**Elżbieta Sowa**

# Picard-Vessiot extensions for real fields

**PhD Thesis**

written under the supervision of
dr hab. Zbigniew Hajto prof. UJ

**Jagiellonian University**
**Institute of Mathematics**
**Kraków 2011**

# Acknowledgements

I would like to thank my thesis advisor Zbigniew Hajto for his guidance, instant support and inspiring discussions during last years.

I wish to thank Teresa Crespo for inviting me to Barcelona for the conference *Galois Theory and Explicit Methods*, where I could speak about my work. I am grateful for her advices concerning my work and also for stylistic remarks.

Further I would like to thank Jakub Byszewski, Julia Hartmann and Akira Masuoka for their critical comments.

# Contents

# Introduction

Picard-Vessiot theory can be described as Galois theory of linear differential equations. This theory is a generalization of classical Galois theory for polynomial equations to homogeneous linear differential equations. Picard-Vessiot theory is due to E. Picard and E. Vessiot and in rigorous form to E. Kolchin, who built on the work of J.F. Ritt in differential algebra. It was made more accessible by the book of I. Kaplansky [15]. We refer the reader also to [7], [8], [22] and [28] for the results of Picard-Vessiot theory.

Picard-Vessiot theory has been built under the hypothesis that the field of constants $C_K$ of the differential field $K$, over which the differential equation is defined, is algebraically closed. In this case, one obtains existence and uniqueness, up to $K$-differential isomorphisms, of the Picard-Vessiot extension of the differential equation and that the differential Galois group of the differential equation, defined as the group of $K$-differential automorphisms of its Picard-Vessiot extension, is a linear algebraic group over $C_K$. It is worth considering whether the condition $C_K$ algebraically closed can be weakened. In particular, the case of real fields is interesting.

Many interesting and significant results concerning differential algebra for real fields can be found in papers by M. Singer, T. Dyckerhoff, T. Grill, M. Knebusch, M. Tressl (see [35], [9], [12], [13]). But an existence theorem for Picard-Vessiot extension even in the case $C_K = \mathbb{R}$ has never been proved. The reason for that might be a commentary of Armand Borel, which can be found in his article contained in *Selected Works of Ellis Kolchin* (see [3]). Borel wrote about the proof by Kolchin of the existence theorem of Picard-Vessiot theory:

*This is under our standing assumption that $C_F$ is algebraically closed (of char. 0). If not, then Seidenberg has produced an equation such that $C_E \neq C_F$ for all differential field extensions $E$ generated over $F$ by a fundamental set of solutions of that equation.*

But if we take a close look at the example of Seidenberg mentioned above (see [32], [18], chapter 6, ex.1 or chapter 4.1 of this work) we will see that the base field $F$ is *not a real field.*

A Picard-Vessiot extension is a differential field extension $K \subset L$ such that there exists a following homogeneous linear ordinary differential equation $\mathcal{L}(Y) := Y^{(n)} + a_{n-1}Y^{(n-1)} + \ldots + a_1Y' + a_0Y = 0$ with coefficients in $K$ having a fundamental set of solutions $y_1, \ldots, y_n$ in $L$ which differentially generates $L$ over $K$ and moreover the fields of constants of $K$ and $L$ coincide. Kolchin proved the existence of a Picard-Vessiot extension for a given homogeneous linear ordinary differential equation over a differential field with algebraically closed field of constants. In one of his papers Kolchin indicates that the difficulty in proving the existence of a Picard-Vessiot extension for a given equation lies in proving that such an extension brings in no new constants (see [19]). He also comments that this problem was formulated earlier in 1933 by Reinhold Baer in his commentary which appears in Felix Klein's book *Vorlesungen über hypergeometrische Funktion* (see [16], page 333).

The main result of this work is proving that for a given homogeneous linear ordinary differential equation defined over a real differential field $K$ with field of constants a real closed field $F$ there exists a Picard-Vessiot extension which is also a real field.

In our work we do not use Tannakian categories, so our methods are not restricted to the linear case. This should make it possible to generalize our results to the non linear case, following the landmark paper of Malgrange [23].

Our work is organised as follows:

In chapter 1 we introduce the notions of differential ring and differential field and we study some preliminary facts of differential algebra. We also prove Ritt-Raudenbusch Basis Theorem which is an equivalent of Hilbert's Basis Theorem for radical differential ideals and a differential version of primary decomposition theorem. We introduce the very useful notion of Taylor morphism and present a differential version of the primitive element theorem.

In chapter 2 we give a brief introduction to the theory of real and real closed fields. We present Tarski-Seidenberg Principle and its consequences. We also study some other results needed in further chapters, like Skolem-Löwenheim Theorem.

In chapter 3 we introduce the basic definitions and state some essential results of Picard-Vessiot theory. We consider differential fields of characteristic zero with algebraically closed fields of constants. Here we present the theorem on the existence and uniqueness of Picard-Vessiot extension in such case and the Fundamental Theorem of Picard-Vessiot Theory.

The last chapter contains our new results. We study homogeneous linear ordinary differential equations defined over a real differential field $K$ differentially finitely generated over a real closed field $F$ considered as a differential field with trivial derivation, with field of constants equal to $F$. In this case we construct a real Picard-Vessiot extension. We obtain the general result by applying the Kuratowski-Zorn lemma. Finally, we give a short commentary on the Fundamental Theorem of Picard-Vessiot Theory in the case considered.

**List of notations**.

If $K$ is a field then we denote by:

| | |
|---|---|
| $K[X_1, \ldots, X_n]$ | the ring of polynomials in $X_1, \ldots, X_n$ over $K$ |
| $K(X_1, \ldots, X_n)$ | the field of rational functions in $X_1, \ldots, X_n$ over $K$ |
| $K\{X_1, \ldots, X_n\}$ | the ring of differential polynomials in $X_1, \ldots, X_n$ over$K$ |
| $K\langle X_1, \ldots, X_n\rangle$ | the field of differential rational functions in $X_1, \ldots, X_n$ over $K$ |
| $K[[X]]$ | the ring of power series over $K$ |
| $K((X))$ | the field of fractions of $K[[X]]$ |

If $S$ is a subset of a ring (resp. differential ring) $A$ then we denote by:

| | |
|---|---|
| $(S)$ | the ideal in $A$ generated by $S$ |
| $[S]$ | the differential ideal in $A$ generated by $S$ i.e. generated by elements of $S$ and their derivatives |
| $\{S\}$ | the smallest radical differential ideal in $A$ containing $S$ |

If $A$ is a subring of a ring $B$, and $S$ is a subset of $B$ then we denote by $A[S]$ the smallest subring of $B$ containing $A$ and $S$.

If $K$ is a subfield of a field $L$, and $S$ is a subset of $L$ then we denote by $K(S)$ the smallest subfield of $L$ containing $A$ and $S$.

If $A \subset B$ is a differential ring extension, and $S$ is a subset of $B$ then we denote by $A\{S\}$ the smallest differential subring of $B$ containing $A$, $S$ and all derivatives of elements of $S$.

If $K \subset L$ is a differential field extension, and $S$ is a subset of $L$ then we denote by $K\langle S\rangle$ the smallest differential subfield of $L$ containing $A$, $S$ and all derivatives of elements of $S$.

For a given field $K$ we denote by $\overline{K}$ its algebraic closure. If $K$ is an ordered field, then by $\overline{K}^r$ we denote the real closure of $K$.

If $K$ is a differential field (resp. ring), then by $C_K$ we denote its subfield (resp. subring) of constants.

By $\mathfrak{c}$ we denote the cardinality of $\mathbb{R}$, i.e. continuum; by $\aleph$ an arbitrary cardinality.

# Chapter 1

# Differential algebra

In this chapter we recall some basic definitions and facts of differential algebra.

## 1.1 Differential rings and their extensions

**Definition 1.1.1.** *Let $A$ be a ring. A map $d : A \to A$ satisfying*

$$d(a+b) = d(a) + d(b),$$

$$d(ab) = d(a)b + ad(b)$$

*is called a derivation of the ring $A$. So it is an additive map satisfying Leibniz rule. A commutative ring with identity endowed with a derivation is called a differential ring.*

We write $a' = d(a)$ and $a'', a''', \dots a^{(n)}$ for succesive derivations of $a \in A$. A differential ring which is a field is called a *differential field.* Note that:

$$d(1) = 0, \quad d(a^{-1}) = -\frac{d(a)}{a^2} \quad \text{and} \quad d(a^n) = na^{n-1}d(a),$$

where $a^{-1}$ denotes the inverse of $a$.

Examples:

1) The simplest example of a derivation is the *trivial derivation* i.e. $\forall a \in A :\ d(a) = 0$. Note that every commutative ring with identity can be seen as

a differential ring with the trivial derivation. Over $\mathbb{Z}$ and over $\mathbb{Q}$ the trivial derivation is the only possible one.

2) The ring of infinitely differentiable functions $C^\infty(\mathbb{R})$ with the usual derivation $\frac{d}{dx}$ is a differential ring.

3) The ring of analytic functions $\mathcal{O}(\mathbb{C})$ wit the usual derivation $\frac{d}{dz}$ is also a differential ring.

4) Every vector field is a derivation.

If $A$ is an integral domain, we can extend the derivation from $A$ to the quotient field $Fr(A)$ in a unique way, by defining

$$\left(\frac{a}{b}\right)' = \frac{a'b - ab'}{b^2} \qquad \text{for} \quad \frac{a}{b} \in Fr(A).$$

In the same way we can extend derivation from a differential ring with no zero divisors to the ring of fractions $S^{-1}A$, where $S$ is a multiplicative subset of $A$. For example the differential ring $\mathcal{O}(\mathbb{C})$ is an integral domain. We can extend its derivation to its field of fractions i.e. the field of meromorphic functions.

Let $A$ be a differential ring. By $A[X]$ we denote the polynomial ring in one indeterminate over $A$. We can extend the derivation from $A$ to $A[X]$, by assigning to $X'$ an arbitrary value in $A[X]$. Analogously, if $K$ is a differential field, we extend derivation to the field of rational functions $K(X)$. By iteration, we extend derivation to $A[X_1, \dots, X_n]$ or $K(X_1, \dots X_n)$.

In any differential ring $A$ we can distinguish a subring

$$C_A := \{a \in A | d(a) = 0\},$$

called *ring of constants*. If $A$ is a field, so is $C_A$.

Let $(A, d)$ and $(B, D)$ be differential rings. An inclusion $A \subset B$ is a *differential ring extension*, if the derivation of $B$ extends the derivation of $A$, i.e. $D|_A = d$. Let $S$ be a subset of a differential ring $B$. We denote by $A\{S\}$ the smallest differential subring of $B$ containing $A$, $S$ and the derivatives of elements of $S$. It is the *differential $A$-subalgebra of $B$ generated by $S$ over $A$*.

Analogously, if $K \subset L$ is a differential field extension, $S$ is a subset of $L$, we denote by $K\langle S\rangle$ the *differential subfield of $L$ generated by $S$ over $K$*.

If $S$ is a finite set, then the extension $K \subset K\langle S\rangle$ is called *differentially finitely generated.*

## 1.2 Ideals and morphisms

Let $I$ be an ideal of a differential ring $A$.

**Definition 1.2.1.** *$I$ is a differential ideal if $d(I) \subset I$.*

It is easy to see that an intersection of differential ideals is a differential ideal.

**Definition 1.2.2.** *Let $A$ and $B$ be differential rings. A map $\varphi : A \to B$ is called a differential morphism if it is a morphism of rings i.e.*

$$\varphi(a+b) = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = \varphi(a)\varphi(b),$$

$$\varphi(1) = 1$$

*and moreover*

$$[\varphi(a)]' = \varphi(a').$$

In an obvious way we define differential isomorphism and differential automorphism.

Let now $I$ be a differential ideal of a differential ring A. The derivation of $A$ induces a derivation in the quotient ring $A/I$, defined by

$$d(\overline{a}) = \overline{d(a)},$$

where $\overline{a}$ denote the class of an element $a \in A$. If $I$ is a differential ideal of $A$, then $A \to A/I$ is naturally a differential morphism.

If $\varphi : A \to B$ is a differential morphism, then $Ker\varphi$ is a differential ideal in $A$ and $\varphi$ induces a differential isomorphism

$$\overline{\varphi} : A/Ker\varphi \to Im\varphi.$$

**Notation.** Let $A$ be a differential ring and let $S$ be a subset of $A$. By $[S]$ we will denote the *differential ideal generated by $S$*, i.e. the ideal generated by the elements of $S$ and their derivatives. If $S$ is a finite set, i.e. $S = \{s_1, \dots, s_n\}$ we will write $[s_1, \dots, s_n]$.

By $(S)$ we will denote the *ideal generated by* $S$. In particular, when $S = \{s_1, \dots, s_n\}$ we will write $(s_1, \dots, s_n)$.

