$ is the T-linear extension of $R \xrightarrow{\rho} R \otimes_k k[G] \to R \otimes_k k[G] \otimes_k k[G]$, where the second map is $r \otimes f \mapsto r \otimes 1 \otimes f$. Therefore, $g_{1,\text{univ}} \cdot g_{2,\text{univ}} \in G(T)$ is the T-linear extension of $R \to R \otimes_k k[G] \otimes_k k[G] = R \otimes_K R \otimes_K R,\ r \mapsto 1 \otimes 1 \otimes r$. (How this works is maybe best seen when R is of finite type with fundamental solution matrix Y. Then $g_{1,\text{univ}}$ is $Y \otimes 1 \mapsto Y \otimes (Y^{-1} \otimes Y) \otimes 1 \in \mathrm{GL}_n(R \otimes_k k[G] \otimes_k k[G])$ and $g_{2,\text{univ}}$ is $Y \otimes 1 \mapsto Y \otimes 1 \otimes (Y^{-1} \otimes Y) \in \mathrm{GL}_n(R \otimes_k k[G] \otimes k[G])$ and $g_{1,\text{univ}} \cdot g_{2,\text{univ}}$ is $Y \otimes 1 \mapsto Y \otimes (Y^{-1} \otimes Y) \otimes (Y^{-1} \otimes Y) \in \mathrm{GL}_n(R \otimes_k k[G] \otimes_k k[G])$. But under the map $R \otimes_k k[G] \otimes_k k[G] = R \otimes_k (R \otimes_K R)^\delta \otimes_k (R \otimes_K R)^\delta \to R \otimes_K R \otimes_K R$ the matrix $Y \otimes (Y^{-1} \otimes Y) \otimes (Y^{-1} \otimes Y) \in \mathrm{GL}_n(R \otimes_k k[G] \otimes_k k[G])$ becomes $YY^{-1} \otimes YY^{-1} \otimes Y = 1 \otimes 1 \otimes Y \in \mathrm{GL}_n(R \otimes_K R \otimes_K R)$.)

So (as explained in the paragraph before Remark 3.2.9) the morphism $k[G] \to T$ corresponding to $g_{1,\text{univ}} \cdot g_{2,\text{univ}} \in G(T)$ is the restriction to the constants of $R \otimes_K R \to R \otimes_K R \otimes_K R,\ a \otimes b \mapsto a \otimes 1 \otimes b$. □

Exercise 3.2.13. *Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and differential Galois group G. Similar to what is done for the comultiplication in Lemma 3.2.12, find formulas corresponding to the antipode $S\colon k[G] \to k[G]$ and the counit $\varepsilon\colon k[G] \to k$.*

Corollary 3.2.14. *Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and differential Galois group G. Let H be a closed subgroup of G and let I_H be the ideal of $L \otimes_K L$ generated by $\mathbb{I}(H) \subseteq k[G] = (R \otimes_K R)^\delta \subseteq L \otimes_K L$. Define $\Delta\colon L \otimes_K L \to L \otimes_K L \otimes_K L,\ a \otimes b \mapsto a \otimes 1 \otimes b$. Then $\Delta(I_H) \subseteq I_H \otimes_K L + L \otimes_K I_H$.*

Proof. Using Lemma 3.2.12 and that $\mathbb{I}(H) \subseteq k[G]$ is a co-ideal??, we see that the map $R \otimes_K R \to R \otimes_K R \otimes_K R,\ a \otimes b \mapsto a \otimes 1 \otimes b$ maps $\mathbb{I}(H)$ into $\mathbb{I}(H) \otimes_k k[G] + k[G] \otimes_k \mathbb{I}(H) \subseteq k[G] \otimes_k k[G] \subseteq R \otimes_K R \otimes_K R$. This implies the claim. □

3.3 The torsor theorem

Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and differential Galois group $G = G(L/K)$. Let G_K be the base change of G from k to K as in ??. Let $X = \mathrm{Sp}(R)$ be the K-scheme represented by R (as in ??). Note that here K is simply considered as a field, rather than as a δ-field. We will define a (right) action $X \times G_K \to X$ of G_K on X: For a K-algebra T, $x \in X(T)$ and $\tau \in G_K(T) = G(T)$ define

$$x.\tau \colon R \to R \otimes_k T \xrightarrow{\tau} R \otimes_k T \to T,$$

where the first map is the inclusion into the first factor and the last map is $r \otimes t \mapsto x(r)t$. It is straight forward to check that this assignment is functorial in T and defines a right action.

