Differential Algebra

Gleb Pogudin

December 19, 2020

Contents

About

There are following special types of exercises:

- marked with *: is challenging but Gleb thinks he knows a solution;
- marked with **: Gleb does not know a solution;
- marked with §: an open-ended or even philosophical question.

All typos, errors, and comments to be sent to `gleb.pogudin@polytechnique.edu`

Notations and conventions

Unless stated otherwise, all the fields are assumed to be of characteristic zero. The ideal generated by elements $f_1, \ldots, f_\ell$ of a commutative ring R will be denoted $\langle f_1, \ldots, f_\ell \rangle$.

0 Before we start: arithmetic of differential polynomials

0.1 Differential rings, field, polynomials

Definition 0.1 (Some general definitions)**.**

- Let R be a commutative ring. An additive map $\delta\colon R \to R$ is called *a derivation* if it satisfies the Leibniz rule:
$$\delta(ab) = \delta(a)b + a\delta(b) \quad \text{for every } a, b \in R.$$
We will typically denote $\delta(a)$ by a' and, for $n \geqslant 0$, $\delta^n(a)$ by $a^{(n)}$.

- A commutative ring equipped with a derivation is called *a differential ring.* If the ring is a field, it is called *a differential field.*

- For a differential ring, a subring closed under the derivation is called *a differential subring.* The same for subfields.

- A differential ring which is an algebra over its differential subfield, is called *a differential algebra.*

Example 0.2.

- Any ring can be considered as a differential ring with respect to the zero derivation.

- Consider the ring $\mathbb{C}[x]$ and the field $\mathbb{C}(x)$. They are a differential ring and a differential field with respect to $\frac{\mathrm{d}}{\mathrm{dx}}$, respectively. Moreover, they are differential algebras over the constant field $\mathbb{C}$.

- Let $D \subset \mathbb{C}$ be a domain in the complex plane. By $\mathrm{Hol}(D)$ and $\mathrm{Mer}(D)$ we denote the set of all holomorphic and meromorphic functions in D, respectively. They are a differential ring and a differential field with respect to $\frac{\mathrm{d}}{\mathrm{dz}}$, respectively.

Remark on PDEs 0.3. The above definitions can be generalized to the PDE case by considering rings (fields, algebras) with respect to several commuting derivations yielding to the notion of *partial differential ring* (or Δ*-ring* if Δ is a fixed set of symbols for derivations).

For example, if $\Delta = \{\delta_1, \delta_2\}$, then $\mathbb{C}[x, y]$ can be equipped with the structure of Δ-ring by defining the actions of δ_1 and δ_2 to be $\frac{\partial}{\partial x}$ and $\frac{\partial}{\partial y}$, respectively.

Notation 0.4. Let x be an element of a differential ring and h be a nonnegative integer. Then we introduce
$$x^{(<h)} := (x, x', \ldots, x^{(h-1)}),$$
$$x^{(\infty)} := (x, x', x'', \ldots).$$
$x^{(\leqslant h)}$ is defined analogously. If $\mathbf{x} = (x_1, \ldots, x_n)$ is a tuple of elements of a differential ring and $\mathbf{h} = (h_1, \ldots, h_n) \in (\mathbb{Z}_{\geqslant 0} \cup \{\infty\})^n$, then
$$\mathbf{x}^{(<h)} := (x_1^{(<h)}, \ldots, x_n^{(<h)}),$$
$$\mathbf{x}^{(<\mathbf{h})} := (x_1^{(<h_1)}, \ldots, x_n^{(<h_n)}),$$
$$\mathbf{x}^{(\infty)} := (x_1^{(\infty)}, \ldots, x_n^{\infty}).$$

Definition 0.5 (Differential polynomials)**.** Let R be a differential ring. Consider a ring of polynomials in infinitely many variables
$$R[x^{(\infty)}] := R[x, x', x'', x^{(3)}, \ldots]$$
and extend the derivation from R to this ring by $(x^{(j)})' := x^{(j+1)}$. The resulting differential ring is called *the ring of differential polynomials in x over R.*

The ring of differential polynomials in several variables is defined by iterating this construction.

Example 0.6. Weierstrass's elliptic function $\wp(z)$ satisfies the following differential equations: $(\wp'(z))^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$. This equation can be written as the following differential polynomial over a constant field $\mathbb{Q}(g_2, g_3)$:
$$(x')^2 - 4x^3 - g_2 x - g_3.$$

Example 0.7. The Wronskian of differential variables $\mathbf{x} = (x_1, x_2, \ldots, x_n)$
$$\mathrm{Wronsk}(x_1, \ldots, x_n) = \begin{vmatrix} x_1 & x_2 & \ldots & x_n \\ x_1' & x_2' & \ldots & x_n' \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{(n-1)} & x_2^{(n-1)} & \ldots & x_n^{(n-1)} \end{vmatrix} \tag{1}$$
is a differential polynomial from $\mathbb{Q}[\mathbf{x}^{(\infty)}]$.

Remark on PDEs 0.8. For a fixed set $\Delta = \{\delta_1, \ldots, \delta_m\}$ of symbols for derivations, one can define Δ-polynomials over a Δ-ring R in the same way by adding an infinite set of variables indexed by $\mathbb{Z}^m_{\geqslant 0}$ so that δ_i acts by incrementing the i-th coordinate. The ring will be denoted by $R[x^{(\infty)}]_\Delta$.

For example, for $\Delta = \{\delta_1, \delta_2\}$, the Jacobian $J = \begin{vmatrix} \delta_1 x & \delta_2 x \\ \delta_1 y & \delta_2 y \end{vmatrix}$ belongs to $\mathbb{Q}[x^{(\infty)}, y^{(\infty)}]_\Delta$.

Definition 0.9. Every differential polynomial $P \in k[x_1^{(\infty)}, \ldots, x_n^{(\infty)}]$ has the following properties:

- For every $1 \leqslant i \leqslant n$, we will call the largest j such that $x_i^{(j)}$ appears in P *the order of P with respect to x_i* and denote it by $\operatorname{ord}_{x_i} P$; if P does not involve x_i, we set $\operatorname{ord}_{x_i} P := -1$.
- *The order of P* is $\operatorname{ord} P := \max\limits_{1 \leqslant i \leqslant n} \operatorname{ord}_{x_i} P$.
- For every $1 \leqslant i \leqslant n$ such that x_i appears in P, *the initial of P with respect to x_i* is the leading coefficient of P considered as a univariate polynomial in $x_i^{(\operatorname{ord}_{x_i} P)}$. We denote it by $\operatorname{init}_{x_i} P$.
- For every $1 \leqslant i \leqslant n$ such that x_i appears in P, *the separant of P with respect to x_i* is

$$\operatorname{sep}_{x_i} P := \frac{\partial P}{\partial x_i^{(\operatorname{ord}_{x_i} P)}}.$$

- A differential polynomial is called *isobaric* if the sum of orders of derivatives in each monomial is the same. The isobaricity is equivalent to homogeneity with respect to the grading induced by the weight function ω defined by $\omega(x_i^{(j)}) = j$ for every $1 \leqslant i \leqslant n, j \geqslant 0$.

Example 0.10. Consider the differential polynomial $P = (x')^2 - 4x^3 - g_2 x - g_3 \in \mathbb{Q}(g_2, g_3)[x^{(\infty)}]$ from Example 0.6. Then

$$\operatorname{ord}_x P = 1, \quad \operatorname{init}_x P = 1, \quad \operatorname{sep}_x P = 2x'.$$

Example 0.11. One can see that (see Example 0.7 for notation):

$$\operatorname{sep}_{x_i} \operatorname{Wronsk}(x_1, \ldots, x_n) = \operatorname{init}_{x_i} \operatorname{Wronsk}(x_1, \ldots, x_n) = (-1)^{i+1} \operatorname{Wronsk}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n).$$

The importance of the notion of the separant is based on the following crucial observation.

Very important observation. *Let $P \in k[\mathbf{x}^{(\infty)}]$ with $\mathbf{x} = (x_1, \ldots, x_n)$, and consider $1 \leqslant i \leqslant n$ such that $h := \operatorname{ord}_{x_i} P \geqslant 0$. Then, for every $j > 0$, there exists $Q \in k[\mathbf{x}^{(<h+j)}]$ such that*

$$P^{(j)} = (\operatorname{sep}_{x_i} P) x_i^{(h+j)} + Q.$$

Remark on PDEs 0.12. The notions of initial and separant (from Definition 0.9) can be generalized to the PDE case. Since, for several derivatives, there is no canonical way to choose "the highest of the derivatves of x appearing in the polynomial", one should fix a monomial ordering on the derivatives of a single variable (considered as monomials in the elements of Δ).

0.2 Differential reduction

The differential reduction algorithm may be viewed as a generalization of the division with remainder for univariate polynomials.

Algorithm 1 Differential reduction

Input differential polynomials $f, g \in k[x^{(\infty)}]$ such that $f \notin k$;

Output a differential polynomial $\widetilde{g} \in k[x^{(\infty)}]$ such that

- $\operatorname{ord}_x \widetilde{g} < \operatorname{ord}_x f$ or $\operatorname{ord}_x \widetilde{g} = \operatorname{ord}_x f = h$ and $\deg_{x^{(h)}} \widetilde{g} < \deg_{x^{(h)}} f$;
- there exist $a, b \in \mathbb{Z}_{\geqslant 0}$ such that

$$(\operatorname{sep}_x f)^a (\operatorname{init}_x f)^b g - \widetilde{g} \in \langle f, f', f'', \ldots \rangle.$$

(Step 1) Set $h := \operatorname{ord}_x f$ and $d := \deg_{x^{(h)}} f$;

(Step 2) While $\operatorname{ord}_x g > h$ do

(a) Set $H := \operatorname{ord}_x g$, $D := \deg_{x^{(H)}} g$;

(b) $g := (\operatorname{sep}_x f) g - (\operatorname{init}_x g)(x^{(H)})^{D-1} f^{(H-h)}$;

(Step 3) While $\deg_{x^{(h)}} g \geqslant d$ do

(a) Set $D := \deg_{x^{(h)}} g$;

(b) $g := (\operatorname{init}_x f) g - (\operatorname{init}_x g)(x^{(h)})^{D-d} f$;

(Step 4) Return g.

Lemma 0.13. *Algorithm 1 always terminates and returns a correct result.*

Proof. Left as an exercise. □

Example 0.14. We will show that the result of the reduction of $g = x'' - 1/2$ with respect to $f = (x')^2 - x$ is zero. Since $\operatorname{ord}_x g > \operatorname{ord}_x f$, we compute:

$$(\operatorname{sep}_x f) g - (\operatorname{init}_x g) f' = (2x')(x'' - 1/2) - 1 \cdot (2xx' - x') = 0.$$

One can interpret this as follows. The solutions of $f = 0$ are $x = (0.5t + c)^2$ (c — arbitrary constant) and $x = 0$, and the former is also a solution of $g = 0$ while the latter is a solution of $\operatorname{sep}_x f = 0$. Therefore, g is reducible to zero because it vanished at all "nonspecial" solutions of f.

