Differential equations from the algebraic standpoint

Gleb Pogudin

September 1, 2024

These are the lecture notes accompanying mini-course "Differential equations from the algebraic standpoint" given within the Welcome days for the "Mathematics and Applications" Master's program at Institut de Mathématiques d'Orsay on September 2-3, 2024.

Introduction

Differential algebra is a branch of algebra aimed at studying differential equations inspired by the way algebraic geometry is used to analyze polynomial equations. The notes bluntly borrow the title from one of the foundational books [1] on the topic by J. Ritt.

[1] Joseph Fels Ritt. *Differential equations from the algebraic standpoint*. American Mathematical Society, 1932. ISBN 978-0821846056. URL `https://archive.org/details/differentialequa033050mbp`

The main question we will study in these notes is: *given a system of differential equations, when it has any solution at all?* In the case of polynomial equations, one possible answer is given by celebrated Hilbert's Nullstellensatz, and we will establish several analogues of it in the differential world.

Prelude: polynomial equations and Hilbert's Nullstellensatz

Consider polynomials $p_1, \ldots, p_m \in \mathbb{C}[x_1, \ldots, x_n]$ and a system of polynomial equations

$$p_1(\mathbf{x}) = 0, \quad p_2(\mathbf{x}) = 0, \quad \ldots, \quad p_m(\mathbf{x}) = 0. \tag{1}$$

We would like to establish a criterion for (1) to have a solution.

Example 1. Consider a bivariate system

$$p_1(x_1, x_2) = x_1^2 + x_1x_2 + x_2^2 = 0, \quad p_2(x_1, x_2) = x_1^3 - x_2^3 - 1 = 0.$$

We can combine the equations as follows:

$$0 = (x_1 - x_2)p_1(x_1, x_2) - p_2(x_1, x_2) = (x_1^3 - x_2^3) - (x_1^3 - x_2^3 - 1) = 1.$$

Since an impossible equality $0 = 1$ can be obtained by combining the equations, we conclude that the system does not have solutions in $\mathbb{C}$.

We generalize the example by associating, to the system (1), an ideal in the polynomial ring $\mathbb{C}[\mathbf{x}]$:

$$\langle p_1, \ldots, p_m \rangle := \{f_1p_1 + \ldots + f_mp_m \mid f_1, \ldots, f_m \in \mathbb{C}[\mathbf{x}]\} \subset \mathbb{C}[\mathbf{x}].$$

Elements of the ideal can be though of as "consequences" of (1), the following lemma makes this precise.

Lemma 1. *Let $R \supset \mathbb{C}$ by any ring containing $\mathbb{C}$. Let $\mathbf{x}^* \in R^n$ satisfy $p_1(\mathbf{x}^*) = \ldots = p_m(\mathbf{x}^*) = 0$. Then, for every $p \in \langle p_1, \ldots, p_m \rangle$, we have $p(\mathbf{x}^*) = 0$.*

Proof. Consider $p \in \langle p_1, \ldots, p_m \rangle$. There exist $f_1, \ldots, f_m \in \mathbb{C}[\mathbf{x}]$ such that

$$p = f_1 p_1 + \ldots + f_m p_m.$$

If we substitute $\mathbf{x} = \mathbf{x}^*$, the right-hand side will vanish, so will p. □

It turns out that the ideal $\langle p_1, \ldots, p_m \rangle$ may unearth a natural obstacle for the system to have a solution.

Proposition 1 (pre-Nullstellensatz)**.** *There exist a ring $R \supset \mathbb{C}$ and a tuple $\mathbf{x}^* \in R^n$ such that $p_1(\mathbf{x}^*) = \ldots = p_m(\mathbf{x}^*) = 0$ if and only if $1 \notin \langle p_1, \ldots, p_m \rangle$.*

Proof. We denote $I := \langle p_1, \ldots, p_m \rangle$. Assume that $1 \in I$. Then Lemma 1 implies that the polynomial 1 would vanish on every solution of (1) in any ring $R \supset \mathbb{C}$. Thus, there are no such solution.

Assume that $1 \in I$. We consider the quotient ring $R := \mathbb{C}[\mathbf{x}]/I$. We denote the image of $\mathbf{x}$ in R by $\mathbf{x}^*$. Since, for every $1 \leqslant i \leqslant m$, $p_i \in I$, we have $p_i(\mathbf{x}^*) = 0$. So we have constructed the desired solution. □

Exercise 1. Show that Proposition 1 still holds if R is assumed to be a field, not a ring[2].

[2] Hint: take the quotient with repspect to a maximal ideal containing I

The proof of Proposition 1 also offer a new point of view on the notion of solution which will be very useful for us, so we also state it as a lemma.

