Lectures on

Computational Differential Algebra

Wei Li

December, 2019[1]

[1]Thanks Lei Fu for preparing the lecture notes in Latex.

Contents

Introduction

References:

(1) **An Introduction to Differential Algebra** by I. Kaplansky, 1957.

(2) **Differential Algebra** by J. F. Ritt, 1950.

(3) **Differential Algebra and Algebraic Groups** by E. R. Kolchin, 1973.

What is differential algebra? It is the subject studying algebraic differential equations from the algebraic standpoint.

Examples of algebraic differential equations:

(1) $\frac{\mathrm{d}^2y}{\mathrm{d}t^2} + 2\frac{\mathrm{d}y}{\mathrm{d}t} + 5y = 0$ (linear ordinary differential equation).

(2) $(\frac{\mathrm{d}y}{\mathrm{d}t})^2 - 4y = 0$ (nonlinear ordinary differential equation).

(3) Heat Equation: $\frac{\partial u}{\partial t} = \gamma(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2})$ (linear partial differential equation).

(4) KDV Equation: $\frac{\partial u}{\partial t} - \frac{\partial^3 u}{\partial x^3} - 6u\frac{\partial u}{\partial x} = 0$ (nonlinear partial differential equation).

In differential algebra, we are not interested in "solving". In fact, it is very hard to solve differential equations in closed form solutions and in general impossible. Our perspective is rather to study the solutions and their properties from an abstract, purely algebraic point of view. This subject enjoys many analogies with commutative algebra and algebraic geometry. Since polynomial equations are algebraic differential equations of order 0, differential algebra could be regarded as a generalization of classical algebraic geometry.

The main focus of this course is to study the set of solutions of a general system of differential polynomials in finitely many differential variables over a differential field. These solution sets are called *differential varieties*.

We address questions like:

(1) Can we replace an infinite system of algebraic differential equations by a finite system without changing the solutions? (*Ritt-Raudenbush basis theorem*)

(2) Decompose a system of algebraic differential equations into finitely many "irreducible" system?

(3) Give a criterion to test whether a system of differential equations have a solution or not? (*Differential Hilbert's Nullstellensatz*)

Chapter 1

Basic Notions of Differential Algebra

In this chapter, we introduce the very basic definitions and constructions of differential algebra and establish some first theorems concerning differential ideals.

1.1 Differential rings

All rings in this course are assumed to be commutative rings with unity 1.

Definition 1.1.1. *A derivation on a ring R is a map $\delta : R \to R$ s.t. for $\forall\, a, b \in R$,*

1) $\delta(a+b) = \delta(a) + \delta(b)$*;*

2) (Leibniz rule) $\delta(ab) = \delta(a)b + a\delta(b)$.

In this case, the element $\delta(a)$ is called the *derivative* of a. Denote $\delta(a), \delta^2(a), \ldots, \delta^n(a)$ for the successive derivatives, by induction on n, we obtain

$$\textit{Leibnize rule} : \delta^n(ab) = \sum_{i=0}^{n} \tbinom{n}{i} \delta^{n-i}(a)\delta^i(b).$$

Clearly,

1) $\forall a \in R, \delta(a^n) = na^{n-1}\delta(a)$.

2) $\delta(0) = \delta(0+0) = 2\delta(0) \Rightarrow \delta(0) = 0$.
$\delta(1) = \delta(1^2) = 2\delta(1) \Rightarrow \delta(1) = 0 \Rightarrow \forall n \in \mathbb{Z}, \delta(n) = 0$.

3) If $a^{-1} \in R$, $\delta(1) = \delta(a \cdot a^{-1}) = \delta(a) \cdot a^{-1} + a \cdot \delta(a^{-1}) = 0 \Rightarrow \delta(a^{-1}) = -\frac{\delta(a)}{a^2}$.

Lemma 1.1.2. *Let R be an integral domain and δ a derivation on R. Then δ has a unique extension to the quotient field* $\mathrm{Frac}(R)$.

Proof. To show Existence. Define for each $\frac{a}{b} \in \mathrm{Frac}(R)$, $\delta(\frac{a}{b}) = \frac{\delta(a)b - a\delta(b)}{b^2}$ and show $\delta : \mathrm{Frac}(R) \to \mathrm{Frac}(R)$ is ① well-defined and ② it is a derivation.

① Suppose $\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc$ and $\delta(a)d + a\delta(d) = \delta(b)c + b\delta(c)$. Show $\delta(\frac{a}{b}) = \frac{\delta(a)b - a\delta(b)}{b^2} = \delta(\frac{c}{d}) = \frac{\delta(c)d - c\delta(d)}{d^2}$.

② Show $\delta(\frac{a}{b} + \frac{c}{d}) = \delta(\frac{a}{b}) + \delta(\frac{c}{d})$ and $\delta(\frac{a}{b} \cdot \frac{c}{d}) = \delta(\frac{a}{b})\frac{c}{d} + \frac{a}{b}\delta(\frac{c}{d})$.
Uniqueness. $\forall \frac{a}{b} \in \mathrm{Frac}(R), \delta(a) = \delta(\frac{a}{b} \cdot b) = \delta(\frac{a}{b})b + \frac{a}{b}\delta(b) \Rightarrow \delta(\frac{a}{b}) = \frac{b\delta(a) - a\delta(b)}{b^2}$.

□

Definition 1.1.3. *A differential ring is a commutative ring R with unity 1 together with a finite set $\Delta = \{\delta_1, \ldots, \delta_m\}$ of mutually commuting derivation operators$\big($i.e., $\forall a \in R, \delta_i(\delta_j(a)) = \delta_j(\delta_i(a))\big)$, denoted by (R, Δ).*

- *If card$(\Delta) = 1$(i.e., $\Delta = \{\delta\}$), (R, δ) is called an ordinary differential ring.*
- *If card$(\Delta) > 1$, (R, Δ) is called a partial differential ring.*

If R is also a field, (R, Δ) is called a differential field.

Examples:

1) Let R be a commutative ring with unity. Define $\delta : R \to R$ by $\delta(a) = 0$ for $\forall a \in R$. Then (R, δ) is a differential ring. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_n$ have no other derivation operators than the zero derivation.

2) Let $R = \mathbb{Q}[x], \delta(x) = 1$. For any $a_0, a_1, \ldots, a_n \in \mathbb{Q}$, $\delta(a_0 + a_1x + \cdots + a_nx^n) = \delta(a_0) + \delta(a_1x) + \cdots + \delta(a_nx^n) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. (R, δ) is a differential ring.

3) Let F be a field of meromorphic functions of n complex variables $x_1, \ldots, x_n$ in a region of $\mathbb{C}^n$. Then $(F, \{\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\})$ is a differential field.

4) If (S, δ) is an ordinary differential ring and $R = S[x]$,then for any arbitrary $f \in R$, $\delta(x) = f$ turns R into a differential ring.
But this notion of arbitrarily defining derivation doesn't work for the partial case.
Non-Exampe: *$R = \mathbb{Q}[x]$. Let $\delta_1(x) = 1, \delta_2(x) = x$. Since $\delta_1(\delta_2(x)) = 1 \neq \delta_2(\delta_1(x)) = 0$, $(R, \{\delta_1, \delta_2\})$ is not a differential ring.*

In this course, we focus on the ordinary differential case and for simplicity, we sometimes use "δ-" instead of "differential". Denote $\Theta = \{\delta^i \,|\, i \in \mathbb{N}\}$.

Definition 1.1.4. *Let (R, δ) be a differential ring and $R_0 \subseteq R$ be a subring of R. If $\delta(R_0) \subseteq R_0$, then $(R_0, \delta|_{R_0})$ is a differential ring. In this case, we say R_0 a differential subring of R and say R a differential overring of R_0.*

If $S \subseteq R$, there exists a smallest differential subring of R containing all the elements of R_0 and S, denoted by $R_0\{S\}$, and S is said to be a set of generators of the differential ring $R_0\{S\}$ over R_0. $R_0\{S\}$ coincides, as a ring, with the ring $R_0[(\delta^i s)_{s\in S, i\in\mathbb{N}}]$. A differential overring of a differential ring R_0 is said to be finitely generated over R_0 if it has a finite set of generators over R_0.

If both R_0 and R are differential fields, R_0 is said to be a differential subfield of R and R is said to be a differential field extension of R_0.

Let L be a differential field extension of K and $S \subseteq L$. Denote by $K[S]$, $K\{S\}$, $K(S)$ and $K\langle S\rangle$ the smallest ring, the smallest differential ring, the smallest field, the smallest differential field containing K and S. Let $\Theta(S) = \{\delta^i(s) \,|\, i \in \mathbb{N}, s \in S\}$. Then $K\{S\} = K[\Theta(S)]$, $K\langle S\rangle = K(\Theta(S))$. L is said to be finitely generated if $\exists$ a finite subset $\{a_1, a_2, \ldots, a_n\} \subseteq L$ s.t. $L = K\langle a_1, \ldots, a_n\rangle$.

Definition 1.1.5. *Let (R, δ) be a differential ring. An element $c \in R$ is said to be a <u>constant</u> if $\delta(c) = 0$. The set of all constants of R is a differential subring of R, called the <u>ring of constants of R</u>, denoted by C_R. If R is a differential field, C_R is a field, called the field of constants of R.*

Examples:

1) $R = \mathbb{Q}[x]$, $\delta(x) = 1$. $C_R = \mathbb{Q}$.

2) $R = \mathbb{Z}_p(x^p)$, $\delta(x) = 1$. Then $C_R = R$.

Lemma 1.1.6. *Let $(\mathcal{F}, \delta)$ be a differential field of characteristic 0 and $C_\mathcal{F} = \mathcal{F}$. Let $L \supseteq \mathcal{F}$ be a differential field extension and L be algebraic over $\mathcal{F}$. Then $C_L = L$.*

Proof. Let $a \in L$. Suppose $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathcal{F}[x]$ is the minimal polynomial of a. Then $\delta(p(a)) = \frac{\partial p}{\partial x}(a) \cdot \delta(a) + \sum_{i=0}^{n} \delta(a_i) a^i = \frac{\partial p}{\partial x}(a) \cdot \delta(a) = 0$. Since $\mathrm{char}(\mathcal{F}) = 0$ and $\frac{\partial p}{\partial x}(a) \neq 0$. Thus $\delta(a) = 0$. □

Remark: Let $L \supseteq \mathcal{F} \supseteq \mathbb{Q}$ and $a \in L$. If a is algebraic over $C_\mathcal{F}$, then $\delta(a) = 0$.

1.2 Differential ideals

Definition 1.2.1. *Let (R, δ) be a differential ring. An ideal $I \lhd R$ is a differential ideal if $\delta(I) \subseteq I$.*

Example: Both $I = (0)$ and $I = R$ are differential ideals of R.

Proposition 1.2.2. *Let $I = (f_1, \ldots, f_s) \subseteq (R, \delta)$ be the ideal in (R, δ) generated by $f_1, \ldots, f_s$. Then I is a differential ideal $\iff \forall i$, $\delta(f_i) \in I$.*

Proof. "$\Rightarrow$" Trivial by definition.
"$\Leftarrow$" For each $f \in I$, $\exists\, g_1, \ldots, g_s \in R$ s.t. $f = g_1 f_1 + \cdots + g_s f_s$. So $\delta(f) = \sum_{i=1}^{s} \delta(g_i) f_i + \sum_{i=1}^{s} \delta(f_i) g_i \in I$, for $\delta(f_i) \in I$ by hypothesis. Thus, $\delta(I) \subseteq I$. □

Notation: Let $S \subseteq (R, \Delta)$. We use $[S]$ to denote the smallest differential ideal of R generated by S. Clearly, $[S] = (\Theta(S)) = (\delta^i s : s \in S)$.

Example: Consider $(\mathbb{Q}[x], \delta)$ with $\delta(x) = 1$. Then $[0]$ and $\mathbb{Q}[x]$ are the only differential ideals in $\mathbb{Q}[x]$. (Indeed, let $[0] \neq I \lhd \mathbb{Q}[x]$ be a differential ideal. Then $\exists\, 0 \neq f \in \mathbb{Q}[x]$ s.t. $I = (f)$. Since I is a differential ideal, $\delta(f) = \frac{\partial f}{\partial x} \in (f)$. If $f \notin \mathbb{Q}$, $f \nmid \frac{\partial f}{\partial x}$. So, $f \in \mathbb{Q} \backslash \{0\}$ and $I = \mathbb{Q}[x]$ follows.)

An ideal $I \lhd (R, \delta)$ is called a radical (resp. prime) differential ideal if

1) $\delta(I) \subseteq I$, and

2) I is a radical ideal (resp. prime ideal).

Notation: Given $I \lhd R$, $\sqrt{I} = \{f \in R \mid \exists\, n \in \mathbb{N} \text{ s.t. } f^n \in I\}$.
Given $S \subseteq (R, \Delta)$, let $\{S\}$ be the smallest radical differential ideal containing S, and say $\{S\}$ is a radical differential ideal generated by S. (It will be clear in which context $\{\cdot\}$ denotes a radical differential ideal or a set).

Now we turn to the construction of radical differnetial ideals. Normally, one may intuitively start with S, consider $[S]$ and then take its radical $\sqrt{[S]}$. However, this might not be sufficient.

Example: Let (R, δ) with $R = \mathbb{Z}_2[x, y], \delta(x) = y$ and $\delta(y) = 0$. Consider $I = [x^2]$. Since $\delta(x^2) = 0, I = (x^2)$. So $\sqrt{I} = (x)$. But $\sqrt{I}$ is not a differential ideal for $\delta(x) = y \notin \sqrt{I}$. So $\{x^2\} \neq \sqrt{[x^2]}$.

Exercise: Construct an example of an ideal $I \subseteq (R, \delta)$ s.t. $[\sqrt{I}]$ is not radical.
(Let $R = \mathbb{C}[x, y]$, $\delta(x) = y$ and $\delta(y) = 0$. Let $I = (xy)$. $\sqrt{I} = (xy), [\sqrt{I}] = [xy] = (xy, y^2)$. $J := [\sqrt{I}]$ is not radical for $y^2 \in J$ but $y \notin J$.)

Example: A maximal differential ideal (i.e., a maximal element in the set of all proper differential ideals) is not necessarily prime. For example, let $R = \mathbb{Z}_2[x]$ with $\delta(x) = 1$. Let $J = [x^2] = (x^2)$. Clearly, J is not prime but J is a maximal differential ideal. Indeed, if $\exists\, I \lhd (R, \delta)$ with $J \subsetneqq I \subseteq R$, then $\exists\, x + b \in I$. But $\delta(x + b) = 1 \in I$, so $I = R$.

However, if the ring R contains the rational field $\mathbb{Q}$, then the radical of a differential ideal is a radical differential ideal (i.e., $\{S,\} = \sqrt{[S]}$).

Theorem 1.2.3. *Let (R, δ) be a differential ring, $\mathbb{Q} \subseteq R$ and let $I \subseteq (R, \delta)$ be a differential ideal. Then, $\sqrt{I}$ is a radical differential ideal.*

Proof. It suffices to show $\sqrt{I}$ is a differential ideal. For this purpose, for each $a \in \sqrt{I}$ (i.e., $\exists\, a \in \mathbb{N}, a^n \in I$), to show $\delta(a) \in \sqrt{I}$. Claim: For each $k, 1 \leq k \leq n$, $a^{n-k}(\delta(a))^{2k-1} \in I$. We show the claim by induction on k and $\delta(a) \in \sqrt{I}$ will follow by allowing $k = n$ $\left((\delta(a))^{2n-1} \in I \Rightarrow \delta(a) \in \sqrt{I}\right)$. If $k = 1$, $\delta(a^n) = na^{n-1}\delta(a) \in I$. Since $\mathbb{Q} \subseteq R$, $a^{n-1}\delta(a) \in I$. Suppose $a^{n-k}(\delta(a))^{2k-1} \in I$ for some $1 \leq k < n$. Then, $\delta(a^{n-k}(\delta(a))^{2k-1}) = (n-k)a^{n-(k+1)}(\delta(a))^{2k} + a^{n-k}(2k-1)\delta(a)^{2k-2}\delta^2(a) \in I$. Multiply the above by $\delta(a)$, we get $a^{n-(k+1)}(\delta(a))^{2k+1} \in I$ and we are done. □

1.3 Decomposition of radical differential ideals

In computational algebraic geometry, we have studied decompositions of radical ideals. In differential algebra, we have analogous arguments.
Let (R, δ) be a differential ring and let I be a radical differential ideal of R.

Lemma 1.3.1. *If $ab \in I$, then $a\delta(b) \in I$ and $\delta(a)b \in I$.*

Proof. $ab \in I \Rightarrow \delta(ab) = \delta(a)b + a\delta(b) \in I \Rightarrow a\delta(b) \cdot \delta(ab) = (a\delta(b))^2 + ab\delta(a)\delta(b) \in I \Rightarrow (a\delta(b))^2 \in I \Rightarrow a\delta(b) \in I$ and $\delta(a)b \in I$. □

Lemma 1.3.2. *Let $S \subseteq R$ be any subset. Then $I : S = \{a \in R \mid aS \subseteq I\}$ is a radical differential ideal.*

Proof. 1) $\forall a, b \in I : S$, $r \in R$, $aS \subseteq I$ and $bS \subseteq I \Rightarrow (a+b)S \subseteq I$ and $raS \subseteq I$
$\Rightarrow a + b \in I : S, ra \in I : S$. So $I : S$ is an ideal.

2) $\forall a \in I : S, aS \subseteq I$. By Lemma 1.3.1, $\delta(a)S \subseteq I \Rightarrow \delta(a) \in I : S$. So $I : S$ is a differential ideal.

3) $\forall a \in R$, suppose $\exists\, n \in \mathbb{N}, a^n \in I : S$. Then $a^n S \subseteq I$. So for $\forall s \in S$, $a^n s \in I \overset{\times s^{n-1}}{\Longrightarrow} a^n s^n \in I \Rightarrow as \in I$ for $\forall s \in S \Rightarrow a \in I : S$.
Thus, $I : S$ is a radical differential ideal.

□

Lemma 1.3.3. *Let S be any subset. Let $a \in R$. Then $a\{S\} \subseteq \{aS\}$.*

Proof. Consider $J = \{aS\} : a$. By Lemma 1.3.2, I is a radical differnetial ideal. Since $S \subseteq J, \{S\} \subseteq J$. Thus, $a\{S\} \subseteq \{aS\}$.

□

Lemma 1.3.4. *For all subsets $S, T \subseteq R$, we have $\{S\}\{T\} \subseteq \{ST\}$. Furthermore, $\{S\} \cap \{T\} = \{ST\}$.*

Proof. Since for each $a \in S$, by Lemma 1.3.3, $a\{T\} \subseteq \{aT\} \subseteq \{ST\}$. By Lemma 1.3.2, $\{ST\} : \{T\}$ is a radical differential ideal containing S. Thus, $\{S\}\{T\} \subseteq \{ST\}$. The assertion $\{S\} \cap \{T\} = \{ST\}$ follows from i) and ii):

i) $ST \subseteq \{S\}, \{T\} \Rightarrow \{ST\} \subseteq \{S\} \cap \{T\}$;

ii) $\forall a \in \{S\} \cap \{T\}, a^2 \in \{S\} \cdot \{T\} \subseteq \{ST\}$. So $a \in \{ST\}$.

□

We use Lemmas 1.3.1-1.3.4 to show the following:

Lemma 1.3.5. *Let $T \subseteq R$ be a subset closed under multiplication and let P be maximal among radical differential ideals that do not intersect T. Then P is prime.*

Proof. Suppose the contrary, i.e., P is not prime. Let $a, b \in R$ be such that $ab \in P$ but $a \notin P$ and $b \notin P$. Hence $P \subsetneqq \{P, a\}, P \subsetneqq \{P, b\}$. Thus, $\exists\, t_1 \in \{P, a\} \cap T$, $\exists\, t_2 \in \{P, b\} \cap T$. So $t_1 t_2 \in T$ but $t_1 t_2 \in \{P, a\} \cdot \{P, b\} \subseteq \{P, ab\} = P$, a contradiction to $P \cap T = \emptyset$. □

In a commutative ring R, the nilradical $\sqrt{(0)}$ of R is the intersection of all the prime ideals of R and every radical ideal of R is the intersection of all prime ideals containing it. In differential algebra, we have a similar result.

Now, we are ready to state our main theorem of this section.

Theorem 1.3.6. *Let $I \subsetneqq R$ be a radical differential ideal. Then I can be represented as an intersection of prime differential ideals.*

Proof. We first construct for each $x \notin I$ a prime differential ideal P_x such that $P_x \supseteq I$ and $x \notin P_x$. Let $T = \{x^n \mid n \in \mathbb{N}\}$. The set $U = \{P \subseteq R \mid P \text{ is a radical differential ideal of } R, I \subseteq P, P \cap T = \emptyset\}$ is nonempty since $I \in U$. By Zorn's Lemma, $\exists$ a maximal element P_x in U. P_x is prime by Lemma 1.3.5, and since $P_x \cap T = \emptyset$, $x \notin P_x$. Clearly, $I = \bigcap\limits_{x \notin I} P_x$ is an intersection of prime differential ideals. □

In Section 1.2, we gave an example showing a maximal differential ideal might not be prime. But if $\mathbb{Q} \subseteq R$, then a maximal differential ideal in R is always prime.

Corollary 1.3.7. *Let $\mathbb{Q} \subseteq (R, \delta)$ and M be maximal among proper differential ideals. Then M is prime.*

Proof. Consider $\{M\} = \sqrt{[M]} = \sqrt{M}$. If $\sqrt{M} = R$, then $1 \in \sqrt{M} \Rightarrow 1 \in M$, which contradicts M being proper. Therefore, $\sqrt{M} = M$, M is a radical differential ideal. By Theorem 1.3.6, $M = \bigcap\limits_{\alpha \notin M} P_\alpha$ where P_α is a prime differential ideal. Therefore, for all $\alpha \notin M, M = P_\alpha$ and thus, M is prime. □

Remark: A differential ring R with $\mathbb{Q} \subseteq R$ is called a *Ritt Algebra*. We have shown in Section 1.2 and Section 1.3, in a Ritt Algebra:

1) The radical differential ideal $\{S\} = \sqrt{[S]}$;

2) A maximal differential ideal is a prime differential ideal;

3) Even in a Ritt Algebra R, the quotient R/M (M is a maximal differential ideal) might not be a differential field.
   Example: Let $R = \mathbb{Q}[x]$ with $\delta(x) = 1$. Then $[0]$ is the unique maximal differential ideal. $R/[0] = R$ is not a differential field.

Chapter 2

Differential polynomial rings and differential varieties

Let (K, δ) be a differential field of characteristic 0. We hope to develop an algebraic structure and algebraic theory for ordinary differential equations.

Definition 2.0.1. *Let (L, δ) be a differential field extension of (K, δ). A subset S of L is said to be differentially dependent over K if the set $(\delta^k(s))_{k\in\mathbb{N}, s\in S}$ is algebraically dependent over K. In the contrary case, S is said to be δ-independent over K, or a family of differential indeterminates over K. In the case $S = \{\alpha\}$, we say that α is differentially algebraic over K or differentially transcendental over K respectively.*

Example: Let $(K, \delta) = (\mathbb{Q}(x), \frac{\mathrm{d}}{\mathrm{d}x})$ and $(L, \delta) = (\mathbb{C}(x, \mathrm{e}^x), \frac{\mathrm{d}}{\mathrm{d}x})$. Clearly, each $c \in \mathbb{C}$ and $\alpha = \mathrm{e}^x$ are differentially algebraic over K.

Definition 2.0.2. *The ring of differential polynomials with coefficients in K in the differential indeterminates $y_1, \ldots, y_n$ is the ring of polynomials*

$$K[\delta^k y_j \mid k \in \mathbb{N}, j = 1, \ldots, n], \text{ denoted by } K\{y_1, \ldots, y_n\}.$$

Its elements are called differential polynomials. $K\{y_1, \ldots, y_n\}$ is a differential ring with the derivation operator δ extending $\delta\mid_K$ and $\delta(\delta^k y_j) = \delta^{k+1}(y_j)$.

Example:

1) $u_{xx} = v_x \longleftrightarrow \delta^2 y_1 - \delta y_2 = 0.$

2) $(\frac{\mathrm{d}u}{\mathrm{d}t})^2 = 4u\frac{\mathrm{d}^2u}{\mathrm{d}t^2} \longleftrightarrow (\delta y_1)^2 - 4y_1\delta^2(y_1) = 0.$

Definition 2.0.3. *Let (R_1, δ_1) and $(R_2.\delta_2)$ be two differential rings. A differential homomorphism of (R_1, δ_1) to (R_2, δ_2) is a ring homomorphism $\varphi : R_1 \to R_2$ such that $\varphi \circ \delta_1 = \delta_2 \circ \varphi$. If R_0 is a common differential subring of R_1 and R_2, and $\varphi\mid_{R_0} = \mathrm{id}_{R_0}$, φ is called a differential homomorphism over R_0.*

$$\begin{array}{ccc} a & \xrightarrow{\varphi} & \varphi(a) \\ \downarrow{\scriptstyle \delta_1} & & \downarrow{\scriptstyle \delta_2} \\ \delta_1(a) & \xrightarrow{\varphi} & \varphi(\delta_1(a)) \end{array}$$

We give two examples of differential homomorphisms:

1) Let $(K,\delta) \subseteq (L,\delta)$ be two differential fields. Then $\mathrm{id}_K : (K,\delta) \to (L,\delta)$ is a differential homomorphism.