Exercise 3.3.1. *Check that the above assignment is functorial in T and defines a right action $X \times G_K \to X$.*

Theorem 3.3.2 (Torsor theorem)**.** *Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and differential Galois group G. Then $X = \mathrm{Sp}(R)$ is a G_K-torsor under the above defined (right) action.*

Proof. Let us first determine the dual map $R \to R \otimes_K (k[G] \otimes_k K) = R \otimes_k k[G]$ of $X \times G_K \to X$. To do this, we have to plug the universal point p_{univ} of $X \times G_K$ into the definition of the action (Remark 3.1.8). Note that with $T = R \otimes_k k[G]$ (considered as a K-algebra)

$$p_{\mathrm{univ}} \in (X \times G_K)(T) = X(T) \times G_K(T)$$

can be identified with $(x'_{\mathrm{univ}}, g'_{\mathrm{univ}}) \in X(T) \times G_K(T)$, where $x'_{\mathrm{univ}} \colon R \to R \otimes_k k[G] = T$ is the inclusion into the first factor and $g'_{\mathrm{univ}} \colon R \otimes_k T \to R \otimes_k T$ is obtained from $g_{\mathrm{univ}} \colon R \otimes_k k[G] \to R \otimes_k k[G]$ (described in Remark ??) via the base change $k[G] \to R \otimes_k k[G] = T$. In other words, g'_{univ} is the T-linear extension of the map

$$\begin{array}{rccc} \psi \colon & R & \to & R \otimes_K R = R \otimes_k k[G] \to R \otimes_k R \otimes_k k[G] = R \otimes_k T \\ & r & \mapsto & 1 \otimes r \qquad\qquad r \otimes f \mapsto r \otimes 1 \otimes f \end{array}$$

Therefore $x'_{\mathrm{univ}}.g'_{\mathrm{univ}} \colon R \xrightarrow{\psi} R \otimes_k R \otimes_k k[G] \to R \otimes_k k[G]$, where the last map is $r_1 \otimes r_2 \otimes f \mapsto r_1 r_2 \otimes f$. This shows that the dual map of $X \times G_K \to X$ is $R \to R \otimes_K R = R \otimes_k k[G]$, where the first map is the the inclusion into the second factor. The dual of $X \times G_K \to X \times X,\ (x, g) \mapsto (x, x.g)$ is therefore the map $R \otimes_K R \to R \otimes_k k[G]$, which is the inverse of $R \otimes_k (R \otimes_K R)^\delta \to R \otimes_K R$. This is clearly an isomorphism (Proposition 3.2.5). □

The above proof shows that the torsor theorem is merely a geometric reinterpretation of Proposition 3.2.5.

Exercise 3.3.3. *torsor action is right multiplication of matrices??*

3.4 Krull dimension and transcendence degree

Corollary 3.4.1. *Let L/K be a Picard-Vessiot extension of finite type with differential Galois group G. Then*

$$\mathrm{trdeg}(L/K) = \dim(G).$$

Chapter 4

The Galois correspondence

Throughout this chapter K is a differential field of characteristic zero and $k = K^\delta$ is its field of constants.

In this chapter we establish the Galois correspondence; a bijection between the intermediate differential fields of a Picard-Vessiot extension and the closed subgroups of its differential Galois group. This bijection is sometimes also referred to as the first fundamental theorem of differential Galois theory. The second fundamental theorem states that an intermediate differential field is itself Picard-Vessiot over the base field if and only if the corresponding closed subgroup is normal. Moreover, in this situation, the differential Galois group of the intermediate differential is the corresponding quotient of the differential Galois group of the original Picard-Vessiot extension.

4.1 The first fundamental theorem

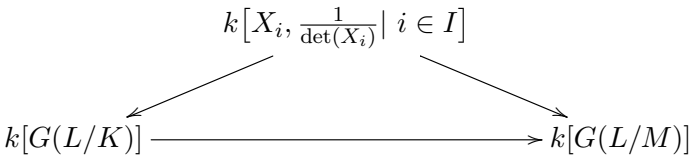
An *intermediate δ-field* M of a δ-field extension L/K is a δ-subfield M of L such that $K \subseteq M \subseteq L$. We begin by explaining how an intermediate δ-field gives rise to a closed subgroup of the differential Galois group.

Lemma 4.1.1. *Let M be an intermediate δ-field of a Picard-Vessiot extension L/K. Then L/M is a Picard-Vessiot extension and $G(L/M)$ is naturally a closed subgroup of $G(L/K)$.*

Proof. Let $\mathcal{F} = (\delta(y) = A_i y)_{i \in I}$ be a family of linear differential systems over K such that L/K is a Picard-Vessiot extension for $\mathcal{F}$. Then, clearly, L/M is a Picard-Vessiot extension for $\mathcal{F}$. The Picard-Vessiot ring R of L/K is generated as a K-algebra by the entries and the inverse of the determinant of matrices $Y_i \in \mathrm{GL}_{n_i}(L)$ satisfying $\delta(Y_i) = AY_i$. The Picard-Vessiot ring of L/M is generated by the same elements but as an M-algebra. Therefore, the Picard-Vessiot ring of L/M is RM, the M-subalgebra of L generated by R.

Let T be a k-algebra. An automorphism g of $RM \otimes_k T$ over $M \otimes_k T$ is determined by the matrices $C_i(g) \in \mathrm{GL}_{n_i}(T)$ satisfying $g(Y_i) = Y_i C_i(g)$ for all $i \in I$ (Lemma 3.2.10). In particular, g restricts to an automorphism of $R \otimes_k T \subseteq RM \otimes_k T$ over $K \otimes_k T$. We therefore have an injective morphism of groups $G(L/M)(T) \to G(L/K)(T)$. As these morphisms are functorial in T, we can consider $G(L/M)$ as a subfunctor of $G(L/K)$. By Lemma 3.2.10 we can consider $G(L/K)$ and $G(L/M)$ as closed subgroups of $\prod_i \mathrm{GL}_{n_i}$. As $G(L/M)$ is closed in $\prod_i \mathrm{GL}_{n_i}$, it must also be closed in $G(L/K)$. In terms of the

coordinate rings, the argument is that in the commutative diagram



the right vertical map is surjective, so also the horizontal map is surjective.