Lemma 2. *Let $p_1, \ldots, p_m \in \mathbb{C}[\mathbf{x}]$. Let $\varphi \colon \mathbb{C}[\mathbf{x}] \to R$ be a homomorphism to a $\mathbb{C}$-algebra R such that $\langle p_1, \ldots, p_m \rangle \subset \operatorname{Ker} \varphi$. Then $\varphi(x_1), \ldots, \varphi(x_n)$ is a solution of $p_1(\mathbf{x}) = \ldots = p_m(\mathbf{x}) = 0$ in R.*

While Proposition 1 gives us some information about the existence of solutions, it may be not very satisfactory since one is typically interested in solving (1) in $\mathbb{C}$, not in some arbitrary ring. And the celebrated Hilbert's Nullstellensatz (its weak form) states that one can replace R with $\mathbb{C}$ in Proposition 1.

Theorem 1 (weak Nullstellensatz)**.** *System* (1) *has a solution in $\mathbb{C}^n$ if and only if $1 \notin \langle p_1, \ldots, p_m \rangle$.*

Proof. [3] If $1 \in \langle p_1, \ldots, p_m \rangle$, then the system does not have a solution by Proposition 1. Assume that $1 \notin \langle p_1, \ldots, p_m \rangle =: I$. Let $\mathfrak{m}$ be a maximal ideal containing I, and define $R := \mathbb{C}[\mathbf{x}]/\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, R is a field. If $R = \mathbb{C}$, then we get a solution by Lemma 2. Otherwise, we choose $a \in R \setminus \mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, a is

[3] While the theorem remains true if $\mathbb{C}$ is replaced by any algebraically closed field, the proof uses the uncountablity of $\mathbb{C}$. Proofs not relying on this assumption are typically longer.

transcendental[4] over $\mathbb{C}$. Consider a set $\Lambda := \{\frac{1}{a-\alpha} \mid \alpha \in \mathbb{C}\}$. Elements of Λ are linearly independent over $\mathbb{C}$: indeed, any dependence of the form

$$\lambda_1 \frac{1}{a-\alpha_1} + \ldots + \lambda_N \frac{1}{a-\alpha_N} = 0$$

would, after multiplying by $\prod_{i=1}^{N}(a-\alpha_i)$, yield a polynomial equation[5] for a over $\mathbb{C}$. Linear independence of the elements of Λ implies that the dimension of R over $\mathbb{C}$ is uncountable. However, the dimension of $\mathbb{C}[\mathbf{x}]$ over $\mathbb{C}$ is countable, so we arrive at a contradiction with the assumption $R \neq \mathbb{C}$. □

[4] that is, a does not satisfy any polynomial equation with coefficients in $\mathbb{C}$

[5] *Question:* why would this equation be nonzero?

Exercise 2. Show that Theorem 1 does not hold if $\mathbb{C}$ is replaced with $\mathbb{R}$.

Why is the criterion provided by Theorem 1 useful? On the theoretical side, it allows to establish correspondence between solution sets and ideals (so-called strong Nulstellensatz) because it basically says that any nontrivial ideal must correspond to at least one point. From more computational point of view, the condition $1 \in \langle p_1, \ldots, p_m \rangle$ is well-suited to be checked algorithmically. In particular, it operates in the field generated by the coefficients of the system and does not require any approximate numerical computations which may associate with nonlinear system solving. Perhaps, the most popular way to do this would be using Gröbner bases [6] which are beyond the scope of the present note. A more theoretical algorithm can be obtained from the following bound [7].

[6] Bernd Sturmfels. What is ... gröbner basis? *Notices of American Mathematical Society*, 52(10):1199–1203, 2005. URL https://math.berkeley.edu/~bernd/what-is.pdf

[7] János Kollár. Sharp effective Nullstellensatz. *Journal of the American Mathematical Society*, 1(4):963, October 1988. URL http://dx.doi.org/10.2307/1990996

Theorem 2 (Effective Nullstellensatz)**.** *For every $1 \leqslant i \leqslant n$, we denote $d_i := \deg p_i$. Assume that the system* (1) *does not have solutions in $\mathbb{C}^n$. Then there exist $f_1, \ldots, f_m \in \mathbb{C}[\mathbf{x}]$ such that*

$$f_1 p_1 + \ldots + f_m p_m = 1 \tag{2}$$

and $\deg f_i \leqslant \prod_{i=1}^{m} d_i$.

Indeed, thanks to such degree bound, one can write $f_1, \ldots, f_m$ with undetermined coefficients, and (2) will become a system of linear equations on these coefficients. The proof of the bound is quite nontrivial, we will show how one can much easier establish the existence of such a bound.

We finish this section with a version [8] of Theorem 1 due to S. Lang [9] which we will use as a tool in the differential case.