2) Take an element $\vec{a} = (a_1,\ldots,a_n) \in L^n$, then the map

$$\begin{array}{rcc} \varphi_{\vec{a}} : K\{y_1,\ldots,y_n\} & \longrightarrow & L \\ f(y_1,\ldots,y_n) & \longmapsto & f(a_1,\ldots,a_n) \\ \delta^k(y_i) & \longmapsto & \delta^k(a_i) \end{array}$$

is a differential homomorphism over K. (uniquely determined by the value $\varphi(y_i)$.) Here, $f(a_1,\ldots,a_n)$ means replacing $\delta^k(y_i)$ for $\delta^k(a_i)$ in $f(y_1,\ldots,y_n)$.

Proposition 2.0.4. *Let (R_1,δ) and (R_2,δ) be two differential rings and $\varphi : R_1 \to R_2$ be a differential homomorphism. Then* $\mathrm{Ker}(\varphi)$ *is a differential ideal.*

Proof. $\mathrm{Ker}(\varphi)$ is an ideal of R, since φ is a homomorphism of rings. For each $r \in \mathrm{Ker}(\varphi), \varphi(r) = 0$, so $\delta(\varphi(r)) = 0 = \varphi(\delta(r)) \Rightarrow \delta(r) \in \mathrm{Ker}(\varphi)$. □

Corollary 2.0.5. *Let (R,δ) be a differential ring and I be an ideal of R. Then I is a differential ideal of $R \iff (R/I,\delta)$ is a differential ring.*

Proof. "⇒" Let $r + I \in R/I$. Define

$$\delta(r+I) = \delta(r) + I. \quad (*)$$

To show $(*)$ is well-defined, let $r_1 + I = r_2 + I$, we need to show $\delta(r_1) + I = \delta(r_2) + I$. Since $r_1 - r_2 \in I$ and I is a differential ideal, $\delta(r_1 - r_2) = \delta(r_1) - \delta(r_2) \in I$. So $\delta(r_1) + I = \delta(r_2) + I$.
To show $(*)$ is a derivation on R/I. Let $r_1+I, r_2+I \in R/I$, then $\delta(r_1+I+r_2+I) = \delta(r_1+r_2+I) = \delta(r_1)+\delta(r_2)+I = \delta(r_1+I)+\delta(r_2+I)$ and $\delta((r_1+I)(r_2+I)) = \delta(r_1r_2+I) = \delta(r_1)r_2+r_1\delta(r_2)+I = \delta(r_1+I)\cdot(r_2+I) + (r_1+I)\cdot\delta(r_2+I)$.

"⇐" Let $\varphi : R \to R/I$ be defined by $\varphi(r) = r + I$ for each $r \in R$. Then $\forall\, r \in R, \varphi(\delta(r)) = \delta(r)+I = \delta(r+I) = \delta(\varphi(r))$, so φ is a differential homomorphism. By Proposition 2.0.4, $I = \mathrm{Ker}(\varphi)$ is a differential ideal of R. □

Definition 2.0.6. *Let $\Sigma \subseteq K\{y_1,\ldots,y_n\}$ and $\eta = (\eta_1,\ldots,\eta_n)$ be a point from $(L,\delta) \supseteq (K,\delta)$. We call η a* differential zero *of Σ if for each $f \in \Sigma, f(\eta) = 0$, (that is, $\Sigma \subseteq \mathrm{Ker}(\varphi_\eta : K\{y_1,\ldots,y_n\} \to L^n)$).*

In algebraic geometry, we consider algebraic varieties in an algebraic closed field. In differential algebra, we have similar concepts to define differential varieties.

Definition 2.0.7. *(K,δ) is called* differentially closed *if for all $F \subseteq K\{y_1,\ldots,y_n\}$, if $\exists\,(L,\delta) \supseteq (K,\delta)$ and $\eta \in L^n$ s.t. $F(\eta) = 0$, then $\exists\,\xi \in K^n$ s.t. $F(\xi) = 0$.*
Let $(L,\delta) \supseteq (K,\delta)$. (L,δ) is called a differential closure *of (K,δ) if*

1) (L,δ) is differentially closed, and

2) for every differentially closed field $(M,\delta) \supseteq (K,\delta)$, there is a differential embedding $\varphi : L \hookrightarrow M$ with $\varphi\,|_K = \mathrm{id}_K$.

Definition 2.0.8. *Let (E, δ) be a fixed differential closure of (K, δ). The set of differential zeros of $\Sigma \subseteq K\{y_1, \ldots, y_n\}$ is called a differential variety over K, denoted by $\mathbb{V}_E(\Sigma)$ or $\mathbb{V}(\Sigma)$. For a subset $V \subseteq E^n$, we denote $\mathbb{I}(V) = \{f \in K\{y_1, \ldots, y_n\} \mid \forall \xi \in V, f(\xi) = 0\}$ to be the set of all differential polynomials in $K\{y_1, \ldots, y_n\}$ which vanish at each point of V. Clearly, $\mathbb{I}(V)$ is a radical differential ideal.*

Let $\eta = (\eta_1, \ldots, \eta_n)$ be a point from a differential extension field of (K, δ). η is called a generic point of a differential ideal $I \subseteq K\{y_1, \ldots, y_n\}$ if $\forall f \in K\{y_1, \ldots, y_n\}, f(\eta_1, \ldots, \eta_n) = 0 \Leftrightarrow f \in I$.

Example: In the algebraic case, $I = (x^2 + y^2 - 1) \subseteq \mathbb{Q}[x, y]$ has a generic point $(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2})$. Also, $(\cos(\theta), \sin(\theta))$ is another generic point. So generic points are not unique.

Lemma 2.0.9. *Let $P \subseteq K\{y_1, \ldots, y_n\}$ be a differential ideal. Then P has a generic point $\Leftrightarrow$ P is prime.*

Proof. "$\Rightarrow$" Suppose η is a generic point of P. Then $P = \mathbb{I}(\eta)$ is a prime differential ideal.
"$\Leftarrow$" Suppose P is a prime differential ideal. Then $K\{y_1, \ldots, y_n\}/P$ is a differential domain. Let $L = \mathrm{Frac}(K\{y_1, \ldots, y_n\}/P)$ and $\bar{y}_i = y_i + P$. Then $(\bar{y}_1, \ldots, \bar{y}_n) \in L^n$ is a generic point of P. Indeed, $\forall f \in P, f(\bar{y}_1, \ldots, \bar{y}_n) = f(y_1, \ldots, y_n) + P = \bar{0} \in L$ and $\forall f \in K\{y_1, \ldots, y_n\}$, if $f(\bar{y}_1, \ldots, \bar{y}_n) = 0$, then $f(y_1, \ldots, y_n) \in P$.

□

In this chapter, we will prove the differential analog of Hilbert basis theorem for the differential polynomial ring, i.e., the Ritt-Raudenbush basis theorem. Before that, we first introduce characteristic set method, which is the main computational tool in differential algebra and also could provide some theoretical insights. The idea behind characteristic sets is similar to the notion of Gröbner basis.

2.1 Differential characteristic sets

Motivated Example (Ideal membership problem):

① In $\mathbb{Q}[x]$, every ideal is of the form $I = (f)$ for some $f \in \mathbb{Q}[x]$. By the Euclidean division algorithm, $g = qf + r$ with $r = \mathrm{rem}(g, f)$. Then $g \in I \Leftrightarrow r = 0$.

② In $\mathbb{Q}[x_1, \ldots, x_n]$, given an ideal $I = (f_1, \ldots, f_s) \subseteq \mathbb{Q}[x_1, \ldots, x_n]$, we use Gröbner basis to test whether $g \in I$.

③ How about the differential ideal membership problem? (differential characteristic sets)

Let (K, δ) be a differential field of characteristic zero. The differential polynomial ring $K\{Y\} \triangleq K\{y_1, \ldots, y_n\}$ in the differential variables $Y = \{y_1, \ldots, y_n\}$ can be viewed as a polynomial ring in the algebraic variables $\Theta(Y) \triangleq \{\delta^i(y_j) \mid i \in \mathbb{N}, j = 1, \ldots, n\}$. (i.e., $K\{Y\} = K[\Theta(Y)]$)

A differential ranking on $\Theta(Y)$ is a total ordering on $\Theta(Y)$ satisfying

(1) $u < \delta(u)$ for all $u \in \Theta(Y)$ and

(2) if $u, v \in \Theta(Y)$ with $u < v$, then $\delta(u) < \delta(v)$.

Example:

- The set $\Theta(y) = \{\delta^i(y) : i \in \mathbb{N}\}$ has a unique ranking $y < \delta(y) < \delta^2(y) < \delta^3(y) < \cdots$.
- Two important rankings on $\Theta(Y)$ are the following:
  1) Elimination ranking: $y_i > y_j \Rightarrow \delta^k(y_i) > \delta^l(y_j)$ for any $k, l \in \mathbb{N}$.
  2) Orderly ranking: $k > l \Rightarrow \delta^k(y_i) > \delta^l(y_j)$ for all $i, j \in \mathbb{N}$.

Lemma 2.1.1. *Every ranking is a well-ordering (i.e., every nonempty subset of $\Theta(Y)$ has a least element).*

Proof. Let $U \subseteq \Theta(Y)$ and $U \neq \emptyset$. For each $j \in \{1, \ldots, n\}$, if $\exists i \in \mathbb{N}$ s.t. $\delta^i(y_j) \in U$, then set $k_j = \min\{i \mid \delta^i(y_j) \in U\}$ and set $u_j = \delta^{k_j}(y_j)$. Then the least element of U is the least element in the finite set of u_j's. □

Until the end of this subsection, we assume a ranking $\mathscr{R}$ is fixed. And by convention, $1 < \delta^i(y_j)$. (Denote $\delta(a), \delta^2(a), \delta^k(a)$ by $a', a'', a^{(k)} (k \geq 3)$ respectively).

Definition 2.1.2. *Let $f \in K\{y_1, \ldots, y_n\}\backslash K$. The* leader *of f is the largest element of $\Theta(Y)$ with respect to $\mathscr{R}$ which appears effectively in f, denoted by u_f or $\mathrm{ld}(f)$. By the two conditions in the definition of ranking, for each $i \in \mathbb{N}$, $\mathrm{ld}(\delta^i(f)) = \delta^i(\mathrm{ld}(f))$. We write f as a univariate polynomial of u_f, then $f = I_d(u_f)^d + I_{d-1}(u_f)^{d-1} + \cdots + I_1 u_f + I_0$, where I_i is free of u_f and $d = \deg(f, u_f)$. The leading coefficient I_d is called the* initial *of f and denoted by I_f. The pair $\mathrm{rk}(f) := (u_f, d)$ is called the* rank *of f.*

Example: Let $f = (y')^2 - 4y \in \mathbb{Q}\{y\}$. Then $u_f = \mathrm{ld}(f) = y'$ and $\mathrm{I}_f = 1$. Apple δ to f, then we have $\delta(f) = 2y'y'' - 4y'$. So we get $u_{\delta(f)} = y'' = \delta(u_f)$ and $\mathrm{I}_{\delta(f)} = 2y' = \frac{\partial f}{\partial y'}$.

Note that in the above example, $\deg(\delta(f), u_{\delta(f)}) = 1$ and $\mathrm{I}_{\delta(f)} = \frac{\partial f}{\partial u_f}$.

Definition 2.1.3. *Let $f \in K\{y_1, \ldots, y_n\}\backslash K$. $\frac{\partial f}{\partial u_f}$ is called the* separant *of f, denoted by S_f.*

Remark:

1) $f = \sum_{i=0}^d I_i {u_f}^i \Longrightarrow \delta(f) = \sum_{i=1}^d I_i \delta({u_f}^i) + \sum_{i=0}^d \delta(I_i){u_f}^i = (\sum_{i=1}^d I_i \cdot i \cdot {u_f}^{i-1})\delta(u_f) + \sum_{i=0}^d \delta(I_i){u_f}^i = \mathrm{S}_f \cdot \delta(u_f) + \sum_{i=0}^d \delta(I_i){u_f}^i$.
   Note that $u_{\delta(f)} = \delta(u_f)$, $\mathrm{I}_{\delta(f)} = \mathrm{S}_f$ and $\deg(\delta(f), u_{\delta(f)}) = 1$. ($\mathrm{char}(K) = 0$)
   Also, for $k > 0$, $\delta^k(f) = \mathrm{S}_f \cdot \delta^k(u_f) +$ tail polynomial involving derivatives less than $\delta^k(u_f)$.
   So $u_{\delta^k(f)} = \delta^k(u_f)$, $\mathrm{I}_{\delta^k(f)} = \mathrm{S}_f$, $\deg(\delta^k(f), u_{\delta^k(f)}) = 1$.
   ((K, δ) is a δ-field, c is algebraic over $K \Rightarrow$ there is a unique way to make $(K(c), \delta)$ a δ-field.)
2) By convention, for $f \in K\backslash\{0\}, u_f = 1$.

Definition 2.1.4. *Let $f, g \in K\{Y\}$, we say that f is* partially reduced *with respect to g if none of the proper derivatives of u_g ($\delta^i(u_g)$ with $i > 0$) appears effectively in f.*

Example:

1) Let $f = y^2, g = y + 1$. Since $u_g = y$ and none of the proper derivatives of y appears in f, f is partially reduced with respect to g.
2) Let $f = 2y\delta(y)^2 + y$ and $g = y + 1$. Since $\delta(u_g) = \delta(y)$ appears in the first term of f, f isn't partially reduced with respect to g.

Definition 2.1.5. *We say f is* reduced *with respect to g if*

1) f is partially reduced with respect to g, and

2) $\deg(f, u_g) < \deg(g, u_g)$.

Definition 2.1.6. *A subset $\mathcal{A} \subseteq K\{y_1, \ldots, y_n\}$ is called an autoreduced set if any element of $\mathcal{A}$ is reduced with respect to any other element of $\mathcal{A}$.*

Let $\mathcal{A} \subseteq K\{Y\}\backslash K$ and $F \in K\{Y\}$. We say F is partially reduced w.r.t. $\mathcal{A}$ if ....

Remark: If an autoreduced set $\mathcal{A}$ contains an element $A \in K\backslash\{0\}$, then $\mathcal{A} = \{A\}$.

Lemma 2.1.7. *Every autoreduced set of $K\{y_1, \ldots, y_n\}$ is finite.*

Proof. Let $\mathcal{A}$ be an autoreduced set. For each $i = 1, \ldots, n$, there exists at most one differential polynomial $A \in \mathcal{A}$ such that $\mathrm{ld}(A) = \delta^k(y_i)$ for some $k \in \mathbb{N}$, for two differential polynomials A_1, A_2 with $\mathrm{ld}(A_j) = \delta^{k_j}(y_i)$ couldn't be reduced with respect to each other. Thus $|A| \leq n$.
(For the partial differential case, we need to use Dickson lemma to show every autoreduced set is finite.) □

Definition 2.1.8. *Let $f, g \in K\{y_1, \ldots, y_n\}\backslash K$. We say f has lower rank than g ($f < g$) if* $\mathrm{rk}(f) <_{lex} \mathrm{rk}(g)$. *($<_{lex}$ is a well-ordering of $\Theta(Y) \times \mathbb{N}^*$.) By convention, each element of $K\backslash\{0\}$ has lower rank than elements of $K\{Y\}\backslash K$.*

Notation: We use $f \leq g$ to denote either $f < g$ or f and g have the same rank. (" $\leq$ " is a pre-order among $K\{y_1, \ldots, y_n\}$.)

In the following, we write an autoreduced set in the order of increasing rank, i.e., $\mathcal{A} = A_1, \ldots, A_p$ with $\mathrm{rk}(A_1) <_{lex} \mathrm{rk}(A_2) <_{lex} \cdots <_{lex} \mathrm{rk}(A_p)$.

Let $\mathcal{A} = A_1, \ldots, A_p$ and $\mathcal{B} = B_1, \ldots, B_q$ be two autoreduced sets. We say $\mathcal{A} < \mathcal{B}$ if either

1) $\exists\, k\, (\leq \min\{p, q\})$ such that $\forall\, i < k, \mathrm{rk}(A_i) = \mathrm{rk}(B_i)$ and $A_k < B_k$, or

2) $p > q$ and for each $i \leq q, \mathrm{rk}(A_i) = \mathrm{rk}(B_i)$.

If neither $\mathcal{A} < \mathcal{B}$ nor $\mathcal{B} < \mathcal{A}$, we say $\mathcal{A}$ and $\mathcal{B}$ are of the same rank. $\mathcal{A}$ and $\mathcal{B}$ have the same rank $\Leftrightarrow$ $p = q$ and $\forall\, i \leq p, \mathrm{rk}(A_i) = \mathrm{rk}(B_i)$. Say $\mathcal{A} \leq \mathcal{B}$ iff $\mathcal{A} < \mathcal{B}$ or $\mathcal{A}$ and $\mathcal{B}$ have the same rank. (" $\leq$ " is a pre-order.)

Example: Consider $K\{y_1, y_2\}$ and take the orderly ranking with $y_1 < y_2$. Let $\mathcal{A} = \{A_1 = (y_2')^2 + 1, A_2 = y_1'' + y_2\}$, $\mathcal{B} = \{B_1 = y_2' + 2\}$ and $\mathcal{C} = \{C_1 = (y_2')^2 + 2\}$. Since $\mathrm{rk}(A_1) > \mathrm{rk}(B_1), \mathcal{B} < \mathcal{A}$. Since $\mathrm{rk}(A_1) = \mathrm{rk}(C_1)$ and $|\mathcal{A}| > |\mathcal{C}|, \mathcal{A} < \mathcal{C}$.

Proposition 2.1.9. *Any nonempty set of autoreduced sets in $K\{Y\} = K\{y_1, \ldots, y_n\}$ contains an autoreduced set of lowest rank.*

Proof. Let U be any nonempty set of autoreduced sets of $K\{Y\}$. Define by induction a sequence of subsets of U as follows: $U_0 \triangleq U$, for $i > 0$, define $U_i = \{\mathcal{A} \in U_{i-1} \mid \mathrm{card}(\mathcal{A}) \geq i$, the i-th element of $\mathcal{A}$ is of lowest rank$\}$. Then $U_0 \supseteq U_1 \supseteq \cdots$. By Lemma 2.1.7, $\exists\, i \in \mathbb{N}$ (actually $i \leq n$ in the ordinary differential case) such that $U_i \neq \emptyset$ and $U_{i+1} = \emptyset$. Actually, any element of U_i is an autoreduced set in U of lowest rank. □

Definition 2.1.10. *Let $I \subseteq K\{Y\}$ be a differential ideal. An autoreduced set of lowest rank contained in I is called a* characteristic set *of I (with respect to the given ranking).*

Remark: By convention, $\emptyset$ and $\{a\}$ with $a \in K^*$ are autoreduced sets. (Here, $\mathrm{rk}(a) = (1,1)$.)

We start to introduce pesudo-division of differential polynomials:

Lemma 2.1.11. *Let $\mathcal{A} = A_1, \ldots, A_p$ be an autoreduced set in $K\{Y\}$ and $F \in K\{Y\}$. Then there exist $\tilde{F} \in K\{Y\}$ and $t_i \in \mathbb{N}$ satisfying*

1) $\tilde{F}$ is partially reduced with respect to $\mathcal{A}$,

2) the rank of $\tilde{F}$ is not higher than that of F,

3) $\prod_{i=1}^{p} \mathrm{S}_{A_i}^{t_i} F \equiv \tilde{F} \bmod [\mathcal{A}]$.

More precisely, $\prod_{i=1}^{p} \mathrm{S}_{A_i}^{t_i} F - \tilde{F}$ can be expressed as a linear combination of derivatives $\theta(A_i)$ with coefficients in $K\{Y\}$ such that $\theta(u_{A_i}) \leq u_F$.

Proof. If F is partially reduced with respect to $\mathcal{A}$, then set $\tilde{F} = F$ and $t_i = 0\,(i \leq p)$. Otherwise, F contains a proper derivative $\delta^k(u_{A_i})$ of the leader of some A_i. Let v_F be such derivatives of the maximal rank. We shall prove the lemma by induction on v_F. Suppose for all $G \in K\{Y\}$ that doesn't involve a proper derivative of any u_{A_i} of rank $\geq v_F$, the corresponding $\tilde{G}$ and natural numbers are defined satisfying the desired properties. There exists a unique $A \in \mathcal{A}$ such that $v_F = \delta^k(u_A)$ for some $k > 0$. If $A = \sum_{i=0}^{d} I_i {u_A}^i$, then

$$\delta^k(A) = \mathrm{S}_A \delta^k(u_A) + T \text{ with } T \text{ having lower rank than } \delta^k(u_A) = v_F.$$

Denoting $l = \deg(F, v_F)$ and write F as $F = \sum_{i=0}^{l} J_i {v_F}^i$ where $J_0, \ldots, J_l$ don't involve proper derivatives of any u_{A_i} of rank $\geq v_F$. Hence ${\mathrm{S}_A}^l F = \sum_{i=0}^{l} J_i {\mathrm{S}_A}^{l-i} (\mathrm{S}_A v_F)^i \equiv \sum_{i=0}^{l} J_i {\mathrm{S}_A}^{l-i} (-T)^i \bmod (\delta^k(A))$. Clearly, $G = \sum_{i=0}^{l} J_i {\mathrm{S}_A}^{l-i} (-T)^i$ doesn't involve proper derivatives of any u_{A_i} of rank $\geq v_F$. By the induction hypothesis, $\exists\, \tilde{G}$ partially reduced with respect to $\mathcal{A}$ and $k_i \in \mathbb{N}$ such that $\prod_{i=1}^{p} \mathrm{S}_{A_i}^{k_i} G \equiv \tilde{G} \bmod [\mathcal{A}]$. Now it suffices to set $\tilde{F} = \tilde{G}$, $t_i = \begin{cases} k_i, & A_i \neq A \\ k_i + l, & A_i = A \end{cases}$. □

Remark: $\tilde{F}$ constructed by the process in the proof is called the *partial remainder* of F w.r.t $\mathcal{A}$.

Recall the pseudo reduction algorithm in commutative algebra:
Let D be an integral domain and v an indeterminate over D. Let $F, A \in D[v]$ be of respective degrees d_F, d_A. Suppose $A = I_{d_A} v^{d_A} + \cdots + I_1 v + I_0 \neq 0$ with $I_i \in D$. Let $e = \max\{d_F - d_A + 1, 0\}$. Then we can compute unique $Q, R \in D[v]$ s.t. $I_{d_A}^e F = QA + R$ and $\deg(R) < \deg(A)$.

Theorem 2.1.12. *Let $\mathcal{A} = A_1, \ldots, A_p$ be an autoreduced set in $K\{y_1, \ldots, y_n\}$. If $F \in K\{y_1, \ldots, y_n\}$, then $\exists$ a δ-polynomial F_0 ($\underline{\delta\text{-remainder}}$ of F) and $r_i, t_i \in \mathbb{N}$ such that*

1) F_0 is reduced w.r.t $\mathcal{A}$,

2) The rank of F_0 is no higher than the rank of F,

3) $\prod_{i=1}^{p} \mathrm{S}_{A_i}^{t_i} \mathrm{I}_{A_i}^{r_i} F \equiv F_0 \bmod [\mathcal{A}]$.

Proof. Let $\tilde{F}$ be the partial remainder of F with respect to $\mathcal{A}$ and $\prod_{i=1}^{p} \mathrm{S}_{A_i}^{t_i} F \equiv \tilde{F} \bmod [\mathcal{A}]$. Let $r_p = \max\{0, \deg(F, u_{A_p}) - \deg(A_p, u_{A_p}) + 1\}$. Then $\exists\, F_{p-1} \in K\{Y\}$ partially reduced with respect to $\mathcal{A}$ and reduced with respect to A_p such that $\mathrm{I}_{A_p}^{r_p} \tilde{F} \equiv F_{p-1} \bmod (A_p)$. If $p = 1$, then we are done. Otherwise, we can find r_{p-1} and $F_{p-2} \in K\{Y\}$ partially reduced with respect to $\mathcal{A}$ and reduced with respect to A_{p-1}, A_p s.t. $\mathrm{I}_{A_{p-1}}^{r_{p-1}} \mathrm{I}_{A_p}^{r_p} \tilde{F} \equiv F_{p-2} \bmod (A_{p-1}, A_p)$ and is not higher than $\tilde{F}$. Continuing in this way, we get F_0 satisfying the desired properties.