The radical $rad(I)$ of the ideal $I$ is the intersection of all prime ideals containing $I$. But the radical of a differential ideal is not always a differential ideal. Hence it is not true in general that the radical of a differential ideal is an intersection of prime differential ideals. Differential rings for which radicals of their differential ideals are also differential ideals are called *Keigher rings.* For example every differential $\mathbb{Q}$-algebra is a Keigher ring (see corollary 1.4.1). A differential ring which is also an algebra over $\mathbb{Q}$ is called a *Ritt algebra.* Also any ring of constants is a Keigher ring. This way we can see abstract (i.e. non-differential) rings as Keigher rings. If $A$ is a Ritt algebra, $I$ is a diferential ideal of $A$ and $\mathscr{P}$ is the family of prime differential ideals containing $I$, then $rad(I) = \bigcap \mathscr{P}$ (see theorem 1.5.1)

## 1.3 Differential polynomials

Let $A$ be a differential ring. Let $A[Y_i]$ denote the polynomial ring in the indeterminates $Y_i, i \in \mathbb{N} \cup \{0\}$ over $A$. We define $Y_i' := Y_{i+1}$. In this way we obtain a differential ring, which we denote by $A\{Y\}$. The elements of $A\{Y\}$ are called *differential polynomials in the indeterminate* $Y$. These are ordinary polynomials in $Y$ and their derivatives.

By proceeding inductively we obtain the ring of differential polynomials $A\{Y_1, \dots, Y_n\}$ in $n$ variables. We observe that $A\{Y_1, \dots, Y_n\}$ is a differential $A$-algebra differentially generated over $A$ by $\{Y_1, \dots, Y_n\}$ with ring of constants $C_{A\{Y_1,\dots,Y_n\}} = C_A$. If $A$ is an integral domain, so is $A\{Y_1, \dots, Y_n\}$. However there is no an equivalent of Hilbert Basis Theorem. The ring $A\{Y_1, \dots, Y_n\}$ is no longer noetherian.

If $K$ is a differential field, then $K\{Y\}$ has no zero divisors. As it was said before, we can extend derivation to the field of fractions, which we denote by $K\langle Y\rangle$. The elements of $K\langle Y\rangle$ are called *differential rational functions of* $Y$. In a similar way we can obtain the field of rational functions $K\langle Y_1, \dots, Y_n\rangle$ in $n$ variables.

Moreover, if $A$ is a differential $K$-algebra and $a_1, \dots, a_n \in A$ are arbitrary elements, then there exists a unique differential $K$-algebra homomorphism $\varphi : K\{Y_1, \ldots, Y_n\} \to A$ such that $\varphi(Y_i) = a_i$ for $i = 1, \ldots, n$. We write $f(a_1, \ldots, a_n)$ instead of $\varphi(f)$.

If $K \subset L$ is a differential field extension, then elements $a_1, \ldots, a_n \in L$ are said to be *differentially algebraically dependent over* $K$ if there exists a nonzero differential polynomial $f \in K\{Y_1, \ldots, Y_n\}$ such that $f(a_1, \ldots, a_n) = 0$. Otherwise we call them *differentially algebraically independent.* An element $a \in L$ is *differentially algebraic over* $K$ if there exists a nonzero differential polynomial $f \in K\{Y\}$ such that $f(a) = 0$.

Let $A$ be a differential ring.

**Definition 1.3.1.** *The greatest $j$ such that $Y^{(j)}$ appears in $f \in A\{Y\}$ is called the order of $f$. We denote it by $ord(f)$.*

If $f \in A\{Y\}$ is of order $n$, then we can write it in the form

$$f(Y) = \sum_{i=0}^{k} g_i(Y, Y', \ldots, Y^{(n-1)})(Y^{(n)})^i,$$

where $k$ is the *degree* of $f$ in $Y^{(n)}$ and $g_k$ is the *leading coefficient* of $f$ (J. F. Ritt called it the *initial* of $f$).

**Definition 1.3.2.** *Let $f \in A\{Y\}$ such that $ord(f) = n$. We define $s := \frac{\partial f}{\partial Y^{(n)}}$ and call $s$ the separant of $f$.*

When we compute the separant of $f$ we treat $f$ as an algebraic polynomial $f \in A[Y, Y', \ldots, Y^{(n)}]$, i.e. we treat as constants the elements of $A$ and all lower derivatives of $Y$. For example: the separant of $f(Y) = (Y''')^5 - 4Y''$ is $s(Y) = 5(Y''')^4$.

If $a \in L$ is an element differentially algebraic over $K$, then the *minimal polynomial* of $a$ over $K$ is an irreducible polynomial $f \in K\{Y\}$ of the lowest order, say $r$, and of smallest degree in $Y^{(r)}$. Then the abstract field $K(a, a, \ldots a^{(r)})$ is a differential field. We differentiate $f(a) = 0$ to see that $a^{(r+1)} \in K(a, a, \ldots a^{(r)})$. The elements $a, a', \ldots a^{(r-1)}$ are then algebraically independent over $K$, and $a^{(r)}$ is algebraic over $K(a, a, \ldots a^{(r-1)})$

We define an order relation of the ring $A\{Y\}$ called *ranking*. Let $f, g \in A\{Y\}$. We say that $f$ *is of lower rank than* $g$ *(or that* $f$ *is lower than* $g$*)* if $ord(f) < ord(g)$ or if

$$ord(f) = ord(g) = q \quad \text{and} \quad deg_{Y^{(q)}} f < deg_{Y^{(q)}} g.$$

We denote it $f << g$. The relation $<<$ is transitive. Two differential polynomials $f, g \in A\{Y\}$ are of *the same rank* if there is no difference established by the foregoing criteria.

**Fact 1.3.1.** *Every subset* $S \subset A\{Y\}$ *contains a differential polynomial which is not of higher rank than any other differential polynomial in* $S$*.*

*Proof.* If $S \cap A \neq \varnothing$ then any differential polynomial from $S \cap A$ satisfies our requirements. If $S \cap A = \varnothing$, we denote

$$q = min\{ord(f) \,|\, f \in S\} \quad \text{and} \quad S_1 = \{f \in S \,|\, ord(f) = q\}.$$

We denote $t = min\{deg_{Y^{(q)}} f \,|\, f \in S_1\}$. Every differential polynomial $f_0 \in S_1$ of degree $t$ satisfies our requirements, i.e. no differential polynomial from $S$ is of lower rank than $f_0$.

□

So $<<$ is a *well-order relation.*

**Remark 1.3.1.** *For a given differential polynomial* $f$ *the separant of* $f$ *and the leading coefficient of* $f$ *are both lower than* $f$*.*

## 1.4 Ritt-Raudenbush basis theorem

In this section we will state and prove Ritt-Raudenbush basis theorem which is a crucial point in proving the existence of finite irredundant decomposition into prime differential ideals for radical differantial ideals. It is an analog of the Hilbert basis theorem, but not straightforward. If we replace ideals by differential ideals we obtain a *false* statement. For example differential ideals in $A\{Y\}$ of the form $I_n = [Y^2, (Y')^2, \ldots, (Y^{(n)})^2]$ do not satisfy ascending chain condition (ACC). This property holds true for radical differential ideals over a Ritt algebra.

**Notation.** For an arbitrary subset $S$ of a differential ring $A$ we denote by $\{S\}$ the smallest radical differential ideal containing $S$. If $A$ is a Keigher ring, then $\{S\} = rad([S])$.

Now we will prove some auxiliary lemmas.

**Lemma 1.4.1.** *Let $A$ be a differential ring and let $I$ be a radical differential ideal in $A$. Then*

$$\forall a, b \in A : \, ab \in I \Rightarrow a'b \in I \, \wedge ab' \in I.$$

*Proof.* Since $I$ is a differential ideal, then $(ab)' = a'b + ab' \in I$. Then we multiply by $a'b$ and obtain that $(a'b)^2 + aba'b' \in I$. Since $I$ is radical, then $a'b \in I$. Analogously we prove that $ab' \in I$

□

**Lemma 1.4.2.** *Let $A$ be a differential ring and $S$ a multiplicative subset of $A$. Let $I$ be a radical differential ideal in $A$. We denote*

$$T := \{a \in A : \, aS \subset I\}.$$

*Then $T$ is a radical differential ideal. We denote it by $(I : S)$.*

*Proof.* Straightforwardly we obtain that $T$ is an ideal. By lemma 1.4.1 we get that $a'S \subset I$. If $a^n \in T$, then $a^n S \subset I$. In particular $\forall s \in S : \, a^n s^n \in I$. Since $I$ is radical, then $as \in I$. So $a \in T$.

□

**Lemma 1.4.3.** *Let $A$ be a differential ring and let $x \in A$. If $T$ and $S$ are multiplicative subsets of $A$, then*

1. *$x\{S\} \subset \{xS\}$*
2. *$\{S\}\{T\} \subset \{ST\}$*

*Proof.* 1. By lemma 1.4.2 $T = \{a \in A : \, xa \in \{xS\}\}$ is a radical differential ideal. Since $S \subset T$, then $\{S\} \subset T = (\{xS\} : x)$.
2. From 1. we have that $a\{T\} \subset \{aT\}$, for all $a \in \{S\}$.

□

**Lemma 1.4.4.** *Let $A$ be a Ritt algebra. Then*

$$\forall a \in A \quad \forall n \in \mathbb{N} \quad (a')^{2n-1} \in [a^n].$$

*Proof.* We have $(a^n)' = na^{n-1}a'$. Since $\mathbb{Q} \subset A$, we can divide by $n$ and obtain that

$$a^{n-1}a' \in [a^n]. \tag{1.1}$$

Hence we have the thesis for $n = 1$, i.e. $a' \in [a]$.

Let now $n > 1$. By differentiating (1.1) we obtain

$$(n-1)a^{n-2}(a')^2 + a^{n-1}a'' \in [a^n].$$

We multiply by $a'$ and we have

$$(n-1)a^{n-2}(a')^3 + a^{n-1}a''a' \in [a^n].$$

Using (1.1) we obtain that $a^{n-2}(a')^3 \in [a^n]$. Hence we have the thesis for $n = 2$, i.e. $(a')^3 \in [a^2]$.

In analogous way we obtain the thesis for every $n \in \mathbb{N}$.

□

**Corollary 1.4.1.** *Let $A$ be a Ritt algebra and let $I$ be a diferential ideal in $A$. Then $rad(I)$ is a radical differential ideal. In particular the nilradical ideal $rad((0))$ is always a differential ideal.*

*Proof.* Let $a \in rad(I)$. Then there exists $n \in \mathbb{N}$ such that $a^n \in I$. By lemma 1.4.4 we have that $(a')^{2n-1} \in [a^n] \subset I$, so $a' \in rad(I)$.

□

**Remark 1.4.1.** *Let $A$ be a Ritt algebra. Then $A$ has ACC on radical differential ideals if and only if every radical differential ideal $I$ in $A$ is finitely generated, i.e. there exists $a_1, \ldots, a_n \in I$ such that $I = \{a_1, \ldots, a_n\}$.*

*Proof.* Let $\{I_i\}_{i\in\mathbb{N}}$ be a family of radical differential ideals of $A$ such that $I_i \subseteq I_{i+1}$ for every $i \in \mathbb{N}$. Let $J = \bigcup_{i\in\mathbb{N}} I_i$. $J$ is a radical differential ideal in $A$, so there exists $f_1, \dots, f_s \in J$ such that $J = \{f_1, \dots, f_s\}$. Hence $J = \bigcup_{i=1}^{r} I_i$, where $r \in \mathbb{N}$ is such that for all $i = 1, \dots, s$ $f_i \in I_r$. So $I_i = I_r$ for all $i \geq r$.

Conversely, we assume that $A$ has ACC on radical differential ideals. Let $I$ be an arbitrary radical differential ideal in $A$ and let $\Sigma$ denote the set of all finitely generated radical differential ideals of $A$ contained in $I$ . We observe that $rad((0)) \in \Sigma$, hence $\Sigma \neq \varnothing$. So there exist a maximal element in $\Sigma$. Let us denote this element by $J = \{b_1, \dots, b_k\}$. If $I \neq J$, then we consider the ideal $\{b_1, \dots, b_k, a\}$, where $a \in I$ and $a \notin J$. It is a finitely generated radical differential ideal which strictly contains $J$. We get a contradiction with the maximality of $J$. So $I = J$ and $I$ is finitely generated.

□

**Observation.** Suppose that the ideal $\{a, S\}$ is a *finitely generated* radical differential ideal of a Ritt algebra $A$. Then there exist $x_1, \dots, x_k \in S$ such that $\{a, S\} = \{a, x_1, \dots, x_k\}$. Indeed, suppose that $\{a, S\} = \{y_1, \dots, y_l\}$. By the corollary above we obtain that $\{a, S\} = rad([a, S])$. Hence for all $i = 1, \dots, l$ there exist $z_{ij} \in S$ and $\alpha_j, \beta_{ijk} \in A$ such that

$$y_i^n = \sum \alpha_j a^{(j)} + \sum \beta_{ijk} z_{ij}^{(k)}.$$

So $\{a, S\} = \{a, z_{ij}\}$.