0.3 Exercises

Exercise 0.1. Consider the polynomial P from Example 0.6 with $g_2 = 0, g_3 = 1$, that is, $P = (x')^2 - 4x^3 - 1$. Show that $x'' - 6x^2$ reduces to zero with respect to P.

Exercise 0.2. Verify that the following differential polynomials are reduced to zero with respect to $(x')^2 - x^2$

1. $x'' - x$;
2. $\operatorname{Wronsk}(x, x')$.

Try to explain why.

Exercise 0.3. Could it happen that a derivative of an irreducible nonconstant differential polynomial is

1. reducible?
2. non-squarefree?

Exercise 0.4.

1. Show that there is no $q \in \mathbb{C}[x^{(\infty)}]$ such that $q' = \operatorname{Wronsk}(x, x') = \begin{vmatrix} x & x' \\ x' & x'' \end{vmatrix}$ (see (1)).
2. Propose an algorithm that takes $p \in \mathbb{C}[x^{(\infty)}]$ as input and determines whether it has an integral (that is, there exists $q \in \mathbb{C}[x^{(\infty)}]$ such that $q' = p$).

Exercise ** **0.5.** Note that, although $\mathrm{Wronsk}(x, x') \in \mathbb{Q}[x^{(\infty)}]$ does not have an integral, the differential rational function $\frac{\mathrm{Wronsk}(x,x')}{(x')^2}$ does. Propose an algorithm that takes $p \in \mathbb{C}[x^{(\infty)}]$ and checks whether there exists a differential rational function r *of lower order* such that pr has an integral.

Exercise § **0.6.** Would it be possible to reformulate the algorithm from Exercise 0.4 in the language of homology, that is to define a "natural" map from $\mathbb{C}[x^{(\infty)}]$ so that its kernel is exactly the set of all the derivatives?

Exercise 0.7. Prove that the following identity holds in $\mathbb{Q}[x_1^{(\infty)}, \ldots, x_n^{(\infty)}, y^{(\infty)}]$:

$$\mathrm{Wronsk}(x_1 y, x_2 y, \ldots, x_n y) = y^n \,\mathrm{Wronsk}(x_1, \ldots, x_n).$$

Exercise 0.8. Let $f(z)$ be a meromorphic function such that $P(f(z)) = 0$ for some $P(x) \in \mathbb{C}[x^{(\infty)}]$. Show that $\frac{1}{f(z)}$ also satisfies a polynomial differential equation of order at most $\operatorname{ord}_x P$. What can be said about the degree of this equation (in terms of P)?

1 Differential ideals

We will use the following fact from commutative algebra of polynomial rings in infinitely many variables.

Theorem 1.1 (Follows from the main theorem of [6])**.** *Let Λ be a countable set, F be a field, E be an algebraically closed field of uncountable transcendence degree over F, and I be an ideal in $F[x_\lambda \mid \lambda \in \Lambda]$. Then, for every $f \in F[x_\lambda \mid \lambda \in \Lambda]$, the following are equivalent:*

- *there exists N such that $f^N \in I$;*
- *for every homomorphism $\phi \colon F[x_\lambda \mid \lambda \in \Lambda] \to E$ such that $I \subset \ker \phi$, $\phi(f) = 0$.*

1.1 Differential ideals, their radicals and prime components

Definition 1.2 (Differential ideal)**.** Let $S := R\{x_1, \ldots, x_n\}$ be a ring of differential polynomials over a differential ring R. An ideal $I \subset S$ is called *a differential ideal* if $a' \in I$ for every $a \in I$.

One can verify that, for every $f_1, \ldots, f_s \in S$, the ideal

$$\langle f_1^{(\infty)}, \ldots, f_s^{(\infty)} \rangle$$

is a differential ideal. Moreover, this is the minimal differential ideal containing $f_1, \ldots, f_s$, and we will denote it by $\langle f_1, \ldots, f_s \rangle^{(\infty)}$.

Example 1.3. Consider a constant field $\mathbb{Q}(\omega)$, where ω is a transcendental constant. In $\mathbb{Q}(\omega)[x^{(\infty)}, y^{(\infty)}]$, consider the ideal $[x' - \omega y, y' + \omega x]$. This ideal contains, for example, $x'' + \omega^2 x$, the harmonic oscillator equation, becuase:

$$x'' + \omega^2 x = (x' - \omega y)' + \omega(y' + \omega x) \in \langle x' - \omega y, y' + \omega x \rangle^{(\infty)}.$$

It turns out that two fundamental operations in commutative algebra, taking the radical of an ideal and prime decomposition of a radical ideal, respect the differential structure.

Proposition 1.4 (Taking radical is differential-friendly)**.** *Let $I \subset R$ be a differential ideal in a differential ring R such that $\mathbb{Q} \subset R$. Then the radical*

$$\sqrt{I} := \{f \in R \text{ such that } \exists N \colon f^N \in I\}$$

is also a differential ideal.

Proof. We will prove the proposition by first proving that,

$$\text{for every } m \geqslant 1 \colon x' \in \sqrt{\langle x^m \rangle^{(\infty)}} \subset \mathbb{Q}[x^{(\infty)}]. \tag{2}$$

Proving (2) would imply, for every $m \geqslant 0$, that there exists $M(m)$ such that $(x')^{M(m)}$ can be written as a $\mathbb{Q}[x^{(\infty)}]$-linear combination of the derivatives of x^m. Then, if $a \in \sqrt{I}$ with $a^n \in I$, plugging $x = a$ into such representation would yield that $(a')^{M(n)} \in I$.

In order to prove (2), consider any homomorphism (not necessarily differential) $\phi\colon \mathbb{Q}[x^{(\infty)}] \to \mathbb{C}$ such that $\langle x^m \rangle^{(\infty)} \subset \ker \phi$. Then $\phi(x) = 0$. Observe that, due to the pigeonhole principle, $(x^m)^{(m)}$ can be written as:

$$(x^m)^{(m)} = m!(x')^m + x \cdot Q,$$

for some $Q \in \mathbb{Q}[x^{(\infty)}]$. Applying ϕ to the both sides and using $\langle x^m \rangle^{(\infty)} \subset \ker \phi$, we obtain

$$0 = \phi((x^m)^{(m)}) = m!\phi((x')^m) + \phi(x)\phi(Q) = m!\phi(x')^m.$$

Therefore, $\phi(x') = 0$, so $x' \in \sqrt{\langle x^n \rangle^{(\infty)}}$ due to Theorem 1.1. □

Remark 1.5. A refined version of this proof will be discussed in the next section (Lemma 2.5). A more "syntactic" proof can be found in [5, Lemma 1.7] which yields that $M(m) \leqslant 2^m$ in the notation of the proof above. Sharp bounds these exponents were obtained in [9] (see also [1]). See also Exercises 1.2 and 1.3.

Proposition 1.6 (Prime decompositions are differential-friendly)**.** *Let $R \supset \mathbb{Q}$ be a differential ring. Then every radical differential ideal in R is an intersection of prime differential ideals.*

The proof of the proposition will rely on the following "arithmetic" property of radical differential ideals.

Lemma 1.7. *Let $R \supset \mathbb{Q}$ be a differential ring. Let $A, B \subset R$. Then*

$$\sqrt{\langle A \cdot B \rangle^{(\infty)}} = \sqrt{\langle A \rangle^{(\infty)} \cdot \langle B \rangle^{(\infty)}}.$$

Proof. Since $\langle A \cdot B \rangle^{(\infty)} \subseteq \langle A \rangle^{(\infty)} \cdot \langle B \rangle^{(\infty)}$, we have $\sqrt{\langle A \cdot B \rangle^{(\infty)}} \subseteq \sqrt{\langle A \rangle \cdot \langle B \rangle^{(\infty)}}$.

In the other direction, observe that the differential ideal $\langle A \rangle^{(\infty)} \cdot \langle B \rangle^{(\infty)}$ is generated as an ideal by the products of the form $a^{(i)} b^{(j)}$, where $a \in A, b \in B, i, j \geqslant 0$. Exercise 1.7 implies that $a^{(i)} b^{(j)} \in \sqrt{\langle ab \rangle^{(\infty)}} \subseteq \sqrt{\langle A \cdot B \rangle^{(\infty)}}$. □

Corollary 1.8. *Let S be a multiplicatively closed subset of a differential ring $R \supset \mathbb{Q}$ such that $0 \notin S$. Consider a maximal differential ideal I not containing S. Then I is prime.*

Proof. Assume that I is not prime, so there are $a_1, a_2 \in R$ such that $a_1 a_2 \in I$ and $a_1, a_2 \notin I$. The maximality of I implies that there exist $s_1, s_2 \in S$ such that $s_i \in \sqrt{\langle I, a_i \rangle^{(\infty)}}$ for $i = 1, 2$. Then Lemma 1.7 implies that

$$s_1 s_2 \in \sqrt{\langle I, a_1 \rangle^{(\infty)}} \sqrt{\langle I, a_2 \rangle^{(\infty)}} \subseteq \sqrt{\langle I, a_1 \rangle^{(\infty)} \cdot \langle I, a_2 \rangle^{(\infty)}} = \sqrt{I},$$

so we have arrived at a contradiction. □

Proof of Proposition 1.6. Let $I \subset R$ be a radical differential ideal. Consider $a \notin I$. Then $S := \{a^i \mid i \geqslant 1\}$ is a multiplicatively closed set disjoint with I. Consider a maximal differential ideal containing I and not intersecting S. Corollary 1.8 implies that this ideal is prime. Therefore, the intersection of all prime differential ideals containing I does not contain a. Thus, this intersection is equal to I. □

Remark 1.9. We will show later (Corollary 1.18) that a radical ideal in $k[\mathbf{x}^{(\infty)}]$ (with $\mathbf{x} = (x_1, \ldots, x_n)$) is an intersection of finitely many prime differential ideals yielding that the prime components of a radical differential ideal are differential ideals.

Remark on PDEs 1.10. All the proofs in this subsection can be used verbatim for the case of several commuting derivations.