□

Remark: The reduction procedures above could be summarized in an algorithm, called the *Ritt-Kolchin algorithm* to compute the δ-remainder of a δ-polynomial F with respect to an autoreduced set $\mathcal{A}$. Denote F_0 above by $\delta\text{-rem}(F, \mathcal{A})$, or $F \underset{\mathcal{A}}{\to} F_0$.

Example: Consider $K\{y_1, y_2\}$ and fix the orderly ranking with $y_1 > y_2$.

(1) Let $f = y_1$ and $\mathcal{A} = A_1 = y_2 y_1$. Here $f \underset{\mathcal{A}}{\to} 0$, and $\mathrm{I}_{A_1} f - 0 \in [\mathcal{A}]$.

(2) Let $f = y_1' + 1$ and $\mathcal{A} = A_1 = y_2 y_1^2$. $u_{A_1} = y_1$ and $\mathrm{S}_{A_1} = 2y_2 y_1$. Clearly, f is not partially reduced with respect to $\mathcal{A}$. $\delta(A_1) = 2y_2 y_1 y_1' + y_2' y_1^2$. The partial remainder of f with respect to $\mathcal{A}$ is $2y_2 y_1 - y_2' y_1^2 = \tilde{f}$ and $\mathrm{S}_{A_1} f - A_1' = \tilde{f}$. $\mathrm{I}_{A_1} \tilde{f} - \mathrm{I}_{\tilde{f}} A_1 = y_2(2y_2 y_1 - y_2' y_1^2) - (-y_2') y_2 y_1^2 = 2y_2^2 y_1$, reduced with respect to $\mathcal{A}$. So $f \underset{\mathcal{A}}{\to} 2y_2^2 y_1$ and $\mathrm{I}_{A_1} \mathrm{S}_{A_1} f - 2y_2^2 y_1 = -y_2' A_1 + \mathrm{I}_{A_1} A_1' \in [\mathcal{A}]$.

Theorem 2.1.13. *Let $\mathcal{A}$ be an autoreduced set of a proper differential ideal $I \subseteq K\{y_1, \ldots, y_n\}$. Then the followings are equivalent:*

(1) $\mathcal{A}$ is a characteristic set of I.

(2) $\forall f \in I$, δ-rem$(f, \mathcal{A})$=0.

(3) I doesn't contain a nonzero δ-polynomial reduced with respect to $\mathcal{A}$.

Proof. (2) $\Leftrightarrow$ (3) is clear.
"(1) $\Rightarrow$ (3)" Suppose $f \in I \backslash \{0\}$ is reduced with respect to $\mathcal{A} = A_1, \ldots, A_p$. Let $k \in \mathbb{N}$ be maximal such that $\mathrm{rk}(A_k) < \mathrm{rk}(f)$. Then $A_1, \ldots, A_k, f$ is an autoreduced set lower than $\mathcal{A}$. (Here, in the case $\mathrm{rk}(f) < \mathrm{rk}(A_1)$, take $k = 0$ and $\{f\}$ is an autoreduced set $< \mathcal{A}$.) Thus, we get a contradiction, and (3) is valid.
"(3) $\Rightarrow$ (1)" Assume (3) is valid. Suppose $\mathcal{A} = A_1, \ldots, A_p$ is not a characteristic set of I. Then $\exists\, \mathcal{B} = B_1, \ldots, B_q$, an autoreduced set of I of lower rank than $\mathcal{A}$. Thus, by definition, either (1) $\exists\, k \leq \min\{p, q\}$ such that for $i < k$, $\mathrm{rk}(A_i) = \mathrm{rk}(B_i)$ and $A_k > B_k$, or (2) $q > p$ and for $i \leq p$, $\mathrm{rk}(A_i) = \mathrm{rk}(B_i)$. Then either B_k or B_{p+1} is nonzero and reduced with respect to $\mathcal{A}$. □

Remark: By Theorem 2.1.13, if $\mathcal{A} = A_1, \ldots, A_p$ is a characteristic set of $I \subseteq K\{Y\}$, then $\mathrm{I}_{A_i}, \mathrm{S}_{A_i} \notin I$ $(\forall i = 1, \ldots, p)$.

A characteristic set of I can be obtained by the following procedure (non-constructive) : choose $A_1 \in I$ of minimal rank. Choose A_2 of minimal rank in the set $\{f \in I \mid f \text{ is reduced with respect to } A_1\}$. Then A_1, A_2 is autoreduced. Choose A_3 of minimal rank in the set $\{f \in I \mid f \text{ is reduced with respect to } A_1, A_2\}$. Then A_1, A_2, A_3 is autoreduced. Continue like this. The process must terminate for an autoreduced set is finite. In the end, we will obtain an autoreduced set $\mathcal{A} := A_1, \ldots, A_p$ of I such that no polynomial in I is reduced with respect to $\mathcal{A}$. Clearly, $\mathcal{A}$ is a characteristic set of I.

Lemma 2.1.14. *Let $\mathcal{A}$ be a characteristic set of a proper δ-ideal $I \subseteq K\{Y\}$. Denote $\mathrm{H}_{\mathcal{A}}^{\infty}$ to be the multiplicative set generated by initials and separants of elements in $\mathcal{A}$ and set $\mathrm{sat}(\mathcal{A}) := [\mathcal{A}] : \mathrm{H}_{\mathcal{A}}^{\infty} = \{f \in K\{Y\} \mid \exists\, M \in \mathrm{H}_{\mathcal{A}}^{\infty}, Mf \in [\mathcal{A}]\}$. Then $I \subseteq \mathrm{sat}(\mathcal{A})$. Furthermore, if I is prime, $I = \mathrm{sat}(\mathcal{A})$.*

Proof. By Theorem 2.1.13, $\forall\, f \in I, \delta\text{-rem}(f, \mathcal{A}) = 0$. Thus, $\exists\, i_A, t_A \in \mathbb{N}\,(A \in \mathcal{A})$ s.t. $\prod_{A\in\mathcal{A}} \mathrm{I}_A^{i_A}\mathrm{S}_A^{t_A} f \in [\mathcal{A}]$, i.e., $f \in \mathrm{sat}(\mathcal{A})$. If I is prime, for each $f \in \mathrm{sat}(\mathcal{A})$, $\exists\ i_A, t_A$ s.t. $\prod_{A\in\mathcal{A}} \mathrm{I}_A^{i_A}\mathrm{S}_A^{t_A} f \in [\mathcal{A}] \subseteq I$. Since $\mathrm{I}_A, \mathrm{S}_A$ are not in I, $f \in I$. □

Exercise: Develop a division algorithm as follows:
Input: $f \in K\{Y\}$ and an autoreduced set $\mathcal{A} = A_1, \ldots, A_p$ w.r.t. a fixed ranking.
Output: $g \in K\{Y\}$, the δ-remainder of f w.r.t. $\mathcal{A}$. (i.e. 1). g is reduced w.r.t. $\mathcal{A}$, 2). $\exists\, i_k, j_k \in \mathbb{N}$ s.t. $\mathrm{I}_{A_1}^{i_1} \cdots \mathrm{I}_{A_p}^{i_p} \mathrm{S}_{A_1}^{j_1} \cdots \mathrm{S}_{A_p}^{j_p} f - g \in [\mathcal{A}]$).

2.2 The Ritt-Raudenbush basis theorem

Hilbert basis theorem: Every ideal of $K[y_1, \ldots, y_n]$ is finitely generated. (Every ascending chain of ideals in $K[y_1, \ldots, y_n]$ is finite.)
One might hope ACC condition holds for differential ideals in $K\{y_1, \ldots, y_n\}$. However, this is not true.
Non-example: Consider $K\{y\}$ with $\mathbb{Q} \subseteq (K, \delta)$. The sequence of differential ideals $[y^2] \subseteq [y^2, (y')^2] \subseteq [y^2, (y')^2, (y'')^2] \subseteq \cdots$ doesn't stabilize in $K\{y\}$.

Definition 2.2.1. *A differential ring is called Ritt-Noetherian if the set of radical differential ideals satisfies the ascending chain condition (ACC).*

Lemma 2.2.2. *Let (R, δ) be a differential ring. Then R is Ritt-Noetherian $\Leftrightarrow$ every radical differential ideal I of R is finitely generated as a radical differential ideal. (i.e. $\exists\, f_1, \ldots, f_s \in I$ s.t. $I = \{f_1, \ldots, f_s\}$).*

Proof. "$\Rightarrow$" Let I be an arbitrary radical differential ideal of R. Suppose I is not finitely generated as a radical differential ideal. Then we can construct a strict increasing sequence of radical differential ideals, i.e., $\{a_1\} \subsetneqq \{a_1, a_2\} \subsetneqq \cdots \subsetneqq \{a_1, a_2, \ldots, a_p\} \subsetneqq \cdots$.
"$\Leftarrow$" Let $I_1 \subseteq I_2 \subseteq \cdots$ be sequence of radical differential ideals. Take $I = \bigcup_{i=1}^{\infty} I_i$. Then I is a radical differential ideal. Thus, $\exists\, f_1, \ldots, f_s \in I$ s.t. $I = \{f_1, \ldots, f_s\}$. Since each $f_i \in I$, $\exists\, m \in \mathbb{N}$ s.t. $f_i \in I_m$ $(\forall\, i = 1, \ldots, s)$. So $\{f_1, \ldots, f_s\} \subseteq I_m \subseteq I \Rightarrow I_m = I_{m+j} = \{f_1, \ldots, f_s\}$ for $j \in \mathbb{N}$. □

Theorem 2.2.3. *Let (K, δ) be a differential field with $\mathbb{Q} \subseteq K$. The differential polynomial ring $K\{y_1, \ldots, y_n\}$ is Ritt-Noetherian.*

Proof. By Lemma 2.2.2, it suffices to prove that every radical differential ideal of $K\{y_1, \ldots, y_n\}$ is finitely generated as radical differential ideals. Suppose the contrary and $\exists$ a radical differential ideal of $K\{y_1, \ldots, y_n\}$ that is not finitely generated. By Zorn's lemma, $\exists$ a maximal radical differential ideal $J \subseteq K\{y_1, \ldots, y_n\}$ that is not finitely generated.
Claim: J is a prime differential ideal.
If not, then $\exists\, a, b \in K\{y_1, \ldots, y_n\}$ s.t. $a, b \notin J$ but $ab \in J$. Since $\{a, J\} \supsetneqq J$ and $\{b, J\} \supsetneqq J$, $\{a, J\}$ and $\{b, J\}$ are finitely generated as radical differential ideals. Then $\exists\, f_1, \ldots, f_s, g_1, \ldots, g_t \in J$ s.t. $\{a, J\} = \{a, f_1, \ldots, f_s\}$ and $\{b, J\} = \{b, g_1, \ldots, g_t\}$. (Indeed, as $\{a, J\}$ is finitely generated, $\exists\, h_1, \ldots, h_l$ s.t. $\{a, J\} = \{h_1, \ldots, h_l\}$. For each i, $h_i \in \{a, J\} \Rightarrow \exists\, m_i$ s.t. $h_i^{m_i} \in [a, J]$. So $\exists\, f_1, \ldots, f_s \in J$ s.t. $h_i^{m_i} \in [a, f_1, \ldots, f_s]$. Thus, $h_i \in \{a, f_1, \ldots, f_s\} \Rightarrow \{a, J\} \Rightarrow \{h_1, \ldots, h_l\} \subseteq$

$\{a, f_1, \ldots, f_s\} \subseteq \{a, J\}$)
Hence,

$$\begin{aligned} J^2 &\subseteq \{a, J\} \cdot \{b, J\} = \{a, f_1, \ldots, f_s\} \cdot \{b, g_1, \ldots, g_t\} \\ &\subseteq \{ab, ag_j, bf_i, f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t\} \triangleq P \\ &\subseteq J. \end{aligned}$$

For each $f \in J$, $f^2 \in J^2 \subseteq P \Rightarrow f \in P \Rightarrow J = P = \{ab, ag_j, bf_i, f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t\}$, which contradicts to the hypothesis that J is not finitely generated.

Fix a ranking on $\Theta(Y)$ and take a characteristic set $\mathcal{A}$ of J under this ranking. Let $\mathcal{A} = A_1, \ldots, A_p$ and denote $\mathrm{IS} \triangleq \prod_{i=1}^{p} (\mathrm{I}_{A_i} \mathrm{S}_{A_i}) \in K\{Y\}$. Since J is prime, $J = \mathrm{sat}(\mathcal{A}) = [\mathcal{A}] : \mathrm{H}_{\mathcal{A}}^{\infty} \subseteq \{\mathcal{A}\} : (\mathrm{IS})$. Since $\mathrm{I}_{A_i}, \mathrm{S}_{A_i} \notin J$ for each i, $\mathrm{IS} \notin J$. Thus $\{J, \mathrm{IS}\}$ is finitely generated as a radical differential ideal. That is, $\exists\, h_1, \ldots, h_l \in J$ s.t. $\{J, \mathrm{IS}\} = \{h_1, \ldots, h_l, \mathrm{IS}\}$. Thus,

$$\begin{aligned} J^2 &\subseteq J \cdot \{J, \mathrm{IS}\} = J \cdot \{h_1, \ldots, h_l, \mathrm{IS}\} \\ &\subseteq \{h_1, \ldots, h_l, \mathcal{A}\} (\text{for } \mathrm{IS} \cdot J \subseteq \{\mathcal{A}\}) \\ &\subseteq J. \end{aligned}$$

Hence, $J = \{h_1, \ldots, h_l, A_1, \ldots, A_p\}$, which leads to a contradiction. So every radical differential ideal of $K\{y_1, \ldots, y_n\}$ is finitely generated as a radical differential ideal. □

Example 1: $[y^2] \subsetneqq [y^2, (y')^2] \subsetneqq [y^2, (y')^2, (y'')^2] \subsetneqq \cdots$ is an infinite increasing sequence of differential ideals.

Proof. Let $I_n = [y^2, (y')^2, \ldots, (y^{(n)})^2]$ with $n \geq 0$. Define weight for each $y^{(i)}y^{(j)}$ to be $\mathrm{wt}(y^{(i)}y^{(j)}) = i + j$. Let V_n be a subspace of $K\{Y\}$ generated by all $y^{(i)}y^{(j)}$ of degree 2 and weight n. Then we get

$$\begin{aligned} V_0 &= \mathrm{Span}_K(y^2) \\ V_1 &= \mathrm{Span}_k(yy') \\ V_2 &= \mathrm{Span}_K(yy'', (y')^2) \\ V_3 &= \mathrm{Span}_K(yy^{(3)}, y'y'') \\ &\vdots \\ V_{2n} &= \mathrm{Span}_K(yy^{(2n)}, y'y^{(2n-1)}, \ldots, (y^{(n)})^2) \\ V_{2n+1} &= \mathrm{Span}_K(yy^{(2n+1)}, y'y^{(2n)}, \ldots, y^{(n)}y^{(n+1)}) \end{aligned}$$

Clearly, $\dim V_{2n} = \dim V_{2n+1} = n + 1$ for $n \in \mathbb{N}$.
Claim: (1) $V_{2n+2} = \mathrm{Span}_K(\delta^2(V_{2n}), (y^{(n+1)})^2)$.
(2) $I_n \cap V_{2n+2} = \mathrm{Span}_K(\delta^2(V_{2n})) \subsetneqq V_{2n+2}$.
To show (1), note that $\delta^2(y^{(k)}y^{(2n-k)}) \in V_{2n+2}$ and

$$\begin{pmatrix} \delta^2(yy^{(2n)}) \\ \delta^2(y'y^{(2n-1)}) \\ \vdots \\ \delta^2((y^{(n)})^2) \\ (y^{(n+1)})^2 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 2 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 2 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 2 & 2 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}}_{A} \begin{pmatrix} yy^{(2n+2)} \\ y'y^{(2n+1)} \\ \vdots \\ y^{(n)}y^{(n+2)} \\ (y^{(n+1)})^2 \end{pmatrix}$$

$\mathrm{Det}(A) = 1 \Rightarrow \{\delta^2(V_{2n}), (y^{(n+1)})^2\}$ is a basis of $V_{2n+2} \Rightarrow$ (1) is valid.

To show (2), since $V_{2n} \subseteq I_n$ [1], $\mathrm{Span}_K\{\delta^2(V_{2n})\} \subseteq I_n \cap V_{2n+2}$. And

$$I_n \cap V_{2n+2} \subseteq \mathrm{Span}_K(\delta^{2n+2-2k}(y^{(k)})^2 : k = 0, \ldots, n) = \mathrm{Span}_K(\delta^2[\delta^{2n-2k}(y^{(k)})^2] : k = 0, \ldots, n) \subseteq \mathrm{Span}_K(\delta^2(V_{2n})).$$

Thus, $I_n \cap V_{2n+2} = \mathrm{Span}_K(\delta^2(V_{2n})) \subsetneqq V_{2n+2}$. Hence, $V_{2n} \subseteq I_n$ and $V_{2n+2} \not\subseteq I_n$ for all $n \in \mathbb{N}$. Thus, $I_n \subsetneqq I_{n+1} \, \forall \, n \in \mathbb{N}$. □

Theorem 2.2.4. *Let R be a differential ring which is Ritt-Noetherian and $\mathbb{Q} \subseteq R$. Then for every radical differential ideal $I \subsetneqq R$, there exist a finite number of prime differential ideals $P_1, \ldots, P_l$ s.t.*

$$I = \bigcap_{i=1}^{l} P_i. \tag{2.1}$$

Moreover, if (2.1) is irredundant ($\forall \, i, \bigcap_{j \neq i} P_j \not\subseteq P_i$), then this set of prime ideals is unique. In this case, $P_1, \ldots, P_l$ are called prime components *of I.*

Proof. Suppose the statement is false, i.e., the set $A = \{I \mid I \subsetneqq K\{y_1, \ldots, y_n\}$ is a radical differential ideal and I is not a finite intersection of prime differential ideals$\}$ is not empty. Since R is Ritt-Noetherian, every ascending chain of radical differential ideals has an upper bound in A. By Zorn's lemma,A has a maximal element $J \in A$. Clearly, J is not prime. So $\exists \, a, b \notin J$ but $ab \in J$. Thus, $\{J, a\} \supsetneqq J$ and $\{J, b\} \supsetneqq J$. Also, $\{J, a\} \neq R$. Indeed, if not, then $1 \in \{J, a\}$. Since $\mathbb{Q} \subseteq R, 1 \in [J, a]$ and $1 = f + \sum * \delta^k(a)$, where $f \in J$. By $ab \in J$ and J is radical, $b\delta^k(a) \in J \, \forall \, k \in \mathbb{N}$. So $b = fb + \sum * b\delta^k(a) \in J$, contradicting to $b \notin J$. Similarly, $\{J, b\} \neq R$ could be shown.
By the maximality of J, $\exists \, P_1^a, \ldots, P_l^a, P_{l+1}^b, \ldots, P_{l+t}^b$ prime differential ideals in R s.t.

$$\{J, a\} = P_1^a \cap \cdots \cap P_l^a \text{ and}$$
$$\{J, b\} = P_{l+1}^b \cap \cdots \cap P_{l+t}^b.$$

Now show $J = \{J, a\} \cap \{J, b\}$. Indeed, let $f \in \{J, a\} \cap \{J, b\}$, then $f^2 \in \{J, a\} \cdot \{J, b\} \subseteq \{J, ab\} \subseteq J \Rightarrow f \in J$. Thus, $J = \{J, a\} \cap \{J, b\} = P_1^a \cap \cdots \cap P_l^a \cap P_{l+1}^b \cap \cdots \cap P_{l+t}^b$, contradicting to the hypothesis $J \in A$. So the first statement is valid.

Uniqueness. Suppose $I = \bigcap_{i=1}^{l} P_i = \bigcap_{j=1}^{t} Q_j$ be irredundant intersections. For each $j = 1, \ldots, t$, $\bigcap_{i=1}^{l} P_i \subseteq Q_j$. Then $\exists \, i_0 \in \{1, \ldots, l\}$ s.t. $P_{i_0} \subseteq Q_j$. Indeed, suppose the contrary, then $\exists \, f_i \in P_i \backslash Q_j$ for each $i = 1, \ldots, l$. Thus, $f_1 f_2 \cdots f_l \in \bigcap_{i=1}^{l} P_i \subseteq Q_j$, which yields a contradiction. Similarly, $\exists \, j_0 \in \{1, \ldots, t\}$ s.t. $Q_{j_0} \subseteq P_{i_0} \subseteq Q_j$. Since $I = \bigcap_{j=1}^{t} Q_j$ is irredundant, $j_0 = j$ and $P_{i_0} = Q_j$. Thus, $l = t$ and $\exists$ a permutation $\sigma \in S_l$ s.t. $P_i = Q_{\sigma(i)}$. □

Corollary 2.2.5. *Every proper radical differential ideal $I \subsetneqq K\{y_1, \ldots, y_n\}$ ($\mathrm{char}(K) = 0$) can be written as a finite intersection of prime differential ideals. If $I = \bigcap_{i=1}^{l} P_i$ is irredundant, P_i are called prime components of I.*

[1] $(y^{(n)})^2 \in I_n, (y^{(n-1)})^2 \in I_n \Rightarrow y^{(n-1)}y^{(n+1)} \in I_n, (y^{(n-2)})^2 \in I_n \Rightarrow 2y^{(n+2)}y^{(n-2)} + 8y^{(n+1)}y^{(n-1)} + 6(y^{(n)})^2 \in I_n \Rightarrow y^{(n-2)}y^{(n+2)} \in I_n, \ldots, yy^{(2n)} \in I_n$.

Example: $I = \{y'^2 - 4y\} \subseteq \mathbb{Q}\{y\}$. Then $I = \{y'^2 - 4y, y'' - 2\} \cap \{y\}$ (Chapter 3).

We end this chapter by giving an example illustrating a differential ideal is not finitely generated as a differential ideal.

Example 2: The radical differential ideal $\{xy\} \subseteq K\{x, y\}$ is not finitely generated as a differential ideal. In other words, there doesn't exist finitely many differential polynomials $f_1, \ldots, f_s \in K\{x, y\}$ s.t. $\{xy\} = [f_1, \ldots, f_s]$.

Proof. Let $I = \{xy\} \subseteq K\{x, y\}$ and $J = (x^{(i)}y^{(j)} : i, j \in \mathbb{N}) \subseteq K\{x, y\}$.
Claim A: $I = J$.
Indeed, $J \subseteq I$, for $xy \in I \overset{\text{Lemma 1.3.1}}{\Longrightarrow} \forall\, i, j \in \mathbb{N}, x^{(i)}y^{(j)} \in I$.
It is easy to show that J is a differential ideal and the following fact:

$$f \notin J \Leftrightarrow f \text{ has a term not involving any } y^{(j)} \text{ (or } x^{(i)}).$$

The fact implies that $J \subseteq \{xy\}$ is a radical differential ideal and $I = J$ follows.

Now suppose the contrary, i.e., $\exists\, f_1, \ldots, f_s \in K\{x, y\}$ s.t. $I = [f_1, \ldots, f_s]$. Since $I = J$, then $\exists\, q \in \mathbb{N}$ s.t. $f_i \in [x^{(i)}y^{(j)} : 0 \leq i, j \leq q]$. Hence, $I = [x^{(i)}y^{(j)} : 0 \leq i, j \leq q]$. In particular, $x^{(q+1)}y^{(q+1)} \in [x^{(i)}y^{(j)} : 0 \leq i, j \leq q]$, we obtain $(y^{(q+1)})^2 \in [y^{(i)}y^{(j)} : i, j \leq q]\,(*)$ by substituting $x = y$ in the expression of $x^{(q+1)}y^{(q+1)}$ in terms of $x^{(i)}y^{(j)}(i, j \leq q)$.

Use the notation in Example 1, $(y^{(q+1)})^2 \in V_{2q+2}$ and $V_{2q+2} = \mathrm{Span}_K(\delta^2(V_{2q}), (y^{(q+1)})^2)$.
But, $[y^{(i)}y^{(j)} : i, j \leq q] \cap V_{2q+2} = \mathrm{Span}_K(\delta^2(V_{2q}))$.
Indeed, $V_{2q} \subseteq [(y^{(i)})^2 : i \leq q] \subseteq [y^{(i)}y^{(j)} : i, j \leq q] \Rightarrow \delta^2(V_{2q}) \subseteq [y^{(i)}y^{(j)} : i, j \leq q] \cap V_{2q+2}$.
On the other hand, $\forall\, f \in [y^{(i)}y^{(j)} : i, j \leq q] \cap V_{2q+2}$,

$$\begin{aligned} f &= \sum_{0 \leq i,j \leq q} c_{ij}\delta^{2q+2-i-j}(y^{(i)}y^{(j)}) \\ &= \sum_{0 \leq i,j \leq q} c_{ij}\delta^2\big(\delta^{2q-i-j}(y^{(i)}y^{(j)})\big) \in \mathrm{Span}_K(\delta^2(V_{2q})). \end{aligned}$$

Since $(y^{(q+1)})^2 \notin \mathrm{Span}_K(\delta^2(V_{2q}))$, $(y^{(q+1)})^2 \notin [y^{(i)}y^{(j)} : i, j \leq q]$, contradicts to $(*)$.