[8] Unlike Theorem 1, this theorem is true only for uncountable fields. Luckily, $\mathbb{C}$ is still fine.

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

Theorem 3 (Countable weak Nullstellensatz)**.** *Let I be an ideal in a polynomial ring $\mathbb{C}[x_1, x_2, \ldots]$ in countably many variables. Then the ideal has a solution in $\mathbb{C}$ if and only if $1 \notin I$.*[10]

[10] *Question:* does the proof of Theorem 1 work for this statement?

Setting up the scene: differential rings, fields, ideals

TO ADAPT THIS APPROACH TO THE DIFFERENTIAL SETTING, we need to define some structures where the coefficients, solutions, and equations will live. For the coefficients and solutions, the relevant notions are differential rings and fields.

Definition 1 (Differential rings, fields, and algebras)**.** Let R be a commutative ring. An additive map $\delta\colon R \to R$ is called *a derivation*[11] if it satisfies the Leibniz rule:

$$\delta(ab) = \delta(a)b + a\delta(b) \quad \text{for every } a, b \in R.$$

A commutative ring equipped with a derivation is called *a differential ring*. If the ring is a field, it is called *a differential field*. If a differential ring R_1 is an algebra over its differential subring R_0, then we say that R_1 is *a differential R_0-algebra*.

For differential rings R_1 and R_2 with the derivations δ_1 and δ_2, a ring homomorphism $\varphi\colon R_1 \to R_2$ is called a *differential homomorphism* is $\varphi \circ \delta_1 = \delta_2 \circ \varphi$.

Example 2.

- Any ring can be turned into a differential ring with respect to the zero derivation (that is, $a' = 0$ for every $a \in R$).
- The ring of polynomials $\mathbb{C}[x]$ is a differential ring with respect to the standard derivation $\frac{\mathrm{d}}{\mathrm{dx}}$. Similarly, the field of rational functions $\mathbb{C}(x)$ is a differential field. Furthermore, both of them are differential $\mathbb{C}$-algebras.
- Consider any domain[12] $\mathcal{D} \subset \mathbb{C}$. Then the sets of holomorphic and meromorphic functions on it are differential rings with respect to the standard derivation $\frac{\mathrm{d}}{\mathrm{dz}}$.

Exercise 3. Which or the following rings are differential rings with respect to the standard derivation? Differential fields?

1. meromorphic functions on a domain $\mathcal{D} \subset \mathbb{C}$;
2. meromorphic functions in an open[13] set $U \subset \mathbb{C}$;
3. $\mathcal{C}^1$ functions on an interval $[a, b]$;
4. $\mathcal{C}^\infty$ functions on an interval $[a, b]$.

Now we can define the ring of differential polynomials where the nonlinear differential equations will live.

[11] We will typically denote $\delta(a)$ by a' and, for $n \geqslant 0$, $\delta^n(a)$ by $a^{(n)}$.

[12] That is, an open and connected set.

[13] But not necessarily connected!

Definition 2 (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 analogously.

Example 3. The equation $x'(t) = x(t)$ defining the exponential function can be written as a differential polynomial $x' - x \in \mathbb{C}[x^{(\infty)}]$.

Exercise 4. The Wronskian determinant of functions x_1 and x_2

$$\begin{vmatrix} x_1 & x_2 \\ x_1' & x_2' \end{vmatrix} = x_1 x_2' - x_1' x_2$$

is an element of the differential polynomial ring $\mathbb{C}[x_1^{(\infty)}, x_2^{(\infty)}]$.

Definition 3 (Differential ideal)**.** An ideal I in a differential ring is called *a differential ideal* if $a' \in I$ for evey I.

For elements $a_1, \ldots, a_m \in R$, the minimal differential ideal containing them is an ideal generated by $a_1^{(\infty)}, \ldots, a_m^{(\infty)}$ and will be denoted by $\langle a_1, \ldots, a_m \rangle$.

Example 4. Consider $x' - x \in \mathbb{C}[x^{(\infty)}]$. The differential ideal defined by it $\langle x' - x \rangle^{(\infty)}$ is generated as an ideal by $x^{(i+1)} - x^{(i)}$ for all $i \geqslant 0$.

Exercise 5. Define a nonzero derivation on $\mathbb{C}[x]$ such that the ideal $\langle x \rangle$ is differential.[14]

[14] Hint: any map of the form $p(x)\frac{\mathrm{d}}{\mathrm{d}x}$ is a derivation.

Since a differential ideal is closed under derivation, the quotient ring is naturally equipped with derivation by taking the derivative of a class $a + I$ to be the class of $a' + I$.[15]

[15] *Question:* why doesn't this definition depend on the representative of $a + I$?