Definition 1.11 (Differential spectrum)**.** We will call the set of all prime differential ideals of a differential ring R *the differential spectrum* of R and denote by $\operatorname{diffspec} R$ (we will introduce the corresponding topology later). We will denote the set of all prime differential ideals in R containing a set S by $\mathbb{V}(S) \subset \operatorname{diffspec} R$. Then Proposition 1.6 implies that, for radical ideals $I, J \subset R$, we have $I = J \iff \mathbb{V}(I) = \mathbb{V}(J)$. Using the language of algebraic geometry, we will say that an element $f \in R$ vanishes at $P \in \operatorname{diffspec} R$ if $f \in P$.

Lemma 1.12. *Let R be a differential ring. Prove that*

1. *for every subsets and $S, T \subset R$, $\mathbb{V}(S \cdot T) = \mathbb{V}(S) \cup \mathbb{V}(T)$;*
2. *a radical ideal $I \subset R$ is prime if and only if, for every subsets $S, T \subset R$, $\mathbb{V}(I) = \mathbb{V}(S) \cup \mathbb{V}(T)$ implies that $\mathbb{V}(I) = \mathbb{V}(S)$ or $\mathbb{V}(I) = \mathbb{V}(T)$.*

Proof. Left as Exercise 1.8 □

1.2 Bad news: no Noetherianity in general

Proposition 1.13. *The following chain of ideals in $\mathbb{Q}[x^{(\infty)}]$ is an infinite strictly ascending chain:*

$$\langle x^2\rangle^{(\infty)} \subsetneq \langle x^2, (x')^2\rangle^{(\infty)} \subsetneq \langle x^2, (x')^2, (x'')^2\rangle^{(\infty)} \subsetneq \ldots$$

Proof. For $i \geqslant 0$, we denote $I_i := \langle x^2, (x')^2, \ldots, (x^{(i)})^2\rangle^{(\infty)}$. We will show that $p := (x^{(i+1)})^2 \notin I_i$. Assume the contrary. Since I_i is generated by homogeneous polynomials of degree two, $(x^{(i+1)})^2$ must be a $\mathbb{Q}$-linear combination of the derivatives of the generators. Moreover, since the generators of I_i are also isobaric, $(x^{(i+1)})^2$ must be a $\mathbb{Q}$-linear combination of

$$p_0 := (x^2)^{(2i+2)},\ p_1 := ((x')^2)^{(2i)},\ \ldots,\ p_i := ((x^{(i)})^2)''.$$

Since p_0 involves $xx^{(2i+2)}$ which does not appear in either of $p_1, \ldots, p_i, p$, p_0 will not appear in the linear combination. Analogously, p_1 involves $x'x^{(2i+1)}$ which does not appear in either of $p_2, \ldots, p_i, p$, so p_1 will not appear in the linear combination as well. Continuing in the same way, we show that none of $p_0, \ldots, p_i$ will appear in the linear combination arriving at a contradiction. □

1.3 Prime univariate ideals

In this section we will show that prime univariate ideals over differential rings admit a concise representation. This fact is an important tool in differential algebra (with the role similar to the fact that univariate polynomials over a field form a PID), and we will use it in the proof of the Ritt-Raudenbush theorem.

Notation 1.14. Let I be an ideal in ring R, and $a \in R$. Then:

$$I \colon a^\infty := \{b \in R \mid \exists N \colon a^N b \in I\}.$$

Proposition 1.15 (Univariate prime ideals)**.** *Let $R \supset \mathbb{Q}$ be a differential ring, and $P \subset R[x^{(\infty)}]$ be a prime differential ideal such that $P \neq \sqrt{\langle P \cap R\rangle^{(\infty)}}$. Let f be an element of the lowest degree among the elements of the lowest order in $P \setminus \sqrt{\langle P \cap R\rangle^{(\infty)}}$. Then $\operatorname{sep}_x(f)\operatorname{init}_x(f) \notin P$ and*

$$P = \langle P \cap R, f\rangle^{(\infty)} \colon (\operatorname{sep}_x(f)\operatorname{init}_x(f))^\infty.$$

Proof. Let $P_0 := \sqrt{\langle P \cap R\rangle^{(\infty)}}$, $s := \operatorname{sep}_x f$, $\ell := \operatorname{init}_x f$, $h := \operatorname{ord}_x f$, and $d := \deg_{x^{(h)}} f$. We will show that $s, \ell \notin P$.

- If $\ell \in P$ then, due to the minimality of f, we have $\ell \in P_0$. Then $f - \ell(x^{(h)})^d \in P$ is of lower degree than f, so it belongs to P_0. Hence, $f = (f - \ell(x^{(h)})^d) + \ell(x^{(h)})^d$ belongs to P_0 as well.
- If $s \in P$ then, due to the minimality of f, we have $s \in P_0$. Then $f - \frac{1}{d}sx^{(h)}$ is of lower degree than f, so it belongs to P_0. Hence, $f = (f - \frac{1}{d}sx^{(h)}) + \frac{1}{d}sx^{(h)} \in P_0$.

The primality of P implies that $s\ell \notin P$. Let $P_1 := \langle P_0, f\rangle^{(\infty)} \colon (s\ell)^\infty$.

First we show that $P_1 \subseteq P$. Let $g \in P_1$. Then there exists N such that $s^N \ell^N g \in \langle f, P_0\rangle^{(\infty)} \subset P$. The primality of P implies that $g \in P$.

Now we show that $P \subseteq P_1$. Let $g \in P$. We perform the differential reduction (Algorithm 1) of g with respect to f. It will yield $a, b \in \mathbb{Z}_{\geqslant 0}$ and $\widetilde{g}$ such that

$$s^a \ell^b g - \widetilde{g} \in \langle f\rangle^{(\infty)}.$$

Since $g, f \in P$, $\widetilde{g}$ belongs to P. The minimality of f implies that $\widetilde{g} \in P_0$. Therefore, $g \in P_1$. □

1.4 Good news: Noetherianity for radical differential ideals (the Ritt-Raudenbush theorem and its corollaries)

Theorem 1.16 (Ritt-Raudenbush)**.** *Let k be a differential field, and let $I \subset k[\mathbf{x}^{(\infty)}]$, where $\mathbf{x} = (x_1, \ldots, x_n)$, be a radical differential ideal. Then there exist $f_1, \ldots, f_s \in k[\mathbf{x}^{(\infty)}]$ such that*

$$I = \sqrt{\langle f_1, \ldots, f_s\rangle^{(\infty)}}.$$

Corollary 1.17 (ACC for radical differential ideals)**.** *Let k be a differential field. Let*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

be an ascending chain of radical differential ideals in $k[\mathbf{x}^{(\infty)}]$. Then there exists N such that $I_N = I_{N+1} = I_{N+2} = \dots$.

Proof of Corollary 1.17. Let $I := \bigcup_{i=0}^{\infty} I_i$. Then I is a radical differential ideal. Theorem 1.16 provides us $f_1, \dots, f_s$ such that $I = \sqrt{\langle f_1, \dots, f_s \rangle^{(\infty)}}$. Since $f_1, \dots, f_s \in I$, there exists N such that $f_1, \dots, f_s \in I_N$. Therefore, $I_N = I_{N+1} = \dots = I$. □

Corollary 1.18 (Finite primary decomposition)**.** *Let k be a differential field, and let $I \subset k[\mathbf{x}^{(\infty)}]$ be a radical differential ideal. Then there exist prime differemtial ideals $P_1, \dots, P_s \subset k[\mathbf{x}^{(\infty)}]$ such that*

$$I = P_1 \cap P_2 \cap \dots \cap P_s.$$

Proof of Corollary 1.18. Proposition 1.6 implies that there exists a set $\{P_\lambda\}_{\lambda \in \Lambda}$ of prime differential ideals in $k[\mathbf{x}^{(\infty)}]$ such that $I = \bigcap_{\lambda \in \Lambda} P_\lambda$. By removing unnecessary P_λ's, we will further assume that this decomposition is irredundant. If Λ is infinite, then let $\{\lambda_0, \lambda_1, \dots\}$ be a countable subset of Λ. Then the irredundancy of the decomposition implies that

$$\bigcap_{i=0}^{\infty} P_{\lambda_i} \subsetneq \bigcap_{i=1}^{\infty} P_{\lambda_i} \subsetneq \bigcap_{i=2}^{\infty} P_{\lambda_i} \subsetneq \dots$$

is an infinite strictly ascending chain of radical differential ideals. This contradicts Corollary 1.17. □

1.5 Proof of the Ritt-Raudenbash theorem (Theorem 1.16)

The Ritt-Raudenbash theorem (Theorem 1.16) will follow by induction on the number of differential variables from the Theorem 1.20 below.

Definition 1.19 (Basis property)**.** Let I be a radical differential ideal in a differential ring R. A set $\{f_\lambda\}_{\lambda \in \Lambda} \subset R$ is called *a basis* of I if $I = \sqrt{\langle f_\lambda \mid \lambda \in \Lambda \rangle^{(\infty)}}$. If $|\Lambda| < \infty$, we say that I has *a finite basis*.

We will say that a differential ring R *has the basis property* if every radical differential ideal R has a finite basis. In particular, Theorem 1.16 states that differential polynomial rings have the basis property.

Theorem 1.20. *Let $R \supset \mathbb{Q}$ be a differential domain ring with the basis property. Then $R[x^{(\infty)}]$ also has the basis property.*

Lemma 1.21. *If a radical ideal I of a differential ring R has a finite basis, then one can choose a finite basis from any basis of I.*

Proof. Let $\{g_1, \dots, g_s\}$ and $\{f_\lambda\}_{\lambda \in \Lambda}$ be two bases of I such that the former is finite. Since the expression of a suitable power of each of g_i's in terms of f_λ's involves only finitely many terms, then there exists a finite subset $\Omega \subset \Lambda$ such that $g_i \in \sqrt{\langle f_\lambda \mid \lambda \in \Omega \rangle^{(\infty)}}$ for every $1 \leqslant i \leqslant s$. Therefore, $\{f_\lambda\}_{\lambda \in \Omega}$ is a finite subbasis. □

Proof of Theorem 1.20. Assume the contrary. Consider the set of all radical differential ideals in $R[x^{(\infty)}]$ not having a finite basis. This set satisfies the conditions of the Zorn's lemma. Let I be any maximal element in this set.

First we will prove that I is prime. Assume the contrary. Lemma 1.12 implies that exist radical ideals J_1, J_2 such that $\mathbb{V}(I) = \mathbb{V}(J_1) \cup \mathbb{V}(J_2)$ and $\mathbb{V}(I) \subsetneq \mathbb{V}(J_i)$ for $i = 1, 2$. Due to the maximality of I, there exist $B_1, B_2 \subset R$ such that $J_i = \sqrt{\langle B_i \rangle^{(\infty)}}$ for $i = 1, 2$. Then, using Lemma 1.12, we have

$$\mathbb{V}(I) = \mathbb{V}(J_1) \cup \mathbb{V}(J_2) = \mathbb{V}(B_1) \cup \mathbb{V}(B_2) = \mathbb{V}(B_1 B_2),$$

and this gives us a finite basis $B_1 B_2$ for I.