**Lemma 1.4.5 (Division lemma).** *Let $A$ be a Ritt algebra and let $f \in A\{Y\}$ be irreducible of order $n$. We consider a polynomial $g \in [f] \setminus \{0\}$. Then $ord(g) \leq n$. Moreover if $ord(g) = n$, then $f$ divides $g$.*

*Proof.* STEP 1: We will prove that

$$\forall r \geq 1 : \, f^{(r)} = sY^{(n+r)} + f_r(Y, Y', \dots, Y^{(n+r-1)}),$$

where $s$ is the separant of $f$. Since $f$ is of order $n$ it can be written in the form $f = \sum_{i=0}^{m} \alpha_i (Y^{(n)})^i$, where $\forall i \geq 1 : \, ord(\alpha_i) \leq n-1$. Hence $f' = \sum_{i=0}^{m} [\alpha_i' (Y^{(n)})^i + i\alpha_i (Y^{(n)})^{i-1} Y^{(n+1)}]$. We put $f_1 = \sum_{i=0}^{m} \alpha_i' (Y^{(n)})^i$, and we obtain that $f' = sY^{(n+1)} + f_1$, i.e. the formula holds true for $r = 1$. Suppose that this holds true for some $r \geq 1$. Then $f^{(r+1)} = s'Y^{(n+r)} + sY^{(n+r+1)} + f_r'$.

We put $f_{r+1} = f_r' + s'Y^{(n+r)}$. We have then $ord(f_{r+1}) \leq n + r$ and $f^{(r+1)} = sY^{(n+r+1)} + f_{r+1}$.

STEP 2: We consider $g \in [f] \setminus \{0\}$, i.e. $g = \sum_{i=0}^{k} a_i f^{(i)}$. For $k = 0$ the lemma is true, so let $k \geq 1$. If the order of $g$ is higher than $n$, let us say $n + k$, then we may depress it. We substitute $Y^{(n+k)}$ by $-\frac{f_k}{s}$. We obtain an equation of the form $s^m g = \sum_{i=0}^{k-1} b_i f^{(i)}$. Then we replace $Y^{(n+k-1)}$ by $-\frac{f_{k-1}}{s}$. We repeat the process until we find $m$ and obtain that $s^m g = af$, for $a \in A\{Y\}$. Now $f$ does not divide $s$ (because $f$ is of higher degree). Since $f$ is irreducible, then $f$ divides $g$ and $ord(f) = ord(g)$.

□

**Lemma 1.4.6.** *Let $A$ be a Ritt algebra and let $f \in A\{Y\}$ be irreducible of order $n$. Then for every $g \in A\{Y\}$, we can find $h \in A\{Y\}$, such that*

$$ord(h) \leq n \quad \wedge \quad \exists m \in \mathbb{N} : \, s^m g = h \, (mod[f]),$$

*where $s$ denote the separant of $f$.*

*Proof.* We carry the proof by induction on $<<$. We may assume that $ord(g) = n + r$, where $r \geq 1$. Suppose that $deg_{Y^{(n+r)}} g = m$. Then $g = \sum_{i=1}^{m} p_i(Y, Y', \ldots, Y^{(n+r-1)})(Y^{(n+r)})^i$. Suppose that the thesis holds true for all $p << g$. By lemma 1.4.5, there exist $f_r$ of order at most $n + r - 1$ such that $f^{(r)} = sY^{(n+r)} + f_r(Y, Y', \ldots, Y^{(n+r-1)})$.

Let $h = s^m g - (f^{(r)})^m p_m$. Then $h = s^m g \, (mod[f])$. Since $h << g$, then by inductive assumption we obtain the thesis.

□

The procedure above is unique. We call $h$ the *reminder* of $g$ with respect to $f$.

**Lemma 1.4.7.** *Let $A$ be a Ritt algebra and let $f \in A\{Y\} \setminus A$ be irreducible of the form $f(Y) = \sum_{i=0}^{r} \alpha_i (Y^{(n)})^i$, where $ord(\alpha_i) \leq n - 1$ for $i = 1, \ldots, r$. Let $s$ denote the separant of $f$. Then for every $g \in A\{Y\}$, we can find $h \in A\{Y\}$, such that*

$$h << f \quad \wedge \quad \exists p, q : \, \alpha_r^p s^q g = h \, (mod[f]).$$

*Proof.* By lemma 1.4.6 there exists $h_1 \in A\{Y\}$ of order at most $n$ and there exists $q$ such that $s^q g = h_1\,(mod[f])$. By the division algorithm for polynomials we obtain that $\alpha_r^p h_1 = h\,(mod[f])$, for some $p$ and $h \in A\{Y\}$ of degree lower than $r$.

□

Now we are ready to prove Ritt-Raudenbush basis theorem.

**Theorem 1.4.1 (Ritt-Raudenbusch Basis Theorem).** *Let $A$ be a Ritt algebra such that every radical differential ideal $I$ is finitely generated. Then every radical differential ideal in $A\{Y\}$ is finitely generated.*

*Proof.* Let us denote by $S$ the set of all non-finitely generated radical differential ideals in $A\{Y\}$. By Kuratowski-Zorn lemma there exists a maximal element in S. Let us denote it by $M$.

STEP 1: We will prove that $M$ is prime. We suppose that it is not, i.e. there exist $a, b \in A$ such that $ab \in M, a \notin M$ and $b \notin M$. Since $M$ is maximal, then $\{a, M\}$ and $\{b, M\}$ are finitely generated, i.e. there exist $x_1, \ldots, x_p, y_1, \ldots y_q \in M$ such that $\{a, M\} = \{a, x_1, \ldots, x_p\}$ and $\{b, M\} = \{b, y_1, \ldots y_q\}$. By lemma 1.4.3 $\{a, M\}\{b, M\} \subset \{ab, x_1y_1, \ldots, x_py_q\} \subset M$.

If $c \in M$, then $c^2 \in \{a, M\}\{b, M\}$. Hence $c^2 \in \{ab, x_1y_1, \ldots, x_py_q\}$. Since $\{ab, x_1y_1, \ldots, x_py_q\}$ is radical, then $c \in \{ab, x_1y_1, \ldots, x_py_q\}$. Thus $M = \{ab, x_1y_1, \ldots, x_py_q\}$. We have a contradiction with the assumption that $M$ is non-finitely generated.

STEP 2: The ideal $M \cap A$ is finitely generated in $A$. Let us denote by $I$ the finitely generated differential ideal in $A\{Y\}$ generated by $M \cap A$. We denote by $f$ the polynomial of lowest rank in $M - I$. Suppose that $f$ is of the form $f(Y) = a(Y^{(n)})^r + g(Y)$, where $g << f$. We observe that $a \notin M$. Otherwise $g \in M$ and we have a contradiction with the minimality of $f$.

Let us denote by $s$ the separant of $f$. We observe that $s \notin M$. Indeed, if $s \in M$, then $s \in I$ (since $s << f$). Hence $f(Y) - \frac{1}{r}Y^{(n)}s \in M - I$ and we have a contradiction with the minimality of $f$. Since $M$ is prime, then $as \notin M$. Hence $\{as, M\}$ is finitely generated. Suppose $\{as, M\} = \{as, z_1, \ldots, z_k\}$, for some $z_1, \ldots, z_k \in M$.

Let $g(Y) \in M$. By lemma 1.4.7, we can find $p$ and $q$ such that $a^p s^q g = h\,(mod[f])$, where $h << f$. Since $f$ is minimal in $M - I$, then $h \in I$. Hence $a^p s^q g \in \{I, f\}$ and since $\{I, f\}$ is radical, $asg \in \{I, f\}$. So $asM \subset \{I, f\}$. We obtain that $M \subseteq M\{as, M\} = M\{as, z_1, \ldots, z_k\}$. By lemma 1.4.3 we have that $M\{as, z_1, \ldots, z_k\} \subseteq \{asM, Mz_1, \ldots, Mz_k\} \subseteq \{I, f, z_1, \ldots, z_k\} \subseteq M$. We obtain that $M = \{I, f, z_1, \ldots, z_k\}$, so $M$ is finitely generated.

□

Inductively we obtain the result above for the differential ring $A\{Y_1, \ldots, Y_n\}$. In particular, if $K$ is a differential field of characteristic zero and $I$ is a radical differential ideal in $K\{Y_1, \ldots, Y_n\}$, then there exist $f_1, \ldots, f_s \in I$ such that $I = rad([f_1, \ldots, f_s])$, i.e. the ideal $I$ has a *finite basis.*

**Proposition 1.4.1.** *Let $K$ be a differential field of characteristic zero and let $A$ be a finitely differentially generated $K$-algebra. Then there exist $n \in \mathbb{N}$ and a differential ideal $I$ of $K\{Y_1, \ldots, Y_n\}$ such that*

$$\varphi : K\{Y_1, \ldots, Y_n\}/I \to A$$

*is a differential isomorphism.*

*Proof.* $A$ is a finitely differentially generated $K$-algebra, so there exists a finite subset $S = \{s_1, \ldots, s_n\}$ of $A$ such that $A = K\{S\}$. We consider a differential ring homomorphism $\psi : K[Y_i^{(j)}] \to A$ such that $\psi|_K = id_K$ and $\psi(Y_i^{(j)}) = s_i^{(j)}$. Since $A = K\{s_1, \ldots, s_n\}$, then $Im(\psi) = A$. So $\psi$ induces a differential isomorphism $\varphi$ such that $I = Ker(\varphi)$.

□

**Corollary 1.4.2.** *Let $K$ be a differential field of characteristic zero and let $A$ be finitely differentially generated $K$-algebra. Let $I$ be a radical differential ideal of $A$. Then there exist $f_1, \ldots f_s \in I$ such that $I = rad([f_1, \ldots, f_s])$.*

## 1.5 Decomposition of radical differential ideals

In this section we present Ritt theorem concerning decomposition of a radical differential ideal into a finite intersection of prime differential ideals.

**Theorem 1.5.1.** *Let $A$ be a differential ring, such that $A$ has ACC for radical differential ideals. Then every radical differential ideal in $A$ is an intersection of a finite number prime differential ideals.*

*Proof.* We suppose the contrary. Let us denote by $S$ the set of radical differential ideals in $A\{Y\}$ which are not an intersection of finitely many prime differential ideals. By Kuratowski-Zorn lemma there exists a maximal element in $S$. We denote this ideal by $M$. Since $M$ is not prime, then there exist $a, b \in A$ such that $ab \in M$ and $a, b \notin M$. Hence $\{a, M\}$ and $\{b, M\}$ are larger that $M$, and hence they are intersections of finitely many prime differential ideals. By lemma 1.4.3 $\{a, M\}\{b, M\} \subseteq \{ab, M\} \subset M$.

If $c \in \{a, M\} \cap \{b, M\}$, then $c^2 \in M$ and since $M$ is radical, $c \in M$. We obtain that $M = \{a, M\} \cap \{b, M\}$. So $M$ is the intersection of a finite number of prime differential ideals.

□

**Corollary 1.5.1.** *Let $K$ be a differential field of characteristic zero and let $A$ be a finitely differentially generated $K$-algebra. Let $I$ be a proper radical differential ideal of $A$. Then there exist finitely many prime differential ideals $P_1, \ldots, P_s$ of $A$ such that*

$$I = P_1 \cap \ldots \cap P_s.$$

*Moreover, when $P_i \nsubseteq P_j$ for all $i \neq j$, $i, j \in \{1, \ldots, s\}$, then the set $\{P_1, \ldots, P_s\}$ is unique.*

As a consequence of the decomposition theorem we obtain the following result:

**Proposition 1.5.1.** *Let $A$ be a Ritt algebra and let $P$ be a proper maximal differential ideal of $A$. Then $P$ is prime.*

*Proof.* Since $A$ is a Keigher ring, $rad(P)$ is a differential ideal. This means that $P$ is radical, because $P$ is a maximal differential ideal. By theorem 1.5.1 $P$ is an intersection of prime differential ideals containing it. Due to the maximality of $P$, we obtain that $P$ is prime.

□

## 1.6 Taylor morphism

Let $B$ be a commutative ring with unity. We denote by $B[[X]]$ the *ring of power series* in one variable $X$ over $B$. It is a differential ring with derivation given by

$$\Big(\sum_{n\geq 0} a_n X^n\Big)' = \sum_{n\geq 1} n a_n X^{n-1}.$$

This means that we have $X' = 1$ and $a' = 0$, $\forall a \in B$. The ring of constants of $B[[X]]$ is clearly $B$.

**Definition 1.6.1.** *Let $A$ be a differential ring and let $B$ be a Ritt algebra. Let $\sigma : A \to B$ be a ring homomorphism (not necessary differential). The mapping*

$$T_\sigma : A \to B[[X]], \qquad a \mapsto \sum_{n\geq 0} \frac{\sigma(a^{(n)})}{n!} X^n,$$

*is called the Taylor morphism associated to $\sigma$.*

**Notation.** Let $I$ be an ideal of a differential ring $A$. Let

$$I^\sharp = \{a \in I \,|\, \forall n \in \mathbb{N} :\, a^{(n)} \in I\}.$$

It is the largest differential ideal of $A$ contained in $I$.