Example 5. Describe the quotient ring $\mathbb{C}[x^{(\infty)}]/\langle x' - x \rangle^{(\infty)}$ (cf. Example 4) and the derivation on it.

Example 6. This is a differential version of Example 1 we started with. Consider a system of differential equations:

$$p_1(x) = x' - x = 0, \quad p_2(x) = x' - 1 = 0.$$

The solutions of the first equation in the ring of analytic functions are of the form αe^t, and none of these functions satisfy the second equation, so there are no analytic solutions.

We can say more by combining the equations as follows:

$$0 = p_1' - p_2' + p_2 = (x'' - x') - x'' + (x' - 1) = -1. \tag{3}$$

Since we obtained an impossible equality $0 = -1$, the original system could not have a solution in any differential $\mathbb{C}$-algebra, not just in analytic functions.

Exercise 6. Find a combination of the type (3) for $p_1(x) = x' - x$ and $p_2(x) = x^{(\ell)} - 1$.

We are now in the position to formulate and prove this first, "boring", Nullstellensatz, the differential analogue of Proposition 1.

Proposition 2. *Let $p_1, \ldots, p_n \in \mathbb{C}[\mathbf{x}^{(\infty)}]$ be differential polynomials. Then the system $p_1(\mathbf{x}) = \ldots = p_m(\mathbf{x}) = 0$ has a solution in some differential $\mathbb{C}$-algebra R if and only if $1 \notin \langle p_1, \ldots, p_m \rangle^{(\infty)}$.*

Proof. Assume that the system has a solution $\mathbf{x}^* \in R^n$ in a differential ring R but $1 \in \langle p_1, \ldots, p_m \rangle^{(\infty)}$. The latter implies that there exist an integer ℓ and $a_{i,j}(\mathbf{x}) \in \mathbb{C}[\mathbf{x}^{(\infty)}]$ with $1 \leqslant i \leqslant m$ and $0 \leqslant j \leqslant \ell$ such that

$$1 = \sum_{i=1}^{m} \sum_{j=0}^{\ell} a_{i,j}(\mathbf{x})(p_i(\mathbf{x}))^{(j)}.$$

We plug $\mathbf{x}^*$ into the right-hand side of this equality. Since $p_i(\mathbf{x}^*) = 0$, the same is true for $(p_i(\mathbf{x}))^{(j)}$ for every j. So the right-hand side is equal to zero, and we arrive at a contradiction which proves the implication.

In the other direction, we assume that $1 \notin I := \langle p_1, \ldots, p_m \rangle^{(\infty)}$. Since I is a differential ideal, the image of derivation on $\mathbb{C}[\mathbf{x}^{(\infty)}]$ is well-defined in $R := \mathbb{C}[\mathbf{x}^{(\infty)}]/I$. Therefore, the natural projection $\mathbb{C}[\mathbf{x}^{(\infty)}] \to R$ is a homomorphism of differential rings. So we can take the image of $\mathbf{x}$ under this homomorphism to be a solution of the system in R. $\square$

Algebraic life of the Taylor formula

Again, the solvability criterion given by Proposition 2 may not look that spectacular since it allows to ensure the existence of solution only in *some differential ring*. Similarly to the Hilbert's Nullstellensatz (Theorem 1), we will show that one can replace R with a very particular differential ring.

Theorem 4 (Differential Nullstellensatz, power series version)**.** *Let $p_1, \ldots, p_n \in \mathbb{C}[\mathbf{x}^{(\infty)}]$ be differential polynomials. Then the system $p_1(\mathbf{x}) = \ldots = p_m(\mathbf{x}) = 0$ has a solution in the power series ring $\mathbb{C}[\![t]\!]$ if and only if $1 \notin \langle p_1, \ldots, p_m \rangle^{(\infty)}$.*

Proof. One direction (the existence of solution implies $1 \notin \langle p_1, \ldots, p_m \rangle^{(\infty)}$) follows from Proposition 2.

Assume that $1 \notin I := \langle p_1, \ldots, p_m \rangle^{(\infty)}$. Let us look at I as an ideal in a polynomial ring in countably many variables. Countable Nullstellensatz (Theorem 3) implies that this ideal has a solution (as an algebraic ideal) in $\mathbb{C}$. In other words, there exists a homomorphism (non-differential!) from a differential $\mathbb{C}$-algebra $R := \mathbb{C}[\mathbf{x}^{(\infty)}]/I$ to $\mathbb{C}$, we denote it by φ. We define a new map $\Phi \colon R \to \mathbb{C}[\![t]\!]$ by the formula[16]

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

[16] Which is simply the Taylor series!