Let $I_0 := \sqrt{\langle I \cap R \rangle^{(\infty)}}$. Due to Proposition 1.15 applied to I, there exists $f \in I$ and $g \notin I$ such that $I = \langle I_0, f \rangle^{(\infty)} \colon g^\infty$. The maximality of I implies that $\sqrt{\langle I, g \rangle^{(\infty)}}$ has a finite basis.

Lemma 1.21 implies that there exist $f_1, \ldots, f_m \in I$ such that $\sqrt{\langle I, g\rangle^{(\infty)}} = \sqrt{\langle f_1, \ldots, f_m, g\rangle^{(\infty)}}$. We claim that

$$I = I_1 := \sqrt{\langle I_0, f, f_1, \ldots, f_m\rangle^{(\infty)}}. \tag{3}$$

Since $I_0 \subseteq I$ and $f, f_1, \ldots, f_m \in I$, $I_1 \subseteq I$. To prove the reverse inclusion, consider $q \in I$. Then there exists N such that $g^N q \in \langle I_0, f\rangle^{(\infty)}$. Consider $P \in \mathbb{V}(I_1)$.

- If $g(P) \neq 0$, then q must vanish at P.
- If $g(P) = 0$, then $P \in \mathbb{V}(g, f_1, \ldots, f_m) \subset \mathbb{V}(I)$, so q vanishes at P.

Therefore, $q \in I_1$. Thus (3) is proved. Since $I_0 \subset R$, it has a finite basis, so (3) gives a finite basis for I. □

1.6 Caveat: finite basis $\neq$ finitely generated

Although the Ritt-Raudenbash theorem shows that any radical differential ideal in a differential polynomial ring can be defined (as a radical differential ideal) by finitely many differential polynomials, it does not imply that any such ideal is finitely generated as a differential ideal.

Proposition 1.22. *The radical differential ideal $\sqrt{\langle xy\rangle^{(\infty)}} \subset \mathbb{Q}[x^{(\infty)}, y^{(\infty)}]$ is not finitely generated as a differential ideal.*

Proof. First we show that $\sqrt{\langle xy\rangle^{(\infty)}}$ is generated by $S = \{x^{(i)}y^{(j)} \mid i, j \geqslant 0\}$ as an ideal. $S \subset \sqrt{\langle xy\rangle^{(\infty)}}$ by Exercise 1.7. Consider any element $f \in \sqrt{\langle xy\rangle^{(\infty)}}$. Since any monomial containing derivatives of both x and y is divisible by an element of S, modulo $\langle S\rangle$, f is equivalent to a differential polynomial of the form $f_0 + f_1 + c$, where $f_0 \in \mathbb{Q}[x^{(\infty)}]$ and $f_1 \in \mathbb{Q}[y^{(\infty)}]$ have zero constant term, and $c \in \mathbb{Q}$. We will show that $f_0 + c = 0$. Assume that $f_0 + c \neq 0$. Consider a homomorphism $\phi\colon \mathbb{Q}[x^{(\infty)}, y^{(\infty)}] \to \mathbb{Q}$ such that

$$\phi(y^{(i)}) = 0 \quad \text{for every } i \geqslant 0 \quad \text{and } \phi(f_0 + c) \neq 0.$$

Then $\ker \phi \supset \sqrt{\langle xy\rangle^{(\infty)}}$ and $\phi(f) \neq 0$, so $f \notin \sqrt{\langle xy\rangle^{(\infty)}}$. Similarly $f_1 + c = 0$, so $f_0 = f_1 = c = 0$. Therefore, $\sqrt{\langle xy\rangle^{(\infty)}} = \langle S\rangle$.

Assume that $\sqrt{\langle xy\rangle^{(\infty)}} = \langle g_1, \ldots, g_\ell\rangle^{(\infty)}$ for some $g_1, \ldots, g_\ell \in \mathbb{Q}[x^{(\infty)}, y^{(\infty)}]$. Since all elements in S are homogeneous and isobaric, then, for every $f \in \sqrt{\langle xy\rangle^{(\infty)}}$, its homogeneous isobaric components also belong to the ideal. Therefore, replacing $g_1, \ldots, g_\ell$ with their homogeneous isobaric components if necessary, we will further assume that they are homogeneous and isobaric. Moreover, we will assume that $\deg g_1 = \ldots = \deg g_r = 2$, and $\deg g_i > 2$ for $i > r$ (r may be zero). The homogeneity of the generators imply that each element of S must be a $\mathbb{Q}$-linear combination of the derivatives the $g_1, \ldots, g_r$. For every $1 \leqslant i \leqslant h$, we will denote the sum of the orders of the variables in any monomial of g_i (which is the same for different monomials due to the isobaricity) by h_i. Then the isobaricity of the generators implies that each element of

$$xy^{(r)},\ x'y^{(r-1)},\ \ldots,\ x^{(r)}y$$

is a $\mathbb{Q}$-linear combination of $g_1^{(r-h_1)}, \ldots, g_r^{(r-h_r)}$. However, it is impossible to write $r+1$ linearly independent vector as a linear combinations of r vectors. □

1.7 Special case: differential ideals of dynamical models

In this section, we consider a class of systems of differential equations ubiquitous in applications (so-called *state-space representation* of a model), show that they have extremely nice algebraic properties, and demonstrate an application of differential algebra to modeling (and to special functions, see Example 1.29). More precisely, we will consider systems of the form

$$\begin{cases} \mathbf{x}' = \mathbf{f}(\mathbf{p}, \mathbf{x}, \mathbf{u}), \\ \mathbf{y} = \mathbf{g}(\mathbf{p}, \mathbf{x}, \mathbf{u}), \end{cases} \tag{4}$$

where

- $\mathbf{p} = (p_1, \ldots, p_s)$ are unknown scalar parameters;
- $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_m)$, and $\mathbf{u} = (u_1, \ldots, u_\ell)$ are function variables refereed to as the state, output, and input variables, respectively;

- $\mathbf{f}, \mathbf{g}$ are vectors of polynomials in $\mathbb{C}[\mathbf{p}, \mathbf{x}, \mathbf{u}]$ of dimensions n and m, respectively.

System (4) can be interpreted as follows. The input variables $\mathbf{u}$ are the functions determined by the experimenter/modeller (e.g., an external force or a drug injection). Together with the parameter values and the initial conditions for the state variables $\mathbf{x}$, they completely define the dynamics of the $\mathbf{x}$-variables. The output variables $\mathbf{y}$ are the quantities measured/observed in the experiment. The typical questions asked about such systems include:

- is it possible to determine infer the values of the parameters (identifiability) or reconstruct the values of the state variables (observability);
- is it always possible to achieve the desired behaviour of the system by chosing appropriate input functions (controllability and control design);
- which functions in $\mathbf{x}$ and $\mathbf{u}$ remain constant along the trajectories (first integrals).

Example 1.23 (Predator-prey model)**.** The following model describes the coexistence of two species, prey (x_1) and predators (x_2), so that the population of prey can be observed and controlled:

$$\begin{cases} x_1' = ax_1 - bx_1x_2 + u, \\ x_2' = -cx_2 + dx_1x_2, \\ y = x_1. \end{cases} \tag{5}$$

To put (4) into the context of differential algebra, consider a constant differential field $k = \mathbb{C}(\mathbf{p})$ to be a purely transcendental extension of $\mathbb{C}$ by the parameters. Then (4) can be recasted into the following $n + m$ differential polynomials:

$$\mathbf{x}' - \mathbf{f}(\mathbf{x}, \mathbf{u}),\ \mathbf{y} - \mathbf{g}(\mathbf{x}, \mathbf{u}) \in k[\mathbf{x}^{(\infty)}, \mathbf{y}^{(\infty)}, \mathbf{u}^{(\infty)}], \tag{6}$$

where the dependence of $\mathbf{f}$ and $\mathbf{g}$ on $\mathbf{p}$ is made implicit as $\mathbf{p}$ belongs to the field of coefficients.

Proposition 1.24. *In the notation above, consider differential ideal*

$$I := \langle \mathbf{x}' - \mathbf{f}(\mathbf{x}, \mathbf{u}),\ \mathbf{y} - \mathbf{g}(\mathbf{x}, \mathbf{u}) \rangle^{(\infty)} \subset k[\mathbf{x}^{(\infty)}, \mathbf{y}^{(\infty)}, \mathbf{u}^{(\infty)}].$$

1. *On the ring $k[\mathbf{x}^{(\infty)}, \mathbf{y}^{(\infty)}, \mathbf{u}^{(\infty)}]$ considered as a polynomial ring in infinitely many variables, consider the lexicographic monomial ordering corresponding to any ordering on the variables such that*

   (a) $y_{i_1}^{(i_2)} > x_{i_3}^{(i_4)} > u_{i_5}^{(i_6)}$ for every $i_1, \ldots, i_6$;

   (b) $i_1 > i_2 \implies a_{j_1}^{(i_1)} > a_{j_2}^{(i_2)}$ for every $a \in \{x, y, u\}$ and j_1, j_2.

   Then the set of all the derivatives of (6) forms a Gröbner basis of I with respect to this ordering.

2. *As a commutative algebra, $k[\mathbf{x}^{(\infty)}, \mathbf{y}^{(\infty)}, \mathbf{u}^{(\infty)}]/I$ is isomorphic to $k[\mathbf{x}, \mathbf{u}^{(\infty)}]$. In particular, I is a prime differential ideal.*

Proof.

1. Note that the leading terms of $(x_i' - f_i(\mathbf{x}, \mathbf{u}))^{(j)}$ and $(y_i - g_i(\mathbf{x}, \mathbf{u}))^{(j)}$ will be $x_i^{(j+1)}$ and $y_i^{(j)}$, respectively. Therefore, the leading terms of all the derivatives of (6) will be distinct variables. Therefore, this set is a Gröbner basis by the first Buchberger's criterion.

2. The result of the reduction of any polynomial with respect to the Gröbner basis from the previous part of the proposition belongs to $k[\mathbf{x}, \mathbf{u}^{(\infty)}]$, and none of the elements of this subring is reducible with respect to the basis. Therefore, the quotient with respect to I will be isomorphic to $k[\mathbf{x}, \mathbf{u}^{(\infty)}]$.

$\square$

Now we will demonstrate how the structure of this ideal can be used in applications.

Definition 1.25 (Field of definition)**.** Let $J \subset K[x_1^{(\infty)}, \ldots, x_n^{(\infty)}]$ be a differential ideal over a differential field K. Then the smallest differential subfield $L \subset K$ such that J is generated by $J \cap L[x_1^{(\infty)}, \ldots, x_n^{(\infty)}]$ is called the field of definition of J.