□

In the situation of Lemma 4.1.1, we will henceforth usually identify $G(L/M)$ with a closed subgroup of $G(L/K)$.

Exercise 4.1.2. *Show that in the situation of Lemma 4.1.1, the morphism $k[G(L/K)] \to k[G(L/M)]$ of coordinate rings, corresponding to the closed embedding $G(L/M) \to G(L/K)$, is the restriction of $R \otimes_K R \to RM \otimes_M RM$, $a \otimes b \mapsto a \otimes b$ to $(R \otimes_K R)^\delta \to (RM \otimes_M RM)^\delta$. Use this to show (again) that $k[G(L/K)] \to k[G(L/M)]$ is surjective.*

Having seen how to pass from an intermediate δ-field to a closed subgroup, we now would like to go the other way. As in classical Galois theory, one associates to a closed subgroup its *fixed field*. Since the differential Galois group does not act on the Picard-Vessiot extension but only on the Picard-Vessiot ring, one has to be a bit careful with how to define the *fixed field*.

Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R. Let T be a k-algebra and $g \in G(L/K)$. We would like to say what it means for an element $a \in L$ to be *fixed by* g. Since $g\colon R \otimes_k T \to R \otimes_k T$ this is obvious if $a \in R$: It means that $g(a \otimes 1) = a \otimes 1$. In general, $g\colon R \otimes_k T \to R \otimes_k T$ extends to an automorphism $g\colon \mathrm{Frac}(R \otimes_k T) \to \mathrm{Frac}(R \otimes_k T)$, where $\mathrm{Frac}(R \otimes_k T)$ is the total ring of fractions of $R \otimes_k T$, i.e., the localization of $R \otimes_k T$ at the multiplicatively closed subset of all non-zero divisors of $R \otimes_k T$ (see Appendix ??). Since $R \otimes_k T \subseteq L \otimes_k T$, it is clear that an element of the form $b \otimes 1$ with $b \in R \smallsetminus \{0\}$ is a non-zero divisor of $R \otimes_k T$. Therefore $L \otimes_k T \subseteq \mathrm{Frac}(R \otimes_k T)$ and so the expression $g(a \otimes 1) = a \otimes 1$ also makes sense in general. For a closed subgroup H of $G(L/K)$ we define the *fixed field* of H as

$$L^H = \{a \in L |\ a \text{ is fixed by all } g \in H(T) \text{ for all } k\text{-algebras } T\ \}.$$

Lemma 4.1.3. *Let L/K be a Picard-Vessiot extension and let H be a closed subgroup of $G(L/K)$. Then L^H is an intermediate δ-field of L/K.*

Proof. This follows immediately from the fact that $g\colon \mathrm{Frac}(R \otimes_k T) \to \mathrm{Frac}(R \otimes_k T)$ is a $K \otimes_k T$-δ-automorphism for every $g \in H(T)$ and every k-algebra T. □

The following lemma will be helpful for obtaining a better understanding of L^H.

Lemma 4.1.4. *Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and differential Galois group G. Let I be an ideal of $k[G]$ and let $\widetilde{I}$ denote the of $L \otimes_K L$ generated by $I \subseteq k[G] = (R \otimes_K R)^\delta \subseteq L \otimes_K L$. Then $\widetilde{I} \cap (R \otimes_K R) = R \otimes_k I$ and $\widetilde{I} \cap k[G] = I$.*

Proof. It suffices to prove $\widetilde{I} \cap (R \otimes_K R) = R \otimes_k I$. The inclusion $R \otimes_k I \subseteq \widetilde{I} \cap (R \otimes_K R)$ is obvious. Note that we can think of $L \otimes_K L$ as the localization of $R \otimes_K R$ at the multiplicatively closed subset $S = \{a \otimes b \in R \otimes_K R |\ a, b \in R \smallsetminus \{0\}\}$. Therefore, by Lemma ??appendix, $\widetilde{I} \cap (R \otimes_K R) = \{f \in R \otimes_K R |\ \exists\ s \in S\ :\ sf \in R \otimes_k I\}$. So we

have to show that $sf \in R \otimes_k I$ implies $f \in R \otimes_k I$ for $f \in R \otimes_k k[G]$ and $s \in S$. Let us first consider the case that $s = a \otimes 1$ with $a \in R \setminus \{0\}$. Choose a k-basis $(b_j)_{j\in J}$ of $k[G]$ such that $(b_j)_{j\in J'}$ is a k-basis of I for some $J' \subseteq J$. Then f is uniquely of the form $f = \sum_{j\in J} a_j \otimes b_j \in R \otimes_k k[G]$. As $sf = \sum_{j\in J} aa_j \otimes b_j \in R \otimes_k I$ we must have $aa_j = 0$ for $j \notin J'$. Thus $a_j = 0$ for $j \notin J'$ and so $f \in R \otimes_k I$ as desired.