□

Chapter 3

The Differential Algebra-Geometry Dictionary

Let (K, δ) be a differential field of characteristic 0. Let $K\{Y\} = K\{y_1, \ldots, y_n\}$ be the differential polynomial ring in the differential variables $y_1, \ldots, y_n$ over K. Any $\Sigma \subseteq K\{Y\}$ defines a system of algebraic differential equations. The main objective of differential algebra is to study the solutions of such system (i.e., differential varieties, our main protagonists).

3.1 Ideal-Variety correspondence in differential algebra

Recall the definitions of differentially closed fields and differential varieties:

For $f \in K\{Y\} = K\{y_1, \ldots, y_n\}$ and $\eta = (\eta_1, \ldots, \eta_n) \subseteq L^n$ with $(L, \delta) \supseteq (K, \delta)$, η is a differential zero of f if $f(\eta) = 0$. Here, $f(\eta)$ means replacing $\delta^k y_i$ by $\delta^k \eta_i$ in $f(y_1, \ldots, y_n)$.

(E, δ) is differentially closed if for all $F \in E\{y_1, \ldots, y_n\}$, whenever $\exists\, (L, \delta) \supseteq (E, \delta)$ and $\eta \in L^n$ s.t. $F(\eta) = 0$, there exists $\xi \in E^n$ s.t. $F(\xi) = 0$.

Let $(K, \delta) \subseteq (E, \delta)$. (E, δ) is called a differential closure of (K, δ) if

1) (E, δ) is differentially closed, and

2) for every differentially closed field $(M, \delta) \supseteq (K, \delta)$, there is a differential embedding $\varphi : E \hookrightarrow M$ with $\varphi\,|_K = \mathrm{id}_K$.

Throughout this chapter, $(E, \delta) \supseteq (K, \delta)$ is a fixed differentially closed field. By a differential affine space, we mean any E^n for $n \in \mathbb{N}$. An element $(\eta_1, \ldots, \eta_n) \in E^n$ is called a point.

A set $V \subseteq E^n$ is called a δ-variety over K if $\exists\, \Sigma \subseteq K\{Y\}$ s.t.

$$V = \mathbb{V}(\Sigma) \triangleq \{\eta \in E^n \mid f(\eta) = 0, \forall\, f \in \Sigma\}.$$

Let $\Pi = \{\delta\text{-varieties in } E^n \text{ over } K\}$. Then Π satisfies:

1) $\emptyset, E^n \in \Pi$;

2) If $V_1, V_2 \in \Pi, V_1 \cup V_2 \in \Pi$;

3) Any intersection of elements of Π is an element of Π.

So Π is a topology on E^n, called the Kolchin topology, as compared to the Zariski topology in algebraic geometry. A δ-variety is called a Kolchin-closed set. For a set $S \subseteq E^n$, the smallest δ-variety (with respect to inclusion) containing S is called the Kolchin closure of S, denoted by S^{Kol}.

For a subset $S \subseteq E^n$, define $\mathbb{I}(S) = \{f \in K\{y_1, \ldots, y_n\} \mid \forall \eta \in S, f(\eta) = 0\}$. It is easy to show that $\mathbb{I}(S)$ is a radical δ-ideal in $K\{Y\}$, called the vanishing δ-ideal of S.

Proposition 3.1.1. *1) If $S_1 \subseteq S_2 \subseteq E^n$, then $\mathbb{I}(S_2) \subseteq \mathbb{I}(S_1)$.*

2) If $P_1 \subseteq P_2 \subseteq K\{Y\}$, then $\mathbb{V}(P_2) \subseteq \mathbb{V}(P_1)$.

3) If $S \subseteq E^n$, then $V = \mathbb{V}(\mathbb{I}(S))$ is the Kolchin closure of S and $\mathbb{I}(V) = \mathbb{I}(S)$.

Proof. 1) and 2) are straightforward.
To show 3): Let $S^{\text{Kol}} = \mathbb{V}(\Sigma)$ for $\Sigma \subseteq K\{Y\}$. For every $f \in \Sigma, f \mid_S \equiv 0 \Rightarrow f \in \mathbb{I}(S)$. So $\Sigma \subseteq \mathbb{I}(S)$. Thus, $V = \mathbb{V}(\mathbb{I}(S)) \subseteq \mathbb{V}(\Sigma) = S^{\text{Kol}}$. Hence, $S^{\text{Kol}} = V$.

$S \subseteq V \Rightarrow \mathbb{I}(V) \subseteq \mathbb{I}(S)$. If $\exists f \in \mathbb{I}(S) \backslash \mathbb{I}(V)$, then $\exists \eta \in V$ s.t. $f(\eta) \neq 0$. Set $\Sigma_1 = \mathbb{I}(V) \cup \{f\}$. Then $\Sigma_1 \subseteq \mathbb{I}(S) \Rightarrow \mathbb{V}(\Sigma_1) \supseteq \mathbb{V}(\mathbb{I}(S)) = V$. Since $\eta \in V, \eta \in \mathbb{V}(\Sigma_1)$. So $f(\eta) = 0$, which yields a contradiction. □

Now we have two maps between Π and the set of radical δ-ideals in $K\{Y\} = K\{y_1, \ldots, y_n\}$:

$$\begin{array}{rccc} \mathbb{I}: & \{\delta\text{-varieties in } E^n \text{ over } K\} & \longrightarrow & \{\text{ radical } \delta\text{-ideals in } K\{Y\}\} \\ & V & & \mathbb{I}(V) \end{array}$$

and

$$\begin{array}{rccc} \mathbb{V}: & \{\text{ radical } \delta\text{-ideals in } K\{Y\}\} & \longrightarrow & \{\delta\text{-varieties in } E^n \text{ over } K\} \\ & J & & \mathbb{V}(J) \end{array}$$

Corollary 3.1.2. *For every δ-variety V, $\mathbb{V}(\mathbb{I}(V)) = V$. Hence $\mathbb{I}$ is injective and $\mathbb{V}$ is surjective.*

Proof. By Proposition 3.1.1, $V = V^{\text{Kol}} = \mathbb{V}(\mathbb{I}(V))$. □

A point $\eta \in L^n$ ($L \supseteq K$ a differential extension field) is a *generic zero* of a differential ideal I if $I = \mathbb{I}(\eta)$. Clearly, a differential ideal I is prime $\Leftrightarrow$ I has a generic zero.
"$\Rightarrow$": If I is prime, set $L = \text{Frac}(K\{y_1, \ldots, y_n\}/I)$. Then $(\bar{y}_1, \ldots, \bar{y}_n) \in L^n$ is a generic zero of I.

Next section, we will give the differential Nullstellensatz theorem (both the weak and strong analogues of the Hilbert's Nullstellensatz theorem). Continuing Corollary 3.1.2, we will show $\mathbb{I}$ and $\mathbb{V}$ are inclusion-reversing bijective maps. For the content in this section, all the results are valid even if E is not differentially closed. But for the differential Nullstellensatz theorem to be valid, E is required to be differentially closed.

3.2 Differential Nullstellensatz

The Hilbert Nullstellensatz in algebraic geometry has two forms:
Theorem (Weak Nullstellensatz)
Let $F \subseteq K[x_1, \ldots, x_n]$. Then $\mathcal{V}(F) = \{\eta \in \bar{K}^n \mid F(\eta) = 0\} = \emptyset \Leftrightarrow 1 \in (F)$.
Theorem (Strong Nullstellensatz)
Let $F \subseteq K[x_1, \ldots, x_n]$ and $f \in K[x_1, \ldots, x_n]$. If $f \mid_{\mathcal{V}(F)} \equiv 0$, then $f \in \sqrt{(F)}$.
We have differential versions of Hilbert Nullstellensatz in differential algebra.

Theorem 3.2.1 (Weak Differential Nullstellensatz)**.** *Let $F \subseteq K\{y_1, \ldots, y_n\}$ and $(E, \delta) \supseteq (K, \delta)$ a differentially closed field. Then $\mathbb{V}(F) = \{\eta \in E^n \mid F(\eta) = 0\} = \emptyset \Leftrightarrow 1 \in [F]$.*

Proof. It suffices to show that if $[F] \neq K\{y_1, \ldots, y_n\}$, then $\exists\, \eta \in E^n$ s.t. $f(\eta) = 0$ for all $f \in F$. Since $1 \notin [F]$, $\sqrt{[F]} \neq K\{y_1, \ldots, y_n\}$. Let $\sqrt{[F]} = \cap_{i=1}^{l} P_i$ be the minimal prime decomposition. Let $M = \mathrm{Frac}(K\{y_1, \ldots, y_n\}/P_1)$. Then M is a differential extension field of K and $(\bar{y}_1, \ldots, \bar{y}_n) \in M^n$ is a generic zero of P_1. $F \subseteq P_1$ implies that $(\bar{y}_1, \ldots, \bar{y}_n)$ is a differential zero of F. Since $E \supseteq K$ is differentially closed, there exists $\eta = (\eta_1, \ldots, \eta_n) \in E^n$ s.t. $\forall\, f \in F, f(\eta) = 0$. □

Theorem 3.2.2 (Differential Nullstellensatz)**.**

- *Let $F \subseteq K\{y_1, \ldots, y_n\}$ and $f \in K\{y_1, \ldots, y_n\}$. If f vanishes at every differential zero of F in E^n, then $f \in \{F\}$.*
- $\mathbb{I}(\mathbb{V}(F)) = \{F\}$.

Proof. (Use Rabinowitsch's trick for the case $f \neq 0$)

Intruduce a new differential indeterminate t and consider the new differential polynomial set $F, 1-ft$ in $K\{y_1, \ldots, y_n, t\}$. Since f vanishes at every differential zero in E^n of F, $\mathbb{V}(F, 1-ft) \subseteq E^{n+1}$ is the emptyset. By the weak differential Nullstellensatz, $1 \in [F, 1-ft] \subseteq K\{y_1, \ldots, y_n, t\}$. Hence, $\exists\, A_i, B_i \in K\{y_1, \ldots, y_n, t\}$ and $s \in \mathbb{N}$ s.t.

$$1 = \sum_{i=0}^{s} A_i F^{(i)} + \sum_{j=0}^{s} B_j (1 - ft)^{(j)}.$$

Since $f \neq 0$, replace t by $\frac{1}{f}$ at both sides, then we have

$$1 = \sum_{i=0}^{s} A_i(y_1, \ldots, y_n, \tfrac{1}{f}) F^{(i)}.$$

There exists $m \in \mathbb{N}$ s.t. $f^m \sum_{i=0}^{s} A_i(y_1, \ldots, y_n, \frac{1}{f}) \in K\{y_1, \ldots, y_n\}$ and we have $f^m \in [F]$. □

Remark: As above, we give an abstract proof for the weak differential Nullstellensatz following Ritt. The first constructive proof was given by Seidenberg using elimination theory.

The Differential Nullstellensatz and Corollary 3.1.2 show that the two maps $\mathbb{I}$ and $\mathbb{V}$ are bijections.

Theorem 3.2.3. *The maps $V \to \mathbb{I}(V)$ and $I \to \mathbb{V}(I)$ define inclusion reversing bijections between the set of all differential varieties in E^n over K and the set of all radical differential ideals in $K\{y_1, \ldots, y_n\}$.*

Definition 3.2.4. *Let $V \subseteq E^n$ be a differential variety. Then the differential ring*

$$K\{V\} := K\{y_1, \ldots, y_n\}/\mathbb{I}(V)$$

is called the differential coordinate ring of V.[1]

$W \subseteq E^n$ is called a differential subvariety of V if $W \subseteq V$ and W is a differential variety in E^n.[2]

Theorem 3.2.3 can be generalized to arbitrary differential varieties in place of $\mathbb{A}^n = E^n$.

Corollary 3.2.5. *Let $V \subseteq E^n$ be a differential variety. The map*

[1] Since for any $a \in V$, $\bar{f}_1 = \bar{f}_2$ implies $f_1(a) = f_2(a)$. So $K\{V\}$ could be regarded as a ring of differential functions on V.

[2] Assume all differential varieties are over K unless indicated.

$$W \longmapsto \{f \in K\{V\} \mid f(a) = 0 \ \forall\, a \in W\}$$

is an inclusion reversing bijection between the set of differential subvarieties of V and the set of radical differential ideals in $K\{V\}$.

Remark: (Effective Hilbert Nullstellensatz and Effective differential Nullstellensatz)

Effective Nullstellensatz

Let $P_1, \ldots, P_m \in \mathbb{C}[x_1, \ldots, x_n] = \mathbb{C}[X]$ have degree at most $D \geq 1$. If $P_1, \ldots, P_m$ have no common zero in $\mathbb{C}^n$, then there are polynomials $A_1, \ldots, A_m \in \mathbb{C}[X]$ of degree bounded by $\mathrm{B}(D, n, m)$ s.t. $1 = A_1P_1 + \cdots + A_mP_m$.[3]

- $\deg(A_i) \leq 2(2D)^{2^{n-1}}$ (Hermann, Math. Ann., 1926)
- lower bound: $\deg(A_i) \geq D^n - D^{n-1}$ (Masser-Philippon)
- $\deg(A_i) \leq \mu n D^\mu + \mu D$ for $\mu = \min\{m, n\}$
  $\leq 2n^2 D^\mu$ (Brownawell, Ann. Math., 1987)
- $\deg(A_iP_i) \leq \begin{cases} d_1 d_2 \cdots d_m & \text{if } m \leq n \\ d_1 \cdots d_{n-1} d_m & \text{if } m > n > 1 \\ d_1 + d_m - 1 & \text{if } m > n = 1 \end{cases}$ (Kollar, J. Amer. Math. Soc., 1988)

  Here $\deg(P_i) = d_i$ and assume $d_1 \geq d_2 \geq \cdots \geq d_m > 2$.
- $\deg(A_iP_i) \leq \begin{cases} N'(d_1, \ldots, d_m; n) & \text{if } m \leq n \\ 2N'(d_1, \ldots, d_m; n) - 1 & \text{if } m > n \end{cases}$ (Jelonek, Invent. Math., 2005. New Proof)

Subsequent work on sharper bounds or new proofs.

Effective Differential Nullstellensatz

If $F_1, \ldots, F_k \in K\{y_1, \ldots, y_n\}$ have no common differential zeros in E^n, then $\exists\, s \in \mathbb{N}$ and $A_{ij} \in K\{y_1, \ldots, y_n\}$ s.t. $1 = \sum_{i=1}^{k} \sum_{j=0}^{s} A_{ij} F_i^{(j)}$.

To give a bound for s in terms of the order h, degree d and # derivation operators m and # differential variables n.[4]

Focus on the ordinary differential case:

- $s \leq A(q, \max\{n, h, d\})$.[5] (Golubitsky, J. Algebra, 2009)
- K: constant differential field. $s \leq (n(h+1)d)^{2^{c(n(e+1))^3}}$ for a universal constant $c > 0$.
  (D' Alfonso, J. complexity, 2014)
- $s \leq (nTd)^{2^{O(n^3(T+1)^3)}}$ (Gustavson, Adv. Math., 2016)

[3] If such a degree bound $\mathrm{B}(D, n, m)$ for A_i exists, to decide whether $P_1 = \cdots = P_m = 0$ has a zero is reduced to solve linear equations.

[4] If such a computable bound is given, to decide whether $\mathbb{V}(F_1, \ldots, F_k) = \emptyset$ or not is reduced to an algebraic problem and then results about effective Hilbert Nullstellensatz could be applied here.

[5] $A(\cdot, \cdot)$ Ackermann function $\begin{cases} A(0, n) = n + 1 \\ A(m+1, 0) = A(m, 1) \\ A(m+1, n+1) = A(m, A(m+1, n)) \end{cases}$

- $s \leq \begin{cases} D^{nh-p+1}2^{p+1} & \text{if } D \geq 2 \\ p+1 & \text{if } D = 1. \end{cases}$ Here $p = \dim((F))$ in $K[y_i^{(j)} : j \leq h]$.
  (Ovchinnikov, Arxiv:1610.04022v6, 2018)

Example: $F = \{y_1^2, y_1 - y_2^2, \ldots, y_{n-1} - y_n^2, 1 - y_n'\}, \mathbb{V}(F) = \emptyset$.
$1 \notin (F, \ldots, F^{(2^n-1)})$ and $1 \in (F, \ldots, F^{(2^n)})$. So $s \geq 2^n$.

3.3 Irreducible decomposition of differential varieties

A differential variety $V \subseteq E^n$ is said to be irreducible if V is not the union of two proper differential subvarieties.

Lemma 3.3.1. *A differential variety V is irreducible $\Leftrightarrow \mathbb{I}(V) \subseteq K\{y_1, \ldots, y_n\}$ is prime.*

Proof. "$\Rightarrow$" For any $f, g \in K\{Y\}, fg \in \mathbb{I}(V)$, we have

$$V = \mathbb{V}(\mathbb{I}(V), fg) = \mathbb{V}(\mathbb{I}(V), f) \cup \mathbb{V}(\mathbb{I}(V), g).$$

V is irreducible $\Rightarrow \mathbb{V}(\mathbb{I}(V), f) = V$ or $\mathbb{V}(\mathbb{I}(V), g) = V$. Equivalently, $f \in \mathbb{I}(V)$, or $g \in \mathbb{I}(V)$. So $\mathbb{I}(V)$ is prime.

"$\Leftarrow$" If $V = V_1 \cup V_2$, then $\mathbb{I}(V) = \mathbb{I}(V_1) \cap \mathbb{I}(V_2)$. Since $\mathbb{I}(V)$ is prime, $\mathbb{I}(V_1) \subseteq \mathbb{I}(V)$ or $\mathbb{I}(V_2) \subseteq \mathbb{I}(V)$, for otherwise, $\exists\, f_i \in \mathbb{I}(V_i) \backslash \mathbb{I}(V), i = 1, 2$, but $f_1 f_2 \in \mathbb{I}(V_1) \cap \mathbb{I}(V_2) = \mathbb{I}(V)$, which yields a contradiction. If $\mathbb{I}(V_1) \subseteq \mathbb{I}(V)$, then $V = V_1$; and in the other case, $V = V_2$. □

Theorem 3.3.2. *Any differential variety V is a finite union of irreducible differential varieties, i.e., $V = \bigcup_{i=1}^{l} V_i$ with V_i irreducible differential subvariety of V. Call $V = \bigcup_{i=1}^{l} V_i$ an irreducible decomposition of V. If $V = \bigcup_{i=1}^{l} V_i$ is an irredundant/minimal irreducible decomposition (in the sense $V_i \not\subseteq \bigcup_{j \neq i} V_j, \forall\, i$), then the set $\{V_1, \ldots, V_l\}$ is unique for V.*

Proof. By Theorem 2.2.4 and Corollary 2.2.5,

$$\mathbb{I}(V) = \bigcap_{j=1}^{l} P_j \text{ for } P_j \text{ prime differential ideals.}$$

$\Longrightarrow V = \mathbb{V}(\mathbb{I}(V)) = \mathbb{V}(\bigcap_{j=1}^{l} P_j) = \bigcup_{j=1}^{l} \mathbb{V}(P_j)$ is an irreducible decomposition of V.

Uniqueness: If $V = \bigcup_{i=1}^{l} V_i$ and $V = \bigcup_{j=1}^{m} W_j$ are two irredundant irreducible decomposition of V, then we have two irredundant prime decomposition for $\mathbb{I}(V)$, i.e.,

$$\mathbb{I}(V) = \bigcap_{i=1}^{l} \mathbb{I}(V_i) \text{ and } \mathbb{I}(V) = \bigcap_{j=1}^{m} \mathbb{I}(W_j).$$

By Theorem 2.2.4, $l = m$ and $\exists\, \sigma \in S_l$ s.t. $\mathbb{I}(V_i) = \mathbb{I}(W_{\sigma(i)})$. Hence, $V_i = W_{\sigma(i)}$ for $i = 1, \ldots, l$. □

Remark: Each irreducible differential variety V_i in the irredundant irreducible decomposition $V = \bigcup_{i=1}^{l} V_i$ is called an irreducible component of V. These $V_1, \ldots, V_l$ are called the maximal irreducible differential subvarieties contained in V.

Components of a single Algebraic differential equation

Let $A \in K\{y_1, \ldots, y_n\}\backslash K$ be algebraically irreducible (not the product of two differential polynomials in $K\{Y\}\backslash K$). We are going to study the prime decomposition of the radical differential ideal $\{A\}$.

Example: Let $A = y''^2 - y \in K\{y\}$. Then $A' = 2y''y^{(3)} - y', A'' = 2y''y^{(4)} + 2(y^{(3)})^2 - y''$, $A^{(3)} = 2y''y^{(5)} + 6y^{(3)}y^{(4)} - y^{(3)}$.

$\Rightarrow 2y^{(3)}A^{(3)} + A'' - 6y^{(4)}A'' = y''(4y^{(3)}y^{(5)} - 12(y^{(4)})^2 + 8y^{(4)} - 1)$.
So $\{A\} = \{A, y''\} \cap \{A, 4y^{(3)}y^{(5)} - 12(y^{(4)})^2 + 8y^{(4)} - 1\}$.

Select an arbitrary differential ranking $\mathscr{R}$ on $\Theta(Y)$ and take the separant S_A under $\mathscr{R}$. Let $\mathrm{ld}(A) = y_p^{(h)}$ for some $p \in \{1, \ldots, n\}$ and $h \in \mathbb{N}$. The order of A in y_i is defined to be $\mathrm{ord}(A, y_i) = \max\{k \mid \deg(A, y_i^{(k)}) \geq 1\}$. The order of A is defined to be $\mathrm{ord}A = \max_i\{\mathrm{ord}(A, y_i)\}$. Let $P_1 = \{A\} : \mathrm{S}_A = \{f \in K\{Y\} \mid \mathrm{S}_A f \in \{A\}\}$.

Lemma 3.3.3. *1) P_1 is prime.*

2) For a differential polynomial $F \in K\{Y\}, F \in P_1 \Leftrightarrow \delta$-rem$(F, A) = 0$. In particular, if $F \in P_1$ and $\mathrm{ord}(F, y_p) \leq \mathrm{ord}(A, y_p) = h$, then F is divisible by A.

Proof. 1) Let $fg \in P_1$ with $f, g \in K\{Y\}$. Let f_1 and g_1 be the partial remainder of f and g w.r.t. A. Then $\exists\, a, b \in \mathbb{N}$ s.t.

$$\mathrm{S}_A^a f \equiv f_1 \bmod [A], \quad \mathrm{S}_A^b g \equiv g_1 \bmod [A].$$

$\Rightarrow \mathrm{S}_A^{a+b+1} fg \equiv \ S_A f_1 g_1 \bmod [A]$.
Since $fg \in P_1 = \{A\} : \mathrm{S}_A$, $\mathrm{S}_A f_1 g_1 \in \{A\}$. Thus, $\exists\, l, q \in \mathbb{N}$ s.t.

$$(\mathrm{S}_A f_1 g_1)^l = MA + M_1 A' + M_2 A'' + \cdots + M_q A^{(q)}. \quad (*)$$

If $q = 0$, ... When $q > 0$.
Recall that for $k \geq 1, A^{(k)} = \mathrm{S}_A y_p^{(h+k)} + T_k$ with T_k free of $y_p^{(h+k)}$. Note that S_A, f_1, g_1 are free from $y_p^{(h+1)}, \ldots, y_p^{(h+q)}$. Now replace $y_p^{(h+k)}$ by $-\frac{T_k}{\mathrm{S}_A}$ for $k = 1, \ldots, q$ at both sides of $(*)$, then we have

$$(\mathrm{S}_A f_1 g_1)^l = \overline{M} \cdot A \text{ where } \overline{M} = M\,|_{y_p^{(h+k)} = -\frac{T_A}{\mathrm{S}_A}}.$$

Clearing fractions, we have $\mathrm{S}_A^t (f_1 g_1)^l = N \cdot A$. Since A is irreducible and $A \nmid \mathrm{S}_A, A \mid f_1 g_1$ and thus $A \mid f_1$ or $A \mid g_1$. Suppose that $A \mid f_1$. Then $\mathrm{S}_A^a f \in \{A\}$ and it follows that $f \in \{A\} : \mathrm{S}_A = P_1$ and P_1 is prime.

2) If δ-rem$(F, A) = 0$, then $F \in \mathrm{sat}(A) = [A] : \mathrm{S}_A^\infty$ (had better mention A is a characteristic set of $[A] : \mathrm{S}_A^\infty$ and $[A] : \mathrm{S}_A^\infty$ is prime) $\subseteq \{A\} : \mathrm{S}_A = P_1$.

Conversely, let $F \in P_1$, then $\mathrm{S}_A F \in \{A\}$. Let R be the partial remainder of F w.r.t. A, then $\mathrm{S}_A^m F \equiv R \bmod [A]$. $\mathrm{S}_A F \in \{A\} \Rightarrow \mathrm{S}_A R \in \{A\} \Rightarrow \exists\, l \in \mathbb{N}$ s.t. $(\mathrm{S}_A R)^l = MA + M_1 A' + \cdots + M_t A^{(t)}$, By the procedure in 1), we can show R is divisible by A. So δ-rem$(F, A) = 0$.