Consider ideal I from Proposition 1.24. It has been shown in [8, Theorem 21] that the field of definition of
$$I \cap k[\mathbf{y}^{(\infty)}, \mathbf{u}^{(\infty)}]$$
is exactly *the field of multi-experiment identifiable functions*, that is, the functions in the parameters whose values can be determined from sufficiently many experiments with generic independent inputs and initial conditions.

Example 1.26. Consider the following model:

$$\begin{cases} x_1' = p_1 x_2, \\ x_2' = p_2 x_1, \\ y = x_1. \end{cases}$$

In this case, $I = \langle x_1' - p_1 x_2, x_2' - p_2 x_1, y - x_1\rangle^{(\infty)}$. We can find at least one element $I \cap \mathbb{C}(p_1, p_2)[y^{(\infty)}]$ in by
$$y'' = x_1'' = p_1 x_2' = p_1 p_2 x_1 = p_1 p_2 y.$$
Moreover, one can show that $I \cap \mathbb{C}(p_1, p_2)[y^{(\infty)}] = \langle y'' - p_1 p_2 y\rangle^{(\infty)}$. Hence, its field of definition is $\mathbb{Q}(p_1 p_2)$, so the value $p_1 p_2$ can be found experimentally while p_1 and p_2 cannot (look at the system an convince yourself in this!).

Proposition 1.27. *Assume that $m = 1$, that is, the system has only one output. Consider a polynomial f in $I \cap k[y^{(\infty)}, \mathbf{u}^{(\infty)}]$ of the lowest possible degree among the polynomials of the lowest possible order in y.*

1. *Normalize f so that at least one of the coefficients is 1. Then the remaining coefficients generate the field of definition of $I \cap k[y^{(\infty)}, \mathbf{u}^{(\infty)}]$ and, consequently, the field of multi-experiment identifiable functions.*

2. *We define*
$$I_j := \langle (\mathbf{x}' - \mathbf{f}(\mathbf{x}, \mathbf{u}))^{(<j)}, (y - g(\mathbf{x}, \mathbf{u}))^{(\leqslant j)}\rangle \subset k[\mathbf{x}^{(\leqslant j)}, y^{(\leqslant j)}, \mathbf{u}^{(\leqslant j)}].$$
Then $f \in I_n$. In particular, f can be found using a Gröbner basis computation.

Proof.

1. Proposition 1.24 implies that I is prime, so $J := I \cap k[y^{(\infty)}, \mathbf{u}^{(\infty)}]$ is prime as well. Since none of the derivatives of $\mathbf{u}$ appear as in the leading terms of the Gröbner basis of I described in Proposition 1.24, $I \cap k[\mathbf{u}^{(\infty)}] = \{0\}$. Applying Proposition 1.15 to J viewed as a univariate prime differential ideal over $k[\mathbf{u}^{(\infty)}]$, we deduce that
$$J = \langle f\rangle^{(\infty)} \colon g^{\infty},$$
where g is the product of the initial and separant of f. Let F be the field generated by the coefficients of f (after the normalization). Due to the minimality of f, any set of generators of J must contain f, so F is contained in the field of definition of J. Now we will show that J is generated by $J \cap F[y^{(\infty)}, \mathbf{u}^{(\infty)}]$. Consider any element $p \in J$. Then there exists N, r and $a_0, \ldots, a_r \in k[y^{(\infty)}, \mathbf{u}^{(\infty)}]$ such that
$$g^N p = \sum_{i=0}^{r} a_i f^{(i)}. \tag{7}$$
Let $\{e_\lambda\}_{\lambda \in \Lambda}$ be a basis of k over F. We write $p = \sum\limits_{\lambda \in \Lambda} p_\lambda e_\lambda$ and $a_i = \sum\limits_{\lambda \in \Lambda} a_{i,\lambda} e_\lambda$ so that p_λ's and $a_{i,\lambda}$'s have the coefficient in F. Then, equating the coefficients at each e_λ in (7), we see that $p_\lambda \in J$ for every $\lambda \in \Lambda$, so p belongs to the ideal generated by $J \cap F[y^{(\infty)}, \mathbf{u}^{(\infty)}]$.

2. Since, in the Gröbner basis described in Proposition 1.24, the leading term has the highest order, reduction with respect to this basis does not increase the order. Therefore, we have, for every $j \geqslant 0$,
$$I \cap k[y^{(\leqslant j)}, \mathbf{u}^{(\leqslant j)}] = I_j.$$
Since the polynomials in $k[y^{(\leqslant n)}, \mathbf{u}^{(\leqslant n)}]$ not reducible with respect to the Gröbner basis are exactly $k[\mathbf{x}, \mathbf{u}^{(\leqslant n)}]$, the transcendence degree of $k[\mathbf{x}^{(\leqslant n)}, y^{(\leqslant n)}, \mathbf{u}^{(\leqslant n)}]/I_n$ is equal to $|\mathbf{x}| +$

$(n+1)|\mathbf{u}| = n + (n+1)\ell$. One the other hand, the transcendence degree of $k[y^{(\leqslant n)}, \mathbf{u}^{(\leqslant n)}]$ is equal to $(1+|\mathbf{u}|)(n+1) = (n+1)(\ell+1)$. Therefore, $I_n \cap k[y^{(\infty)}, \mathbf{u}^{(\infty)}] \neq \{0\}$. Since $I \cap k[\mathbf{u}^{(\infty)}] = \{0\}$, we have $\operatorname{ord}_y f \leqslant n$.

It remains to show that $f \in k[y^{(\leqslant n)}, \mathbf{u}^{(\leqslant n)}]$. Assume the contrary. Then f involves the derivatives of $\mathbf{u}$ of order higher than n. Since the reduction with respect to the Gröbner basis replaces y or $\mathbf{x}$ variables with a differential polynomial of the same or lower order, the order in y and $\mathbf{x}$ of all the intermediate results in the reduction of f with respect to the basis will not exceed n. Therefore, if we write f as a polynomial in $\mathbf{u}^{(n+1)}, \mathbf{u}^{(n+2)}, \ldots$ over $k[y^{(\leqslant n)}, \mathbf{u}^{(\leqslant n)}]$, then all the coefficients will also belong to I. If $f \notin k[y^{(\leqslant n)}, \mathbf{u}^{(\leqslant n)}]$, then at least one of them is of lower degree than f contradicting to the minimality of f.

□

Proposition 1.27 yields an algorithm for computing the functions identifiable from multiple experiments.

Example 1.28 (Predator-prey, continued)**.** Consider the predator-prey model (5) from Example 1.23. Proposition 1.27 implies that the field of multi-experiment functions (which is equal to the field of definition) is generated by the coefficients of the minimal polynomial for y over $\mathbb{C}(a,b,c,d)[u^{(\infty)}]$. We will compute this polynomial using the second part of Proposition 1.27. We have $n = 2$, and the polynomial must belong to the ideal generated by

$$\begin{aligned} &x_1' - ax_1 + bx_1x_2 - u, && x_2' + cx_2 - dx_1x_2, \\ &x_1'' - ax_1' + bx_1'x_2 + bx_1x_2' - u', && x_2'' + cx_2' - dx_1'x_2 - dx_1x_2', \\ &y - x_1 && y' - x_1', \quad y'' - x_1''. \end{aligned}$$

The last element in the Gröbner basis with respect to the lexicographic ordering with

$$x_1'' > x_2'' > x_1' > x_2' > x_1 > x_2 > y'' > y' > y > u' > u$$

is exactly the element of lowest order in y over $\mathbb{C}(a,b,c,d)[u,u']$:

$$ady^3 - dy^2y' - acy^2 + cyy' + yy'' - (y')^2.$$

Then the field of definition (and the field of multi-experiment identifiable functions) is

$$\mathbb{C}(ad, d, ac, c) = \mathbb{C}(a, c, d)$$

meaning that the values of a, c, d can be inferred from a series of experiments while the value of b cannot.

Example 1.29 (Differential-algebraic functions)**.** In this exercise, we will demonstrate that equations of the form (4) appear not only in modelling. Paineleve transcendents are one of the fundamental special functions. Transcendent of type I is a solution of the following differential equation over $\mathbb{C}(t)$ (considered as a differential field with respect to $\frac{\mathrm{d}}{\mathrm{d}t}$):

$$y'' = 6y^2 + t.$$

Consider the problem of finding a differential equation for $z = y^2$. This can be reduced to find a consequence of

$$\begin{cases} t' = 1, \\ y_1' = 6y_2^2 + t, \\ y_2' = y_1', \\ z = y^2. \end{cases} \tag{8}$$

Here t, y_1, y_2 play the role of the state variables and z plays the role of the output. We have $n = 3$, so the desired equation will belong to the ideal generated by two more derivatives of (8). Computation similar to the one from the previous example shows that

$$z^5(z')^2 + \frac{1}{3}z^5z' + \frac{1}{36}z^5 - \frac{1}{144}z^4(z''')^2 + \frac{1}{48}z^3z'z''z''' - \frac{1}{96}z^2(z')^3z''' - \frac{1}{64}z^2(z')^2(z'')^2 + \frac{1}{64}z(z')^4z'' - \frac{1}{256}(z')^6 = 0.$$

1.8 Exercises

Exercise 1.1. Consider $I := \langle x'' + x, x^2 + y^2 - 1\rangle^{(\infty)} \subset \mathbb{Q}[x^{(\infty)}, y^{(\infty)}]$. Find at least one differential polynomial in $I \cap \mathbb{Q}[y^{(\infty)}]$. Try to give its trigonometric interpretation.

Exercise 1.2. Use [4, Theorem 1.3] to derive a bound $M(m) \leqslant m^2$ (in the notation of the proof of Proposition 1.4) from the proof of Proposition 1.4.

Exercise* 1.3. Prove that, for every $n \geqslant 1$, there exists positive $c_n \in \mathbb{Q}_n$ such that

$$\operatorname{Wronsk}(1, x, x^2, \ldots, x^n) = c_n (x')^{\frac{n(n+1)}{2}}. \tag{9}$$

Use this to prove that (in the notation of the proof of Proposition 1.4) that $M(m) \leqslant \frac{m(m+1)}{2}$.

Exercise§ 1.4. How could one generalize the identity (9) to get expressions with $(x'')^N$?

Exercise 1.5. Show that, for every $n > 1$,

$$x' \notin \sqrt{\langle x^n, (x^n)', \ldots, (x^n)^{(n-1)}\rangle}.$$

(Hint: how would you formulate the negation of the Nullstellensatz?)