We next treat the special case $s = 1 \otimes b$ with $b \in R \setminus \{0\}$. Note that the flip $\mu\colon R \otimes_K R \to R \otimes_K R,\ a \otimes b \mapsto b \otimes a$ is a K-δ-automorphism. In particular, it preserves the constants, i.e., $\mu(k[G]) = k[G]$. So $\mu(R \otimes_k I)$ is an ideal of $R \otimes_K R$ of the form $R \otimes_k I'$ for some ideal I' of $k[G]$. Moreover, $(b \otimes 1) \cdot \mu(f) = \mu((1 \otimes b) \cdot f) \in \mu(R \otimes_k I) = R \otimes_k I'$. From the special case proved above, we obtain $\mu(f) \in \mu(R \otimes_k I)$. Therefore $f \in R \otimes_k I$.

Finally we treat the general case $s = a \otimes b \in S$. Then $sf = (a \otimes 1)(1 \otimes b)f \in R \otimes_k I$. Successively applying the above two special cases yields $f \in R \otimes_k I$ as desired. □

The following lemma provides an explicit description of L^H in terms of the defining ideal of H.

Lemma 4.1.5. *Let L/K be a Picard-Vessiot extension with Picard-Vessiot ring R and let H be a closed subgroup of $G = G(L/K)$ with defining ideal $\mathbb{I}(H) \subseteq k[G]$. Let I_H denote the ideal of $L \otimes_K L$ generated by $\mathbb{I}(H) \subseteq k[G] = (R \otimes_K R)^\delta \subseteq L \otimes_K L$. Then*

$$L^H = \{a \in L|\ a \otimes 1 - 1 \otimes a \in I_H\}. \tag{4.1}$$

Proof. Let $h_{\text{univ}} \in H(T)$, where $T = k[H]$, be the universal element of H, i.e., $h_{\text{univ}}\colon R \otimes_k k[H] \to R \otimes_k k[H]$ is the $k[H]$-linear extension of $R \xrightarrow{\rho} R \otimes_k k[G] \to R \otimes_k k[H]$. We will first show that

$$L^H = \{a \in L|\ a \text{ is fixed by } h_{\text{univ}}\}. \tag{4.2}$$

The inclusion "$\subseteq$" being obvious, assume that $a \in L$ is fixed by h_{univ} and let $h \in H(T)$ for some k-algebra T. Then $h\colon R \otimes_k T \to R \otimes_k T$ is the T-linear extension of $R \xrightarrow{\rho} R \otimes_k k[G] \to R \otimes_k k[H] \to R \otimes_k T$. Write $a = \frac{b}{c}$ with $b, c \in R$. Note that $h(a \otimes 1) = a \otimes 1$ if and only if $h(b \otimes 1)(c \otimes 1) = h(c \otimes 1)(b \otimes 1)$ in $R \otimes_k T$. By assumption, $h_{\text{univ}}(a) = a$ and so $h_{\text{univ}}(b \otimes 1)(c \otimes 1) = h_{\text{univ}}(c \otimes 1)(b \otimes 1) \in R \otimes_k k[H]$. Therefore also $h(b \otimes 1)(c \otimes 1) = h(c \otimes 1)(b \otimes 1) \in R \otimes_k T$. This proves (4.2).

Let us next prove (4.1). Assume that $a \in L^H$ and write, as above, $a = \frac{b}{c}$ with $b, c \in R$. Since a is fixed by h_{univ} we have $h_{\text{univ}}(b \otimes 1)(c \otimes 1) = h_{\text{univ}}(c \otimes 1)(b \otimes 1) \in R \otimes_k k[H]$.

Note that $h_{\text{univ}}(b \otimes 1) \in R \otimes_k k[H]$ is the image of $1 \otimes b \in R \otimes_K R$ under $R \otimes_K R = R \otimes_k k[G] \to R \otimes_k k[H]$. Therefore $h_{\text{univ}}(b \otimes 1)(c \otimes 1) = h_{\text{univ}}(c \otimes 1)(b \otimes 1) \in R \otimes_k k[H]$ signifies that $c \otimes b \in R \otimes_K R$ and $b \otimes c \in R \otimes_K R$ have the same image under $R \otimes_K R = R \otimes_k k[G] \to R \otimes_k k[H]$, i.e., $c \otimes b - b \otimes c$ lies in the ideal of $R \otimes_K R$ generated by $\mathbb{I}(H)$. Since in $L \otimes_K L$ we can divide by $c \otimes c$, we see that $a \otimes 1 - 1 \otimes a \in I_H$.

Conversely, let us assume that $a = \frac{b}{c} \in L$ is such that $a \otimes 1 - 1 \otimes a \in I_H$. Then $(c \otimes c) \cdot (a \otimes 1 - 1 \otimes a) = b \otimes c - c \otimes b \in I_H \cap (R \otimes_K R) = R \otimes_k \mathbb{I}(H)$ by Lemma 4.1.4. So $c \otimes b$ and $b \otimes c \in R \otimes_K R = R \otimes_k k[G]$ have the same image in $R \otimes_k k[H]$. In other words, $h_{\text{univ}}(b \otimes 1)(c \otimes 1) = h_{\text{univ}}(c \otimes 1)(b \otimes 1) \in R \otimes_k k[H]$ and so $h_{\text{univ}}(a) = a$. Hence $a \in L^H$ by (4.2). □

The following lemma is probably the hardest step in proving the Galois correspondence.