□

Proposition 3.3.4. $\{A\} = P_1 \cap \{A, \mathrm{S}_A\}$.

Proof. Clearly, $\{A\} \subseteq P_1 \cap \{A, \mathrm{S}_A\}$. Suppose $f \in P_1 \cap \{A, \mathrm{S}_A\}$, it suffices to show $f \in \{A\}$. Since $f \in \{A, \mathrm{S}_A\}$, $\exists\, l \in \mathbb{N}$, $f^l = T_1 + T_2$ for $T_1 \in [A], T_2 \in [\mathrm{S}_A]$. $f \in P_1 \Rightarrow \mathrm{S}_A f \in \{A\} \Rightarrow \delta^k(\mathrm{S}_A) f \in \{A\}$. So $f^{l+1} \in \{A\}$ and $f \in \{A\}$ follows. □

Let $\{A, \mathrm{S}_A\} = Q_1 \cap \cdots \cap Q_t$ be the minimal prime decomposition of $\{A, \mathrm{S}_A\}$. Then $\{A\} = P_1 \cap Q_1 \cap Q_1 \cap \cdots \cap Q_t$. Suppressing those Q_i with $P_1 \subseteq Q_i$ and denote the left Q_i's by $P_2, \ldots, P_r$. Then $\underline{\{A\} = P_1 \cap \cdots \cap P_r}$ is the minimal prime decomposition of $\{A\}$.

Claim For each separant S of A under any arbitrary ranking, $\mathrm{S} \notin P_1 = \{A\} : \mathrm{S}_A$ and $\mathrm{S} \in P_2, \ldots, P_r$.

Proof. $\mathrm{S} \notin P_1$ follows from Lemma 3.3.3 and the fact $A \nmid \mathrm{S}$. Since $\{A, \mathrm{S}_A\} \subseteq P_2, \ldots, P_r$, $\mathrm{S}_A \in P_1, \ldots, P_r$. $\mathrm{S} \in P_2, \ldots, P_r$ follows from the fact that $\{P_1, \ldots, P_r\}$ are the unique irreducible components of $\{A\}$. □

Remark: A is the differential characteristic set of $P_1 = \{A\} : \mathrm{S}_A = \{A\} : \mathrm{S} = \mathrm{sat}(A)$ (S is the separant of A under any other ranking). P_1 or $\mathbb{V}(P_1)$ is called the *general component* of $A = 0$. $P_2, \ldots, P_r$ are called *singular components* of $A = 0$.

Example: $n = 1, A = (y')^2 - 4y$, $\mathrm{S}_A = 2y'$. $\{A, \mathrm{S}_A\} = \{(y')^2 - 4y, 2y'\} = [y]$. $A' = 2y'(y'' - 2)$, so $y'' - 2 \in \{A\} : \mathrm{S}_A$, $y'' - 2 \notin [y]$. $\{A\} : \mathrm{S}_A \supseteq [(y')^2 - 4y, y'' - 2] = ((y')^2 - 4y, y'' - 2, y''', \cdots)$. Then $I = ((y')^2 - 4y, y'' - 2, y''', \cdots)$ is prime for $K\{y\}/I \cong K[y, y']/(A)$. Thus, $\{A\} : \mathrm{S}_A = [(y')^2 - 4y, y'' - 2]$ is the general component of A and $[y]$ is the singular component of A. To solve $(y')^2 - 4y$ over $K = (\mathbb{R}(x), \frac{\mathrm{d}}{\mathrm{d}x})$: $\frac{\mathrm{d}y}{\mathrm{d}x} = \pm 2\sqrt{y} \Rightarrow \frac{\mathrm{d}y}{2\sqrt{y}} = \pm \mathrm{d}x \Rightarrow \sqrt{y} = \pm x + c$. So $y = (x + c)^2$ or $y = 0$. (c an arbitrary constant).

Definition: A differential zero $\eta \in E^n$ of A is called a *nonsingular zero* if $\exists$ a separant S of A s.t. $\mathrm{S}(\eta) \neq 0$. And if $\mathrm{S}(\eta) = 0$ for all separants of A, η is called a *singular solution/zero* of $A = 0$.

Nonsingular zeros belong to the general component of A, but the general component of A may contain singular solutions of A.

Example: $A = (y')^2 - y^3 \in K\{y\}$. $\mathrm{S}_A = 2y'$. Since $\mathbb{V}(A, \mathrm{S}_A) = \{0\}$, $\eta = 0$ is the only singular solution of $A = 0$. $A' = 2y'y'' - 3y^2y' = 2y'(y'' - \frac{3}{2}y^2) \Rightarrow \{A\} = \{A, y'' - \frac{3}{2}y^2\} \cap [y] = \{A, y'' - \frac{3}{2}y^2\} = \mathrm{sat}(A)$. Thus, $\eta = 0$ is embedded in the general component of $A(= 0)$. (Geometrically, $K = (\mathbb{C}(t), \frac{\mathrm{d}}{\mathrm{d}t})$, $\eta_c = \frac{1}{4(t+c)^2}$ is a one-parameter family of nonsingular solutions (c arbitrary constant). $\lim_{c \to \infty} \eta_c = 0$.)

Ritt's problem (Still open!) Given $A \in K\{y_1, \ldots, y_n\}$ irreducible with $A(0, \ldots, 0) = 0$, decide whether $(0, \ldots, 0) \in \mathbb{V}(\mathrm{sat}(A))$?

With deep results not covered in our course (Low power theorem), we have Ritt's component theorem.

Theorem 3.3.5. *Let $A \in K\{y_1, \ldots, y_n\}$ be a differential polynomial not in K. Let $\{A\} = P_1 \cap \cdots \cap P_r$ be the minimal prime decomposition of $\{A\}$, then $\exists\, B_i \in K\{y_1, \ldots, y_n\}$ irreducible s.t. $P_i = \mathrm{sat}(B_i), i = 1, \ldots, r$. In particular, if A is irreducible, then $\exists\, i_0$ s.t. $B_{i_0} = aA$ ($a \in K^*$) and for $i \neq i_0$, A involves a proper derivative of the leader of each B_i w.r.t. any ranking and* $\mathrm{ord}(B_i) < \mathrm{ord}(A)$.

Chapter 4

Extensions of differential fields

Let (K, δ) be a differential field of characteristic 0. Let x be an indeterminate over K. Then δ can be extended to a derivation δ_0 on $K[x]$ s.t. $\delta_0(x) = 0$ given by $\delta_0(\sum_{i=0}^{l} r_i x^i) = \sum_{i=0}^{l} \delta(r_i) x^i$. There is also a derivation on $K[x]$ s.t. $\frac{\mathrm{d}}{\mathrm{d}x}(K) = 0$ and $\frac{\mathrm{d}}{\mathrm{d}x}(x) = 1$ given by $\frac{\mathrm{d}}{\mathrm{d}x}(\sum_{i=0}^{l} r_i x^i) = \sum_{i=1}^{l} i r_i x^{i-1}$.

Any derivation δ_1 on $K[x]$ which extends δ is given by

$$\delta_1 = \delta_0 + \delta_1(x)\tfrac{\mathrm{d}}{\mathrm{d}x}.$$

Conversely, by defining $\delta_1(x) = p(x) \in K[x]$, $\delta_1 = \delta_0 + p(x)\frac{\mathrm{d}}{\mathrm{d}x}$ is a derivation on $K[x]$ extending δ.

Proof. First suppose δ_1 is a derivation on $K[x]$ extending δ. Then $\forall\, f = \sum_{i=0}^{r} r_i x^i \in K[x]$, $\delta_1(f) = \sum_{i=0}^{r} \delta(r_i) x^i + \sum_{i=1}^{r} i r_i x^{i-1} \delta_1(x) = \delta_0(f) + \delta_1(x)\frac{\mathrm{d}}{\mathrm{d}x}(f)$. So $\delta_1 = \delta_0 + \delta_1(x)\frac{\mathrm{d}}{\mathrm{d}x}$. Now let $\delta_1 : K[x] \to K[x]$ be defined by $\delta_1(f) = \delta_0(f) + \delta_1(x)\frac{\mathrm{d}}{\mathrm{d}x}(f)$. Then $\forall\, a \in K$, $\delta_1(a) = \delta_0(a) + \delta_1(x)\frac{\mathrm{d}}{\mathrm{d}x}(a) = \delta(a)$;

$$\forall\, f, g \in K[x],\ \delta_1(f+g) = \delta_0(f+g) + \delta_1(x)\frac{\mathrm{d}}{\mathrm{d}x}(f+g) = \delta_1(f) + \delta_1(g),$$

$$\delta_1(fg) = \delta_0(fg) + \delta_1(x)\frac{\mathrm{d}}{\mathrm{d}x}(fg) = \delta_1(f)g + f\delta_1(g).$$

Thus, δ_1 is a derivation which extends δ. □

Theorem 4.0.1. *Let $K \subseteq L$ be fields of characteristic 0. Then any derivation on K could be extended to a derivation on L. This extension is unique if and only if L is algebraic over K.*

Proof. Let δ be a derivation on K. First suppose $L = K(\alpha)$. If α is transcendental over K, then there exists a derivation δ_0 on $K[\alpha]$ s.t. $\delta_0 \mid_K = \delta_K$ and $\delta_0(\alpha) = 0$. So now extends to a derivation on $L = K(\alpha)$. If α is algebraic over K, let $F(x)$ be the minimal polynomial of α over K. Let $g(x) \in K[x]$ be a polynomial to be determined. δ extends to a derivation δ_0 on $K[x]$ by setting $\delta_0(x) = 0$. So $\delta_1 = \delta_0 + g(x)\frac{\mathrm{d}}{\mathrm{d}x}$ is a derivation on $K[x]$. We want to choose $g(x)$ s.t. δ_1 maps the ideal $F \cdot K[x]$ to itself. The condition for this is that $\delta_1(F)(\alpha) = 0$, or $\delta_0(F)(\alpha) + g(\alpha)\frac{\mathrm{d}F}{\mathrm{d}x}(\alpha) = 0$. Since $\frac{\mathrm{d}F}{\mathrm{d}x}(\alpha) \neq 0$, $g(\alpha) = -\frac{\delta_0(F)(\alpha)}{\frac{\mathrm{d}F}{\mathrm{d}x}(\alpha)}$. $K(\alpha) = K[\alpha]$ implies that we can find $g(x) \in K[x]$ with desired property. Choose $g(x) \in K[x]$ s.t. δ_1 maps $F \cdot K[x]$ to itself. Now δ_1 induces a map $\bar{\delta}_1$ on $K[x]/F \cdot K[x]$ by $\bar{\delta}_1(A(x) + F \cdot K[x]) = \delta_1(A(x)) + F \cdot K[x]$ and this $\bar{\delta}_1$ is the desired derivation on $K(\alpha) = K[\alpha]$. ($\bar{\delta}_1(\alpha) = g(\alpha) = -\delta_0(F)(\alpha)/F'(\alpha)$.)

For the general case, let $E = \{(K_1, \delta_1) \mid K \subseteq K_1 \subseteq L \text{ and } \delta_1 \mid_K = \delta_K\}$. Then E is nonempty. Let $(K_1, \delta_1) \subseteq (K_2, \delta_2) \subseteq \cdots \subseteq (K_n, \delta_n) \subseteq \cdots$ be an ascending chain in E. Then $(\bigcup_i K_i, \bar{\delta})$ with $\forall\, a \in K_i$, $\bar{\delta}(a) = \delta_i(a)$ is in E. By Zorn's lemma, $\exists$ a maximal element (M, δ_M) in E. Clearly, $M = L$.

Uniqueness If L is not algebraic over K, then $\exists\, \alpha \in L$ transcendental over K. There will be more than one derivation on $K[\alpha]$ which extends δ on K. If L is algebraic over K, for each $\alpha \in L$, let $F(x) = \sum_{i=0}^{d} r_i x^i \in K[x]$ be the minimal polynomial of α over K. Let D be the derivation on L which extends δ on K. $F(\alpha) = 0 \Rightarrow 0 = D(F(\alpha)) = D(\sum_{i=0}^{d} r_i \alpha^i) = \sum_{i=0}^{d} \delta(r_i)\alpha^i + (\sum_{i=1}^{d} i r_i \alpha^{i-1}) D(\alpha)$ $\Rightarrow D(\alpha) = -(\sum_{i=0}^{d} \delta(r_i)\alpha^i)/(\sum_{i=1}^{d} i r_i \alpha^{i-1})$ which is unique. □

Corollary 4.0.2. *If $K \subseteq L$ are fields of characteristic 0 and δ be a derivation on L s.t. $\delta(K) \subseteq K$. If $\alpha \in L$ is algebraic over K, then $\delta(\alpha) \in K(\alpha)$. In particular, if $\alpha \in L$ is algebraic over a constant subfield of L, then α is a constant.*

With the language of differential polynomials, Definition 2.0.1 can be restated as:

Definition 4.0.3. *Let $K \subseteq L$ be differential field extensions and $\alpha \in L$. If $\exists\, p(y) \in K\{y\}\backslash\{0\}$ s.t. $p(\alpha) = 0$, then α is said to be differential algebraic over K. Otherwise, α is called differentially transcendental over K. Let $\alpha_1, \ldots, \alpha_n \in K$, we call $\alpha_1, \ldots, \alpha_n$ differentially algebraically dependent over K if $\exists\, F(y_1, \ldots, y_n) \in K\{y_1, \ldots, y_n\}^*$ s.t. $F(\alpha_1, \ldots, \alpha_n) = 0$. Otherwise, they are said to be differentially transcendental over K.*

Lemma 4.0.4. *Let $K \subseteq L$ be differential fields of characteristic 0 and $\alpha \in L$. Then α is differential algebraic over $K \Leftrightarrow \text{tr.deg}K\langle\alpha\rangle/K < \infty$.*

Proof. "⇒" Suppose α is differential algebraic over K. Let $A(y) \in K\{y\}$ be a characteristic set of $\mathbb{I}(\alpha) \subseteq K\{y\}$.[1] Assume $\text{ord}(A) = n$. Claim: $\text{tr.deg}K\langle\alpha\rangle/K = n$. Clearly, $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ are algebraically independent over K and $\alpha^{(n)}$ is algebraic over $K(\alpha, \alpha', \ldots, \alpha^{(n-1)})$. And $A(\alpha) = 0 \Rightarrow \mathrm{S}_A(\alpha) \cdot \alpha^{(n+1)} + T_A(\alpha) = 0$, where $T_A(\alpha) \in K(\alpha, \ldots, \alpha^{(n)}) \Rightarrow \alpha^{(n+1)} = -\frac{T_A(\alpha)}{\mathrm{S}_A(\alpha)} \in K(\alpha, \alpha', \ldots, \alpha^{(n)})$. $\Rightarrow \forall\, k \in \mathbb{N}$, $\alpha^{(n+k)} \in K(\alpha, \alpha', \ldots, \alpha^{(n)})$. So $K\langle\alpha\rangle = K(\alpha, \alpha', \ldots, \alpha^{(n)})$ and $\text{tr.deg}K\langle\alpha\rangle/K = n$.

"⇐" $n = \text{tr.deg}K\langle\alpha\rangle/K < \infty$ impies that $\alpha, \alpha', \alpha'', \ldots, \alpha^{(n)}$ are algebraically dependent over K. So α is differential algebraic over K. □

Remark:

1) If α is differential algebraic over K and $f(y) \neq 0$ is a differential polynomial of minimal order which vanishes at α, then $\text{tr.deg}K\langle\alpha\rangle/K = \text{ord}(f)$.

2) The result "⇒" is false in the partial differential case $(K, \{\delta_1, \ldots, \delta_m\})$, where $\text{tr.deg}K\langle\alpha\rangle/K$ might be infinity but the differential type[2] of $K\langle\alpha\rangle$ is $\leq m - 1$.

Example: $K = (\mathbb{R}(x), \frac{\mathrm{d}}{\mathrm{d}x})$, $L = (K\langle \mathrm{e}^x, \sin(x)\rangle, \frac{\mathrm{d}}{\mathrm{d}x})$. Since $\frac{\mathrm{d}}{\mathrm{d}x}(\mathrm{e}^x) = \mathrm{e}^x$ and $(\frac{\mathrm{d}}{\mathrm{d}x})^2(\sin(x)) = -\sin(x)$, e^x and $\sin(x)$ are differentially algebraic over K with $\text{tr.deg}K\langle\mathrm{e}^x\rangle/K = 1, \text{tr.deg}K\langle\sin(x)\rangle/K = 1$.

[1] $A(y)$ is of minimal order and minimal degree under the desired order.

[2] Differential type is the degree of differential dimension polynomial of $\mathbb{I}(\alpha)$

We say $L \subseteq K$ is differential algebraic over K, if each element $a \in L$ is differential algebraic over K. Note that every differential field extension with finite transcendence degree is differential algebraic over K. But the converse doesn't hold.

Lemma 4.0.5. *Let $L \supseteq K$ be a differential field extension and $a, b \in L$ which are differential algebraic over K. Then $a+b, ab, \delta(a)$ and a^{-1} $(a \neq 0)$ are differential algebraic over K. In particular, a differential field extension generated by differential algebraic elements is differential algebraic over K and the set of all elements in L which are differential algebraic over K is a differential algebraic differential field extension of K.*

Proof. Since $\mathrm{tr.deg}K\langle a\rangle/K < \infty$ and $\mathrm{tr.deg}K\langle b\rangle/K < \infty$, we have $\mathrm{tr.deg}K\langle a, b\rangle/K = \mathrm{tr.deg}K\langle a\rangle/K + \mathrm{tr.deg}K\langle a\rangle\langle b\rangle/K\langle a\rangle < \infty$. □

Lemma 4.0.6. *Let $K \subseteq L \subseteq M$ be differential fields. Then M is differential algebraic over $K \Leftrightarrow$ M is differential algebraic over L and L is differential algebraic over K.*

Proof. "$\Rightarrow$" Valid by definition.

"$\Leftarrow$" For any $a \in M$, a is differential algebraic over L, so $\exists\, p(y) \in L\{y\}\backslash\{0\}$ s.t. $p(a) = 0$. Denote the coefficient set of $p(y)$ to be $\{b_1, \ldots, b_t\} \subseteq L$. Then $\mathrm{tr.deg}K\langle b_1, \ldots, b_t, a\rangle/K = \mathrm{tr.deg}K\langle b_1, \ldots, b_t\rangle/K + \mathrm{tr.deg}K\langle b_1, \ldots, b_t, a\rangle/K\langle b_1, \ldots, b_t\rangle < \infty$. Thus, $\mathrm{tr.deg}K\langle a\rangle/K < \infty$ and a is differential algebraic over K. □

4.1 Differential primitive theorem

It is a well-known theorem of algebra that a finite algebraic extension of a field K of characteristic 0 has a primitive element ω:

$$K(a_1, \ldots, a_n) = K(\omega).$$

In this section, we treat analogous problem for arbitrary differential field of characteristic 0.

Note that $\mathbb{Q}\langle\pi, \mathrm{e}\rangle$ is a finitely generated differential extension field of $\mathbb{Q}$ $(\delta(\pi) = \delta(\mathrm{e}) = 0)$. Clearly, $\mathbb{Q}\langle\pi, \mathrm{e}\rangle \neq \mathbb{Q}\langle\omega\rangle$ for any $\omega \in \mathbb{Q}\langle\pi, \mathrm{e}\rangle$. So to derive an analog of primitive element theorem in differential algebra, we need some restrictions. For the ordinary differential fields, the mild condition is that (K, δ) contains a non-constant element (i.e., $\exists\, \eta \in K$ s.t. $\eta' \neq 0$).

We need two lemmas for preparation to state the main theorem. Throughout this section, (K, δ) is a fixed differential field of characteristic 0 containing a non-constant.

A set of elements $\eta_1, \ldots, \eta_s$ of K is called *linearly dependent* if there exists a relation

$$c_1\eta_1 + \cdots + c_s\eta_s = 0,$$

where the c_i's are constant elements in K, not all zero.

The wronskian determinant of $\eta_1, \ldots, \eta_s$ is defined as

$$\mathrm{wr}(\eta_1, \ldots, \eta_s) = \begin{vmatrix} \eta_1 & \cdots & \eta_s \\ \eta_1' & \cdots & \eta_s' \\ \cdots & \cdots & \cdots \\ \eta_1^{(s-1)} & \cdots & \eta_s^{(s-1)} \end{vmatrix}.$$

Lemma 4.1.1. *Let $\eta_1, \ldots, \eta_s$ be elements in K. Then $\eta_1, \ldots, \eta_s$ are linearly independent $\Leftrightarrow$ $wr(\eta_1, \ldots, \eta_s) = 0$, i.e.,*

$$\begin{vmatrix} \eta_1 & \cdots & \eta_s \\ \eta_1' & \cdots & \eta_s' \\ \cdots & \cdots & \cdots \\ \eta_1^{(s-1)} & \cdots & \eta_s^{(s-1)} \end{vmatrix} = 0 \qquad (*)$$

Proof. "⇒" Suppose $\eta_1, \dots, \eta_s$ are linearly dependent. Then $\exists\, c_1, \dots, c_s$, constants of K, not all zero s.t. $c_1\eta_1 + \cdots + c_s\eta_s = 0$. Differentiate the relation $s-1$ times, we get a system of linear equations for c's:

$$\begin{cases} c_1\eta_1 + \cdots + c_s\eta_s = 0 \\ c_1\eta_1' + \cdots + c_s\eta_s' = 0 \\ \qquad \cdots\cdots \\ c_1\eta_1^{(s-1)} + \cdots + c_s\eta_s^{(s-1)} = 0 \end{cases}$$

has a nonzero solution. So $(*)$ holds.

"⇐" Suppose we have $(*)$. We now show $\eta_1, \dots, \eta_s$ are linearly dependent by induction on s. If $s = 1$, $\eta_1 = 0 \Rightarrow \eta_1$ is linearly dependent. Suppose it is valid for the case $\leq s-1$ and we treat for the case s. By $(*)$, $\exists\, c_1, \dots, c_s \in K$, not all zero s.t.

$$c_1\eta_1^{(j)} + \cdots + c_s\eta_s^{(j)} = 0 \quad (**) \quad \text{for } j = 0, \dots, s-1.$$

If $\mathrm{wr}(\eta_1, \dots, \eta_{s-1}) = \begin{vmatrix} \eta_1 & \cdots & \eta_{s-1} \\ \eta_1' & \cdots & \eta_{s-1}' \\ \cdots & \cdots & \cdots \\ \eta_1^{(s-2)} & \cdots & \eta_{s-1}^{(s-2)} \end{vmatrix} = 0$, by the induction hypothesis, $\eta_1, \dots, \eta_{s-1}$ are linearly dependent, so $\eta_1, \dots, \eta_s$ are linearly dependent too.

So it suffices to consider the case $\mathrm{wr}(\eta_1, \dots, \eta_{s-1}) \neq 0$. Then in this case $c_s \neq 0$. By dividing c_s on both sides when necessary, we can take $c_s = 1$. For $j = 0, \dots, s-2$, differentiate $(**)$ and then subtract the equation $(**)$ corresponding to $j+1$, then we have

$$c_1'\eta_1^{(j)} + \cdots + c_{s-1}'\eta_{s-1}^{(j)} = 0 \text{ for } j = 0, \dots, s-2.$$

Since $\mathrm{wr}(\eta_1, \dots, \eta_{s-1}) \neq 0$, we have c_i'$= 0$ for $i = 1, \dots, s-1$. Thus, $\eta_1, \dots, \eta_s$ are linearly dependent. □

Lemma 4.1.2. *If G is a nonzero differential polynomial in $K\{y_1, \dots, y_n\}$, there exist elements $\eta_1, \dots, \eta_n$ in K such that $G(\eta_1, \dots, \eta_n) \neq 0$.*

Proof. It suffices to treat a differential polynomial in a single indeterminate y (the case $n = 1$). Take a nonconstant $\xi \in K$. Fix any $r \in \mathbb{N}$.