Exercise 1.6. Use any computer algebra system (or the course package https://github.com/pogudingleb/DifferentialAlgebra) to find the smallest number N such that

$$(x')^N \in \langle x^n, (x^n)', \ldots, (x^n)^{(n)}\rangle$$

for $n = 2, 3, 4, 5$.

Exercise 1.7. Use the argument from the proof of Proposition 1.4 to show that if I is a radical differential ideal in a differential ring R and $ab \in I$, then $ab' \in I$.

Exercise 1.8. Prove Lemma 1.12.

Exercise 1.9. The following problem has been proposed at the 40th International Mathematical Tournament of Towns[1]:

> Rockefeller and Marx play the following game. There are $n > 1$ cities, each with the same number of citizens. At the start of the game every citizen has exactly one coin (all coins are identical). On his turn, Rockefeller chooses one citizen from every city, then Marx redistributes their coins between them so that the new distribution is different from one immediately before. Rockefeller wins if at some moment there will be at least one citizen in every city with no coins. Prove that Rockefeller can always win, no matter how Marx plays, if in every city there are $2n - 1$ citizens.

Taking this statement for granted, show that, for every $n > 1$,

$$(x_1' \cdot \ldots \cdot x_n')^{2n-1} \in \langle x_1 \cdot \ldots \cdot x_n\rangle^{(\infty)} \subset \mathbb{Q}[x_1^{(\infty)}, \ldots, x_n^{(\infty)}].$$

Exercise* 1.10. Give an example of a radical differential ideal $I \subset \mathbb{Q}[x^{(\infty)}]$ such that there is no $f \in \mathbb{Q}[x^{(\infty)}]$ such that $I = \sqrt{\langle f\rangle^{(\infty)}}$. (Hint: look at the previous lecture)

Exercise* 1.11. Is the ideal $\langle \operatorname{Wronsk}(x, x')\rangle^{(\infty)}$ radical? Prime?

Exercise 1.12.** Is it true that every prime differential ideal in $\mathbb{Q}[x^{(\infty)}]$ is finitely generated as a differential ideal?

Exercise 1.13. Prove that, in Proposition 1.15, if R is a field, then the saturation with respect to the initial is not necessary.

Exercise 1.14. Consider a differential ideal $\langle y', x' - yx\rangle \in \mathbb{Q}[x^{(\infty)}, y^{(\infty)}]$. Show that it is prime and find a representation for it as in Proposition 1.15.

Exercise 1.15. Let A be a differential algebra over k without zero divisors which is generated as a differential algebra by a single element and is not isomorphic to $k[x^{(\infty)}]$. Prove that A can be embedded into a differential algebra which is finitely generated as a commutative algebra.

(Hint: use Proposition 1.15 and localization)

[1] the full problem set is here https://www.turgor.ru/en/problems/40/fall-40-A-eng-auth.pdf. By the way, the tournament of towns is one of the best high school olympiads in the world, see https://www.turgor.ru/en/

Exercise 1.16. Using Example 1.29, find a differential equation satisfied by $\sin(\sin t)$.

Exercise 1.17. Consider now the case when the right-hand sides of (4) are rational function. Bringing to the common denominator, we will write $f_i = \frac{F_i}{Q}$ for $1 \leqslant i \leqslant n$ and $g_j = \frac{G_j}{Q}$ for $1 \leqslant j \leqslant m$, where F_i's, G_j's and Q are polynomials. The corresponding differential ideal would be

$$I := \langle Qx_1' - F_1, \ldots, Qx_n' - F_n, Qy_1' - G_1, \ldots, Qy_m' - G_m \rangle^{(\infty)} \colon Q^{\infty}.$$

Prove the following analogues of the statements from Section 1.7.

1. Ideal I is a prime differential ideal.
2. The intersection of I with the subring generated by the derivatives of the orders at most j is equal to
$$I_j := \langle (Q\mathbf{x} - \mathbf{F}(\mathbf{x}, \mathbf{u}))^{(<j)}, (Q\mathbf{y} - \mathbf{G}(\mathbf{x}, \mathbf{u}))^{(\leqslant j)} \rangle \colon Q^{\infty}.$$
3. It $m = 1$, then the ideal I_n contains the minimal differential equation for y.

Exercise 1.18. Use Exercise 1.17 to derive a second order differential equation for $\frac{1}{\sin t} + \frac{1}{\cos t}$.

Exercise** 1.19. Derive a first order differential equation for $\frac{1}{\sin t} + \frac{1}{\cos t}$.

2 Solutions: power series

In this section, we restrict our attention to differential equations with complex coefficients. In the algebraic language, this means that we will consider differential algebras over $\mathbb{C}$. The main goal of the section is to consider formal power series solutions of such equations. Apart from high practical relevance, power series solution turn out to be very natural from the algebraic standpoint: they correspond to the set of complex point of the differential algebra considered as a commutative algebra.

2.1 Taylor homomorphisms and Nullstellensatz for power series

Lemma 2.1 (Taylor homomorphism)**.** *Let A be a differential algebra over $\mathbb{C}$, and let $\varphi\colon A \to \mathbb{C}$ be a (not necessarily differential) homomorphism of $\mathbb{C}$-algebras. Consider the Taylor homomorphism $T(\varphi)\colon A \to \mathbb{C}[\![t]\!]$ defined by*

$$T(\varphi)(a) := \sum_{i=0}^{\infty} \varphi(a^{(i)}) \frac{t^i}{i!}.$$

If we consider $\mathbb{C}[\![t]\!]$ as a differential algebra with respect to $\frac{\mathrm{d}}{\mathrm{d}t}$, $T(\varphi)$ is a homomorphism of differential algebras.

Proof. Verified by a direct computation. □

Notation 2.2. We introduce *the evaluation homomorphism* $e\colon \mathbb{C}[\![t]\!] \to \mathbb{C}$ by $e(f(t)) := f(0)$. Note that this is a $\mathbb{C}$-homomorphism.

Proposition 2.3. *Let A be a differential algebra over $\mathbb{C}$. Consider two sets:*

$$\operatorname{spec}_{\mathbb{C}}(A) := \{\varphi\colon A \to \mathbb{C} \mid \varphi \textit{ is a (not necessarily differential) homomorphism of } \mathbb{C}\textit{-algebras}\}$$
$$\operatorname{diffspec}_{\mathbb{C}[\![t]\!]} A := \{\Phi\colon A \to \mathbb{C}[\![t]\!] \mid \Phi \textit{ is a homomorphism of differential } \mathbb{C}\textit{-algebra}\}.$$

The following maps define a bijection between these sets

$$\begin{array}{ccc} \operatorname{spec}_{\mathbb{C}} A & \Longleftrightarrow & \operatorname{diffspec}_{\mathbb{C}[\![t]\!]} A \\ \varphi & \longrightarrow & T(\varphi) \\ e \circ \Phi & \longleftarrow & \Phi. \end{array}$$

Proof. Verified by a direct computation. □

Proposition 2.4 (Nullstellensatz for power series)**.** *Let $f_1, \ldots, f_\ell, g \in \mathbb{C}[x_1^{(\infty)}, \ldots, x_n^{(\infty)}]$. Then the following statements are equivalent:*

1. *g vanishes on every solution of $f_1 = \ldots = f_\ell = 0$ in $\mathbb{C}[\![t]\!]$;*

2. $g \in \sqrt{\langle f_1, \dots, f_\ell \rangle^{(\infty)}}$.

Proof. If $g \in \sqrt{\langle f_1, \dots, f_\ell \rangle^{(\infty)}}$, then there exist $M, N \geqslant 1$ and $c_{i,j} \in k[x_1^{(\infty)}, \dots, x_n^{(\infty)}]$ for $1 \leqslant i \leqslant \ell$ and $0 \leqslant j \leqslant N$ such that

$$g^N = \sum_{i,j} c_{i,j} (f_i)^{(j)}.$$

Evaluating the above equality at any power series solution of $f_1 = \ldots = f_\ell = 0$ will vanish the right-hand side yielding that $g = 0$ on this solution.

Assume that $g \notin \sqrt{\langle f_1, \dots, f_\ell \rangle}$. Theorem 1.1 implies that there exists a homomorphism $\varphi \colon k[x_1^{(\infty)}, \dots, x_n^{(\infty)}] \to \mathbb{C}$ such that $\varphi(g) \neq 0$ and $\ker \varphi \supseteq \sqrt{\langle f_1, \dots, f_\ell \rangle}$. Then one can check that

$$T(\varphi)(f_1) = \ldots = T(\varphi)(f_\ell) = 0, \quad \text{and} \quad T(\varphi)(g) \neq 0.$$

Therefore, $(T(\varphi)(x_1), \dots, T(\varphi)(x_n))$ is a power series solution of $f_1 = \ldots = f_\ell = 0$ which does not vanish g. $\square$

We will demonstrate the power of this Nullstellensatz by giving much more natural proofs of the ideal membership statements used in Proposition 1.4 and Lemma 1.7.

Lemma 2.5.

1. *For every $n \geqslant 1$, $x' \in \sqrt{\langle x^n \rangle^{(\infty)}} \subset \mathbb{Q}[x^{(\infty)}]$.*
2. *$xy' \in \sqrt{\langle xy \rangle^{(\infty)}} \subset \mathbb{Q}[x^{(\infty)}, y^{(\infty)}]$.*

Proof. To prove the first part, consider any power series solution $x(t) \in \mathbb{C}[\![t]\!]$ of the equation $x^n = 0$. Clearly, $x(t) = 0$, so we have $x'(t) = 0$ as well, so $x' \in \sqrt{\langle x^n \rangle}$ by Proposition 2.4.

To prove the second part, consider $x(t), y(t) \in Ct$ such that $x(t)y(t) = 0$. Then $x(t) = 0$ or $y(t) = 0$. In both cases, we have $x(t)y'(t) = 0$. $\square$

2.2 Do these solutions converge?

Example 2.6 (Answer: no)**.** Consider the ideal $I = \langle x' - 1, x^2y' + y - x \rangle^{(\infty)} \subset \mathbb{C}[x^{(\infty)}, y^{(\infty)}]$ corresponding to the system

$$\begin{cases} x' = 1, \\ x^2 y' + y = x. \end{cases}$$

By direct computation, one can verify that the following is a power series solution of the system

$$x(t) = t, \quad y(t) = \sum_{i=0}^{\infty} (-1)^i i! t^i.$$

It turns out that one can find a function with this analytic expansion, and this will be so-called Eular function, see [7, Example 2.2.4] for details.

However, the following theorem and the corollary imply that "many" of the formal power series solutions have positive radius of convergence.