Lemma 4.1.6. *Let L/K be a Picard-Vessiot extension and let H be a closed subgroup of $G(L/K)$. Let the ideal I_H of $L \otimes_K L$ be defined as in Lemma 4.1.5. Then*

$$I_H = \left(a \otimes 1 - 1 \otimes a|\ a \in L^H\right) \subseteq L \otimes_K L.$$

Proof. The inclusion "$\supseteq$" holds by (4.1). To prove "$\subseteq$" we consider the map

$$\psi\colon L \otimes_{L^H} L \to (L \otimes_K L)/I_H,\ a \otimes b \mapsto \overline{a \otimes b}.$$

Note that ψ is well-defined (because of "$\supseteq$") and surjective. We will show that ψ is injective (and therefore an isomorphism). But let us first show that this implies the lemma: We have a commutative diagram

$$\begin{array}{ccc} & L \otimes_K L & \\ \swarrow & & \searrow \\ L \otimes_{L^H} L & \xrightarrow{\quad\psi\quad} & (L \otimes_K L)/I_H \end{array}$$

The kernel of the left vertical map is $\left(a \otimes 1 - 1 \otimes a |\ a \in L^H\right) \subseteq L \otimes_K L$, because

$$L \otimes_{L^H} L \to (L \otimes_K L)/\left(a \otimes 1 - 1 \otimes a |\ a \in L^H\right),\ b \otimes c \mapsto \overline{b \otimes c}$$

is well-defined. The kernel of the right vertical map is I_H. Since ψ is an isomorphism, the two kernels agree.

Let us now show that ψ is injective. Suppose, for a contradiction, that ψ is not injective. Let $d = \sum_{i=1}^n a_i \otimes b_i \in L \otimes_{L^H} L$ be a non-zero element of $\ker(\psi)$ such that n is minimal. If $n = 1$ then $a_1 \otimes b_1 \in I_H$ and therefore also $1 \otimes 1 \in I_H$. Thus $1 \in \mathbb{I}(H)$ by Lemma 4.1.4; a contradiction. Thus $n > 1$.

The minimality of n implies that the a_i's are L^H-linearly independent and also that the b_i's are L^H-linearly independent. Without loss of generality we may assume that $b_n = 1$. Since the b_i's are L^H-linearly independent, this implies $b_1 \notin L^H$ (as $b_n = 1$). Therefore $b_1 \otimes 1 - 1 \otimes b_1 \in L \otimes_K L$ does not lie in I_H by Lemma 4.1.5. Hence there exists an L-linear map $\eta\colon L \otimes_K L \to L$ with $\eta(f) = 0$ for all $f \in I_H$ and $\eta(b_1 \otimes 1 - 1 \otimes b_1) \neq 0$, where $L \otimes_K L$ is considered as an L-vector space with respect to the first factor, i.e. $\lambda(a \otimes b) = \lambda a \otimes b$ for $\lambda, a, b \in L$. Consider $d' = \sum_{i=1}^n a_i \otimes \eta(1 \otimes b_i - b_i \otimes 1) \in L \otimes_{L^H} L$. Because $\eta(b_1 \otimes 1 - 1 \otimes b_1) \neq 0$ and the a_i's are L^H-linearly independent, $d' \neq 0$. Moreover, since $b_n = 1$ the sum actually only goes from 1 to $n-1$. By the minimality of n we have $d' \notin \ker(\psi)$. We will finish the proof by establishing the contradictory $\psi(d') = 0$. We have

$$\begin{aligned} \psi(d') &= \sum_{i=1}^n \overline{a_i \otimes \eta(1 \otimes b_i - b_i \otimes 1)} = \sum_{i=1}^n \overline{a_1 \otimes \eta(1 \otimes b_i)} + \sum_{i=1}^n \overline{a_i \otimes \eta(b_i \otimes 1)} = \\ &= \sum_{i=1}^n \overline{a_i \otimes \eta(1 \otimes b_i)} + \sum_{i=1}^n \overline{a_i \otimes b_i \eta(1 \otimes 1)} = \sum_{i=1}^n \overline{a_i \otimes \eta(1 \otimes b_i)} + \psi(d)(1 \otimes \eta(1 \otimes 1)) = \\ &= \sum_{i=1}^n \overline{a_i \otimes \eta(1 \otimes b_i)} \end{aligned}$$

because $\psi(d) = 0$. It thus suffices to show that $\sum_{i=1}^n a_i \otimes \eta(1 \otimes b_i) \in L \otimes_K L$ lies in I_H. To this end we consider, as in Corollary 3.2.14, the map $\Delta\colon L \otimes_K L \to L \otimes_K L \otimes_K L,\ a \otimes b \mapsto a \otimes 1 \otimes b$. Note that $\sum_{i=1}^n a_i \otimes \eta(1 \otimes b_i) \in L \otimes_K L$ is the image of $\sum_{i=1}^n a_i \otimes b_i \in L \otimes_K L$ under $L \otimes_K L \xrightarrow{\Delta} L \otimes_K L \otimes_K L \xrightarrow{L \otimes \eta} L \otimes_K L$, where $L \otimes \eta\colon L \otimes_K L \otimes_K L \to L \otimes_K L,\ a \otimes b \otimes c \mapsto a \otimes \eta(b \otimes c)$. Because $\sum_{i=1}^n a_i \otimes b_i \in I_H$ and $\Delta(I_H) \subseteq I_H \otimes_K L + L \otimes_K I_H$ by Corollary 3.2.14, it suffices to show that $L \otimes \eta$ maps $I_H \otimes_K L + L \otimes_K I_H$ into I_H. As η vanishes on I_H, we have $(L \otimes \eta)(L \otimes_K I_H) = 0$. On the other hand, $(L \otimes_K \eta)(a \otimes b \otimes c) = (a \otimes b) \cdot (1 \otimes \eta(1 \otimes c))$ as η is L-linear. Therefore $(L \otimes \eta)(I_H \otimes_K L) \subseteq I_H$ and so $(L \otimes \eta)(I_H \otimes_K L + L \otimes_K I_H) \subseteq I_H$ as desired. $\square$