**Proposition 1.6.1.** *Let $A$, $B$, $\sigma$ and $T_\sigma$ be as above. Let $C_A$ denote the subring of constants in $A$ and let $A_0$ be a differential subring of $A$. Then:*

1. *$T_\sigma$ is a differential homomorphism and $ker(T_\sigma) = \big(ker(\sigma)\big)^\sharp$,*
2. *$T_\sigma$ is an $A_0$-algebra homomorphism if and only if $\forall a \in A_0 :\, \sigma(a') = 0$. In particular it is a $C_A$-algebra homomorphism.*
3. *If $B$ is a reduced ring, then $ker(T_\sigma)$ is a radical ideal,*
4. *If $B$ has no zero divisors, then $ker(T_\sigma)$ is a prime ideal.*
5. *If $A$ is a field, then $T_\sigma(A)$ is a field.*

*Proof.* (1) Let $u, v \in A$. A straightforward computation give us that $T_\sigma(u + v) = T_\sigma(u) + T_\sigma(v)$ and also $T_\sigma(u') = [T_\sigma(u)]'$. To obtain multiplicativity we use the Leibniz rule $(uv)^{(n)} = \sum_{i=1}^{n} \binom{n}{i} u^i v^{n-i}$. Now

$$T_\sigma(u) = 0 \Leftrightarrow \sum_{n\geq 0} \frac{\sigma(u^{(n)})}{n!} X^n = 0 \Leftrightarrow \forall n \geq 0 \quad \sigma(u^{(n)}) = 0 \Leftrightarrow u \in (ker(\sigma))^\sharp.$$

(2) If $T_\sigma$ is an $A_0$-algebra homomorphism, i.e. $T_\sigma(a) = \sigma(a)$, for all $a \in A_0$, then we compare the coefficients of $T_\sigma(a) = \sum_{n\geq 0} \frac{\sigma(a^{(n)})}{n!} X^n$ with $\sigma(a)$ to obtain that $\forall a \in A_0 : \sigma(a') = 0$.

Now let us assume that $\sigma(a') = 0$ for all $a \in A_0$. Then $\forall a \in A_0 \forall n \geq 1$ : $\sigma(a^{(n)}) = 0$. So $T_\sigma(a) = \sigma(a)$.

(3) If $B$ is reduced, so is $B[[X]]$. Hence

$$a \in rad[\ker(T_\sigma)] \Leftrightarrow \exists n : T_\sigma(a^n) = 0 \Leftrightarrow [T_\sigma(a)]^n = 0 \Rightarrow T_\sigma(a) = 0 \Leftrightarrow a \in \ker(T_\sigma).$$

(4) If $B$ is an integral domain, so is $B[[X]]$. Hence

$$uv \in \ker(T_\sigma) \Leftrightarrow T_\sigma(uv) = T_\sigma(u)T_\sigma(v) = 0 \Rightarrow u \in \ker(T_\sigma) \vee v \in \ker(T_\sigma).$$

(5) If $a, b \in A$ are elements such that $ab = 1$, then $T_\sigma(ab) = T_\sigma(a)T_\sigma(b) = 1$. Hence every nonzero element in $T_\sigma(A)$ is invertible.

□

**Remark 1.6.1.** *If $I$ is a proper radical (resp. prime) ideal of a Ritt algebra $A$, then $I^\sharp$ is also a radical (resp. prime) ideal.*

*Proof.* This follows from the previous theorem (3) and (4).

□

## 1.7 The primitive element theorem

Let us recall the primitive element theorem. It says that *if $K \subset L$ is a finite separable field extension, then there exists an element $\theta \in L$, such that* $L = K(\theta)$. Below we present the differential version of the primitive element theorem. We will use this result in the proof of the embedding theorem in section 4.2.

**Theorem 1.7.1** (**Primitive element theorem**). *Let $F$ be a differential field of characteristic 0, such that $C_F \subsetneq F$. Let $u$ and $v$ be elements differentially algebraic over $F$. Then there exist $\alpha \in F$ such that $F\langle u, v\rangle = F\langle u+\alpha v\rangle$.*

The proof needs the following lemma (see [29], chapter 2, §22, pp.35-36).

**Lemma 1.7.1.** *Let $F$ be a differential field of characteristic zero, with field of constants $C_F \subsetneq F$. Let $f \in F\{Y_1, \ldots, Y_n\}$ be nonzero. Then there exist $y_1, \ldots, y_n \in F$ such that $f(y_1, \ldots, y_n) \neq 0$.*

*Proof of lemma.* It is sufficient to prove the lemma in case $n = 1$. Let $\alpha \in F \setminus C_F$ and $k \in \mathbb{Z}_+$. We will prove that if $ord(f) \leq k$ then there exists an element

$$y_* = a_0 + a_1\alpha + \ldots + a_k\alpha^k, \tag{1.2}$$

where $a_i \in C_F$ for $i = 0, 1, \ldots, k$, such that $f(y_*) \neq 0$.

We suppose the contrary, i.e. we consider $g \in F\{Y\}$, $g \neq 0$ of the lowest rank such that $g$ vanishes on any element of the form 1.2. We denote by $l$ the order of $g$. We observe that $0 < l \leq k$. Now if we substitute $Y$ in $g$ by $y_*$ (respectively $Y^{(i)}$ by $D^i y_* = a_1\alpha^{(i)} + \ldots + a_k(\alpha^k)^{(i)}$ for $i = 1, \ldots, l$), we obtain zero. So if we treat this expression as a polynomial in variables $a_0, \ldots, a_k$ it must be identically equal to zero. Hence its partial derivatives $\frac{\partial g}{\partial a_0}, \ldots, \frac{\partial g}{\partial a_k}$ are also zero. We compute them to obtain the following system of equations:

$$\begin{cases} \frac{\partial g}{\partial Y}|_{Y=y_*} = 0 \\ \frac{\partial g}{\partial Y}|_{Y=y_*}\alpha + \frac{\partial g}{\partial Y'}|_{Y=y_*}\alpha' + \ldots + \frac{\partial g}{\partial Y^{(l)}}|_{Y=y_*}\alpha^{(l)} = 0 \\ \frac{\partial g}{\partial Y}|_{Y=y_*}\alpha^2 + \frac{\partial g}{\partial Y'}|_{Y=y_*}(\alpha^2)' + \ldots + \frac{\partial g}{\partial Y^{(l)}}|_{Y=y_*}(\alpha^2)^{(l)} = 0 \\ \ldots \\ \frac{\partial g}{\partial Y}|_{Y=y_*}\alpha^l + \frac{\partial g}{\partial Y'}|_{Y=y_*}(\alpha^l)' + \ldots + \frac{\partial g}{\partial Y^{(l)}}|_{Y=y_*}(\alpha^l)^{(l)} = 0 \end{cases} \tag{1.3}$$

Now we consider 1.3 as a system in the indeterminates $\frac{\partial g}{\partial Y^{(i)}}$ for $i = 0, 1, \ldots, l$. Since $\frac{\partial g}{\partial Y^{(l)}}$ is of lower rank than $g$, hence $\frac{\partial g}{\partial Y^{(l)}}(y_*) \neq 0$. Hence $\frac{\partial g}{\partial Y^{(l)}}$ treated as a polynomial in the indeterminates $a_i$ does not vanish identically. Hence the determinant of system 1.3 is equal to zero. Equivalently the elements $1, \alpha, \alpha^2, \ldots, \alpha^l$ are lineary dependent, i.e. there exists $\beta_0, \ldots, \beta_l \in C_F$ not all equal to zero such that $\beta_0 + \beta_1\alpha + \ldots + \beta_l\alpha^l = 0$. We pick up an algebraic polynomial $h$ of lowest degree such that $h(\alpha) = 0$. Hence $h'(\alpha)\alpha' = 0$. Since $h'(\alpha) \neq 0$, then $\alpha' = 0$. We have a contradiction with the assumption $\alpha \in F \setminus C_F$.

□

Now we will prove the primitive element theorem. We follow the proof of Seidenberg (see [33], §3.). The previous method of proving this theorem can be found in a paper by E. Kolchin (see [20], §4.)

*Proof of the theorem.* We construct a differential field $F\langle X\rangle\langle u, v\rangle$, where $X$ is a differential indeterminate. The elements $u, v$ are differentially algebraic over $F$, so also over $F\langle X\rangle$. The sum and the product of differentially algebraic elements are also differentially algebraic elements. So $w := u + Xv$ is differentially algebraic over $F\langle X\rangle$. Let $f \in F\langle X\rangle\{Y\}$ be the minimal polynomial of $w$. We denote by $k$ the order of $f$. We have a polynomial relation

$$f(X, X', \dots X^{(l)}, w, w', \dots, w^{(k)}) = 0. \tag{1.4}$$

We observe that

$$\frac{\partial w^{(i)}}{\partial X^{(k)}} = \begin{cases} 0 & \text{for}\, i < k \\ v & \text{for}\, i = k \end{cases} \tag{1.5}$$

We compute the partial derivative of 1.4 with respect to $X^{(k)}$ and we obtain that $\frac{\partial f}{\partial X^{(k)}} + \frac{\partial f}{\partial w^{(k)}} \cdot v = 0$. Since $f$ is minimal, then $g(X, w) := \frac{\partial f}{\partial w^{(k)}} \neq 0$. Hence $v \in F\langle X\rangle\langle w\rangle$.

By lemma 1.7.1, we can find $x \in F\langle u, v\rangle$, such that $g(x, u + xv) \neq 0$. In fact we can take $x \in F$. Indeed, by analysing the proof of the lemma 1.7.1, we observe that we can specialize $X$ to a polynomial in the indeterminate $\lambda \in F \setminus C_F$ with constant coefficients. So we choose such an $x \in F$. Hence $v \in F\langle u + xv\rangle$ and $F\langle u + xv\rangle = F\langle u, v\rangle$.

□

# Chapter 2

# Real algebra

In this chapter we briefly review Artin-Schreier theory of ordered fields and real fields. We refer to [2] for more results on real algebra. We also comment on *completeness* of real closed field theory.

## 2.1 Ordered fields, real fields and real closed fields

We recall some definitions and facts of real algebra.

**Definition 2.1.1.** *Let $K$ be a field. An ordering of $K$ is a total order relation $\leq$, which satisfies the following conditions*

$$x \leq y \Rightarrow x + z \leq y + z,$$

$$0 \leq x, 0 \leq y \Rightarrow 0 \leq xy,$$

*for all $x, y, z \in K$.*
*A field $K$ endowed with an ordering is called an ordered field.*

If $K$ is an ordered field, we can extend the *ordering* from $K$ to the ring of polynomials $K[Y]$. If $f \in K[Y]$ and

$$f(Y) = a_n Y^n + a_{n-1} Y^{n-1} + \ldots + a_k Y^k, \quad \text{with} \quad a_k \neq 0,$$

then $f(Y) > 0$ if and only if $a_k > 0$. Now we can extend the ordering to the field of rational functions $K(Y)$ by defining for $f(Y), g(Y) \in K[Y]$

$$\frac{f(Y)}{g(Y)} > 0 \Leftrightarrow f(Y)g(Y) > 0.$$

**Definition 2.1.2.** *Let $K$ be a field. A subset $S \subset K$ is called a cone of $K$ if*

$$x, y \in S \Rightarrow x + y \in S,$$

$$x, y \in S \Rightarrow xy \in S,$$

$$x \in K \Rightarrow x^2 \in S.$$

*The cone $S$ is proper if $-1 \notin S$.*

**Theorem 2.1.1.** *Let $K$ be a field. The following properties are equivalent:*

1. *$K$ can be ordered,*
2. *$K$ has a proper cone,*
3. *$-1 \notin \sum K^2$,*
4. *$\forall x_1, \ldots, x_n \in K \quad \sum_{i=1}^n x_i^2 = 0 \Rightarrow x_1 = \ldots = x_n = 0$.*

**Definition 2.1.3.** *A field $K$ is called a real field if it satisfies one of the equivalent properties in theorem 2.1.1.*

**Remark 2.1.1.** *Note that a real field always has characteristic zero.*

A ring $A$ is said to be *semireal* if $-1$ is not a sum of squares in $A$. It is called *real* when $\sum_{i=1}^n x_i^2 = 0$ implies $x_1 = \ldots = x_n = 0$ for all $n \in \mathbb{N}$ and for all $x_1, \ldots, x_n \in A$. A real ring is semireal. An ideal $I$ of $A$ is *real (semireal)* if the quotient ring $A/I$ is real (semireal). This means that an ideal $I$ of $A$ is real if and only if $\forall a_1, \ldots a_n \in A : \sum_{i=1}^n a_i^2 \in I \Rightarrow a_i \in I$, for $i = 1, \ldots, n$. Real ideals are semireal. As already mentioned, for fields these two notions coincide.

**Definition 2.1.4.** *A real field $K$ which has no nontrivial real algebraic extensions is called a real closed field.*

**Theorem 2.1.2.** *Let $K$ be a field. Then the following properties are equivalent:*

1. *$K$ is a real closed field,*
2. *the ring $K[i] := K[X]/(X^2 + 1)$ is an algebraically closed field.*

For the proof see [2], chapter 1.