Notation 2.7. Let $\mathbb{C}\{t\} \subset \mathbb{C}[\![t]\!]$ be the set of all formal power series with a positive radius of convergence. Note that $\mathbb{C}\{t\}$ is a differential subalgebra of $\mathbb{C}[\![t]\!]$.

Theorem 2.8 (Ritt)**.** *Let A be a differential algebra over $\mathbb{C}$ finitely generated as a differential algebra. Then there is a differential homomorphism $A \to \mathbb{C}\{t\}$.*

Corollary 2.9 (Analytic Nullstellensatz)**.** *Let $f_1, \dots, f_\ell, g \in \mathbb{C}[x_1^{(\infty)}, \dots, x_n^{(\infty)}]$. Then the following statements are equivalent:*

1. *g vanishes on every solution of $f_1 = \ldots = f_\ell = 0$ in $\mathbb{C}\{t\}$;*
2. *$g \in \sqrt{\langle f_1, \dots, f_\ell \rangle^{(\infty)}}$.*

Proof of Corollary 2.9. The fact that $g \in \sqrt{\langle f_1, \ldots, f_\ell \rangle^{(\infty)}}$ implies vanishing on every solution in $\mathbb{C}\{t\}$ follows from Proposition 2.4.

Assume that $g \notin \sqrt{\langle f_1, \ldots, f_\ell \rangle^{(\infty)}}$. Let

$$A = k[x_1^{(\infty)}, \ldots, x_n^{(\infty)}]/\sqrt{\langle f_1, \ldots, f_\ell \rangle^{(\infty)}},$$

and denote the image of g in A by the same letter. Since g is not nilpotent in A, the localization $B := A[1/g]$ is a nonzero algebra. Moreover, the derivation can be extended uniquely from A to B (check this!). B is generated by $1/g$ and the images of $x_1, \ldots, x_n$, so Theorem 2.8 implies that there exists a differential homomorphism $B \to \mathbb{C}\{t\}$ and g is not mapped to zero because g is invertible in B. Composing it with the canonical homomorphisms $k[x_1^{(\infty)}, \ldots, x_n^{(\infty)}] \to A$ and $A \to B$, we obtain a differential homomorphism $k[x_1^{(\infty)}, \ldots, x_n^{(\infty)}] \to \mathbb{C}\{t\}$ sending $f_1, \ldots, f_\ell$ to zero and g to a nonzero element of $\mathbb{C}\{t\}$. □

Our proof of Theorem 2.8 will be based on [3]. It will be based on three propositions below which are of independent interest.

Proposition 2.10. *Let A be a differential $\mathbb{C}$-algebra finitely generated as a commutative algebra. Then the image of any differential homomorphism $A \to \mathbb{C}[[t]]$ is contained in $\mathbb{C}\{t\}$.*

Proof. Let $a_1, \ldots, a_n \in A$ be the elements generating A as a commutative $\mathbb{C}$-algebra. Then there exist $p_1, \ldots, p_n \in \mathbb{C}[x_1, \ldots, x_n]$ such that

$$a_1' = p_1(a_1, \ldots, a_n),\ a_2' = p_2(a_1, \ldots, a_n),\ \ldots,\ a_n' = p_n(a_1, \ldots, a_n).$$

Therefore, the images $f_1, \ldots, f_n \in \mathbb{C}[[t]]$ of any differential homomorphism $A \to \mathbb{C}[[t]]$ satisfy the following system of polynomial ODEs:

$$\begin{cases} x_1' = p_1(x_1, \ldots, x_n), \\ x_2' = p_2(x_1, \ldots, x_n), \\ \ldots, \\ x_n' = p_n(x_1, \ldots, x_n). \end{cases}$$

The existence and uniqueness theorem for differential equations implies that these power series are convergent in some neighbourhood of $t = 0$. □

Proposition 2.11. *Let R be a differential ring without zero divisors. Let A be a differential R-algebra without zero divisors finitely generated as a differential algebra and of finite transcendence degree over R. Then there exists $a \in A$ such that the localization $A[1/a]$ is finitely generated as a commutative R-algebra.*

Proof. We will prove the proposition by induction by the number n of generators of A as a differential R-algebra. If $n = 0$, then $A = R$, so it is finitely generated already.

Assume that the proposition is proved for all R-algebras differentially generated by less than n elements. Let A be differentially generated by $a_1, \ldots, a_n$. Applying the induction hypothesis to $A_0 := R[a_1^{(\infty)}, \ldots, a_{n-1}^{(\infty)}] \subseteq A$, we obtain $b_1 \in A_0$ such that $A_0[1/b_1]$ is finitely generated as a commutative algebra. Consider a surjective differential homomorphism $A_0[x^{(\infty)}] \to A$ defined by $x \mapsto a_n$. Since $a_n^{(\infty)}$ must be algebraically dependent over R, the kernel of this homomorphism, is a nontrivial prime ideal $P \subset A_0[x^{(\infty)}]$. Moreover, since A_0 maps to itself, $P \cap A_0 = \{0\}$. Therefore, Proposition 1.15 implies that

$$P = \langle f \rangle^{(\infty)} (\operatorname{sep}_x f \operatorname{init}_x f)^\infty$$

for some $f \in A_0[x^{(\infty)}]$ of order h. Let $b_2 := \operatorname{sep}_x(f)(a_n)$. The minimality of f implies that $b_2 \neq 0$. We claim that

$$A[1/(b_1 b_2)] = A_0[1/b_1][a_n^{(\leqslant h)}, 1/b_2]. \tag{10}$$

Since $A_0[1/b_1]$ is finitely generated as a commutative R-algebra, this would imply that $A[1/(b_1 b_2)]$ is finitely generated as a commutative k-algebra as well.

In order to prove (10), it is sufficient to show that the derivatives of the generators $a_n^{(\leqslant h)}, 1/b_2$ belong to $A_0[1/b_1][a_n^{(\leqslant h)}, 1/b_2]$. This is clear for $a_n^{(<h)}$, so it remains to show that $a^{(h+1)}$ and $(1/b_2)'$ belong to $A_0[1/b_1][a_n^{(\leqslant h)}, 1/b_2]$. For $a^{(h+1)}$, we write $f' = x^{(h+1)} \operatorname{sep}_x f + g$, here $g \in A_0[x^{(\leqslant h)}]$. Then

$$a^{(h+1)} = \frac{-g(a)}{\operatorname{sep}_x(f)(a)} = \frac{-g(a)}{b_2} \in A_0[a_n^{(\leqslant h)}, 1/b_2].$$

For $(1/b_2)'$, we observe that

$$\left(\frac{1}{b_2}\right)' \in \frac{1}{b_2^2} A_0[a^{(\leqslant h)}] \subset A_0[a_n^{(\leqslant h)}, 1/b_2]. \qquad \square$$

Proposition 2.12. *Let A be a simple differential $\mathbb{C}$-algebra (that is, a differential $\mathbb{C}$-algebra without nontrivial differential ideals) finitely generated as a differential $\mathbb{C}$-algebra. Then A does not contain zero divisors and has finite transcendence degree over $\mathbb{C}$.*

Proof. We will first prove that A does not contain zero divisors. Consider the ideal $\sqrt{\{0\}} \subset A$. This is the set of all nilpotent elements and it is a differential ideal by Proposition 1.4. Since the ideal does not contain 1 and A is simple, it must be zero, so $\{0\}$ is a radical ideal. If A contains zero divisors, then $\{0\}$ is not prime. By Proposition 1.6, it is an intersection of prime differential ideal which is impossible since there are no nontrivial prime differential ideals in A.

Assume that A has infinite transcendence degree over $\mathbb{C}$. We take any finite set of differential generators of $a_1, \ldots, a_n$ of A and arrange in such a way that there exists $r \leqslant n$ such that $a_1, \ldots, a_r$ do not satisfy any nontrivial differential equation over $\mathbb{C}$ and A is of finite transcendence degree over $A_0 := \mathbb{C}[a_1, \ldots, a_r]$. Due to the assumption on $\operatorname{trdeg}_{\mathbb{C}} A$, we have $r \geqslant 1$.

Let $R := \mathbb{C}[a_1^{(\infty)}, \ldots, a_r^{(\infty)}]$. We apply Proposition 2.11 to A as an R-algebra and obtain an element $b \in A$ such that $A_0 := A[1/b]$ is finitely generated over R and still differentially simple. Let $b_1, \ldots, b_s \in A_0$ be generators of A_0 as a R-algebra. Then, for every $j \geqslant 0$, we have

$$jr \leqslant \operatorname{trdeg}_{\mathbb{C}} \mathbb{C}[a_1^{(<j)}, \ldots, a_r^{(<j)}, b_1, \ldots, b_s] \leqslant jr + s.$$

This inequality implies that there exists N such that, for every $j > N$, $a_1^{(j)}, \ldots, a_r^{(j)}$ are algebraically independent over $\mathbb{C}[a_1^{(<j)}, \ldots, a_r^{(<j)}, b_1, \ldots, b_s]$. Consider any homomorphism

$$\varphi\colon k[a_1^{(\leqslant N)}, \ldots, a_r^{(\leqslant N)}, b_1, \ldots, b_s] \to \mathbb{C}\,.$$

Due to the algebraic independence of the rest of derivatives of $a_1, \ldots, a_r$, this homomorphism can be extended to $\varphi\colon A_0 \to \mathbb{C}$ so that $\varphi(a_i^j) = 0$ for every $1 \leqslant i \leqslant r$ and $j > N$. Then the kernel of the Taylor homomorphism $T(\varphi)$ will contain $a_1^{(N+1)}, \ldots, a_r^{(N+1)}$ contradicting to the fact that A_0 is a simple differential algebra. $\square$

Remark 2.13. The proof of the Proposition 2.12 works for every differential field k of characteristic zero. The only extra thing to do is to define the Taylor homomorphism over an arbitrary differential field of characteristic zero.

Proof of theorem 2.8. Consider any maximal differential ideal $J \subset A$. Then $B := A/J$ is a differentially simple algebra. Proposition 2.12 implies that B satisfies the requirements of Proposition 2.11, let b be the element provided by the proposition so that $B[1/b]$ is finitely generated as a commutative algebra. Consider any homomorphism $\Phi\colon B[1/b] \to \mathbb{C}[[t]]$ which exists by Proposition 2.4. Proposition 2.10 implies that the image of Φ is contained in $\mathbb{C}\{t\}$. Therefore, the image of the composition $A \to A/J = B \to B[1/b] \xrightarrow{\Phi} \mathbb{C}[[t]]$ is also contained in $\mathbb{C}\{t\}$. $\square$

2.3 Differential-algebraic power series: closure properties

For the rest of the section, we will focus on the "geometry of the affine line", that is, talk about formal power series satisfying a differential polynomial equation in one differential variables. In this subsection, we will establish several closure properties of this class of power series. We will work in a more general context.