for every $a \in R$. This map is clearly $\mathbb{C}$-linear. In order to show that it is a homomorphism, consider $a, b \in R$. Then

$$\Phi(ab) = \sum_{i=0}^{\infty} \varphi((ab)^{(i)}) \frac{t^i}{i!} = \sum_{i=0}^{\infty} \sum_{j=0}^{i} \binom{i}{j} \varphi(a^{(j)}) \varphi(b^{(i-j)}) \frac{t^i}{i!} =$$
$$= \sum_{i=0}^{\infty} \sum_{j=0}^{i} \left(\varphi(a^{(j)}) \frac{t^j}{j!} \right) \left(\varphi(b^{(i-j)}) \frac{t^{i-j}}{(i-j)!} \right) = \Phi(a)\Phi(b).$$

Finally, in order to show that this is a *differential* homomorphism, we take $a \in R$ and see that

$$\Phi(a') = \sum_{i=0}^{\infty} \varphi(a^{(i+1)}) \frac{t^i}{i!} = \frac{\mathrm{d}}{\mathrm{dt}} \left(\sum_{i=0}^{\infty} \varphi(a^{(i)}) \frac{t^i}{i!} \right) = \frac{\mathrm{d}}{\mathrm{dt}} \Phi(a).$$

Thus, we have constructed a differential homomorphism $R \to \mathbb{C}[\![t]\!]$. Composing it with the natural projection $\mathbb{C}[\mathbf{x}^{(\infty)}] \to R$, we obtain a differential homomorphism $\mathbb{C}[\mathbf{x}^{(\infty)}] \to \mathbb{C}[\![t]\!]$ such that $p_1, \ldots, p_m$ belong to its kernel. Therefore, the images of $\mathbf{x}$ under this homomorphism will provide a solution in $\mathbb{C}[\![t]\!]$. $\square$

The way we used the Taylor formula to convert an arbitrary homomorphism to $\mathbb{C}$ into a differential homomorphism to $\mathbb{C}[\![t]\!]$ will be used later, so we will state it as a separate lemma.

Lemma 3 (Taylor homomorphism)**.** *Let R be a differential $\mathbb{C}$-algebra and $\varphi \colon R \to \mathbb{C}$ be a (non-differential) $\mathbb{C}$-homomorphism. Then the map $\Phi \colon R \to \mathbb{C}[\![t]\!]$ defined by*

$$\Phi(a) := \sum_{i=0}^{\infty} \varphi(a^{(i)}) \frac{t^i}{i!} \quad \textit{for every } a \in R$$

is a homomorphism of differential $\mathbb{C}$-algebras.

Example 7. Consider a differential equation $x' - x = 0$. The corresponding differential ideal $\langle x' - x \rangle^{(\infty)} \subset \mathbb{C}[x^{(\infty)}]$ is generated by $x' - x, x'' - x', x^{(3)} - x'', \ldots$. Consider any $\mathbb{C}$-homomorphism $\varphi \colon \mathbb{C}[x^{(\infty)}]/\langle x' - x \rangle \to \mathbb{C}$. Then all numbers $\varphi(x), \varphi(x'), \varphi(x''), \ldots$

must be equal to the same complex number, denote it by α. Then we have

$$\Phi(x) = \sum_{i=0}^{\infty} \varphi(x^{(i)}) \frac{t^i}{i!} = \alpha \sum_{i=0}^{\infty} \frac{t^i}{i!} = \alpha e^t.$$

This gives us exactly the power series solutions of the original equation $x' - x = 0$.

Corollary 1. *Let R be a differentially finitely generated $\mathbb{C}$-algebra. Then there exists a differential homomorphism $R \to \mathbb{C}[[t]]$.*

Proof. First, we note that the proof of Theorem 4 works for any differential ideal, not necessarily generated by finitely many elements. Assume that R is differentially generated by elements $a_1, \ldots, a_n \in R$. Consider a differential homomorphism $\pi\colon \mathbb{C}[\mathbf{x}^{(\infty)}] \to R$, where $\mathbf{x} = (x_1, \ldots, x_n)$ and $\pi(x_i) = a_i$ for every $1 \leqslant i \leqslant n$. Then we apply Theorem 4 to the kernel of π and obtain a homomorphism $\mathbb{C}[\mathbf{x}^{(\infty)}] \to \mathbb{C}[[t]]$ whose kernel contains $\operatorname{Ker} \pi$, so this homomorphism canbe factored through R yielding a desired differential homomorphism $R \to \mathbb{C}[[t]]$. $\square$

Let's converge, or Ritt's theorem of zeroes

At the moment, Theorem 4 states that the fact that one is not in the differential ideal guarantees an existence of a power series solution. However, power series solutions of a differential equation may have zero radius of convergence and, thus, not define an "honest" function. In this section we will prove the theorem due to Ritt showing that, if there is a power series solution, there is one with nonzero radius of convergence.