Claim: If $G \in K\{y\}$ is a nonzero differential polynomial of order $\leq r$, there exists

$$\eta = c_0 + c_1\xi + \cdots + c_r\xi^r$$

where all the c_i's are constants in K, satisfying $G(\eta) \neq 0$.
Suppose the claim is false and let H be a nonzero differential polynomial of lowest rank which vanishes for every element $c_0 + c_1\xi + \cdots + c_r\xi^r$ (c_i are constants from K). Let $\mathrm{ord}(H, y) = s$. Then $0 < s \leq r$. Introduce algebraic indeterminates $z_0, \dots, z_r$ with z_i'$= 0$. Then $\overline{H} = H(z_0 + z_1\xi + \cdots + z_r\xi^r) \in K[z_0, \dots, z_r]$ is the zero polynomial. Take the partial derivative of $\overline{H}$ w.r.t. $z_0, \dots, z_s$, then

$$\begin{cases} \overline{\dfrac{\partial H}{\partial y}} = 0 \\ \overline{\dfrac{\partial H}{\partial y}}\xi + \overline{\dfrac{\partial H}{\partial y'}}\xi' + \cdots + \overline{\dfrac{\partial H}{\partial y^{(s)}}}\xi^{(s)} = 0 \\ \qquad \cdots\cdots \\ \overline{\dfrac{\partial H}{\partial y}}\xi^s + \overline{\dfrac{\partial H}{\partial y'}}(\xi^s)' + \cdots + \overline{\dfrac{\partial H}{\partial y^{(s)}}}(\xi^s)^{(s)} = 0 \end{cases} \quad \Big(\overline{\dfrac{\partial H}{\partial y^{(j)}}} = \dfrac{\partial H}{\partial y^{(j)}}(z_0 + \cdots + z_r\xi^r) \Big)$$

So

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ \xi & \xi' & \cdots & \xi^{(s)} \\ \cdots & \cdots & \cdots & \cdots \\ \xi^s & (\xi^s)' & \cdots & (\xi^s)^{(s)} \end{pmatrix} \begin{pmatrix} \overline{\frac{\partial H}{\partial y}} \\ \overline{\frac{\partial H}{\partial y'}} \\ \vdots \\ \overline{\frac{\partial H}{\partial y^{(s)}}} \end{pmatrix} = 0$$

Since $\frac{\partial H}{\partial y^{(s)}}$ is of lower rank than H, $\overline{\frac{\partial H}{\partial y^{(s)}}} \neq 0$. Thus,

$$\begin{vmatrix} \xi' & (\xi^2)' & \cdots & (\xi^s)' \\ \xi'' & (\xi^2)'' & \cdots & (\xi^s)'' \\ \cdots & \cdots & \cdots & \cdots \\ \xi^{(s)} & (\xi^2)^{(s)} & \cdots & (\xi^s)^{(s)} \end{vmatrix} = \mathrm{wr}(\xi', (\xi^2)', \ldots, (\xi^s)') = 0.$$

So $\exists\, c_1, \ldots, c_s$ constants of K, not all zero s.t. $c_1\xi' + c_2(\xi^2)' + \cdots + c_s(\xi^s)' = 0$. Then $c_1\xi + c_2\xi^2 + \cdots + c_s\xi^s = c_0$ with c_0 a constant. Thus ξ is algebraic over the constant field of K. By Corollary 4.0.2, $\xi' = 0$, a contradiction to the hypothesis $\xi' \neq 0$. So we can find some $\eta = c_0 + c_1\xi + \cdots + c_r\xi_r$ with c_i constants s.t. $G(\eta) \neq 0$. □

Remark:

1) Lemma 4.1.2 is false without the restriction that (K, δ) contains at least a nonconstant element. A non-example: $K = \mathbb{Q}$, $G(y) = y'$.

2) For the partial differential case $(K, \{\delta_1, \ldots, \delta_m\})$, the condition that "$\exists\, \xi \in K$ s.t. $\xi' = 0$" should be replaced by

$$\text{“ } \exists\, \xi_1, \ldots, \xi_m \in K \text{ s.t. } \begin{vmatrix} \delta_1(\xi_1) & \cdots & \delta_1(\xi_m) \\ \delta_2(\xi_1) & \cdots & \delta_2(\xi_m) \\ \cdots & \cdots & \cdots \\ \delta_m(\xi_1) & \cdots & \delta_m(\xi_m) \end{vmatrix} \neq 0. \text{ ”}$$

The lemma is called " non-vanishing of differential polynomials ".

3) This is the differential analog of the following result in Algebra:

" Let K be an infinite field. Then for any nonzero polynomial $f \in K[y_1, \ldots, y_n]$, $\exists\, (a_1, \ldots, a_n) \in K^n$ s.t. $f(a_1, \ldots, a_n) \neq 0$. "

Theorem 4.1.3 (Differential Primitive Element Theorem)**.** *Let (K, δ) be a <u>non-constant</u> differential field of characteristic 0 (i.e., $\exists\, b \in K$, $\delta(b) \neq 0$). Assume $K\langle\alpha_1, \ldots, \alpha_n\rangle$ is differential algebraic over K. Then $\exists\, \xi \in K\langle\alpha_1, \ldots, \alpha_n\rangle$ s.t. $K\langle\alpha_1, \ldots, \alpha_n\rangle = K\langle\xi\rangle$.*[3]

Proof. It suffices to show that if γ, β are differential algebraic over K, then $\exists\, e \in K$ s.t.

$$K\langle\gamma, \beta\rangle = K\langle\gamma + e\beta\rangle.$$

Introduce a new differential indeterminate t over $K\langle\gamma, \beta\rangle$ and consider $\gamma + t\beta \in K\langle t\rangle\langle\gamma, \beta\rangle$. By Lemma 4.0.5, $\gamma + t\beta$ is differential algebraic over $K\langle t\rangle$. Consider the prime differential ideal $\mathbb{I}(\gamma + t\beta) \subseteq K\langle t\rangle\{y\}$ and suppose $A(y) \in K\langle t\rangle\{y\}$ is a characteristic set of $\mathbb{I}(\gamma + t\beta)$. Then $A(\gamma + t\beta) = 0$

[3] In other words, every finitely generated differential algebraic extension field of (K, δ) is generated by a single element.

but $S_A(\gamma + t\beta) \neq 0$. Assume $\mathrm{ord}(A) = s$. Clearing denominators when necessary, we can take $A \in K\{t, y\}$ and write $A(t, y)$ for convenience.

Now we have $A(t, \gamma + t\beta) = 0$ but $\frac{\partial A}{\partial y^{(s)}}(t, \gamma + t\beta) \neq 0$. Note that

$$\frac{\partial((\gamma + t\beta)^{(k)})}{\partial t^{(s)}} = \begin{cases} 0, & k < s \\ \beta, & k = s \end{cases} \quad \text{for } k \leq s.$$

Take the partial derivative of $A(t, \gamma + t\beta) = 0$ w.r.t. $t^{(s)}$, we have

$$\frac{\partial A}{\partial t^{(s)}}(t, \gamma + t\beta) + \beta \cdot \frac{\partial A}{\partial y^{(s)}}(t, \gamma + t\beta) = 0.$$

Since $\frac{\partial A}{\partial y^{(s)}}(t, \gamma + t\beta) \neq 0$ belongs to $K\langle\gamma, \beta\rangle\{t\}$, by Lemma 4.1.2, $\exists\, e \in K$ s.t. $\frac{\partial A}{\partial y^{(s)}}(e, \gamma + e\beta) \neq 0$. Thus, $\beta = -\frac{\frac{\partial A}{\partial t^{(s)}}(e, \gamma + e\beta)}{\frac{\partial A}{\partial y^{(s)}}(e, \gamma + e\beta)} \in K\langle\gamma + e\beta\rangle$ and $K\langle\gamma, \beta\rangle = K\langle\gamma + e\beta\rangle$ follows. □

Corollary 4.1.4. *Let (K, δ) be a nonconstant differential field. Let $K\langle\eta_1, \ldots, \eta_n\rangle$ be a differential algebraic extension field of K. Then $\exists\, e_1, \ldots, e_n \in K$ s.t. $K\langle\eta_1, \ldots, \eta_n\rangle = K\langle e_1\eta_1 + \cdots + e_n\eta_n\rangle$.*

Remark: G. Pogudin proved the differential primitive theorem for the case

$$\begin{cases} ①K' = \{0\}; \\ ②K\langle\eta_1, \ldots, \eta_n\rangle \text{ has a nonconstant} \end{cases}.$$

("The primitive element theorem for differential fields with zero derivation on the ground field. J. Pure Appl. Algebra, 4035-4041, 2015.")

4.2 Differential transcendence bases

Let R be a differential ring. Elements $\alpha_1, \ldots, \alpha_n$ in a differential over-ring S of R are called differentially algebraically dependent over R if there exists a nonzero $G \in R\{y_1, \ldots, y_n\}$ s.t. $G(\alpha_1, \ldots, \alpha_n) = 0$. Otherwise, $\alpha_1, \ldots, \alpha_n$ are called differentially (δ-) algebraically independent over R. A subset of S is called δ-algebraically independent over R if all its subsets are δ-algebraically independent over R.

Definition 4.2.1. *Let $K \subseteq L$ be an extension of differential fields and $A \subseteq L$. An element $b \in L$ is called* δ-algebraically dependent on *A (over K) if b is δ-algebraic over $K\langle A\rangle$. A subset B of L is called δ-algebraically dependent on A (over K) if every element of B is δ-algebraically dependent on A.*[4]

Lemma 4.2.2. *Let $K \subseteq L$ be an extension of δ-fields, $A \subseteq L$ and $b \in L$. Then b is δ-algebraically dependent on A if and only if $\exists\, f \in K\{y_1, \ldots, y_n, z\}$ and $a_1, \ldots, a_n \in A$ such that $f(a_1, \ldots, a_n, z) \neq 0$ and $f(a_1, \ldots, a_n, b) = 0$.*

Proof. Assume b is δ-algebraically dependent on A. Then by definition, b is δ-algebraically over $K\langle A\rangle$, so $\exists$ a nonzero $g \in K\langle A\rangle\{z\}$ s.t. $g(b) = 0$. Let $\{a_1, \ldots, a_n\} \subseteq A$ be the subset appearing effectively in the coefficients of g. After multiplying g by appropriate element from $K\{a_1, \ldots, a_n\}$, we can assume $g \in K\{a_1, \ldots, a_n, z\}$. Thus, this g satisfies the desired property. The converse is obvious. □

[4]Note: Since K is our base differential field, for simplicity, we usually omit "over K".

Lemma 4.2.3. *Let $K \subseteq L$ be an extension of δ-fields and A be a subset of L which is δ-algebraically independent over K. Let $b \in L$. If A, b are δ-algebraically dependent over K, then b is δ-algebraic over $K\langle A\rangle$.*

Proof. Since A, b are δ-algebraically dependent over K, then $\exists\, 0 \neq f \in K\{y_1, \ldots, y_n, z\}$ s.t. $f(a_1, \ldots, a_n, b) = 0$ for some $a_1, \ldots, a_n \in A$. Since $a_1, \ldots, a_n$ are δ-algebraically independent over K, $f(a_1, \ldots, a_n, z) \neq 0$. Thus, b is δ-algebraic over $K\langle A\rangle$. □

Lemma 4.2.4 (Transitivity of δ-algebraic dependence)**.** *Let $(K, \delta) \subseteq (L, \delta)$ and $A, B, C \subseteq L$. If A is δ-algebraically dependent on B and B is δ-algebraically dependent on C, then A is δ-algebraically dependent on C.*

Proof. By the assumption, $K\langle B\rangle\langle A\rangle$ is δ-algebraic over $K\langle B\rangle$ and $K\langle C\rangle\langle B\rangle$ is δ-algebraic over $K\langle C\rangle$. By Lemma 4.0.6, $K\langle C, B, A\rangle$ is δ-algebraic over $K\langle C\rangle$. Thus, each element of A is δ-algebraic over $K\langle C\rangle$. □

Lemma 4.2.5 (The exchange property)**.** *Let $a_1, \ldots, a_n, b$ be elements from a δ-extension field of K. If b is δ-algebraically dependent on $a_1, \ldots, a_n$ but not on $a_1, \ldots, a_{n-1}$, then a_n is δ-algebraically dependent on $a_1, \ldots, a_{n-1}, b$.*

Proof. Since b is δ-algebraically dependent on $a_1, \ldots, a_n$, by Lemma 4.2.2, there exists $g \in K\{y_1, \ldots, y_n, z\}\backslash\{0\}$ s.t. $g(a_1, \ldots, a_n, z) \neq 0$ and $g(a_1, \ldots, a_n, b) = 0$. Regard g as a univariate δ-polynomial in y_n with coefficients from $K\{y_1, \ldots, y_{n-1}, z\}$, and let $g_1, \ldots, g_n \in K\{y_1, \ldots, y_{n-1}, z\}$ be all the nonzero coefficients. Then $\exists\, i$ s.t. $g_i(a_1, \ldots, a_{n-1}, z) \neq 0$, for otherwise, $g(a_1, \ldots, a_{n-1}, a_n, z) = 0$. Since b is not δ-algebraically dependent on $a_1, \ldots, a_{n-1}$, $g_i(a_1, \ldots, a_{n-1}, b) \neq 0$. So $g(a_1, \ldots, a_{n-1}, y_n, b) \neq 0$ and consequently, a_n is δ-algebraically dependent on $a_1, \ldots, a_{n-1}, b$. □

Proposition 4.2.6. *Let $K \subseteq L$ be an extension of δ-fields and $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_m\}$ be two subsets of L. Assume that 1) A is δ-algebraically independent over K and 2) A is δ-algebraically dependent on B. Then $n \leq m$.*

Proof. Let $r = |A \cap B|$. If $r = n$, then we are done. Now assume $r < n$ and write $B = a_1, \ldots, a_r, b_{r+1}, \ldots, b_m$. Since a_{r+1} is δ-algebraically dependent on $a_1, \ldots, a_r, b_{r+1}, \ldots, b_m$ but not on $a_1, \ldots, a_r$, there will be a b_j $(r+1 \leq j \leq m)$ s.t. a_{r+1} is δ-algebraically dependent on $a_1, \ldots, a_r, b_{r+1}, \ldots, b_j$ but not δ-algebraically dependent on $a_1, \ldots, a_r, b_{r+1}, \ldots, b_{j-1}$. Bt the exchange property (Lemma 4.2.5), b_j is δ-algebraically dependent on $a_1, \ldots, a_r, b_{r+1}, \ldots, b_{j-1}, a_{r+1}$, and thus δ-algebraically dependent on $B_1 := (B\backslash\{b_j\}) \cup \{a_{r+1}\}$. Therefore, B is δ-algebraically dependent on B_1. Since A is δ-algebraically dependent on B, by Lemma 4.2.4, A is δ-algebraically dependent on B_1. Note that $|B_1| = m$ and $|A \cap B_1| = r + 1$. Continuing in this way, we will eventually arrive at $r = n$, i.e., $A \subseteq B_{n-r}$. So $n \leq m$. □

Definition 4.2.7. *Let $(K, \delta) \subseteq (L, \delta)$. A subset A of L is called a* δ-transcendence basis *of L over K if 1) A is δ-algebraically independent over K and 2) L is δ-algebraic over $K\langle A\rangle$.*

By the size of a set, we mean its cardinality if the set is finite, and ∞ otherwise.

Theorem 4.2.8. *Let $(K, \delta) \subseteq (L, \delta)$. Then every δ-generating set of $L \supseteq K$ contains a δ-transcendence basis of L over K. In particular, there exists a δ-transcendence basis of L over K. Moreover, any two δ-transcendence bases of L over K are of the same size.*

Proof. Let M be a δ-generating set of L over K, i.e., $L = K\langle M\rangle$. Let

$$N = \{S \subseteq M \mid S \text{ is } \delta\text{-algebraically independent over } K\}.$$

Then $\emptyset \in N \neq \emptyset$. Clearly, the union of every chain of elements in N is again in N. So by Zorn's lemma, there exists a maximal element A in N.

Claim: A is a δ-transcendence basis of L over K.
We now show the claim. For any $a \in M$, a, A are δ-algebraically dependent over K. By Lemma 4.2.3, a is δ-algebraic over $K\langle A\rangle$, so M is δ-algebraic over $K\langle A\rangle$. And by Lemma 4.0.5, $L = K\langle M\rangle$ is δ-algebraic over $K\langle A\rangle$. Thus, $A \subseteq M$ is a δ-transcendence basis of L over K.

Now suppose A and B are both δ-transcendence bases of L over K. By symmetry, it suffices to show that the size of $A \geq$ the size of B. If A is an infinite set, it is automatically valid. So we may assume A is finite. B is already a finite set. Let B_1 be a finite subset of B. Since A is a δ-transcendence basis of L over K, each element of B_1 is δ-algebraic over $K\langle A\rangle$, and B_1 is δ-algebraically dependent on A. By Proposition 4.2.6, $|B_1| \leq |A|$. Thus, $|B| \leq |A|$. □

Corollary 4.2.9. *Let $(K, \delta) \subseteq (L, \delta)$ and $L = K\langle M\rangle$. If A is a maximal δ-algebraically independent subset of M, then A is a δ-transcendence basis of L over K.*

Theorem 4.2.8 guarantees we can make the following definition:

Definition 4.2.10. *Let $(K, \delta) \subseteq (L, \delta)$. The size of a δ-transcendence basis of L over K is called the* δ-transcendence degree *of L over K. It is denoted by δ-tr.deg(L/K).*

Corollary 4.2.11. *Let $(K, \delta) \subseteq (L, \delta)$ and $L = K\langle a_1, \ldots, a_n\rangle$. Then δ-tr.deg$(L/K) \leq n$, and the δ-transcendence degree of a finitely δ-generated δ-field extension is finite.*

Proof. It is clear from Corollary 4.2.9. □

Corollary 4.2.12. *Let $(K, \delta) \subseteq (L, \delta)$. If L contains n δ-independent elements, then $n \leq \delta$-tr.deg(L/K). In fact, δ-tr.deg$(L/K) = \sup\{n \in \mathbb{N} \mid \exists\, a_1, \ldots, a_n \in L$ which are δ-algebraically independent over $K\}$.*

Proof. Let $a_1, \ldots, a_n \in L$ be δ-algebraically independent over K. We can enlarge $\{a_1, \ldots, a_n\}$ to a δ-generating set B of L over K. Then $\{a_1, \ldots, a_n\}$ is contained in a maximal δ-algebraically independent subset $A' \subseteq B$. By Corollary 4.2.9, A' is a δ-transcendence basis of L over K. Thus, $n \leq \delta$-tr.deg(L/K) and also

$$\sup\{n \in \mathbb{N} \mid \exists\, a_1, \ldots, a_n \in L \text{ which are } \delta\text{-algebraically independent over } K\} \leq \delta\text{-tr.deg}(L/K).$$

The reverse estimate is clear, for a δ-transcendence basis is δ-algebraically independent over K. □

Theorem 4.2.13. *Let $K \subseteq L \subseteq M$ be δ-fields. Then*

$$\delta\text{-tr.deg}(M/K) = \delta\text{-tr.deg}(M/L) + \delta\text{-tr.deg}(L/K).$$

(Here, $\infty + a(\infty) = \infty$).

Proof. Let A be a transcendence basis of L over K and B a δ-transcendence basis of M over L.

Claim: $A \cup B$ is a δ-transcendence basis of M over K.
First, since B is δ-algebraically independent over $K\langle A\rangle$ $(\subseteq L)$, $A \cup B$ is δ-algebraically independent over K. It remains to show M is δ-algebraic over $K\langle A, B\rangle$. Since each element of M is δ-algebraic over $L\langle B\rangle$ and each element of L is δ-algebraic over $K\langle A\rangle$, M is δ-algebraic over $K\langle A, B\rangle$. Thus, $A \cup B$ is a δ-transcendence basis of M over K and $A \cap B = \emptyset$ implies that δ-tr.deg$(M/K) = \delta$-tr.deg$(M/L) + \delta$-tr.deg(L/K). □

Adjoining the differential primitive element theorem, we have

Proposition 4.2.14. *Let $L = K\langle a_1, \ldots, a_n\rangle$ and suppose K contains a nonconstant element in the case $d = \delta\text{-tr.deg}(L/K) = 0$. Then L is δ-generated by no more than $d+1$ elements.*

Proof. In the case $d = 0$, this is the differential primitive element theorem. Assume $d > 0$. Then $\exists\, \{\xi_1, \ldots, \xi_d\} \subseteq \{a_1, \ldots, a_n\}$ s.t. $\xi_1, \ldots, \xi_d$ is a δ-transcendence basis of L over K, and denote the others by $\xi_{d+1}, \ldots, \xi_n$. Then $L = K\langle \xi_1, \ldots, \xi_d\rangle\langle \xi_{d+1}, \ldots, \xi_n\rangle = K\langle \xi_1, \ldots, \xi_d\rangle\langle a_{d+1}\xi_{d+1} + \cdots + a_n\xi_n\rangle$. $(d > 0 \Rightarrow K\langle \xi_1, \ldots, \xi_d\rangle' \neq \{0\})$. □

4.3 Applications to differential varieties

Let (K, δ) be a δ-field of characteristic 0 and $V \subseteq \mathbb{A}^n$ an irreducible δ-variety over K.[5] The coordinate δ-ring of V is $K\{V\} \triangleq K\{y_1, \ldots, y_n\}/\mathbb{I}(V)$. Here $K\{V\}$ is a δ-domain and we consider the δ-quotient field $K\langle V\rangle = \text{Frac}(K\{V\})$. Naturally, $K\langle V\rangle$ is a δ-field extension of K and called the δ-function field of V. Clearly, $(\bar{y}_1, \ldots, \bar{y}_n) \in K\langle V\rangle^n$ is a generic point of V. Given any other generic point $(a_1, \ldots, a_n)$ of V, we have $K\langle V\rangle = K\langle \bar{y}_1, \ldots, \bar{y}_n\rangle \cong K\langle a_1, \ldots, a_n\rangle$ with $\bar{y}_i \leftrightarrow a_i$. In particular, $\delta\text{-tr.deg}K\langle \bar{y}_1, \ldots, \bar{y}_n\rangle/K = \delta\text{-tr.deg}K\langle a_1, \ldots, a_n\rangle/K$.

In order to measure the "size" of a differential variety (i.e., the solution set of algebraic differential equations), we introduce the notion of differential dimension:

Definition 4.3.1. *Let $V \subseteq \mathbb{A}^n$ be an irreducible δ-variety over K. The δ-dimension of V is defined as the δ-transcendence degree of the δ-function field of V over K. That is,*

$$\delta\text{-dim}(V) = \delta\text{-tr.deg}K\langle V\rangle/K.$$

For an arbitrary V with irreducible components $V_1, \ldots, V_m$,

$$\delta\text{-dim}(V) = \max_i \delta\text{-dim}(V_i).$$

Another equivalent definition of differential dimension in the language of differential ideals is given by Ritt:

Definition 4.3.2. *Let $P \subseteq K\{y_1, \ldots, y_n\}$ be a prime δ-ideal. A δ-variable set $U \subseteq \{y_1, \ldots, y_n\}$ is called a δ-independent set modulo P if $P \cap K\{U\} = \{0\}$. A* parametric set of P *is a maximal δ-independent set modulo P. The δ-dimension of P (or $\mathbb{V}(P)$) is defined to be the cardinal number of its parametric set.*

Exercise: Please show different parametric sets of a prime δ-ideal have the same cardinal number. And show Definition 4.3.1 and Definition 4.3.2 are equivalent for prime δ-ideals or irreducible δ-varieties.

Lemma 4.3.3. *Let V be a δ-variety and $W \subseteq V$ a δ-subvariety. Then $\delta\text{-dim}(W) \leq \delta\text{-dim}(V)$.*

Proof. First assume W and V are both irreducible. $W \subseteq V$ implies that $\mathbb{I}(W) \supseteq \mathbb{I}(V)$. Suppose $\delta\text{-dim}(W) = d$ and $\{y_1, \ldots, y_d\}$ is a parametric set of $\mathbb{I}(W)$. Clearly, $\mathbb{I}(V) \cap \{y_1, \ldots, y_d\} = \{0\}$ and $\{y_1, \ldots, y_d\}$ is a δ-independent set modulo $\mathbb{I}(V)$ which could be extended to a parametric set of $\mathbb{I}(V)$. Thus, $\delta\text{-dim}(V) = \delta\text{-dim}(\mathbb{I}(V)) \geq d$.

Now let V and W be arbitrary. Let W_1 be an irreducible component of W with $\delta\text{-dim}(W) = \delta\text{-dim}(W_1)$. Then W_1 is contained in an irreducible component V_1 of V. By the above,

$$\delta\text{-dim}(W) = \delta\text{-dim}(W_1) \leq \delta\text{-dim}(V_1) \leq \delta\text{-dim}(V).$$

[5] Here $\mathbb{A}^n = \bar{K}^n$ with $(\bar{K}, \delta)$ a δ-closed field containing (K, δ).

□

Exercise: Let $W \subseteq V$ be two irreducible δ-varieties with $\delta\text{-dim}(W) = \delta\text{-dim}(V)$. Is $W = V$?

It is true in the algebraic case but not valid in differential algebra:

Non-example: Let $W = \mathbb{V}(y') \subseteq \mathbb{A}^1$ and $V = \mathbb{V}(y'') \subseteq \mathbb{A}^1$. Then $W \subseteq V$ and $\delta\text{-dim}(W) = \delta\text{-dim}(V)$. But $W \neq V$.

This example shows that the differential dimension is not a fine enough measure of size, thus we need a more discriminating measure: the differential dimension polynomial of an irreducible δ-variety V or $\mathbb{I}(V)$.