**Definition 2.1.5.** *Let $K$ be an ordered field. An algebraic extension $L$ of $K$ is called a real closure of $K$ if $L$ is real closed and the inclusion $K \hookrightarrow L$ preserves the ordering of $K$.*

**Theorem 2.1.3.** *Every ordered field $K$ has a real closure which is unique up to $K$-isomorphism.*

For the proof see [2], chapter 1.

**Remark 2.1.2.** *If $F$ is a real field and $K$ its real closure, then the only $F$-automorphism of $K$ is the identity. In this sense uniqueness of real closure is stronger than uniqueness of algebraic closure. We will denote the real closure of an ordered field $F$ by $\overline{F}^r$.*

Examples:

1) $\mathbb{Q}$ and $\mathbb{R}$ with their natural orderings are clearly real fields. Moreover $\mathbb{R}$ is a real closed field.

2) The field of rational functions $\mathbb{R}(X)$ is a real field (see above how it can be ordered).

3) $\mathbb{R}_{alg} := \{x \in \mathbb{R} : x \,\text{is algebraic over}\, \mathbb{Q}\}$ is a real closed field. It is called field of *real algebraic numbers*. It is a real closure of $\mathbb{Q}$, i.e. $\overline{\mathbb{Q}}^r = \mathbb{R}_{alg}$.

4) $\mathbb{R}(X)^\wedge := \{\sum_{i=k}^{\infty} a_i X^{\frac{i}{n}} : k \in \mathbb{Z}, n \in \mathbb{N} \setminus \{0\}, a_i \in \mathbb{R}\}$ is called *field of Puiseux power series with coeffficients in* $\mathbb{R}$. Analogously by $\mathbb{C}(X)^\wedge$ we denote the field of Puiseux power series with coeffficients in $\mathbb{C}$. $\mathbb{C}(X)^\wedge$ is an algebraically closed field. Since $\mathbb{C}(X)^\wedge = \mathbb{R}(X)^\wedge[i]$, then $\mathbb{R}(X)^\wedge$ is real closed.

5) The set $\mathbb{R}(X)^\wedge_{alg}$ of Puiseux series algebraic over $\mathbb{R}(X)$ forms a field. It is a real closure of $\mathbb{R}(X)$ with ordering $\leq$, such that $\forall x \in (-\infty, 0] : x < X$ and $\forall x \in (0, +\infty) : X < x$. For the details see [2], chapter 1, example 1.1.2.

**Lemma 2.1.1.** *Let $I$ be a real ideal of a commutative ring $A$. Then $I$ is radical. If $A$ is noetherian, then all minimal prime ideals containing $I$ are real.*

For the proof see [2], lemma 4.1.5.

**Lemma 2.1.2.** *Let $I$ be a prime ideal of a commutative ring $A$. Then $I$ is real if and only if $Fr(A/I)$ is a real field.*

*Proof.* $Fr(A/I)$ is real if and only if $\forall x_1 \ldots, x_n \in Fr(A/I) \quad \sum_{i=1}^n x_i^2 = 0 \Rightarrow x_1 = \ldots = x_n = 0$ (see theorem 2.1.1). This means $\sum_{i=1}^n x_i^2 \in I \Rightarrow x_1, \ldots, x_n \in I$.

□

## 2.2 The Tarski-Seidenberg principle

The theory of real closed fields admits quantifier elimination. We have a *Tarski-Seidenberg principle*, which states that semialgebraic sets in $K^n$, where $K$ is a real closed field, are stable under projection. Let us recall this theorem.

**Definition 2.2.1.** *Let $K$ be a real closed field. A subset $S \subset K^n$ is a semi-algebraic subset of $K^n$ if it has the form*

$$\bigcup_{i=1}^{p} \bigcap_{j=1}^{g} A_{ij},$$

*where $A_{ij} = \{x \in K^n : f(x) > 0\}$ or $A_{ij} = \{x \in K^n : f(x) = 0\}$ (or $A_{ij} = \{x \in K^n : f(x) < 0\}$) for $i = 1, \ldots p$, $j = 1, \ldots q$, where $f \in K[X_1, \ldots, X_n]$.*

An algebraic set is semi-algebraic. Semi-algebraic subsets of $K$ are exactly the finite unions of intervals. The closure and the interior of a semi-algebraic set are semi-algebraic.

The *Tarski-Seidenberg Principle* states that if $K$ is a real closed field, $A$ is a semialgebraic subset of $K^{n+m}$ and $\pi : K^n \times K^m \to K^n$ is the natural projection (we just forget last $m$ coordinates), then $\pi(A)$ is a semialgebraic subset of $K^n$ (see [2], chapter 1.4. and chapter 2.2).

For our purposes the following corollary of Tarski-Seidenberg Principle will be useful.

**Theorem 2.2.1** (**Transfer Principle**). *Let $F$ be a real closed field and $K$ a real closed extension of $F$. We consider a boolean combination $\beta(X_1, \dots, X_n)$ of polynomial equations and inequalities with coefficients in $F$. If there exists $u = (u_1, \dots, u_n) \in K^n$ such that $\beta(u)$ is true, then there exists $x = (x_1, \dots, x_n) \in F^n$ such that $\beta(x)$ holds true.*

For the proof see [2], chapter 4.1.

We can formulate Tarski-Seidenberg Principle in the language of model theory. If $F$ is a real closed field, then semialgebraic sets in $F^n$ are sets of the form $\{x \in F^n : \Psi(t, x)\}$, where $\Psi(T, X)$ is a first-order formula in the variables $T_1, \dots, T_k, X_1, \dots, X_n$ and $t = (t_1, \dots, t_k)$ are parameters from $F$. The principle states that the language of real closed fields admits elimination of quantifiers, i.e. every first-order formula in the language of real closed fields is equivalent to a quantifier-free formula (see for example [25]).

A consequence of this result is a theorem analogous to the *Principle of Lefschetz*. Let us recall that this principle roughly says that it is enough to prove some result over the complex numbers (where we can make use of analytic and topological properties) and then we automatically get the same result for all algebraically closed fields of characteristic zero. Now we are able to formulate a similar principle for real closed fields. Namely, any formula of first-order language which holds true in one real closed field (for example $\mathbb{R}$) is also true in all real closed fields. So the problem always reduces to answering the questions if the statement of our result can be described in first-order language and if it holds true for some real closed field (for more detail see [30] and [31]). For our purposes we can formulate the following corollary based on this argumentation.

**Corollary 2.2.1.** *Let $F$ be a real field and let $f_i, g_j \in F[X_1, \dots, X_n]$, for $i = 1, \dots, k$ and $j = 1, \dots, l$. The polynomial system*

$$\begin{cases} f_i(X_1, \dots, X_n) & = 0, \quad i = 1, \dots, k \\ g_j(X_1, \dots, X_n) & > 0, \quad j = 1, \dots, l, \end{cases}$$

*has a solution in some real extension of $F$ if and only if it has a solution in all real closed fields containing $F$.*

We present one more important result proved in 1927 by E. Artin and O. Schreier.

**Theorem 2.2.2** (**Artin-Schreier Theorem**). *Let $K$ be a field of arbitrary characteristic. Let $\overline{K}$ denote its algebraic closure. If $K \neq \overline{K}$ and $[\overline{K} : K] < \infty$ then $K$ is a real closed field and $\overline{K} = K(i)$, where $i = \sqrt{-1}$.*

In other words, if $L$ is an algebraically closed field and $K$ a subfield of $L$ such that $1 < [L : K] < \infty$, then $char(K) = 0$ and $L = K(i)$. For the proof see [17], chapter 1.

## 2.3 Some auxiliary results

In this section we present some needed facts concerning real closed field theory. It is a *complete* theory, i.e. for every sentence $p$ described in the language of real closed field theory one can prove $p$ or else negation of $p$.

**Theorem 2.3.1** (**Skolem-Löwenheim Theorem**). *If $T$ is a theory (not necessarilly complete) such that it has an infinite model or finite models of arbitrary large (finite) cardinality, then for every cardinal number $\aleph$ no less than the cardinality of $T$, the theory $T$ has a model of cardinality $\aleph$.*

For the proof of this theorem and for informations concerning needed model theory notions see [27].

For our purposes the following consequence of this theorem will be useful.

**Corollary 2.3.1.** *Let $M$ be an infinite model of the complete theory $T$ in language $L$. Then for every cardinal number $\aleph$ not less than $card(M)$ and not less than $card(L)$, $M$ has an elementary extension of cardinality $\aleph$.*

The theory of real closed fields is *complete*, so this kind of choice of the real closed field is possible. By elementary extension we understand such a field extension $F \subset M$ that every tuple of $F$ satisfies the same formulas in $F$ as in the $M$. In other words one can choose a real closed field extension of arbitrary large cardinality.

In particular if we are interested only in field extensions, one can observe that every purely transcendental extension of a given field $F$ is $F$-isomorphic to a field of rational functions over $F$ of appropriate number of indeterminates. In this case if we need an extension $F \subset M$ of real closed fields with a given transcendence degree say $\aleph$, we can define the field $M$ as the real closure of the field of rational functions over $F$, i.e. $M = \overline{F(X)}^r$, where $X = \{X_i\}_{i \in I}$ for $card(I) = \aleph$.

# Chapter 3

# Picard-Vessiot theory

## 3.1 Basic definitions and facts

For a given field $K$ and for an arbitrary polynomial $f \in K[Y]$ we construct a *splitting field*, i.e. a minimal field $L$ containing $K$ over which $f$ factors into linear factors. Similarly we can associate to a homogeneous linear differential equation of order $n$ defined over the differential field $K$ a minimal extension $L$ of $K$ containing a fundamental set of solutions of this equation (i.e. a set of $n$ solutions linearly independent over $C_L$.).

We shall consider homogeneous linear differential equations defined over a differential field $K$ of the form

$$\mathcal{L}(Y) := Y^{(n)} + a_{n-1}Y^{(n-1)} + \ldots + a_1 Y' + a_0 Y = 0, \tag{3.1}$$

where $a_i \in K$ for $i \in \{0, 1, \ldots, n-1\}$.

If $L$ is a differential field extension of $K$, then the set of solutions of $\mathcal{L}(Y) = 0$ in $L$ is a $C_L$-vector space of dimension $\leq n$.

We can define a Picard-Vessiot extension for equation (3.1) over a differential field $K$. When $K$ is a field of characteristic zero with algebraically closed field of constants $C_K$, then it can be proved that we can always associate to this equation a minimal extension of $K$ containing a fundamental set of solutions of (3.1). In the case described above this extension is unique up to differential $K$-isomorphism.

**Definition 3.1.1.** *A differential field extension $K \subset L$ is a Picard-Vessiot extension for $\mathcal{L}$ if*

1. *$L$ is differentially generated over $K$ by a fundamental system of solutions of $\mathcal{L}(Y) = 0$ in $L$,*
2. *every constant of $L$ lies in $K$,i.e. $C_K = C_L$.*

**Theorem 3.1.1.** *Let $K$ be a differential field of characteristic zero with algebraically closed field of constants $C_K$. Let equation (3.1) be defined over $K$. Then there exists a Picard-Vessiot extension $L$ of $K$ for $\mathcal{L}$ and it is unique up to differential $K$-isomorphism.*

For the proof see [8], chapter 3.

Let us recall how we obtain a Picard-Vessiot extension for $\mathcal{L}$ over $K$ in the case in which $C_K$ is an algebraically closed field. First we construct the *full universal solution algebra.*

We consider the ring $K[Y_{ij}]$, where $0 \leq i \leq n-1$ and $1 \leq j \leq n$. It is a polynomial ring in $n^2$ indeterminates. We extend the derivation of $K$ to $K[Y_{ij}]$ by defining

$$Y'_{ij} = Y_{i+1,j} \quad \text{for} \quad 0 \leq i \leq n-2,$$

$$Y'_{n-1,j} = -a_{n-1}Y_{n-1,j} - \ldots - a_1 Y_{1j} - a_0 Y_{0j}.$$

Notice that in this way we assure that $Y_{0j}$, $1 \leq j \leq n$ are solutions of the considered equation.

We denote $W = \det(Y_{ij})$. We have

$$W = \det \begin{pmatrix} Y_{01} & \ldots & Y_{0n} \\ Y_{11} & \ldots & Y_{1n} \\ \ldots & \ldots & \ldots \\ Y_{n-1,1} & \ldots & Y_{n-1,n} \end{pmatrix} = \det \begin{pmatrix} Y_{01} & \ldots & Y_{0n} \\ Y'_{01} & \ldots & Y'_{0n} \\ \ldots & \ldots & \ldots \\ Y_{01}^{(n-1)} & \ldots & Y_{0n}^{(n-1)} \end{pmatrix}.$$

So $W$ is the wronskian (determinant) of $Y_{01}, \ldots, Y_{0n}$. The elements $Y_{01}, \ldots, Y_{0n}$ are linearly independent over $C_K$ if and only if $W$ is nonzero. Let $\mathcal{W} = \{W^n\}_{n \geq 0}$ be the multiplicative system of the powers of $W$. Let $R := K[Y_{ij}]_{\mathcal{W}}$ be the localization of $K[Y_{ij}]$ in $\mathcal{W}$. The derivation of $K[Y_{ij}]$ extends to $R$ in a unique way (see section 1.1). This differential ring $R$ is called the *full universal solution algebra.* In this way we assure that $Y_{0j}, 1 \leq j \leq n$ form a *fundamental set of solutions.*

Then we consider a maximal differential ideal $M$ of $R$, i.e. a maximal element in the set of all proper differential ideals of $R$, which is proved to be prime (see proposition 1.5.1). Then one can prove that the field of fractions of the integral domain $R/M$ i.e. $L = Fr(R/M)$ fulfills the conditions to be a Picard-Vessiot extension for $\mathcal{L}$ over $K$.