Exercise 4.1.7. *Sweedler correspondence ??*

We are now prepared to establish the (first part of the) Galois correspondence.

Theorem 4.1.8 (First fundamental theorem of differential Galois theory)**.** *Let L/K be a Picard-Vessiot extension with differential Galois group G. The map $M \mapsto G(L/M)$ is an inclusion reversing bijection between the set of intermediate δ-fields of L/K and the set of closed subgroups of G. The inverse map is given by $H \mapsto L^H$.*

Proof. By Lemmas 4.1.1 and 4.1.3 we have well-defined maps in both directions. The "inclusion reversing" is obvious.

Let us show that $L^{G(L/M)} = M$ for every intermediate δ-field M of L/K. Because L/M is Picard-Vessiot with δ-Galois group $G(L/M)$, we may assume that $M = K$. So we have to show that $L^G = K$. Note that I_G is the zero ideal. Therefore, by Lemma 4.1.5,

$$L^G = \{a \in L |\ a \otimes 1 = 1 \otimes a \in L \otimes_K L\} = K.$$

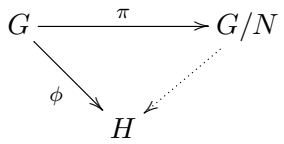
To complete the proof, it now suffices to show that the map $H \mapsto L^H$ is injective. Assume that H_1 and H_2 are closed subgroups of G with $L^{H_1} = L^{H_2}$. Then, $I_{H_1} = I_{H_2}$ by Lemma 4.1.6 and so $\mathbb{I}(H_1) = \mathbb{I}(H_2)$ by Lemma 4.1.4. Therefore $H_1 = H_2$. □

4.2 Quotients of group schemes

Throughout this section k is a field (of arbitrary characteristic).

To form the quotient group G/N of a group G by a normal subgroup N is a fundamental operation in the theory of groups. In the theory of groups schemes this construction is equally important.

Let G be a group scheme over k. A closed subgroup N of G is a *normal* subgroup of G if $N(T)$ is a normal subgroup of $G(T)$ for every k-algebra T. Unfortunately the functor $T \rightsquigarrow G(T)/N(T)$ from the category of k-algebras to the category of groups is usually not representable (see Ex ??). Therefore a more refined definition and construction of the quotient G/N is needed. In the category of groups, the quotient G/N is characterized by the following universal property: The canonical map $\pi\colon G \to G/N$ satisfies $N \subseteq \ker(\pi)$ and if $\phi\colon G \to H$ is any morphism of groups such that $N \subseteq \ker(\phi)$, then there exists a unique morphism $G/N \to H$ such that



commutes.

Definition 4.2.1. *Let G be group scheme with a normal closed subgroup N. A* quotient of G by N *is a*

While Definition 4.2.1 is conceptually very clear, it leaves open the existence of quotients.

4.3 The second fundamental theorem

Theorem 4.3.1. *Let L/K be a Picard-Vessiot extension with differential Galois group G. Let M be an intermediate δ-field of L/K corresponding to the closed subgroup H of G. Then M/K is a Picard-Vessiot extension if and only if H is normal in G. If this is the case, the restriction map $G(L/K) \to G(M/K)$ is a quotient map with kernel $G(L/M)$, in particular, $G(M/K) \simeq G(L/K)/G(L/M)$.*

Proof. Let R denote the Picard-Vessiot ring of L/K. Assume that H is a normal closed subgroup of G. We will show that $R \cap M \subseteq R$ is stable under the action of G, i.e., for every k-algebra T, every $g \in G(L/K)(T)$ maps $(R \cap M) \otimes_k T \subseteq R \otimes_k T$ into $(R \cap M) \otimes_k T$. Let $f \in R \cap M$ and $h \in H(T)$. Then $g^{-1}hg \in H(T)$ because H is normal in G. Therefore $h(g(f)) = g((g^{-1}hg)(f)) = g(f)$ since $f \in M = L^H$. This shows that $g(f) \in L^H = M$. Thus $R \cap M$ is stable under the G-action. For the universal automorphism??, i.e., for $T = k[G]$ and $g \in G(L|K)(T)$ the $k[G]$-linear extension of $\rho\colon R \to R \otimes_k k[G]$, this means that $\rho(R \cap M) \subseteq (R \cap M) \otimes_k k[G]$. So the isomorphism $R \otimes_K R \simeq R \otimes_k k[G]$ maps $(R \cap M) \otimes_K (R \cap M)$ into $(R \cap M) \otimes_k k[G]$. □

Chapter 5

Solving differential equations

Despite the title, the main goal of this chapter is to develop tools to show that many linear differential systems cannot be solved.