The idea of Hilbert polynomial for homogeneous ideals suggests that it might be a way to consider the truncated coordinate ring by order: Let $P \subseteq K\{y_1, \ldots, y_n\}$ be a prime δ-ideal. Denote $K[y_1^{[t]}, \ldots, y_n^{[t]}] = K[y_i^{(j)} : j \leq t, i = 1, \ldots, n]$ and let $P_t = P \cap K[y_1^{[t]}, \ldots, y_n^{[t]}]$. Then P_t is a prime algebraic ideal with dimension $\dim(P_t)$. Kolchin showed that for $t \gg 0$, $\dim(P_t)$ is a numerical polynomial. We state it with the language of (δ-)field extensions.

Theorem 4.3.4 (Kolchin)**.** *Let $P \subseteq K\{y_1, \ldots, y_n\}$ be a prime δ-ideal with a generic point $\eta = (\eta_1, \ldots, \eta_n)$. Then there exists a numerical polynomial $\omega_P(t) \in \mathbb{R}[t]$ with the following properties:*

1) For sufficiently large $t \in \mathbb{N}$, $\dim(P_t) = \omega_P(t)$;

2) $\omega_P(t) = d(t+1) + s$ with $d = \delta\text{-dim}(\mathbb{V}(P))$ and some $s \in \mathbb{N}$;

3) (Computation of $\omega_P(t)$) Let $\mathcal{A} = A_1, \ldots, A_l$ be a characteristic set of P w.r.t. some orderly ranking of $\Theta(Y) = \{\delta^k y_j : k \in \mathbb{N}, j = 1, \ldots, n\}$ and suppose $\mathrm{ld}(A_i) = y_{\sigma(i)}^{(s_i)}$. Then $\omega_P(t) = (n-l)(t+1) + \sum_{i=1}^{l} s_i$.

4) $\omega_P(t) = n(t+1) \Leftrightarrow P = [0]$ (i.e., $\mathbb{V}(P) = \mathbb{A}^n$); $\omega_P(t) = 0 \Leftrightarrow \mathbb{V}(P)$ is a finite set.

Proof. Denote $\eta^{[t]} = (\eta_1, \ldots, \eta_n, \eta_1', \ldots, \eta_n', \ldots, \eta_1^{(t)}, \ldots, \eta_n^{(t)})$. Clearly, $\eta^{[t]}$ is a generic point of $P_t \subseteq K[y_1^{[t]}, \ldots, y_n^{[t]}]$. So $\dim(P_t) = \mathrm{tr.deg} K(\eta^{[t]})/K$. For each $A \in \mathcal{A}$, $A(\eta) = 0$ and $\mathrm{I}_A(\eta) \neq 0$ imply that $u_A(\eta)$ is algebraic over $K(\eta_j^{(k)} : y_j^{(k)} < u_A, j = 1, \ldots, n)$. Repeated differentiation shows that if v is any derivative of u_A, then $v(\eta)$ is algebraic over $K(\eta_j^{(k)} : y_j^{(k)} < v, j = 1, \ldots, n)$. Let M denote the set of all derivatives $y_j^{(k)}$ that are not derivatives of any u_A ($A \in \mathcal{A}$) and let $M(t) = M \cap \{y_j^{(k)} : k \leq t, j = 1, \ldots, n\}$. So, for $t \geq \max\{s_1, \ldots, s_l\}$, we have that

$$K(\eta^{[t]}) \text{ is algebraic over } K\big((v(\eta))_{v \in M(t)}\big).^6 \qquad (*)$$

Thus, $\dim(P_t) = \mathrm{tr.deg} K(\eta^{[t]})/K = \mathrm{Card}(M(t))$. Since

$$M(t) = \underbrace{\{y_{\sigma(i)}, y'_{\sigma(i)}, \ldots, y_{\sigma(i)}^{(s_i-1)} : i = 1, \ldots, l\}}_{\text{derivatives of leading variables}} \cup \underbrace{\{y_j, y_j', \ldots, y_j^{(t)} : j \neq \sigma(1), \ldots, \sigma(l)\}}_{\text{parametric variable parts}},$$

[6] Arrange $\{y_j^{(k)} : k \leq t, j = 1, \ldots, n\} \backslash M(t)$ in increasing order: $u_{A_1} < \cdots$. From the above, u_{A_1} is algebraic over $K\big((v(\eta))_{v \in M(t)}\big)$ and $(*)$ can be shown by induction.

$\mathrm{Card}(M(t)) = (n-l)(t+1) + \sum_{i=1}^{l} s_i$. So $\dim(P_t) = (n-l)(t+1) + \sum_{i=1}^{l} s_i$ for $t \geq \max\{s_1, \ldots, s_l\}$. Denote $\omega_P(t) = (n-l)(t+1) + \sum_{i=1}^{l} s_i$. This finishes the proof of 1) and 3).

To show 4), $\omega_P(t) = n(t+1) \Leftrightarrow M(t) = \{y_j^{(k)} : k \leq t, j = 1, \ldots, n\} \Leftrightarrow P = [0]$; And $\omega_P(t) = 0 \Leftrightarrow M(t) = \emptyset \Leftrightarrow \mathrm{ld}(\mathcal{A}) = \{y_1, \ldots, y_n\} \Leftrightarrow \mathbb{V}(P)$ is a finite set.

It suffices to show $\delta\text{-dim}(P) = n - l$ to complete the proof of 2). Assume $d = \delta\text{-dim}(P) = \delta\text{-tr.deg}K\langle\eta\rangle/K$. W.L.O.G, let $\eta_1, \ldots, \eta_d$ be a differential transcendence basis of $K\langle\eta\rangle$ over K. Thus, $\omega_P(t) = \mathrm{tr.deg}K(\eta_1^{[t]}, \ldots, \eta_n^{[t]})/K = (n-l)(t+1) + \sum_{i=1}^{l} s_i \geq \mathrm{tr.deg}K(\eta_1^{[t]}, \ldots, \eta_d^{[t]})/K = d(t+1)$, and $n - l \geq d$ follows. Conversely, let $\{z_1, \ldots, z_{n-l}\} = \{y_1, \ldots, y_n\} \backslash \{y_{\sigma(1)}, \ldots, y_{\sigma(l)}\}$. Since any nonzero polynomial in $K\{z_1, \ldots, z_{n-l}\}$ is reduced w.r.t. $\mathcal{A}$, we have $K\{z_1, \ldots, z_{n-l}\} \cap P = \{0\}$. So $\{z_1, \ldots, z_{n-l}\}$ is an independent set modulo P and can be enlarged to be a parametric set of P. Thus, $n - l \leq \delta\text{-dim}(P) = d$. Hence, $n - l = d = \delta\text{-dim}(P)$. □

Definition 4.3.5. *Let $V \subseteq \mathbb{A}^n$ be an irreducible differential variety over K and $P = \mathbb{I}(V)$. The above $\omega_P(t)$ is defined as the* differential dimension polynomial *of P or V, also denoted by $\omega_V(t)$.*

Remark:

1) The δ-dimension polynomial of an irreducible δ-variety $V \subseteq \mathbb{A}^n$ is of the form

$$\omega_V(t) = d(t+1) + s, \text{ where } d = \delta\text{-dim}(V).$$

The number s is defined as the *order* of V, denoted by $\mathrm{ord}(V)$. The order is the rigorous definition for the notion "the number of arbitrary constants" of the solution of algebraic differential equations.

2) In the partial differential case, $(K, \{\delta_1, \ldots, \delta_m\})$, we have the similar notion of differential dimension polynomial. There, $\omega_V(t) = a_m\binom{t+m}{m} + a_{m-1}\binom{t+m-1}{m-1} + \cdots + a_1(t+1) + a_0$, where $a_m = \delta\text{-dim}(V)$.

Example: Let $W = \mathbb{V}(y') \subseteq \mathbb{A}^1$ and $V = \mathbb{V}(y'') \subseteq \mathbb{A}^1$. $W \subsetneqq V$ but $\delta\text{-dim}(W) = \delta\text{-dim}(V)$. Note that $\omega_W(t) = 1$ and $\omega_V(t) = 2$.

The next proposition shows that δ-dimension polynomial is a finer measure than δ-dimension.

Proposition 4.3.6. *Let $W, V \subseteq \mathbb{A}^n$ be irreducible δ-varieties and $W \subsetneqq V$. Then $\omega_W(t) < \omega_V(t)$.*

Proof. Let $P_1 = \mathbb{I}(W)$ and $P_2 = \mathbb{I}(V)$. Then $W \subsetneqq V$ implies that $P_1 \supsetneqq P_2$. So for t sufficiently large, $P_1 \cap K[y_1^{[t]}, \ldots, y_n^{[t]}] \supsetneqq P_2 \cap K[y_1^{[t]}, \ldots, y_n^{[t]}]$, consequently,

$$\begin{aligned} \omega_W(t) &= \dim P_1 \cap K[y_1^{[t]}, \ldots, y_n^{[t]}] \\ &< \dim P_2 \cap K[y_1^{[t]}, \ldots, y_n^{[t]}] \\ &= \omega_V(t) \quad \text{for } t \gg 0. \end{aligned}$$

□

We end this section by showing that an irreducible δ-variety is differentially birationally equivalent to an irreducible δ-variety of codimension 1.

We now identify elements of the differential coordinate ring $K\{V\} = K\{y_1, \ldots, y_n\}/\mathbb{I}(V)$ with K-valued functions on V and call them differential polynomial functions on V. And each element of $K\langle V\rangle = \mathrm{Frac}(K\{V\})$ can be identified as a differential rational function on V. If $\eta \in V$, $\frac{f}{g} \in K\langle V\rangle$ is defined at η if $g(\eta) \neq 0$ $(f, g \in K\{V\})$.

Definition 4.3.7. *Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be irreducible δ-varieties over K. A* differential rational map $\varphi : V \cdots \to W$ *is a family $(f_1, \ldots, f_m) \in K\langle V\rangle^m$ such that $\varphi(\eta) = (f_1(\eta), \ldots, f_m(\eta)) \in W$ whenever the coordinate functions $f_1, \ldots, f_m$ are defined at η. φ is called* dominant *if the Kolchin closure of $\varphi(V)$ is W (or equivalently, φ maps a generic point of V to that of W).*

And, φ is called a differential birational map *if φ is dominant and there is a dominant differential rational map $\psi : W \cdots \to V$, called the* generic inverse *of φ such that*

- *if φ is defined at η and ψ is defined at $\varphi(\eta)$, then $\psi(\varphi(\eta)) = \eta$;*
- *if ψ is defined at ξ and φ is defined at $\psi(\xi)$, then $\varphi(\psi(\xi)) = \xi$.*

In this case, we also call V and W are δ-birationally equivalent.

Theorem 4.3.8. *Suppose (K, δ) contains a nonconstant element. Let $P \subseteq K\{u_1, \ldots, u_d, y_1, \ldots, y_{n-d}\}$ be a prime δ-ideal with a parametric set $\{u_1, \ldots, u_d\}$. Then $\exists\, a_1, \ldots, a_{n-d} \in K$ s.t. $[P, \omega - a_1y_1 - \cdots - a_{n-d}y_{n-d}] \subseteq K\{u_1, \ldots, u_d, y_1, \ldots, y_{n-d}, \omega\}$ has a characteristic set of the form*

$$\begin{aligned} &X(u_1, \ldots, u_d, \omega) \\ &I_1(u_1, \ldots, u_d, \omega)y_1 - T_1(u_1, \ldots, u_d, \omega) \\ &\qquad\qquad \vdots \\ &I_{n-d}(u_1, \ldots, u_d, \omega)y_{n-d} - T_{n-d}(u_1, \ldots, u_d, \omega) \end{aligned}$$

w.r.t. the elimination ranking $u_1 < \cdots < u_d < \omega < y_1 < \cdots < y_{n-d}$.

Proof. Let $\eta = (\bar{u}_1, \ldots, \bar{u}_d, \bar{y}_1, \ldots, \bar{y}_{n-d})$ be a generic point of P. Introduce $n - d$ new differential indeterminates $\lambda_1, \ldots, \lambda_{n-d}$ over $K\langle\eta\rangle$. Let

$$J = [P, \omega - \lambda_1 y_1 - \cdots - \lambda_{n-d}y_{n-d}] \subseteq K\{u_1, \ldots, u_d, y_1, \ldots, y_{n-d}, \lambda_1, \ldots, \lambda_{n-d}, \omega\}.$$

Then J is a prime δ-ideal with a generic point

$$\xi = (\bar{u}_1, \ldots, \bar{u}_d, \bar{y}_1, \ldots, \bar{y}_{n-d}, \lambda_1, \ldots, \lambda_{n-d}, \lambda_1\bar{y}_1 + \cdots + \lambda_{n-d}\bar{y}_{n-d}).$$

Since $\delta\text{-dim}(P) = d$, $\delta\text{-tr.deg}K\langle\eta\rangle/K = d$ and

$$\begin{aligned} \delta\text{-tr.deg}K\langle\xi\rangle/K &= \delta\text{-tr.deg}K\langle\eta\rangle/K + \delta\text{-tr.deg}K\langle\eta\rangle\langle\lambda_1, \ldots, \lambda_{n-d}\rangle/K\langle\eta\rangle \\ &= d + n - d = n. \end{aligned}$$

So $J_\lambda = J \cap K\{u_1, \ldots, u_d, \lambda_1, \ldots, \lambda_{n-d}, \omega\} \neq [0]$ and $\{u_1, \ldots, u_d, \lambda_1, \ldots, \lambda_{n-d}\}$ is a parametric set of J_λ. Let $\{R(u_1, \ldots, u_d, \lambda_1, \ldots, \lambda_{n-d}, \omega)\}$ be a characteristic set of J_λ w.r.t. the elimination ranking $u_1 < \cdots < u_d < \lambda_1 < \cdots < \lambda_{n-d} < \omega$. Denote $s = \mathrm{ord}(R, \omega) \geq 0$. Since $R(\bar{u}_1, \ldots, \bar{u}_d, \lambda_1, \ldots, \lambda_{n-d}, \lambda_1\bar{y}_1 + \cdots + \lambda_{n-d}\bar{y}_{n-d}) = 0$, for $j = 1, \ldots, n-d$, take the partial derivative of this identity w.r.t. $\lambda_j^{(s)}$ on both sides, then we obtain

$$\overline{\frac{\partial R}{\partial \lambda_j^{(s)}}} + \overline{\frac{\partial R}{\partial \omega^{(s)}}} \cdot \bar{y}_j = 0, \tag{4.1}$$

where $\overline{\frac{\partial R}{\partial \lambda_j^{(s)}}}$ and $\overline{\frac{\partial R}{\partial \omega^{(s)}}}$ are obtained from $\frac{\partial R}{\partial \lambda_j^{(s)}}$ and $\frac{\partial R}{\partial \omega^{(s)}}$ by substituting $(u_1,\dots,u_d,\lambda_1,\dots,\lambda_{n-d},\omega) = (\bar{u}_1,\dots,\bar{u}_d,\lambda_1,\dots,\lambda_{n-d},\lambda_1\bar{y}_1+\cdots+\lambda_{n-d}\bar{y}_{n-d})$. Note that $\frac{\partial R}{\partial \omega^{(s)}} \notin J_\lambda$, so $\overline{\frac{\partial R}{\partial \omega^{(s)}}} \neq 0$. As $\overline{\frac{\partial R}{\partial \omega^{(s)}}} \in K\{\eta\}\{\lambda_1,\dots,\lambda_{n-d}\}$ is nonzero, by the non-vanishing theorem of nonzero polynomials, $\exists\, a_1\dots,a_{n-d} \in K$ s.t. $\overline{\frac{\partial R}{\partial \omega^{(s)}}}|_{\lambda_i=a_i} \in K\{\eta\}\backslash\{0\}$. Let $I(u_1,\dots,u_d,\omega) = \frac{\partial R}{\partial \omega^{(s)}}|_{\lambda_i=a_i} \in K\{u_1,\dots,u_d,\omega\}$. Then $I(\bar{u}_1,\dots,\bar{u}_d,a_1\bar{y}_1+\cdots+a_{n-d}\bar{y}_{n-d}) = \overline{\frac{\partial R}{\partial \omega^{(s)}}}|_{\lambda_i=a_i} \neq 0$.

Let $J_a = [P, \omega - a_1y_1 - \cdots - a_{n-d}y_{n-d}] \subseteq K\{u_1,\dots,u_d,y_1,\dots,y_{n-d},\omega\}$. Then J_a is a prime δ-ideal with a generic point

$$\xi_a = (\bar{u}_1,\dots,\bar{u}_d,\bar{y}_1,\dots,\bar{y}_{n-d},a_1\bar{y}_1+\cdots+a_{n-d}\bar{y}_{n-d}).$$

Clearly, $I(u_1,\dots,u_d,\omega) \notin J_a$. Let $T_j(u_1,\dots,u_d,\omega) = -\frac{\partial R}{\partial \lambda_j^{(s)}}|_{\lambda_i=a_i}$. By (4.1),

$$I(u_1,\dots,u_d,\omega)y_j - T_j(u_1,\dots,u_d,\omega) \in J_a.$$

Since δ-tr.deg$K\langle\xi_a\rangle/K = d$, $J_a \cap K\{u_1,\dots,u_d,\omega\} \neq [0]$ with a parametric set $\{u_1,\dots,u_d\}$. So its characteristic set consists of a single δ-polynomial. Let $X(u_1,\dots,u_d,\omega)$ be an irreducible polynomial constituting a characteristic set of $J_a \cap K\{u_1,\dots,u_d,\omega\}$ w.r.t the elimination ranking $\mathscr{R}$: $u_1 < \cdots < u_d < \omega$. For each j, take the differential remainder of $Iy_j - T_j$ w.r.t X (under $\mathscr{R}$). Since $I \notin J_a \cap K\{u_1,\dots,u_d,\omega\}$, δ-rem$(Iy_j - T_j, X)$ is of the form $I_jy_j - T_j^0$ where $I_j, T_j^0 \in K\{u_1,\dots,u_d,\omega\}$, $I_j \notin J_a$.

Claim: $X(u_1,\dots,u_d,\omega), I_1y_1 - T_1^0,\dots,I_{n-d}y_{n-d} - T_{n-d}^0$ is a characteristic set of J_a w.r.t. the elimination ranking $u_1 < \cdots < u_d < \omega < y_1 < \cdots < y_{n-d}$. Indeed, for all $f \in J_a$, first perform the Ritt-Kolchin reduction process for f w.r.t. $I_1y_1 - T_1^0,\dots,I_{n-d}y_{n-d} - T_{n-d}^0$, then we get $f_0 \in J_a \cap K\{u_1,\dots,u_d,\omega\}$, thus f_0 could be reduced to 0 by X. Thus, we have proved the theorem. □

Remark:

1) The above irreducible $X(u_1,\dots,u_d,\omega)$ is called a *differential resolvent* of P or $\mathbb{V}(P)$.

2) With the obtained $a_1,\dots,a_{n-d}$, we have $K\langle\bar{u}_1,\dots,\bar{u}_d,\bar{y}_1,\dots,\bar{y}_{n-d}\rangle = K\langle\bar{u}_1,\dots,\bar{u}_d,a_1\bar{y}_1+\cdots+a_{n-d}\bar{y}_{n-d}\rangle$. (Proposition 4.2.14) In the case $d=0$, this is the primitive theorem.

Corollary 4.3.9. *Let (K,δ) contain a nonconstant element. Let $V \subseteq \mathbb{A}^n$ be an irreducible δ-variety. Then V is δ-birationally equivalent to the general component of an irreducible δ-polynomial (i.e., an irreducible δ-variety of codimension 1).*

Proof. Suppose δ-dim$(V) = d$ and $\{u_1,\dots,u_d\}$ is a parametric set of $P = \mathbb{I}(V) \subseteq K\{u_1,\dots,u_d,y_1,\dots,y_{n-d}\}$. By Theorem 4.3.8, $\exists\, a_1\dots,a_{n-d} \in K$ s.t. $J_a = [P,\omega - a_1y_1 - \cdots - a_{n-d}y_{n-d}] \subseteq K\{u_1,\dots,u_d,y_1,\dots,y_{n-d},\omega\}$ has a characteristic set of the form

$$\begin{aligned} &X(u_1,\dots,u_d,\omega)\\ &I_1(u_1,\dots,u_d,\omega)y_1 - T_1(u_1,\dots,u_d,\omega)\\ &\qquad\vdots\\ &I_{n-d}(u_1,\dots,u_d,\omega)y_{n-d} - T_{n-d}(u_1,\dots,u_d,\omega)\end{aligned}$$

w.r.t. the elimination ranking $u_1 < \cdots < u_d < \omega < y_1 < \cdots < y_{n-d}$, where X is irreducible $(*)$.

Let $W = \mathbb{V}(\text{sat}(X)) \subseteq \mathbb{A}^{d+1}$ be the general component of X.

- Define $\varphi : V \cdots \to W$ by $\varphi(u_1,\dots,u_d,y_1,\dots,y_{n-d}) = (u_1,\dots,u_d,a_1y_1+\cdots+a_{n-d}y_{n-d})$

- Define $\psi : W \cdots \to V$ by $\psi(u_1, \ldots, u_d, \omega) = (u_1, \ldots, u_d, \frac{T_1(u_1,\ldots,u_d,\omega)}{I_1(u_1,\ldots,u_d,\omega)}, \ldots, \frac{T_{n-d}(u_1,\ldots,u_d,\omega)}{I_{n-d}(u_1,\ldots,u_d,\omega)})$.

Let $\xi = (\bar{u}_1, \ldots, \bar{u}_d, \bar{y}_1, \ldots, \bar{y}_{n-d})$ be a generic point of V and $\eta = (\bar{u}_1, \ldots, \bar{u}_d, \bar{\omega})$ be a generic point of W. It is easy to show that both φ and ψ are dominant, and $(\psi \circ \varphi)(\xi) = \xi$, $(\varphi \circ \psi)(\eta) = \eta$ from $(*)$. So V and W are δ-birationally equivalent. □

Example: Let $K = (\mathbb{Q}(t), \frac{\mathrm{d}}{\mathrm{d}t})$ and $V = \mathbb{V}(y_1', y_2') \subseteq \mathbb{A}^2(\bar{K})$. Introduce new δ-indeterminates $\omega, \lambda_1, \lambda_2$ and consider $J = [y_1', y_2', \omega - \lambda_1 y_1 - \lambda_2 y_2] \subseteq K\{\omega, \lambda_1, \lambda_2, y_1, y_2\}$. To eliminate y_1, y_2 in order to get $X(\omega) \in K\{\omega\}$, we have

$$R(\omega, \lambda_1, \lambda_2) = \begin{vmatrix} \omega & -\lambda_1 & -\lambda_2 \\ \omega' & -\lambda_1' & -\lambda_2' \\ \omega'' & -\lambda_1'' & -\lambda_2'' \end{vmatrix} = (\lambda_1\lambda_2' - \lambda_1'\lambda_2)\omega'' - (\lambda_1\lambda_2'' - \lambda_1''\lambda_2)\omega' + (\lambda_1'\lambda_2'' - \lambda_1''\lambda_2')\omega.$$

$\mathrm{S}_R y_1 + \frac{\partial R}{\partial \lambda_1''} = \mathrm{S}_R y_1 + (\lambda_2\omega' - \lambda_2'\omega), \mathrm{S}_R y_2 + \frac{\partial R}{\partial \lambda_2''} = \mathrm{S}_R y_2 - (\lambda_1\omega' - \lambda_1'\omega)$ with $\mathrm{S}_R = \lambda_1\lambda_2' - \lambda_1'\lambda_2$. Choose $\lambda_1 = 1, \lambda_2 = t$, then $\overline{\mathrm{S}_R} = 1 \neq 0$. So

$$X(\omega) = \omega'', y_1 + (t\omega' - \omega), y_2 - \omega'$$

is a characteristic set of $[y_1', y_2', \omega - y_1 - ty_2]$ $(\subseteq K\{\omega, y_1, y_2\})$ w.r.t. the elimination ranking $\omega < y_1 < y_2$. Let $W = \mathbb{V}(\omega'') \subseteq \mathbb{A}^1$. Then V and W are δ-birationally equivalent. Indeed, let

$$\begin{array}{rccc} \varphi: & V & \cdots\to & W \\ & (y_1, y_2) & \longmapsto & y_1 + ty_2 \end{array} \quad \text{and} \quad \begin{array}{rccc} \psi: & W & \cdots\to & V \\ & \omega & \longmapsto & (\omega - t\omega', \omega'). \end{array}$$

Then, $\psi \circ \varphi(y_1, y_2) = \psi(y_1 + ty_2) = (y_1 + ty_2 - t(y_1 + ty_2)', (y_1 + ty_2)') = (y_1, y_2)$ and $\varphi \circ \psi(\omega) = \omega - t\omega' + t\omega' = \omega$. Note that $X(\omega)$ is a δ-resolvent of V, and if c_1, c_2 are algebraic indeterminates with $c_1' = c_2' = 0$, then $\mathbb{Q}(t)\langle c_1, c_2\rangle = \mathbb{Q}(t)\langle c_1 + tc_2\rangle$.