Theorem 5 (Ritt's theorem of zeroes)**.** *Let $p_1, \ldots, p_n \in \mathbb{C}[\mathbf{x}^{(\infty)}]$ be differential polynomials. Then the system $p_1(\mathbf{x}) = \ldots = p_m(\mathbf{x}) = 0$ has a power series solution with nonzero convergence radius if and only if $1 \notin \langle p_1, \ldots, p_m \rangle^{(\infty)}$.*

The plan of the proof is the following:

1. We start with taking a maximal differential ideal J containing $p_1, \ldots, p_m$ and consider the differential quotient ring[17] $R := \mathbb{C}[\mathbf{x}^{(\infty)}]/J$.
2. The maximality of J implies that R does not have proper differential ideals. For such a ring we prove that it is a domain (Lemma 4) and it is "small" (Lemma 7).
3. Finally we show that an differential $\mathbb{C}$-algebra with these properties can be embedded into an algebra for which all the homomrphisms to $\mathbb{C}[[t]]$ have nonzero radius of convergence.

[17] It does not have to be a field anymore!

Lemma 4. *Let R be a differentially finitely generated $\mathbb{C}$-algebra without proper differential ideals. Then R does not have zero divisors.*

Proof. Corollary 1 implies that there is a differential homomorphism $R \to \mathbb{C}[\![t]\!]$. Since R does not have proper differential ideals, this homomorphism is an embedding. Since $\mathbb{C}[\![t]\!]$ does not have zero divisors, the same is true for R. □

Now we will prove an important structure theorem for differential algebras. It will use the notion of *localization*, that is, adjoining an inverse of an element to a ring: for a ring R and an element $a \in R$ which is not a zero divisor, we can construct a ring $R\left[\frac{1}{a}\right]$ by adjoining the inverse[18]. Geometrically, taking localization means "prohibiting" homomorphisms (and, thus, solutions) vanishing at a. The following lemma shows that localication behaves naturally with respect to differentiation.

[18] For example, Laurent series is a localization of power series $\mathbb{C}[\![t]\!]$ with respect to t. Check this!

Lemma 5 (Differentiation and localization)**.** *Let R be a differential ring without zero divisors and $a \in R$ be a nonzero element. Then there is a unique way to extend the derivation from R to $R[1/a]$ given by formula*

$$\left(\frac{b}{a^k}\right)' = \frac{ab' - ka'b}{a^{k+1}} \quad \textit{for every } b \in R.$$

Proof. The lemma is proved by direct computation. One can check that the formula defines a map on $R[1/a]$ (that is, does not depend on the choice of the representative of the form $\frac{b}{a^k}$). Then the Leibniz rule is easily verified. Finally, the uniqueness follows from differentiating the equality $1 = \frac{b}{a^k} \cdot a^k$. □

Definition 4 (Differential algebraicity and transcendence)**.** Let R be a differential ring and $S \subset T$ its differential subring. Element $a_1, \ldots, a_\ell \in R$ are called *differentially dependent* over S if there exists a nonzero $p \in S[x_1^{(\infty)}, \ldots, x_\ell^{(\infty)}]$ such that $p(a_1, \ldots, a_\ell) = 0$.

If no such p exists, $a_1, \ldots, a_\ell$ are called *differentially transcendental* over S.

Example 8. Let R be the ring of meromorphic functions on the complex plane. Then $e^z \in R$ is differentially algebraic because it is a zero if $x' - x$.

On the other hand, the Hölder's theorem[19] says that the Gamma function $\Gamma(z) \in R$ is differentially transcendental over $\mathbb{C}$.

[19] Eliakim Moore. Concerning transcendentally transcendental functions. *Mathematische Annalen*, 48:49–74, 1897. URL http://eudml.org/doc/157810

Exercise 7. Prove (without using Hölder's theorem above) that there exists a power series differentially transcendental over $\mathbb{C}$.

Theorem 6. *(cf. Statement 5 in [20]) Let R be a differentially finitely generated $\mathbb{C}$-algebra without zero divisors. Then there exist $a_1, \ldots, a_\ell \in R$*

[20] D. V. Trushin. Inheritance of properties of spectra. *Mathematical Notes*, 88(5–6):868–878, December 2010. URL http://dx.doi.org/10.1134/S0001434610110271

differentially transcendental over $\mathbb{C}$ *and an element* $b \in R$ *such that the differential algebra* $R[1/b]$ *(differential by Lemma 5) is finitely generated (as a non-differential algebra) over* $\mathbb{C}[a_1^{(\infty)}, \ldots, a_\ell^{(\infty)}]$.