Appendix

In this appendix we discuss some basic algebraic definitions and constructions. It is intended for students that are not be familiar with these constructions or could use a refresher.

A.1 Localization

Recall that all rings are commutative. A subset S of a ring R is called *multiplicatively closed* if $1 \in S$ and $g_1 g_2 \in S$ for $g_1, g_2 \in S$. Here are the three most important examples:

- If R is an integral domain, the set of non-zero elements of R is multiplicatively closed.
- For $f \in R$, the set $S = \{1, f, f^2, \ldots\}$ is multiplicatively closed.
- If $\mathfrak{p}$ is a prime ideal of R, then $R \setminus \mathfrak{p}$ is multiplicatively closed.

Lemma A.1.1. *Let S be a multiplicatively closed subset of a ring R. Then*

$$(f, g) \sim (f', g') :\Leftrightarrow \exists\ g'' \in S : g''(fg' - gf') = 0$$

is an equivalence relation on the set of all pairs (f, g) with $f \in R$ and $g \in S$.

Proof. The proof is straightforward but a bit tedious. □

The equivalence class of a pair (f, g) as in Lemma A.1.1 is usually denoted by $\frac{f}{g}$. So $\frac{f}{g} = \frac{f'}{g'}$ if and only if there exists $g'' \in S$ such that $g''(fg' - gf') = 0$. The set of all such equivalence classes is denoted by $S^{-1}R$.

Lemma A.1.2. *The set $S^{-1}R$ of all equivalence classes with respect to the equivalence relation defined in Lemma A.1.1 is a ring with respect to the operations*

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + f'g}{gg'}$$

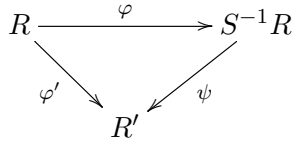
and

$$\frac{f}{g} \cdot \frac{f'}{g'} = \frac{ff'}{gg'}.$$

Proof. One has the check that these operations are well-defined and satisfy the required properties. Again, this is rather straight forward but tedious. □

Note that the map $\varphi\colon R \to S^{-1}R,\ f \mapsto \frac{f}{1}$ is a ring homomorphism. It satisfies the following universal property: If $\varphi'\colon R \to R'$ is any ring homomorphism such that

$\varphi'(s) \in R'$ is invertible in R' for all $s \in S$, then there exists a unique ring homomorphism $\psi\colon S^{-1}R \to R'$ such that



commutes. Indeed, ψ is given by $\psi(\frac{f}{g}) = \varphi'(f)\varphi'(g)^{-1}$.

Here are three important special cases of the above construction.

- If R is an integral domain and $S = R \setminus \{0\}$, then $S^{-1}R = \mathrm{Frac}(R)$ is the field of fractions of R.
- If $f \in R$ and $S = \{1, f, f^2, \dots, \}$ one writes $R_f = S^{-1}R$.
- If $\mathfrak{p}$ is a prime ideal of R and $S = R \setminus \mathfrak{p}$ one writes $R_{\mathfrak{p}} = S^{-1}R$ for "the localization at $\mathfrak{p}$".

Note that $S^{-1}R$ is the zero ring if and only if $0 \in S$. An ideal I of R is called *saturated with respect to* S if $gf \in I$ implies $f \in I$ for $g \in S$ and $f \in R$.

Lemma A.1.3. *Let S be a multiplicatively closed subset of the ring R and $\varphi\colon R \to S^{-1}R,\ f \mapsto \frac{f}{1}$. Then the map $J \mapsto \varphi^{-1}(J)$ is a bijection between the ideals of $S^{-1}R$ and the ideals of R that are saturated with respect to S. The inverse map is $I \mapsto (\varphi(I))$.*

Proof. Let us first verify that $\varphi^{-1}(J)$ is saturated with respect to S. Assume that $s \in S$ and $f \in R$ such that $sf \in \varphi^{-1}(J)$. Then $\varphi(s)\varphi(f)\varphi(sf) \in J$ and because $\varphi(s)$ is invertible in $S^{-1}R$ we find $\varphi(f) \in J$, i.e., $f \in \varphi^{-1}(J)$ as desired.

We claim that $(\varphi(\varphi^{-1}(J)) = J$. The inclusion "$\subseteq$" is clear. Conversely, assume $\frac{f}{g} \in J$ with $f \in R$ and $g \in S$. Then also $\frac{f}{1} \in J$ and so $f \in \varphi^{-1}(J)$. Thus $\frac{f}{1} \in \varphi(\varphi^{-1}(J))$ and therefore $\frac{f}{g} = \frac{1}{g} \cdot \frac{f}{1} \in (\varphi(\varphi^{-1}(J))$.