The quotient ring $R/M$ is *simple*, i.e. it has no proper differential ideals. It is proved that if $R$ has no proper differential ideals, then $C_K = C_L$.

**Theorem 3.1.2.** *Let $K$ be a differential field, with field of constants $C_K$. Let $K \subset R$ be a differential ring extension such that $R$ is finitely generated as a $K$-algebra and has no zero divisors. Let us denote $L = Fr(R)$. If $C_K$ is algebraically closed and $R$ has no proper differential ideals, then $C_L = C_K$.*

For the proof see [8], Proposition 3.5 or [7], Theorem 5.6.4.

The idea behind the proof is the following: every new constant $c \in C_L \backslash C_K$ must be algebraic over $K$ (but then it is algebraic over $C_K$ and since $C_K$ is algebraically closed, this means that $c \in C_K$) or else there exist an element $a \in C_K$ such that $c - a$ is not invertible in R (and then it generates a proper differential ideal). For details see [8], chapter 3.2. or [7], chapter 5.6.

## 3.2 Fundamental theorem of Picard-Vessiot theory

Let us now present the analogous of the fundamental theorem of polynomial Galois theory. If we have a polynomial $f \in K[Y]$ in one variable $Y$ with coefficients in a field $K$, we construct a splitting field $L$ by adjoining to $K$ all roots of the polynomial $f$. In Galois theory for polynomial equations we introduce the *Galois group* of a field extension $K \subset L$. It is the group of all $K$-automorphisms of $L$. If $L$ is a splitting field of a polynomial $f \in K[Y]$, the Galois group of $K \subset L$ is the group of all permutations of the roots of $f$ which preserve all algebraic relations between them.

In differential Galois theory we introduce the so called *differential Galois group*. It consists in all differential $K$-automorphisms of the Picard-Vessiot extension. They preserve the relations between solutions of the given equation and also between their derivatives.

**Definition 3.2.1.** *Let $K \subset L$ be an extension of differential fields. The group*

$$G(L|K) = \{\sigma : L \to L \,|\, \sigma \textit{ is a differential } K\textit{-automorphism}\},$$

*is called the differential Galois group of the extension $K \subset L$.*

If necessary we denote this group by $G_{diff}(L|K)$ to distinguish it from the Galois group defined in polynomial Galois theory.

When $K \subset L$ is a Picard-Vessiot extension of equation (3.1), the Galois group $G(L|K)$ is denoted by $Gal_K(\mathcal{L})$ or $Gal(\mathcal{L})$ and it is called *Galois group of the equation (3.1) over $K$.*

**Remark 3.2.1.** *If $K$ is a differential field and $K \subset L$ is a separable algebraic field extension then the derivation of $K$ extends uniquely to $L$ and moreover every $K$-automorphism of $L$ is a differential one.*

For the proof see [8], proposition 2.3.

In other words, in the case of algebraic separable extensions Galois group and differential Galois group coincide.

Let us recall that an algebraic extension is Galois if and only if it is normal and separable. Moreover if $K$ is a field of characteristic zero, then every element algebraic over $K$ is separable over $K$. For Picard-Vessiot extensions we have the following characterization.

**Theorem 3.2.1.** *Let $K$ be a differential field of characteristic zero with algebraically closed field of constants. If $L$ is an algebraic Picard-Vessiot extension of $K$, then it is a normal algebraic extension.*

For the proof see [8], corollary 3.3.

**Theorem 3.2.2.** *Let $K$ be a differential field of characteristic zero with algebraically closed field of constants. Let $L \subset K$ be a finite Galois extension. Then $L$ is a Picard-Vessiot extension of $K$.*

For the proof see [22], proposition 3.20.

The differential Galois group of a Picard-Vessiot extension is a *linear algebraic group*, i.e. it is isomorphic to a subgroup of the general linear group $GL_n(C_K)$, closed in Zariski topology, where $n$ is the order of the differential equation. For the details see for example [8], chapter 4. Moreover

$$dimG(L|K) = trdeg(L|K).$$

Here we understand the dimension of $G(L|K)$ as its dimension as an algebraic variety.

Let $K \subset L$ be a Picard-Vessiot extension for equation (3.1) and let $M$ be a differential subfield of $L$ such that $K \subset M \subset L$. Then $M \subset L$ is a Picard-Vessiot extension for $\mathcal{L}$, viewed as defined over $M$, with

$$G(L|M) = \{\sigma \in G(L|K) \, : \, \sigma|_M = id_M\}.$$

Let $H$ be a subgroup of $G(L|K)$. We denote by

$$L^H := \{x \in L \,|\, \forall \sigma \in H : \sigma(x) = x\}$$

the subfield of $L$ fixed by the action of $H$. $L^H$ is stable under the derivation of $L$.

**Definition 3.2.2.** *We say that the differential field extension $K \subset L$ is normal if*

$$\forall x \in L \setminus K \, \exists \sigma \in G(L|K) : \, \sigma(x) \neq x.$$

Now we can state the fundamental theorem of Picard-Vessiot theory.

**Theorem 3.2.3** (**Fundamental Theorem**). *Let $K$ be a differential field of characteristic zero with algebraically closed field of constants. Let $K \subset L$ be a Picard-Vessiot extension with differential Galois group $G(L|K)$.*

1. *Then there is a bijective correspondence between Zariski closed subgroups $H$ of $G(L|K)$ and intermediate differential fields $M$ such that $K \subset M \subset L$, given by*

$$H \to L^H, \qquad M \to G(L|M).$$

2. *The differential field extension $K \subset M$ is a Picard-Vessiot extension if and only if $G(L|M)$ is a normal subgroup of $G(L|K)$. Then the restriction morphism*

$$G(L|K) \to G(M|K), \qquad \sigma \mapsto \sigma|_M$$

*induces an isomorphism $G(L|K)/G(L|M) \cong G(M|K)$.*

For the proof see [8], chapter 5.

# Chapter 4

# Picard-Vessiot extensions for real fields

## 4.1 Motivation

**Example 1:**
Let us analyse the example given by A. Seidenberg mentioned in the introduction (see [32] or [18], chapter 6, ex.1). We consider the field of real numbers $\mathbb{R}$ with trivial derivation, i.e. $\forall a \in \mathbb{R} : \ a' = 0$. To $\mathbb{R}$ we adjoin the general solution $a$ of the equation

$$4a^2 + a'^2 = -1, \tag{4.1}$$

such that $a' \neq 0$. Now we take $K = \mathbb{R}\langle a \rangle = \mathbb{R}(a, a')$ to be a base field over which we consider the homogeneous linear differential equation

$$y'' + y = 0. \tag{4.2}$$

It can be proved that the field of constants of $K$ is $\mathbb{R}$. Moreover, if $\xi$ is a nontrivial solution of equation (4.2), then $v = \frac{\xi'}{\xi}$ is a solution of the Riccati equation

$$v' = -1 - v^2. \tag{4.3}$$

It can be also proved that if $v$ is any solution of equation (4.3), then $L = K\langle v \rangle$ contains a new constant, i.e. $\mathbb{R} \subsetneq C_L$.

In Seidenberg's example (4.1) shows that the base field $K$ is not a real field. So it seems to be reasonable to consider homogeneous linear differential equations defined over a real field $K$.

We shall consider the existence of Picard-Vessiot extensions for real differential fields. To understand how delicate is the problem let us analyse two more examples.

**Example 2:** A real field is a field which can be ordered (see chapter 4). We have several possible orderings for a given real field. For example, in the field $\mathbb{Q}(\sqrt{2})$, either $\sqrt{2}$ or $-\sqrt{2}$ can be taken to be positive. So we can consider two different real closures of the field $\mathbb{Q}(\sqrt{2})$. In one of them the element $\sqrt{2}$ has a square root, in the second one it does not.

Here we present a modification of the example given by H. Umemura (see [37]). Instead of the field or rational numbers we consider the field of real numbers.

**Example 3:** Let us consider a differential field extension $\mathbb{R}(x, e^{3x}) \subset \mathbb{R}(x, e^{x})$ with derivation $\frac{d}{dx}$. It is an algebraic extension which is not normal. So it is not Galois. But as it can be easily seen it is a real Picard-Vessiot extension. Indeed, the function $y = e^{x}$ satisfies the homogeneous linear differential equation $y' - y = 0$. By real Picard-Vessiot extension we understand a Picard-Vessiot extension which is an extension of real fields.

Let us recall that in Picard-Vessiot theory over differential fields of characteristic zero with algebraically closed field of constants when we are dealing with finite algebraic extensions a Picard-Vessiot extension appears to be the same as a Galois extension (see theorem 3.2.1 and theorem 3.2.2.). In particular an algebraic Picard-Vessiot extension is a normal algebraic extension if $C_K$ is algebraically closed.

As one can conclude by analysing the example given above, in case of *real differential field extensions* this fact is no longer true.

Our last example explains the condition concerning the field of constants of a given differential field, which appears in the existence theorem (see theorem 4.3.1).

**Example 4:** Let us consider the field $\overline{\mathbb{Q}}^{r}$ with the trivial derivation and a real differential extension $K = \overline{\mathbb{Q}}^{r}\langle e^{\alpha X}\rangle$ of $\overline{\mathbb{Q}}^{r}$, where $\alpha \in \mathbb{R} \setminus \overline{\mathbb{Q}}^{r}$. We consider $K$ as a subfield of $\mathbb{R}((X))$. The derivation of $\mathbb{R}((X))$ is given by $(\sum_{n\geq 0} a_n X^n)' = \sum_{n\geq 1} n a_n X^{n-1}$ and extension to the fraction field. So $(e^{\alpha X})' = \alpha e^{\alpha X}$. Hence $\alpha \in K$ and it is a *new constant*.

## 4.2 The Seidenberg-Singer embedding theorem

Now we will state and prove an embedding theorem which will be crucial in the proof of the existence of a Picard-Vessiot extension for a differential equation defined over a real field $K$ differentially finitely generated over a real closed field $F$ considered as a differential field with trivial derivation, with field of constants equal to $F$.

We will need some auxiliary lemmas. Here we prove a certain version of results of A. Seidenberg presented in [31], which were also explained by M. F. Singer in [35].

**Lemma 4.2.1.** *Let $F$ be an arbitrary field of characteristic zero considered as a differential field with trivial derivation and let $K = F\langle y_1, \dots, y_n\rangle$ be a differential extension of $F$, with derivation $D$. Let $L$ be an arbitrary field of characteristic zero. We denote by $L[[X]]$ the ring of formal power series, which can be seen as a differential ring with derivation $D_L$, where*

$$D_L\Big(\sum_{j\geq 0} a_j \frac{X^j}{j!}\Big) = \sum_{j\geq 1} a_j \frac{X^{j-1}}{(j-1)!}.$$

*Let $\sigma : K \to L$ be an abstract field isomorphism (i.e. not necessary differential) and let $\sigma(D^j y_i) = c_{ij} \in L$. We consider $F$ as a subfield of $L$ via $\sigma$. Then the Taylor morphism $T_\sigma : K \to L[[X]]$ associated to $\sigma$ given by $T_\sigma(y_i) = \bar{y_i} = \sum_j c_{ij} \frac{X^j}{j!}$ defines a differential isomorphism $\varphi : K \to F\langle \bar{y_1}, \dots \bar{y_n}\rangle$.*

*Proof.* By proposition 1.6.1 we get that the Taylor morphism associated with $\sigma$ is a differential homomorphism, such that $\ker(T_\sigma) = (\ker(\sigma))^\sharp$. Since $\sigma$ is an isomorphism, then $T_\sigma$ is a ring monomorphism. So by proposition 1.6.1, (5) we get the differential field isomorphism $\varphi : K \to Im(T_\sigma)$.

□

**Lemma 4.2.2.** *Let $F$ be a real field and let $K$ be a real extension of $F$ of the form $K = F(\{x_\lambda\}_{\lambda\in\Lambda}, y)$, where $x_\lambda$ are algebraically independent over $F$ for $card(\Lambda) \le \aleph$ and $y$ is algebraic over $G = F(\{x_\lambda\}_{\lambda\in\Lambda})$. Let $M$ be a real closed extension of $F$ such that $trdeg(M|F) \ge \aleph$. Then $K$ is isomorphic to a subfield of $M$.*

*Proof.* STEP 1: We consider the real field $G = F(\{x_\lambda\}_{\lambda\in\Lambda})$. We will embed $G$ into $M$. Since $trdeg(M|F) \ge \aleph$, there exist $c_\lambda \in M$ for $\lambda \in \Lambda$ algebraically independent over $F$. We define $S := F(\{c_\lambda\}_{\lambda\in\Lambda})$. Now $G$ and $S$ are two purely transcendental extensions of $F$, whose transcendence degrees over $F$ are equal. So there exists exactly one isomorphism of fields $\varphi : G \to S$ such that $\varphi|_F = id$ and $\varphi(x_\lambda) = c_\lambda$ for $\lambda \in \Lambda$.