The proof of the theorem will use the following lemma which could be nominated to be considered the most important lemma in differential algebra.

Lemma 6 (Really important lemma). *Let* R *be a differential ring and let* $P(x) \in R[x^{(\infty)}]$ *be a differential polynomial. Let* h *be the order of* P*, that is, the largest integer such that* $x^{(h)}$ *appears in* P*. We define* $S := \frac{\partial P}{\partial x^{(h)}}$ *(called* the separant *of* P*). Then, for every* $i > 0$*, there exists* $Q \in R[x^{(<h+i)}]$ *such that*

$$(P(x))^{(i)} = S(x)x^{(h+1)} + Q(x).$$

Proof. We will prove this by induction on i. For $i = 1$, using the chain rule, we have:

$$P(x)' = \sum_{j=0}^{h} x^{(j+1)} \frac{\partial P}{\partial x^{(j)}}.$$

So we can set $Q_1(x) := \sum\limits_{j=0}^{h-1} x^{(j+1)} \frac{\partial P}{\partial x^{(j)}}$ and have

$$P(x)' = S(x)x^{(h+1)} + Q_1(x).$$

Assume that we have

$$P(x)^{(i)} = S(x)x^{(h+i)} + Q_i(x), \quad \text{where } Q_i \in R[x^{(<h+i)}]$$

We differentiate this:

$$P(x)^{(i+1)} = S(x)x^{(h+1)} + \underbrace{S(x)'x^{(h+1)} + Q_i(x)'}_{=:Q_{i+1}(x)}.$$

This proves the induction step. □

Proof of Theorem 6. Let $a_1, \ldots, a_N$ be a set of generators of R as a differential $\mathbb{C}$-algebra. By reordering the generators if necessary, we will further assume that $a_1, \ldots, a_\ell$ is a maximal (with respect to inclusion) differentially transcendental set. Let $R_0 := \mathbb{C}[a_1^{(\infty)}, \ldots, a_\ell^{(\infty)}]$.

Consider $\ell < i \leqslant N$. Since $a_1, \ldots, a_\ell, a_i$ are not differentially transcendental, there exists nonzero $P(x) \in R_0[x^{(\infty)}]$ such that $P(a_i) = 0$. We will pick such P of the smallest possible order in x and, among the ones of smallest possible order, of smallest possible total degree. Denote the order of P by h_i, then $P \in R_0[x, \ldots, x^{(h_i)}]$. We define $\frac{\partial P}{\partial x^{(h_i)}}$. The minimality of P implies that $s_i := S(a_i) \neq 0$. We will prove that

$$R_0[a_i^{(\infty)}] \subset R_0[a_i^{(\leqslant h_i)}] \left[\frac{1}{s_i}\right], \tag{4}$$

We will prove this by proving

$$R_0[a_i^{(\leqslant M)}] \subset R_0[a_i^{(\leqslant h_i)}]\left[\frac{1}{s_i}\right].$$

for every M by induction on M. If $M \leqslant h_i$, the inclusion is clear. Assume that the inclusion has been established for some $M \geqslant h_i$. We differentiate $M + 1 - h_i$ times the equality $P(a_i) = 0$. By Lemma 6, we have:

$$0 = (P(a_i))^{(M+1-h_i)} = s_i a_i^{(M+1)} + Q(a_i^{(\leqslant M)}).$$

Then $a_i^{(M+1)} \in R_0[a_i^{(\leqslant M)}]\left[\frac{1}{s_i}\right]$, and this proves the induction step.

Now we set $s := s_{\ell+1} \ldots s_N$. Then (4) implies that

$$R \subset R_0[a_{\ell+1}^{(\leqslant h_{\ell+1})}, \ldots, a_N^{(\leqslant h_N)}]\left[\frac{1}{s}\right]$$

□

Lemma 7. *Let R be a differentially finitely generated $\mathbb{C}$-algebra without proper differential ideals. Then there exists $b \in R$ such that $R[1/b]$ is finitely generated $\mathbb{C}$-algebra.*

Proof. We apply Theorem 6 to R, and let $a_1, \ldots, a_\ell$, and b be the elements given by the theorem. It is sufficient to show that $\ell = 0$. Assume the contrary. Let $\mathbf{a} := (a_1, \ldots, a_\ell)$ and $R_1 := R[1/b]$. Note that R_1 also does not have any proper differential ideals. Furthermore, R_1 is finitely generated over $\mathbb{C}[\mathbf{a}^{(\infty)}]$. Let $c_1, \ldots, c_N$ be a generating set, so