It remains to show that $\varphi^{-1}((\varphi(I))) = I$ for every ideal I of R that is saturated with respect to S. The inclusion "$\supseteq$" is clear. Conversely, assume that $f \in \varphi^{-1}((\varphi(I)))$, i.e., $\frac{f}{1} \in (\varphi(I))$. Since $\{\frac{h}{g} \in S^{-1}R|\ h \in I,\ g \in S\}$ is an ideal of $S^{-1}R$, we have

$$(\varphi(I)) = \left\{\tfrac{h}{g} \in S^{-1}R|\ h \in I,\ g \in S\right\}.$$

Thus $\frac{f}{1} = \frac{h}{g}$ for some $h \in I$ and $g \in S$. By definition, this implies that $g'(fg - h) = 0$ for some $g' \in S$. But then $gg'f = g'h \in I$. Because I is saturated with respect to S and $gg' \in S$, we find $f \in I$ as desired. □

Corollary A.1.4. *The prime ideals of $S^{-1}R$ are in bijection with the prime ideals $\mathfrak{p}$ of R satisfying $\mathfrak{p} \cap S = \emptyset$.*

Proof. According to Lemma A.1.3 it suffices to prove the following:

(i) For a prime ideal $\mathfrak{p}$ of R we have $S \cap \mathfrak{p} = \emptyset$ if and only if $\mathfrak{p}$ is saturated with respect to I, and in this case

(ii) the ideal $(\varphi(\mathfrak{p}))$ of $S^{-1}R$ is prime.

For (i), note that if $S \cap \mathfrak{p} = \emptyset$ and $gf \in \mathfrak{p}$ with $g \in S$ and $f \in R$, then $f \in \mathfrak{p}$, because $\mathfrak{p}$ is prime and $g \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is saturated with respect to S.

Conversely, assume that $\mathfrak{p}$ is saturated with respect to S and suppose that $f \in \mathfrak{p} \cap S$. Then $f = f \cdot 1 \in \mathfrak{p}$. Because $f \in S$ and $\mathfrak{p}$ is saturated with respect to S, it follows $1 \in \mathfrak{p}$; a contradiction.

For (ii) we can use the description $(\varphi(\mathfrak{p})) = \left\{ \frac{h}{g} \in S^{-1}R |\ h \in \mathfrak{p},\ g \in S \right\}$ from the proof of Lemma A.1.3: If $f, f' \in R$ and $g, g' \in S$ such that $\frac{f}{g} \cdot \frac{f'}{g'} = \frac{ff'}{gg'} \in (\varphi(\mathfrak{p}))$, then $\frac{ff'}{gg'} = \frac{h}{g''}$ for some $h \in \mathfrak{p}$ and $g'' \in S$. Thus $g'''(ff'g'' - hgg') = 0 \in \mathfrak{p}$. Since $h \in \mathfrak{p}$, we find $g'''g''ff' \in \mathfrak{p}$. As $g'''g'' \in S$ and $\mathfrak{p}$ is saturated with respect to S, we see that $ff' \in \mathfrak{p}$. Hence $f \in \mathfrak{p}$ or $f' \in \mathfrak{p}$ and so $\frac{f}{g} \in (\varphi(\mathfrak{p}))$ or $\frac{f'}{g'} \in (\varphi(\mathfrak{p}))$. □

As a special case of Corollary A.1.4, it follows that the prime ideals of $R_\mathfrak{p}$ are in bijection with the prime ideals of R contained in $\mathfrak{p}$. Moreover, $R_\mathfrak{p}$ has a unique maximal ideal, namely, the ideal $(\varphi(\mathfrak{p}))$, which is often denote by $\mathfrak{p}_\mathfrak{p}$.

Recall that an element f of a ring R is called *nilpotent* if $f^n = 0$ for some $n \geq 1$. The set of all nilpotent elements of R is called the *nilradical* of R. It is sometimes denoted by $\sqrt{0}$. It is not too difficult to show directly that the nilradical is an ideal of R. However, this also follows from the following lemma which uses the technique of localization in its proof.

Lemma A.1.5. *Let R be a ring. Then the nilradical of R is the intersection of all prime ideals of R.*

Proof. If $f \in R$ is nilpotent, then $f^n = 0$ for some $n \geq 1$. In particular, $f^n = 0 \in \mathfrak{p}$ for every prime ideal $\mathfrak{p}$. But then also $f \in \mathfrak{p}$ (because $\mathfrak{p}$ is prime).

Conversely, assume that f lies in every prime ideal of $\mathfrak{p}$. Suppose, for a contradiction, that f is not nilpotent. Then R_f is not the zero ring and so contains a prime ideal $\mathfrak{q}$. (By Zorn's lemma every non-zero ring contains a maximal ideal and a maximal ideal is prime.) The inverse image of $\mathfrak{q}$ under the map $R \to R_f$ is a prime ideal of R with $f \notin \mathfrak{p}$ (Corollary A.1.4). This contradicts the assumption that f lies in every prime ideal of R. □

Recall that a ring is *reduced* if its nilradical is zero.

Corollary A.1.6. *A reduced ring with only one prime ideal is a field.*

Proof. Let $\mathfrak{p}$ be the unique prime ideal of R. By Lemma A.1.5 the nilradical of R equals $\mathfrak{p}$. But by assumption the nilradical is zero. Thus $\mathfrak{p}$ is the zero ideal. On the other hand, R contains a maximal ideal and a maximal ideal is prime. Thus $\mathfrak{p}$ is maximal.

So the zero ideal of R is maximal. This implies that R is field. □

A.2 Categories and functors

??

Bibliography

[Tes12] Gerald Teschl. *Ordinary differential equations and dynamical systems*, volume 140 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2012.