STEP 2: We will embed $K = G(y)$ into $M$. We have already constructed an isomorphism $\varphi : G \to S$. We can extend it to an isomorphism of the polynomial rings i.e. $\bar\varphi : G[X] \to S[X]$. Let $f \in G[X]$ be the minimal polynomial of $y$. We have $K \cong G[X]/(f) \cong S[X]/(\bar\varphi f)$, so $S[X]/(\bar\varphi f)$ is a real field and $\bar\varphi f$ has a root in $\overline{S}^r$. By corollary 2.2.1 it has a root, say $y^*$, in $M$. Then we obtain an isomorphism of fields $\psi : K = G(y) \to S(y^*) \subset M$ (see for example [4], chapter 2.1, lemma 2).

□

The existence of the field $M$ postulated in the lemma above is guaranteed by Skolem-Löwenheim theorem (see theorem 2.3.1). As it was mentioned in section 2.3, we may define $M$ as a real closure of the field of fractions of the ring $F[X]$, where $X = \{X_i\}_{i\in I}$ and $card(I) \ge \aleph$.

**Remark 4.2.1.** *We observe that lemma 4.2.2 is also true without assuming the fields $F$ and $K$ to be real if we take the fields of characteristic zero and $M$ to be algebraically closed.*

The following result is based on the embedding theorem proved by A. Seidenberg (see [31]) and then in the real case by M. F. Singer (see [35]).

**Theorem 4.2.1 (Seidenberg-Singer Embedding Theorem).** *Let $F$ be a real closed field considered as a differential field with trivial derivation. Let $(K, D)$ be a real differential extension of $F$, differentially finitely generated over $F$ i.e. $K = F\langle y_1, \ldots, y_n\rangle$ with field of constants $C_K = F$. Let $M$ be a real closed extension of $F$ such that $trdeg(M|F) \ge \mathfrak{c}$. Then $K$ is isomorphic* *to a subfield $K_1 = F\langle \bar{y_1}, \dots, \bar{y_n} \rangle$ of a ring $M[[X]]$, where $\bar{y}_i$ for $i = 1, \dots, n$ are formal power series and the derivation on $K_1$ is $\frac{d}{dX}$.*

*Proof.* By using the primitive element theorem (see theorem 1.7.1) we may assume that $K = F\langle y_1, \dots, y_n \rangle$, where $y_1, \dots, y_{n-1}$ are differentially algebraically independent over $F$ and $y_n$ is differentially algebraic over $G = F\langle y_1, \dots, y_{n-1} \rangle$.

STEP 1: We will embed $G$ into $M$. We consider $G = F(D^j y_i)$, where $i \leq n-1$ and $j \in \mathbb{N}$. By lemma 4.2.2, there exists a field isomorphism $\sigma : G \to S := F(c_{ij}) \subset M$, such that $\sigma(D^j y_i) = c_{ij}$ and $c_{ij} \in M$ are algebraically independent over $F$.

STEP 2: The element $y_n$ is differentially algebraic over $G$. Let $f \in G\{Y_n\}$ be the minimal polynomial of $y_n$. Let $ord(f) = r$. Then $K = G\langle y_n \rangle = G(y_n, Dy_n, \dots, D^r y_n)$, i.e. $G(y_n, Dy_n, \dots, D^r y_n)$ is a differential field. To observe that $D^{r+1} y_n$ is in this field we compute $D[f(y_n)] = 0$ and solve it with respect to $D^{r+1} y_n$.

Then $y_n, Dy_n, \dots, D^{r-1} y_n$ are algebraically independent over $G$ and $D^r y_n$ is algebraic over the field $G_1 := G(y_n, Dy_n, \dots, D^{r-1} y_n)$. So $y_n, Dy_n, \dots, D^{r-1} y_n$ are algebraically independent over the real closed field $F$. By lemma 4.2.2, we can embed $G_1$ and also $K = G_1(D^r y_n)$ into $M$. Again we choose $c_{n0}, \dots c_{n,r-1}$ such that $c_{ij}$ for $i \leq n-1$, $j \in \mathbb{N}$ and $c_{n0}, \dots c_{n,r-1}$ are algebraically independent over $F$. The element $c_{nr}$ is obtained from the condition $\sigma f = 0$.

Since the map $\sigma$ is clearly a field isomorphism, we can apply lemma 4.2.1 and obtain a differential field isomorphism $\varphi : K \to F\langle \overline{y}_1, \dots, \overline{y}_n \rangle$, where $F\langle \overline{y}_1, \dots, \overline{y}_n \rangle$ is a differential subfield of the differential ring $(M[[X]], \frac{d}{dX})$ and $\overline{y}_i$ is the image of $y_i$ in $M$, $1 \leq i \leq n$.

□

## 4.3 Existence theorem

### 4.3.1 First case

Let $K$ be a real differential field differentially finitely generated over its field of constants $F$ (i.e. $K = F\langle y_1 \dots, y_n \rangle$, for some $n \in \mathbb{N}$). We assume that $F$ is real closed. We shall consider a homogeneous linear ordinary differential equation of order $k$ of the form

$$\mathcal{L}(Y) := Y^{(k)} + a_{k-1}Y^{(k-1)} + \ldots + a_1Y' + a_0Y = 0, \tag{4.4}$$

where $a_i \in K$ for $i \in \{0, 1, \ldots, k-1\}$. In this section we prove that there exists a Picard-Vessiot extension for this equation, which moreover is a real field.

**Theorem 4.3.1.** *Let $F$ and $K$ be as above. Let $M$ be a real closed extension of $F$ such that $trdeg(M|F) \geq \mathfrak{c}$. We consider equation (4.4) defined over $K$. Then there exists a Picard-Vessiot extension of $K$ for equation (4.4), which moreover is a real field.*

*Proof.* Let us denote the complexification of $K$ by $\hat{K} = K(i)$, where $i^2 = -1$. Then the field of constant of $\hat{K}$ is $\hat{F} = F(i)$, which is algebraically closed.

We consider equation (4.4) over $\hat{K}$. The field of constants is algebraically closed, so there exists a unique Picard-Vessiot extension of $\hat{K}$ for this equation (see theorem 3.1.1). Let us denote it by $\hat{L} := \hat{K}\langle\eta_1, \ldots, \eta_k\rangle$, where $\eta_1, \ldots, \eta_k$ is a fundamental set of solutions of equation (4.4).

By Seidenberg-Singer embedding theorem (see theorem 4.2.1), our base field $K$ is isomorphic to a subfield of the ring of formal power series over $M$, i.e. there exists a differential isomorphism

$$T_\sigma : K = F\langle y_1, \ldots, y_n\rangle \to K_1 := F\langle \bar{y}_1, \ldots, \bar{y}_n\rangle \subset M[[X]],$$

where $\bar{y}_i$ for $i = 1, \ldots, n$ are formal power series. If we denote by $\hat{M} = M(i)$ the complexification of $M$, then $\hat{K}_1 = \hat{F}\langle y_1, \ldots, y_n\rangle$ is isomorphic to a subfield of $\hat{M}$. $\hat{L}$ is also differentially finitely generated over $\hat{K}$, so it is isomorphic (cf. remark 4.2.1) to an extension of $\hat{K}_1$ in $\hat{M}$. By lemma 4.2.1, we obtain a differential isomorphism

$$\varphi : \hat{L} = \hat{K}\langle\eta_1, \ldots, \eta_k\rangle \to \hat{L}_1 := \hat{K}_1\langle\bar{\eta}_1, \ldots, \bar{\eta}_k\rangle \subset \hat{M}[[X]].$$

So $\bar{\eta}_1, \ldots, \bar{\eta}_k$ is a fundamental set of solutions of equation

$$Y^{(k)} + b_{k-1}Y^{(k-1)} + \ldots + b_1Y' + b_0Y = 0, \tag{4.5}$$

considered over $\hat{K}_1$, where $b_i := T_\sigma(a_i) \in K_1$ for $i = 0, \ldots, k-1$.

The conjugation $c$ in $\hat{M}$ given by $i \mapsto -i$ extends clearly to $\hat{M}[[X]]$. The vector space of solutions $V := \hat{F}\bar{\eta}_1 \oplus \cdots \oplus \hat{F}\bar{\eta}_k$ is $c$-stable. Let $V^c$ be the

$F$-subspace of $V$ fixed by the conjugation $c$. Clearly $\dim_F V^c = k$. Let $L_1$ be the differential subfield of $\hat{L}_1$ generated by $K_1$ and $V^c$. By definition, it is differentially generated over $K_1$ by a fundamental system of solutions of (4.5). As it is a differential subfield of $\hat{L}_1$, $C_{L_1} \subset C_{\hat{L}_1} = \hat{F}$. But $L_1$ is contained in $M[[X]]$, so it is a real field, hence $C_{L_1} = F$. So $L_1$ is a Picard-Vessiot extension for equation (4.5) over $K_1$. Hence $L := \varphi^{-1}(L_1)$ is a Picard-Vessiot extension for equation (4.4) over $K$, and $L$ is a real field.

□

### 4.3.2 General case

Let $F$ be a real closed field considered as a differential field with trivial derivation. Let $K$ be a real differential extension of $F$ of arbitrary differential degree. We assume that the field of constants is $C_K = F$. We consider the equation

$$\mathcal{L}(Y) := Y^{(k)} + a_{k-1}Y^{(k-1)} + \ldots + a_1 Y' + a_0 Y = 0, \tag{4.6}$$

over $K$. We will prove that we can embed $K$ into a real closed extension $M$ of $F$, which is large enough. Then the proof of the existence theorem of Picard-Vessiot extension for $K$ is the same like in section 4.3.1.

By lemma 4.2.2, we can embed into $M$ all these subfields of $K$, which are compositions of differentially transcendental extensions of arbitrary large differential transcendence degree and a differentially algebraic extension of finite differential degree. Let us denote the family of all embeddable subfields of $K$ by $\mathcal{S}$. Let us consider the space $\mathcal{E}$ of embeddings of subfields from $\mathcal{S}$. Clearly $\mathcal{E} \neq \varnothing$. We introduce a partial order relation $\leq$ in $\mathcal{E}$ by

$$\varphi_1 \leq \varphi_2 \Leftrightarrow \varphi_1 \subset \varphi_2,$$

for $\varphi_1, \varphi_2 \in \mathcal{E}$. We observe that every totally ordered subset $\mathcal{G}$ of $\mathcal{E}$ has an upper bound, i.e. $\bigcup_{\varphi_i \in \mathcal{G}} \varphi_i$. Hence by *Kuratowski-Zorn lemma* there exists a maximal element $\varphi_{max}$ in $\mathcal{E}$. We claim that $\varphi_{max}$ is an embedding of $K$. Indeed, if not then there exist a proper subfield $S \in \mathcal{S}$ such that $\varphi_{max}$ is an embedding of $S$. So there exists an element $a \in K \setminus S$ which is not embedded by $\varphi_{max}$. We consider the differential field $S\langle a\rangle$. If $a$ is differentially transcendental over $S$, then there exists clearly an embedding $\psi$ of $S\langle a\rangle$ into

$M$. If $a$ is differentially algebraic over $S$, by lemma 4.2.2, there exists an embedding $\psi$ of $S\langle a\rangle$ into $M$. Hence $\varphi_{max} < \psi$. We have a contradiction with the maximality of $\varphi_{max}$.

## 4.4 Comments concerning construction of Picard-Vessiot extension

Let $K$ and $C_K$ be like in the previous section. Here we give a short commentary on the canonical construction of Picard-Vessiot extension known from the theory of differential fields with algebraically closed field of constants. This method of construction also holds for our case. Let us follow it step by step.

Our goal is to construct a real Picard-Vessiot extension for equation (4.4). The first step is the construction of the full universal solution algebra (see chapter 3). We consider the ring $K[U_{ij}]$, where $0 \leq i \leq k-1$ and $1 \leq j \leq k$. It is a polynomial ring in $k^2$ indeterminates. We extend the derivation of $K$ to $K[U_{ij}]$ (let us denote it by $D$) by defining

$$D(U_{ij}) = U_{i+1,j} \quad \text{for} \quad 0 \leq i \leq k-2,$$

$$D(U_{k-1,j}) = -a_{k-1}U_{k-1,j} - \ldots - a_1 U_{1j} - a_0 U_{0j}.$$

We denote $V = \det(U_{ij})$ the wronskian (determinant) of $U_{01}, \ldots, U_{0k}$. The elements $U_{01}, \ldots, U_{0k}$ are linearly independent over $C_K$ if and only if $V$ is nonzero. Let $\mathcal{V} = \{V^n\}_{n \geq 0}$ be the multiplicative system of the powers of $V$. Let $R := K[U_{ij}]_{\mathcal{V}}$ be the localization of $K[U_{ij}]$ in $\mathcal{V}$. The differential ring $R$ is called the *full universal solution algebra*. It is a real ring, since it is a localization of a polynomial ring in $k^2$ variables over the real field $K$.