Definition 2.14 (Differentially algebraic element)**.** Let $E \supset F$ be an extension of differential fields. An element $a \in E$ is called *differentially algebraic* over F if there exists a nonzero $P \in F[x^{(\infty)}]$ such that $P(a) = 0$.

A power series $f \in \mathbb{C}[[t]]$ will be called *differentially algebraic* if it is differentially algebraic element of $\mathbb{C}((t))$ over $\mathbb{C}$.

The following lemma will be the key to characterizing differentially algebraic elements. It is an analogue of the fact that an element of a field extension is algebraic iff the subfield generated by it is finite extension.

Lemma 2.15. *Let $E \supset F$ be an extension of differential fields. An element $a \in E$ is differentially algebraic over F if and only if*

$$\operatorname{trdeg}_F F(a^{(\infty)}) < \infty.$$

Proof. Assume that $\operatorname{trdeg}_F F(a^{(\infty)}) = h < \infty$. Then $a^{(\leqslant h)}$ are algebraically dependent over F, so there exists a nonzero $P \in F[x^{(\infty)}]$ of order at most h such that $P(a) = 0$.

Now assume that $a \in E$ is differentially algebraic over F. Let $P \in F[x^{(\infty)}]$ be the polynomial of the minimal degree among the polynomials of the minimal order vanishing at a. Let $h = \operatorname{ord}_x P$. Using the very important observation, we can write, for every $k > 0$,

$$a^{(h+k)}(\operatorname{sep}_x P)(a) + Q(a) = 0, \tag{11}$$

where $Q \in F[x^{(<h+k)}]$. Due to the minimality of P, we have $(\operatorname{sep}_x P)(a) \neq 0$, so

$$a^{(h+k)} \in F(a^{(<h+k)}).$$

Iterating this, we obtain:

$$F(a^{(\leqslant h+k)}) = F(a^{(\leqslant h+k-1)}) = \ldots = F(a^{(\leqslant h)}).$$

Therefore, $F(a^{(\infty)}) = F(a^{(\leqslant h)})$, and it has finite transcendence degree. □

Remark 2.16. Note that the proof of Lemma 2.15 implies that $\operatorname{trdeg}_F F(a^{(\infty)})$ is equal to the order of the minimal differential polynomial over F satisfied by a.

Proposition 2.17. *Let $E \supset F$ be an extension of differential fields. Let $a, b \in E$ be differentially algebraic over F and $b \neq 0$. Then $a', a+b, ab, \frac{1}{b}$ are differentially algebraic over F.*

Proof. The statement of the proposition follows from Lemma 2.15 combined with the following transcendence degree bounds.

For a', since $F((a')^{(\infty)}) \subseteq F(a^{(\infty)})$, we have $\operatorname{trdeg}_F F((a')^{(\infty)}) \leqslant \operatorname{trdeg}_F F(a^{(\infty)})$.

For $a+b$, we have $F((a+b)^{(\infty)}) \subseteq F(a^{(\infty)}, b^{(\infty)})$, so

$$\operatorname{trdeg}_F F((a+b)^{(\infty)}) \leqslant \operatorname{trdeg}_F F(a^{(\infty)}) + \operatorname{trdeg}_F F(b^{(\infty)}) < \infty.$$

The cases ab and $\frac{1}{b}$ are left as Exercise 2.9. □

Remark 2.18. The proof of Proposition 2.17 implies that if the orders of the minimal differential polynomials of a and b do not exceed h_1 and h_2, respectively, then the order of the minimal differential polynomial for $a+b$ (resp., ab) does not exceed $h_1 + h_2$.

2.4 Exercises

Exercise 2.1. Consider the function $y(t) = \sum\limits_{i=0}^{\infty} (-1)^i i! t^i$ from Example 2.6. Find a nonzero element $\mathbb{C}[y^{(\infty)}]$ vanishing at this power series.

Exercise 2.2 (Due to Yu.P. Razmyslov)**.** For every integers $n > 1$ and $0 \leqslant a_1 < a_2 < \ldots < a_n$, consider

$$P := \det \begin{vmatrix} x_1^{(a_1)} & x_2^{(a_1)} & \ldots & x_n^{(a_1)} \\ x_1^{(a_2)} & x_2^{(a_2)} & \ldots & x_n^{(a_2)} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{(a_n)} & x_2^{(a_n)} & \ldots & x_n^{(a_n)} \end{vmatrix} \in \mathbb{Q}[x_1^{(\infty)}, \ldots, x_n^{(\infty)}].$$

Prove that $P \in \sqrt{\langle \operatorname{Wronsk}(x_1, \ldots, x_n) \rangle^{(\infty)}}$.

(Hint: use the approach from Lemma 2.5)

Exercise 2.3.** In the notation of the previous exercise, find

- the degree N such that $P^N \in \langle \operatorname{Wronsk}(x_1, \ldots, x_n) \rangle^{(\infty)}$;
- the minimal order H such that $P^N \in \langle \operatorname{Wronsk}(x_1, \ldots, x_n)^{(\leqslant H)} \rangle$;
- the expression of P^N as an element of $\langle \operatorname{Wronsk}(x_1, \ldots, x_n)^{(\leqslant H)} \rangle$.

See the notebook `https://github.com/pogudingleb/DifferentialAlgebra/blob/main/example/Wronskian_Schur.ipynb` for some experimental results for the first question.

Exercise 2.4. Analyze the proof of Theorem 2.8 and show that every differentially finitely generated $\mathbb{C}$-algebra has a homomorphism to the differential ring of *differentially-algebraic* convergent power series.

Exercise 2.5. For every positive integer n, construct a simple differential $\mathbb{C}$-algebra of transcendence degree n.

Exercise 2.6. Construct a differentially finitely generated $\mathbb{C}$-algebra A such that there is no injective differential homomorphism $A \to \mathbb{C}[\![t]\!]$.

Exercise* 2.7 (Convergence in dimension one, following [2])**.**

1. Let $A \subset B \subset C$ be $\mathbb{C}$-algebras such that A and C are finitely generated an $\operatorname{trdeg}_{\mathbb{C}} A = \operatorname{trdeg}_{\mathbb{C}} B = \operatorname{trdeg}_{\mathbb{C}} C = 1$. Prove that B is finitely generated as well.

2. Let A be a differentially finitely generated $\mathbb{C}$-algebra such that $\operatorname{trdeg}_{\mathbb{C}} A = 1$. Prove that, for every differential homomorphism $\Phi\colon A \to \mathbb{C}[\![t]\!]$, we have $\Phi(A) \subset \mathbb{C}\{t\}$.

Exercise 2.8.** Let A be a differentially finitely generated $\mathbb{C}$-algebra with $\operatorname{trdeg}_{\mathbb{C}} A < \infty$. Consider the set X of all points in $\operatorname{spec}_{\mathbb{C}} A$ defining divergent power series solutions. Is it true that X is conatained in a subvariety of codimension two? Is X always a constructible set?

Exercise 2.9. Finish the proof of Proposition 2.17.

Exercise 2.10. Show that the order bound from Remark 2.18 is tight in the following sense: for every h_1, h_2, there exist differential algebraic $f_1, f_2 \in \mathbb{C}[\![t]\!]$ such that the order of the minimal differential polynomial for f_i is h_i for $i = 1, 2$ and the order of the minimal polynomial for $f_1 f_2$ is $h_1 + h_2$.

Exercise 2.11. Let $f, g \in \mathbb{C}[\![t]\!]$ be differentially algebraic power series such that $f(0) = 0$. Show that $g(f(t))$ is also differentially algebraic. If the orders of the minimal polynomials of f and g are h_1 and h_2, respectively, what can be said about the order of the minimal polynomial for $g(f(t))$?

Exercise 2.12. Let $F \subset E$ be an extension of differential fields and $a, b \in E$. Show that, if a is differentially algebraic over F and b is differentially algebraic over $F(a^{(\infty)})$, then b is differentially algebraic over F.

Exercise 2.13. Let $F \subset E$ be an extension of differential fields. Let $a \in E$ be a differentially-algebraic over F, and set $d := \operatorname{trdeg}_F F(a^{(\infty)})$. Let $\mathcal{I}$ be the set of all d-element subsets $\{h_1, \ldots, h_d\}$ of $\mathbb{Z}_{\geqslant 0}$ such that $a^{(h_1)}, \ldots, a^{(h_d)}$ are algebraically independent.

1. Give an example of a such that $\mathcal{I}$ consists of $\{0, 1, \ldots, d-1\}$ only.

2. Give an example of a such that $\mathcal{I}$ consists of all d-element subsets of $\mathbb{Z}_{\geqslant 0}$.

Exercise 2.14. In the notation of Exercise 2.13, show that for $d = 1$ the set $\mathcal{I}$ is always of the form $\{\{0\}, \{1\}, \{2\}, \ldots, \{N\}\}$ for some N, and every nonnegative N is possible.

Exercise 2.15.** In the notation of Exercise 2.13, describe what $\mathcal{I}$ can look like.

References

[1] T. Arakawa, K. Kawasetsu, and J. Sebag. A question of Joseph Ritt from the point of view of vertex algebras, 2020. URL https://arxiv.org/abs/2009.04615.

[2] O. V. Gerasimova and Y. P. Razmyslov. Nonaffine differential-algebraic curves do not exist. *Moscow Univ. Math. Bull.*, 72:89–93, 2017. URL https://doi.org/10.3103/S0027132217030019.

[3] O. V. Gerasimova, Y. P. Razmyslov, and G. A. Pogudin. Rolling simplexes and their commensurability III (Capelli identities and their application to differential algebras). *Journal of Mathematical Sciences*, 221:315–325, 2017. URL https://doi.org/10.1007/s10958-017-3229-3.

[4] Z. Jelonek. On the effective Nullstellensatz. *Inventiones mathematicae*, 162(1):1–17, 2005. URL https://doi.org/10.1007/s00222-004-0434-8.

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

[6] S. Lang. Hilbert's Nullstellensatz in infinite-dimensional space. *Proceedings of the American Mathematical Society*, 3(3):407, 1952. URL https://doi.org/10.2307/2031893.

[7] M. Loday-Richaud. Divergent series and differential equations, 2014. URL https://hal.archives-ouvertes.fr/hal-01011050/document.

[8] A. Ovchinnikov, A. Pillay, G. Pogudin, and T. Scanlon. Computing all identifiable functions for ODE models, 2020. URL https://arxiv.org/abs/2004.07774.

[9] G. Pogudin. Primary differential nil-algebras do exist. *Moscow University Mathematics Bulletin*, 69(1):33–36, 2014. URL http://dx.doi.org/10.3103/S0027132214010069.