$$R_1 = \mathbb{C}[\mathbf{a}^{(\infty)}][c_1, \ldots, c_N].$$

Since the ideal of algebraic relations between $c_1, \ldots, c_N$ over $\mathbb{C}(\mathbf{a}^{(\infty)})$ is finitely generated, one can choose integer H such that it involves only elements of $\mathbb{C}(\mathbf{a}^{(<H)})$. Then the elements $\mathbf{a}^{(\geqslant H)}$ are algebraically independent over $R_0 := \mathbb{C}[\mathbf{a}^{(<H)}][c_1, \ldots, c_N]$. Let $\varphi\colon R_0 \to \mathbb{C}$ be any homomorphism. The independence of $\mathbf{a}^{(\geqslant H)}$ allows to extend it to R_1 by setting $\varphi(a_i^{(H+j)}) = 0$ for every $1 \leqslant i \leqslant \ell$ and $j \geqslant 0$. Let $\Phi\colon R_1 \to \mathbb{C}[[t]]$ be the corresponding Taylor homomorphism from Lemma 3. Then $\operatorname{Ker}\Phi$ contains $a_1^{(H)}$, so it is a proper differential ideal in R_1. Since this is impossible, we conclude that $\ell = 0$. □

Lemma 8. *(Corollary 2.1 in [21]) Let R be a differential $\mathbb{C}$-algebra generated as an algebra by finitely many elements. Then, for every homomorphism $\varphi\colon R \to \mathbb{C}[[t]]$, there is a positive ε such that the radius of convergence of $\varphi(a)$ is at least ε for every $a \in R$.*

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

Proof. Let $b_1, \ldots, b_N$ be the generators of R. Then there exist polynomials $p_1, \ldots, p_N \in \mathbb{C}[x_1, \ldots, x_N]$ such that

$$b_i' = p_i(b_1, \ldots, b_N) \quad \text{for every } 1 \leqslant i \leqslant N.$$

Consider any differential homomorphism $\Phi\colon R \to \mathbb{C}[\![t]\!]$. Then the images $f_1(t) := \Phi(b_1), \ldots, f_N := \Phi(b_N)$ satisfy an ODE system

$$\begin{cases} y_1' = p_1(y_1, \ldots, y_n), \\ \vdots \\ y_N' = p_N(y_1, \ldots, y_N). \end{cases}$$

By the existence and uniqueness theorem for ODEs, this system has a unique power series solution with $y_i(0) = f_i(0)$ for every $1 \leqslant i \leqslant n$ which defines analytic functions in some neighbourhood of $t = 0$. Then $y_1 = f_1, \ldots, y_N = f_N$ is this solution, so $f_1, \ldots, f_N$ have positive radius of convergence. ☐

Example 9 (Could be divergent!)**.** Consider a system

$$p_1 := x' - 1 = 0, \quad p_2 := x^2 y' + y - x = 0.$$

One of its power series solutions is

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

This power series has zero convergence radius. How does this relate with Lemma 8 and Theorem 6. Lemma 8 implies that the quotient algebra $\mathbb{C}[x^{(\infty)}, y^{(\infty)}]/\langle p_1, p_2\rangle^{(\infty)}$ is not finitely generated[22]. Furthermore, if one follows the proof of Theorem 6, then the element b to invert will be $\frac{\partial p_2}{\partial y'} = x^2$. But inverting this element will precisely "prohibit" our divergent solution!

[22] Try to prove this directly: this is doable but not that easy; so we got an analytic proof of an algebraic fact by this!

Finally, we can put everything together and prove the Ritt's theorem of zeroes.

Proof of Theorem 5. Thanks to Theorem 4, it it sufficient to prove that $1 \notin \langle p_1, \ldots, p_m\rangle^{(\infty)}$ implies the existence of a locally converging solution. Let J be a differential maximal ideal of $\mathbb{C}[\mathbf{x}^{(\infty)}]$ containing $\langle p_1, \ldots, p_m\rangle^{(\infty)}$. Let $R := \mathbb{C}[\mathbf{x}^{(\infty)}]/J$ and define the canonical projection by $\pi\colon \mathbb{C}[\mathbf{x}^{(\infty)}] \to R$. Then R does not have zero divisors by Lemma 4. Then Lemma 7 implies that there is $b \in R$ such that $R[1/b]$ is finitely generated as a $\mathbb{C}$-algebra. Consider any differential homomorphism $\Phi\colon R[1/b] \to \mathbb{C}[\![t]\!]$ which exists by Corollary 1. Consider power series $f_1(t) := \Phi(\pi(x_1)), \ldots, f_n(t) := \Phi(\pi(x_n))$. Since $p_1, \ldots, p_m$ belong to the kernel of π, the tuple $(f_1, \ldots, f_n)$ is a solution of $p_1 = \ldots = p_m = 0$. Furthermore, by Lemma 8, these power series have poisitive radius of convergence. ☐