We consider *real differential ideals* of the full universal solution algebra $R$. The crucial point of our construction is to prove that the maximal real differential ideal of $R$, i.e. the maximal element in the set of all proper real differential ideals of $R$, is prime. To this end we shall use a theorem of Ritt (1.5.1).

**Proposition 4.4.1.** *Let $K$ be a differential field of characteristic zero, $R$ a noetherian differential $K$-algebra finitely differentially generated. Let $I$ be a maximal real differential ideal of $R$. Then $I$ is prime.*

*Proof.* $I$ is radical, because it is real (see lemma 2.1.1). Then, by theorem 1.5.1, $I$ is an intersection of a finite number of prime differential ideals, i.e.

$$I = P_1 \cap \ldots \cap P_s. \tag{4.7}$$

Moreover, we can assume that $P_i \nsubseteq P_j$ for all $i \neq j$. Indeed, if some $P_i \subset P_j$ for $i \neq j$, we can omit $P_j$ and reduce the decomposition. Therefore (4.7) is a primary decomposition of the ideal $I$ with

$$rad(P_i) = P_i \neq rad(P_j) = P_j \quad \forall\, i \neq j.$$

Hence, by unicity in theorem 1.5.1, it is a reduced primary decomposition (see [1], chapter 4). So the $P_i's$ are exactly the minimal prime ideals containing $I$.
Now, minimal prime ideals containing the real ideal $I$ are as well real (see lemma 2.1.1). But $I$ is a maximal real differential ideal, so $s = 1$ and $I = P_1$. Therefore $I$ is prime.

□

Let us denote by $E$ the set of all proper maximal real differential ideals of $R$. By lemma above, elements of $E$ are prime ideals. We divide $R$ by an ideal chosen from $E$ and obtain a real integral domain. Then we pass to the field of fractions, which is a real field. Our goal is to obtain a field extension not adding constants. For this reason not all ideals from $E$ may be appropriate for our purposes.

**Conjecture 4.4.1.** *In the set of all proper maximal differential ideals of the real full universal solution algebra constructed above there always exists a real ideal.*

We will show that in the situation considered this conjecture holds true. It gives us the possibility to choose from $E$ such a maximal real differential ideal $J$ which is not contained in any maximal differential ideal. The idea behind this is the following. If we divide $R$ by $J$ we obtain a real integral domain $R/J$ which does not contain any proper real differential ideal and what is more it also does not contain any proper differential ideal.

We obtain the following results:

**Lemma 4.4.1.** *Let $K$ be a real differential field with real closed field of constants $C_K$. Let $A$ be a finitely generated $K$-algebra without zero divisors and let $S = Fr(R)$. If $c \in C_S \setminus C_K$, then $c$ is transcendent over $K$.*

For the proof see [36], lemma 3.1.

**Lemma 4.4.2.** *Let $K$ be a real differential field with real closed field of constants $C_K$. Let $A$ be a finitely generated $K$-algebra without zero divisors and let $a$ be an element of $A$. Then either $a$ is algebraic over $K$ or there is a constant $c \in C_K$ such that $a - c$ is not invertible in $A$.*

For the proof see [36], lemma 3.4.

So if our conjecture holds true, then we obtain that $L^* := Fr(R/J)$ is an extension of $K$ which brings no new constants. Indeed, any element $a \in C_{L^*} \setminus C_K$ is by lemma 4.4.1 transcendent over $K$. Hence by lemma 4.4.2 there exists a constant $c \in C_K$ such that $a - c$ is not invertible in $R/J$. Then the ideal $[a - c]$ is a proper differential ideal in $R/J$. And we have a contradiction. So $L^*$ is a Picard-Vessiot extension, which is also a real field, since $J$ is real (see lemma 2.1.2).

We have already constructed a real field which is the Picard-Vessiot extension for equation (4.4) defined over $K$, i.e. $L = K\langle \gamma_1, \ldots, \gamma_k \rangle \subset M[[X]]$, where $\gamma_1, \ldots, \gamma_k$ is a fundamental set of solutions of this equation. We will prove that the ideal $J$ considered above can always be found.

We define an epimorphism of $K$-algebras

$$\begin{cases} \psi : K[U_{ij}] \to L = K[\gamma_i^{(j)}] \\ \psi(U_{ij}) = \gamma_j^{(j)} \end{cases},$$

which is a differential morphism. We observe that $\psi(V) = det(\gamma_i^{(j)}) \neq 0$, so it is invertible in $L$. By the universal property of the ring of fractions we can extend $\psi$ to a $K$-algebra homomorphism

$$\begin{cases} \widetilde{\psi} : K[U_{ij}]_{\mathcal{V}} \to L \\ \widetilde{\psi}(U_{ij}) = \gamma_j^{(j)} \end{cases}.$$

We define $J := ker(\widetilde{\psi})$. Then we obtain an embedding

$$\lambda : R/J \to L.$$

$L$ is a field, so $R/J$ is an integral domain and $J$ is prime. Hence there exists a fraction field homomorphism $\widetilde{\lambda} : L^* = Fr(R/J) \to L$. Since $L = K\langle \gamma_1, \ldots, \gamma_k \rangle$, then $\widetilde{\lambda}$ is a field isomorphism. By lemma 2.1.2, we obtain that $J$ is real, because $L$ is real.

## 4.5 Comments on the Fundamental Theorem.

Picard-Vessiot theory for differential fields with no algebraically closed field of constants was described by Marvin P. Epstein (see [10] and [11]). His result states that there exists a fundamental system of solutions $(y_1, \ldots, y_n)$ for a homogeneous linear differential equation $\mathcal{L}(Y) = 0$ of order $n$ defined over a differential field $K$ with field of constants $C_K$ (not necessarily algebraically closed), such that the field of constants of $L := K\langle y_1, \ldots, y_n \rangle$ is a normal algebraic extension of $C_K$. He defines such an $L$ to be a Picard-Vessiot extension of $K$ for the equation $\mathcal{L}(Y) = 0$. He also proves a Galois correspondence theorem for such generalized Picard-Vessiot extensions. If we do not allow new constants, the normality of the Picard-Vessiot extension can fail, as it can be easily seen by considering the algebraic case (see example 3 in the first section of this chapter). Hence obtaining Galois correspondence in this context is not possible.

# Bibliography

[1] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, University of Oxford, Addison-Wesley Publishing Company, 1969.

[2] J. Bochnak, M. Coste, M.-F. Roy, *Real Algebraic Geometry*, Springer Verlag, 1998.

[3] A. Borel, *Algebraic Groups and Galois Theory in the Works of Ellis Kolchin* in *Selected works of Ellis Kolchin with commentary*, H. Bass, A. Buium and P.J. Cassidy, eds. American Mathematical Society, Providence, RI, pp. 505-525, 1999.

[4] J. Browkin, *Teoria ciał*, Biblioteka Matematyczna, Tom 49, Państwowe Wydawnictwo Naukowe, Warszawa, 1978.

[5] A. Buium, P. J. Cassidy, *Differential algebraic geometry and differential algebraic groups: From algebraic differential equations to Diophantine geometry* in *Selected works of Ellis Kolchin with commentary*, H. Bass, A. Buium and P.J. Cassidy, eds. American Mathematical Society, Providence, RI, pgs. 567-636, 1999.

[6] P. J. Cassidy, M. F. Singer, *Galois Theory of parametrized differential equations and linear differential algebraic groups*, Differential Equations and Quantum Groups, IRMA Lectures in Mathematics and Theoretical Physics, EMS Publishing House, Vol. 9, pp. 113- 157, 2006.

[7] T. Crespo, Z. Hajto, *Algebraic Groups and Differential Galois Theory*, Graduate Studies in Mathematics 122, American Mathematical Society, 2011.

[8] T. Crespo, Z. Hajto, *Introduction to differential Galois theory*, Cracow University of Technology Publishers, 2007.

[9] T. Dyckerhoff, *Picard-Vessiot extensions over number fields*, Dissertation, Heidelberg, 2005.

[10] M. P. Epstein, *An Existence Theorem in the Algebraic Study of Homogeneous Linear Ordinary Differential Equations*, Proceedings of the American Mathematical Society, Vol. 6, No. 1, pp. 33-41, 1955.

[11] M. P. Epstein, *On the Theory of Picard-Vessiot Extensions*, The Annals of Mathematics, Second Series, Vol. 62, No. 3, pp. 528-547, 1955.

[12] T. Grill, M. Knebusch, M. Tressl, *An Existence Theorem for Systems of Implicit Differential Equations*, Proceedings of the Differential Galois Theory workshop, T. Crespo, Z.Hajto, eds., Banach Center Publications, Vol. 58, Warszawa, 2002, pp. 75-77.

[13] T. Grill, *Contributions to differential, real algebra and its connection to differential equations*, Dissertation, Regensburg, 1997.

[14] J. Hirschfeld, W. H. Wheeler, *Model-completions and model-companions*, Forcing, Arithmetic, Division Rings, Lecture Notes in Mathematics, 454, Berlin / Heidelberg: Springer, pp. 44-54, 1975.

[15] I. Kaplansky, *An introduction to differential algebra*, Hermann, 1957.

[16] F. Klein, *Vorlesungen über hypergeometrische Funktion*, Springer, Berlin, 1933 (reprint 1981).

[17] M. Knebusch, C. Scheiderer, *Einführung in die reele Algebra*, Vieweg Verlag, 1989.

[18] E. Kolchin, *Differential algebra and algebraic groups*, Academic Press, New York, 1973.

[19] E. Kolchin, *Existence theorems connected with Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Bulletin of the American Mathematical Society, Vol. 54, No. 10, pp. 927-932, 1948.

[20] E. Kolchin, *Extensions of Differential Fields, I*, The Annals of Mathematics, Vol. 43, No. 4, 1942, pp.724-729.

[21] S. Lang, *Algebra*, 3rd revised ed., Springer-Verlag, New York, 2002.

[22] A.R. Magid, *Lectures on differential Galois theory*, American Mathematical Society, 1997.

[23] B. Malgrange, *Pseudogroupes de Lie et théorie de Galois différentielle*, Preprint, Institut des Hautes Études Scientifiques (www.ihes.fr), March 2010.

[24] D. Marker, M. Messmer, A. Pillay, *Model Theory of Fields*, Lecture Notes in Logic, 5, Springer, 1996.

[25] M. Marshall, *Positive polynomials and sums of squares*, Mathematical Surveys and Monographs 146, American Mathematical Society 2008.

[26] J. J. Morales-Ruiz, *Differential Galois theory and non-integrability of Hamiltonian systems*, Progress in Mathematics 179, Birkhäuser Verlag, 1999.

[27] B. Poizat, *A Course in Model Theory. An Introduction to Contemporary Mathematical Logic*, Springer-Verlag, New York, 2000.

[28] M. van der Put, M. F. Singer, *Galois theory of linear differential equations*, Grundlehren der Mathematischen Wissenschaften 328, Springer-Verlag, 2003.

[29] J. F. Ritt, *Differential Algebra*, American Mathematical Society, Colloquium Publications, Volume 33, 1950.

[30] A. Seidenberg, *A New Decision Method for Elementary Algebra*, The Annals of Mathematics, Second Series, Vol. 60, pp. 365-374, 1954.

[31] A. Seidenberg, *Abstract Differential Algebra and the Analytic Case*, The Proceedings of the American Mathematical Society, Vol. 9, pp.159-164, 1958.

[32] A. Seidenberg, *Contribution to the Picard-Vessiot theory of homogeneous linear differential equations*, American Journal of Mathematics, Vol. 78, No.4, pp. 808-817, 1956.

[33] A. Seidenberg, *Some basic theorems in differential algebra (characteristic p, arbitrary)*, Transactions of the American Mathematical Society, Vol. 73, pp. 174-190, 1952.

[34] J.-P. Serre, *Lie Algebras and Lie Groups*, Lecture Notes in Mathematics, Vol. 1500, 2nd edition, Springer Verlag, 1992.

[35] M. F. Singer, *The Model Theory of Ordered Differential Fields*, The Journal of Symbolic Logic, Vol. 43, No. 1, pp. 82-91, 1978.

[36] E. Sowa, *Picard-Vessiot extensions for real fields*, Proceedings of American Mathematical Society, Vol. 139, No.7, pp. 2407-2413, 2011.

[37] H. Umemura, *Galois Theory of Algebraic and Differential Equations*, Nagoya Math. J., Vol. 144, pp. 1-58, 1996.

[38] O. Zariski, P. Samuel, *Commutative Algebra, Volume I and II*, D. Van Nostrand Company, Inc, New York, 1960.

Address:
Wydział Matematyki i Informatyki, Uniwersytet Jagielloński
ul. Łojasiewicza 6, 30-348 Kraków, POLAND
elzbieta.sowa@im.uj.edu.pl