Chapter 5

Symbolic-integration for elementary functions

5.1 Symbolic integration of elementary functions

Let (R, D) be a differential ring and $C_R = \{r \in R \mid \mathrm{D}(r) = 0\}$ be the ring of constants of (R, D). We have the following facts:

1) Let 1 be the identity in R, then $\mathrm{D}(1) = 0$.

2) For any $n \in N$, $a \in R$, $\mathrm{D}(a^n) = na^{n-1}\mathrm{D}(a)$.

3) If b is invertible in R, then $\mathrm{D}(\frac{a}{b}) = \frac{\mathrm{D}(a)b - a\mathrm{D}(b)}{b^2}$.

4) If a_i is invertible in R, then for any $m_i \in \mathbb{Z}$, $\frac{\mathrm{D}(a_1^{m_1} \cdots a_s^{m_s})}{a_1^{m_1} \cdots a_s^{m_s}} = \sum_{i=1}^{s} m_i \frac{\mathrm{D}(a_i)}{a_i}$.

5) Let $\mathrm{Der}(R) = \{\mathrm{D} : R \to R \mid \mathrm{D} \text{ is a derivation on } R\}$. Then $\mathrm{Der}(R)$ is a R-module, i.e., $r_1\mathrm{D}_1 + r_2\mathrm{D}_2 \in \mathrm{Der}(R)$ for all $r_1, r_2 \in R$ and $\mathrm{D}_1, \mathrm{D}_2 \in \mathrm{Der}(R)$.

Let (R, D) and $(\bar{R}, \bar{\mathrm{D}})$ be differential rings. If $R \subseteq \bar{R}$ and $\bar{\mathrm{D}}|_R = \mathrm{D}$, then $(\bar{R}, \bar{\mathrm{D}})$ is called a differential extension of (R, D).

Theorem 5.1.1. *1) Let (R, D) be a differential integral domain. Then D can be uniquely extended to the quotient field F of R by*

$$\mathrm{D}(\frac{a}{b}) = \frac{\mathrm{D}(a)b - a\mathrm{D}(b)}{b^2}.$$

2) Let (F, D) be a differential field and α be algebraic over F. Then D can be uniquely extended to the algebraic extension $F(\alpha)$.

3) Let (F, D) be a differential field and t be transcendental over F. Then D can be uniquely extended to $F(t)$ by fixing the value $\mathrm{D}(t) \in F(t)$.

Example: Let $F = \mathbb{Q}(x)$ and $\alpha \in \bar{F}$ satisfying that

$$4\alpha^2 - 9x = 0.$$

Then $\frac{\mathrm{d}}{\mathrm{d}x}(4\alpha^2 - 9x) = 8\alpha\frac{\mathrm{d}\alpha}{\mathrm{d}x} - 9 = 0 \Rightarrow \frac{\mathrm{d}\alpha}{\mathrm{d}x} = \frac{9}{8\alpha}$.

In general, we have

Theorem 5.1.2. *Let (F, D) be a differential field of characteristic 0 and α be algebraic over F. Then $\mathrm{D}(\alpha) \in F(\alpha)$.*

Proof. If $\alpha \neq 0$. Assume that $P \in F[x]$ be the minimal polynomial of α, i.e., $P(\alpha) = 0$ and P is irreducible over F. Write $P = P_d x^d + P_{d-1}x^{d-1} + \cdots + P_0$, with $P_i \in F$ and $P_0 P_d \neq 0$.

$$\mathrm{D}(P(\alpha)) = \mathrm{D}(P)(\alpha) + P_x(\alpha)\mathrm{D}(\alpha),$$

where $\mathrm{D}(P) = \sum_{i=0}^{d} \mathrm{D}(P_i)x^i$, $P_x = \sum_{i=1}^{d} iP_i x^{i-1}$. Since P is irreducible, we have $\gcd(P, P_x) = 1$, which implies $aP + bP_x = 1$ for some $a, b \in F[x]$. Thus,

$$\mathrm{D}(\alpha) = \frac{-\mathrm{D}(P)(\alpha)}{P_x(\alpha)} = -\mathrm{D}(P)(\alpha) \cdot b(\alpha) \in F(\alpha).$$

□

Corollary 5.1.3. *Let $\alpha(x)$ be an algebraic function over $\mathbb{C}(x)$. Then $\alpha(x)$ satisfies a nontrivial linear differential equation with coefficients in $\mathbb{C}[x]$, i.e.,*

$$P_n \cdot \frac{\mathrm{d}^n \alpha}{\mathrm{d}x^n} + P_{n-1} \cdot \frac{\mathrm{d}^{n-1}\alpha}{\mathrm{d}x^{n-1}} + \cdots + P_0 \alpha = 0,$$

where $P_i \in \mathbb{C}[x]$ and $P_n \neq 0$ should be P_i not all zero.

Proof. Since $\frac{\mathrm{d}^i \alpha}{\mathrm{d}x^i} \in \mathbb{C}(x)(\alpha)$ and $[\mathbb{C}(x)(\alpha) : \mathbb{C}(x)] = n < \infty$, we have $\{\alpha, \frac{\mathrm{d}\alpha}{\mathrm{d}x}, \ldots, \frac{\mathrm{d}^n \alpha}{\mathrm{d}\alpha^n}\}$ is linearly dependent over $\mathbb{C}(x)$. □

Example: Let $F = \mathbb{C}(x)$, $\mathrm{D} = \frac{\mathrm{d}}{\mathrm{d}x}$. We first show that $t = \exp(x)$ is transcendental over F.

Note that $\mathrm{D}(t) = t$. Suppose that $\exp(x)$ is algebraic over F. Then there exists an irreducible polynomial $P = P_0 + P_1 y + \cdots + y^n \in F[y]$ with $P_0 \neq 0$ s.t.

$$\begin{aligned}
& t^n + P_{n-1}t^{n-1} + \cdots + P_0 = 0 \\
\Rightarrow\ & nt^{n-1}\mathrm{D}(t) + \mathrm{D}(P_{n-1})t^{n-1} + (n-1)P_{n-1}\mathrm{D}(t)t^{n-2} + \cdots + \mathrm{D}(P_0) = 0 \\
\Rightarrow\ & nt^n + (\mathrm{D}(P_{n-1}) + (n-1)P_{n-1})t^{n-1} + \cdots + \mathrm{D}(P_0) = 0 \\
\Rightarrow\ & \frac{\mathrm{D}(P_0)}{P_0} = n \neq 0.
\end{aligned}$$

Claim: $\mathrm{D}(y) = ny$ has no nonzero solution in $\mathbb{C}(x)$.
If $f = \frac{p(x)}{q(x)}$ is a nonzero solution of $\mathrm{D}(y) = ny$, then

$$\mathrm{D}(f) = \frac{\mathrm{D}(p)q - p\mathrm{D}(q)}{q^2} = \frac{np}{q} \Rightarrow (\mathrm{D}(p) - np)q = p\mathrm{D}(q). \quad (*)$$

Suppose that $q \notin \mathbb{C}$. Then $q = (x-\lambda)^m \bar{q}$, where $\bar{q}(\lambda) \neq 0$.

$$\mathrm{D}(q) = m(x-\lambda)^{m-1}\bar{q} + (x-\lambda)^m \mathrm{D}(\bar{q}) \Rightarrow (x-\lambda)^{m-1} \mid \mathrm{D}(q) \text{ but } (x-\lambda)^m \nmid \mathrm{D}(q).$$

But by $(*)$, we have $q \mid p\mathrm{D}(q)$, $q \mid \mathrm{D}(q)$ (since $\gcd(p, q) = 1$), this implies $(x-\lambda)^m \mid \mathrm{D}(q)$, which yields a contradiction. Thus, $t = \exp(x)$ is transcendental over $\mathbb{C}(x)$.

Remark: By a similar argument, we can prove that $t = \log(x)$ is transcendental over $\mathbb{C}(x)$.

Let $t = \exp(x)$. We can extend $\mathrm{D} = \frac{\mathrm{d}}{\mathrm{d}x}$ on $\mathbb{C}(x)$ to $\mathbb{C}(x)(t)$ by defining $\mathrm{D}t = t$.
Let $t = \log(x)$. We can extend $\mathrm{D} = \frac{\mathrm{d}}{\mathrm{d}x}$ on $\mathbb{C}(x)$ to $\mathbb{C}(x)(t)$ by defining $\mathrm{D}t = \frac{1}{x}$.

Definition 5.1.4 (Elementary extensions)**.** *Let (E, D) be a differential extension of (F, D). Let $t \in E$. We say that*

- *t is* algebraic *over F, if $\exists\, P \in F[x] \backslash F$ s.t. $P(t) = 0$;*
- *t is* exponential *over F, if $\exists\, a \in F$ s.t. $\mathrm{D}(t) = \mathrm{D}(a) \cdot t$;*
- *t is* logarithmic *over F, if $\exists\, a \in F \backslash \{0\}$, s.t. $\mathrm{D}(t) = \frac{\mathrm{D}(a)}{a}$.*
- *t is said to be* elementary *over F if t is algebraic, exponential, or logarithmic over F.*
- *E is said to be* elementary *over F if $E = F(t_1, \ldots, t_n)$ and t_i is elementary over $F(t_1, \ldots, t_{i-1})$ for all $i = 1, \ldots, s$. If $F = \mathbb{C}(x)$, any element of E is called an* elementary function *over $\mathbb{C}(x)$.*

Example: Let $F = \mathbb{C}(x)$, $\mathrm{D} = \frac{\mathrm{d}}{\mathrm{d}x}$. Consider the function

$$f(x) = \frac{\pi}{\sqrt{\log(\exp(\sqrt{\frac{1}{2x^2+1}})^2 + x^2 + 1)}}.$$

We show that $f(x)$ is elementary over $\mathbb{C}(x)$. Let $E = \mathbb{C}(x)(t_1, t_2, t_3, t_4)$ with

$$t_1 = \sqrt{\frac{1}{2x^2+1}}, t_2 = \exp(t_1), t_3 = \log(t_2^2 + x^2 + 1), t_4 = \sqrt{t_3}.$$

Then $f = \frac{\pi}{t_4} \in E$.

Definition 5.1.5. *Let (F, D) be a differential field and $f \in F$. If there exists an elementary extension (E, D) of (F, D) and $g \in E$ s.t. $f = \mathrm{D}(g)$, then we say that f is* elementarily integrable *over F.*

Problem: Given $f \in F = \mathbb{C}(x)(t_1, \ldots, t_n)$, an elementary extension of $\mathbb{C}(x)$, decide whether f is elementarily integrable over F. We will show that the following elementary functions:

$$\exp(x^2),\ \frac{\exp(x)}{x},\ \frac{1}{\log(x)},\ \sin(x^2)$$

have no elementary (indefinite) integrals.

Definition 5.1.6. *Let (K, D) be a differential field, t be transcendental over K. Assume that $\mathrm{D}t \in K[t]$, and $P \in K[t]$. We call P a* special polynomial *if $\gcd(P, \mathrm{D}(P)) = P$, and a* normal polynomial *if $\gcd(P, \mathrm{D}(P)) = 1$.*

Remark: If P is irreducible, then P is either special or normal. If P is not irreducible, then P can be neither special nor normal.

Example:

1) Let $K = \mathbb{C}(x)$, $t = \tan(x)$. Then $\mathrm{D}(t) = 1 + t^2$. Let $P_1 = 1 + t^2$, we have $\mathrm{D}(P_1) = 2t(1 + t^2)$, so P_1 is special, Let $P_2 = t^2$, we have $\mathrm{D}(P_2) = 2t(1 + t^2)$. Then P_2 is neither special nor normal. $P_3 = t$ is normal.

2) Let $K = \mathbb{C}(x)$, $t = \exp(x)$. Then $P_1 = t$ is special and $P_2 = 1 + t$ is normal.

3) Let $K = \mathbb{C}(x)$, $t = \log(x)$. Then all monic irreducible polynomials P are normal since $\deg_t D(P) < \deg_t P$.

Definition 5.1.7. *Let K be a field of characteristic 0 and t be transcendental over K. Let $f \in K(t)$ and $P \in K[t]$ be irreducible. Then $f = P^m \cdot g$, for some $m \in \mathbb{Z}$, $g = \frac{a}{b} \in K(t)$ with $a, b \in K[t]$ and $\gcd(a, b) = 1$ such that $P \nmid ab$, we call m the* order *of f at P, denoted by $\mathrm{ord}_P(f)$.*

Lemma 5.1.8. *Let $P \in K[t]$ be irreducible and $f, g \in K(t)$. Then*

1) $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$;

2) $\mathrm{ord}(f + g) \geq \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\}$. The equality holds when $\mathrm{ord}_P(f) \neq \mathrm{ord}_P(g)$.

Remark: If P is not irreducible, then 1) may not be true. For example, $P = t^2$, $f = g = t$, $\mathrm{ord}_P(fg) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$.

Lemma 5.1.9. *Let (K, D) be a differential field and t be transcendental over K with $\mathrm{D}(t) \in K[t]$. Let $f \in K(t)$ and P be irreducible in $K[t]$. Then*

1) $\mathrm{ord}_P(\mathrm{D}(f)) \geq \mathrm{ord}_P(f) - 1$;

2) If P is a normal polynomial, then

$$\mathrm{ord}_P(\mathrm{D}(f)) = \begin{cases} \geq 0, & \mathrm{ord}_P(f) = 0 \\ \mathrm{ord}_P(f) - 1, & \mathrm{ord}_P(f) \neq 0 \end{cases}$$

Proof. 1) Write $f = P^m g = P^m \frac{a}{b}$, $\gcd(P, ab) = 1$, $m = \mathrm{ord}_P(f)$.
If $m = 0$, then

$$\mathrm{ord}_P(\mathrm{D}(f)) = \mathrm{ord}_P(\mathrm{D}(\frac{a}{b})) = \mathrm{ord}_P(\frac{\mathrm{D}(a)b - a\mathrm{D}(b)}{b^2}) \geq 0 \geq -1.$$

If $m \neq 0$, then

$$\mathrm{D}(f) = (mP^{m-1}\mathrm{D}(P))\frac{a}{b} + P^m\mathrm{D}(\frac{a}{b}) = P^{m-1}(m\mathrm{D}(P)\frac{a}{b} + P\mathrm{D}(\frac{a}{b})).$$

Since $\gcd(P, ab) = 1$, $\mathrm{ord}_P(\frac{a}{b}) = 0$, we obtain $\mathrm{ord}_P(m\mathrm{D}(P)\frac{a}{b}) \geq 0$.

$$\mathrm{D}(\frac{a}{b}) = \frac{b\mathrm{D}a - a\mathrm{D}b}{b^2} \Rightarrow \mathrm{ord}_P(\mathrm{D}(\frac{a}{b})) \geq 0 \Rightarrow \mathrm{ord}_P(P\mathrm{D}(\frac{a}{b})) \geq 1 \Rightarrow \mathrm{ord}_P(m\mathrm{D}(P)\frac{a}{b} + P\mathrm{D}(\frac{a}{b})) \geq 0$$
$$\Rightarrow \mathrm{ord}_P(\mathrm{D}(f)) \geq m - 1 = \mathrm{ord}_P(f) - 1.$$

2) If $\mathrm{ord}_P(f) = 0$, then $\mathrm{ord}_P(\mathrm{D}(f)) \geq 0$. If $\mathrm{ord}_P(f) \neq 0$, then $\mathrm{ord}_P(\mathrm{D}(f)) \geq \mathrm{ord}_P(f) - 1$ by 1). Since P is normal,

$$\gcd(P, \mathrm{D}(P)) = 1 \Rightarrow \mathrm{ord}_P(\mathrm{D}(P)) = 0 \Rightarrow \mathrm{ord}_P\big((mP^{m-1}\mathrm{D}(P))\frac{a}{b}\big) = m - 1.$$

Since $\mathrm{ord}_P(P^m\mathrm{D}(\frac{a}{b})) \geq m$. Then $\mathrm{ord}_P(\mathrm{D}(f)) = m - 1$. □

Remark: Lemma 5.1.9 is very useful in the following discussion. In particular, we have $\mathrm{ord}_P(\frac{\mathrm{D}(f)}{f}) = -1$ if $\mathrm{ord}_P(f) \neq 0$, and $\mathrm{ord}_P(\mathrm{D}(f)) \neq -1$ when P is an irreducible normal polynomial.

Proposition 5.1.10. *Let (K, D) be a differential field and F be a differential extension of K. If $t \in F$ is such that $a = \frac{t'}{t} \in K$ and $a \neq \frac{1}{n}\frac{u'}{u}$ for all $n \in \mathbb{N}$, $u \in K\backslash\{0\}$, then t is transcendental over K, $C_{K(t)} = C_K$ and t is the only irreducible special polynomial in $K[t]$.*

Proof. Assume that t is algebraic over K, then $\exists$ an irreducible polynomial $P = x^n + P_{n-1}x^{n-1} + \cdots + P_1 x + P_0 \in K[x]$ with $P_0 \neq 0$ s.t.

$$t^n + P_{n-1}t^{n-1} + \cdots + P_0 = 0$$

By $\mathrm{D}(t) = at$, we have

$$ant^n + (P'_{n-1} + P_{n-1}(n-1)a)t^{n-1} + \cdots + P'_0 = 0.$$

Then $an = \frac{P'_0}{P_0} \Rightarrow a = \frac{1}{n}\frac{P'_0}{P_0}$, $P_0 \in K\backslash\{0\}$, which contradicts the hypothesis. So t is transcendental over K.
If $C_{K(t)} \neq C_K$, then $\exists\, \frac{p}{q} \in K(t)\backslash K$, $\gcd(p, q) = 1$, satisfies that

$$\mathrm{D}(\frac{p}{q}) = \frac{\mathrm{D}(p)q - p\mathrm{D}(q)}{q^2} = 0 \Rightarrow \mathrm{D}(p)q = p\mathrm{D}(q) \Rightarrow p \mid \mathrm{D}(p) \text{ and } q \mid \mathrm{D}(q) \Rightarrow p, q \text{ are both special.}$$

Claim: Special polynomials in $K[t]$ are of the form bt^m, $b \in K$, $m \in \mathbb{N}$.
Let $P = P_n t^n + \cdots + P_0$ be a polynomial in $K[t]$ with $P_n \neq 0$ and $P_i \neq 0$ for some $i \in \{0, \ldots, n-1\}$. Then $\mathrm{D}(P) = (\mathrm{D}(P_n) + P_n na)t^n + \cdots + \mathrm{D}(P_0)$. If P is special, then $P \mid \mathrm{D}(P)$, we have

$$\begin{aligned} &\frac{\mathrm{D}(P_n) + nP_n a}{P_n} = \frac{\mathrm{D}(P_i) + iP_i a}{P_i} \\ \Rightarrow\ &(n-i)a = \frac{\mathrm{D}(P_i)}{P_i} - \frac{\mathrm{D}(P_n)}{P_n} = \frac{\mathrm{D}(P_i/P_n)}{P_i/P_n} \Rightarrow a = \frac{1}{n-i}\frac{\mathrm{D}(P_i/P_n)}{P_i/P_n} \end{aligned}$$

This contradicts the hypothesis. So the claim is valid and t is the only irreducible special polynomial in $K[t]$. Therefore, $\frac{p}{q} = bt^m$, $b \in K$ and $m \in \mathbb{Z}\backslash\{0\}$. It's easy to check $\mathrm{D}(\frac{p}{q}) \neq 0$ and $C_{K(t)} = C_K$. □

Corollary 5.1.11. $\exp(f(x))$ *is transcendental over $\mathbb{C}(x)$ if $f \in \mathbb{C}(x)\backslash\mathbb{C}$.*

Proof. Let $t = \exp(f(x))$, $f \in \mathbb{C}(x)\backslash\mathbb{C}$. Then $\frac{\mathrm{D}(t)}{t} = \mathrm{D}(f(x))$. If $\mathrm{D}(f) = \frac{1}{n}\frac{\mathrm{D}(g)}{g}$ for some $n \in \mathbb{N}_{>0}$ and $g \in \mathbb{C}(x)\backslash\{0\}$. Let P be any irreducible polynomial in $\mathbb{C}[x]$. Then $\mathrm{ord}_P(\mathrm{D}(f))$ is either ≥ 0 or < -1, but

$$\mathrm{ord}_P(\frac{\mathrm{D}(g)}{g}) = \begin{cases} \geq 0, & \mathrm{ord}_P(g) = 0 \\ -1, & \mathrm{ord}_P(g) \neq 0 \end{cases}.$$

Thus $\mathrm{ord}_P(g) = 0$ for all P, and we obtain $g \in \mathbb{C}$, $\mathrm{D}(f) = 0$, $f \in \mathbb{C}$, a contradiction. t is transcendental over $\mathbb{C}(x)$ by Proposition 5.1.10. □

Proposition 5.1.12. *Let (K, D) be a differential field and F be an differential extension of K. Let $t \in F$ be such that $\mathrm{D}(t) \in K$ and $\mathrm{D}(t) \neq \mathrm{D}(u)$ for any $u \in K$. Then t is transcendental over K, $C_{K(t)} = C_K$ and all irreducible polynomials in $K[t]$ are normal.*

Proof. Assume that t is algebraic over K, then $\exists$ an irreducible polynomial $P = x^n + P_{n-1}x^{n-1} + \cdots + P_1x + P_0 \in K[x]$ with $P_0 \neq 0$ s.t.

$$t^n + P_{n-1}t^{n-1} + \cdots + P_0 = 0.$$

By $\mathrm{D}(t) = a \in K$, we have

$$(na + \mathrm{D}(P_{n-1}))t^{n-1} + (P_{n-1}(n-1)a + \mathrm{D}(P_{n-2}))t^{n-2} + \cdots + P_1a + \mathrm{D}(P_0) = 0$$

Then $na + \mathrm{D}(P_{n-1}) = 0 \Rightarrow \mathrm{D}(t) = a = \mathrm{D}(-\frac{1}{n}P_{n-1})$, a contradiction.
Let $P(t) = t^n + P_{n-1}t^{n-1} + \cdots + P_0 \in K[t]$ be an irreducible polynomial.

$$\begin{aligned}\mathrm{D}(P) &= (na + \mathrm{D}(P_{n-1}))t^{n-1} + (P_{n-1}(n-1)a + \mathrm{D}(P_{n-2}))t^{n-2} + \cdots + P_1a + \mathrm{D}(P_0)\\ &\Rightarrow \deg_t(\mathrm{D}(P)) < \deg_t(P) \Rightarrow \gcd(P, \mathrm{D}(P)) = 1.\end{aligned}$$

Assume that $f = \frac{a}{b} \in C_{K(t)}$ with $\gcd(a, b) = 1$. Then

$$\begin{aligned}&\mathrm{D}(f) = \frac{\mathrm{D}(a)b - a\mathrm{D}(b)}{b^2} = 0 \Rightarrow \mathrm{D}(a)b - a\mathrm{D}(b) = 0 \Rightarrow \mathrm{D}(a)b = \mathrm{D}(b)a\\ &\Rightarrow a \mid \mathrm{D}(a) \text{ and } b \mid \mathrm{D}(b) \Rightarrow a, b \text{ are both special}\\ &\Rightarrow a, b \in K \Rightarrow f \in C_K \Rightarrow C_{K(t)} = C_K.\end{aligned}$$

□

Corollary 5.1.13. $\log(f(x))$ *is transcendental over* $\mathbb{C}(x)$ *if* $f \in \mathbb{C}(x)\backslash\mathbb{C}$.

Proof. Let $t = \log(f(x))$. Then $\mathrm{D}(t) = \frac{\mathrm{D}(f(x))}{f(x)}$. Claim: $\mathrm{D}(t) \neq \mathrm{D}(g)$ for any $g \in \mathbb{C}(x)$.
Otherwise, $\frac{\mathrm{D}(f)}{f} = \mathrm{D}(g)$. Since $f \in \mathbb{C}(x)\backslash\mathbb{C}$, there exists an irreducible polynomial $P \in C[x]$ s.t. $\mathrm{ord}_P(f) \neq 0$. Then $\mathrm{ord}_P(\frac{\mathrm{D}(f)}{f}) = -1$. But $\mathrm{ord}_P(\mathrm{D}(g)) \neq -1$ for any P, a contradiction. □

5.2 Liouville Theorem and its applications

Let $(E, ')$ be a differential extension of $(F, ')$ with $\mathrm{char}(F) = 0$. Let $\alpha \in E$ be an algebraic element over F with the minimal polynomial $P = x^n + \sum_{i=0}^{n-1} P_i x^i \in F[x]$ s.t. $P(\alpha) = 0$. Then $[F(\alpha) : F] = n$ and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of $F(\alpha)$ over F. Assume that $\lambda_1, \ldots, \lambda_n$ be roots of P in $\bar{F}$. Then we have

$$\begin{cases} P_{n-1} = -(\lambda_1 + \cdots + \lambda_n) \\ P_0 = (-1)^n \lambda_1 \cdots \lambda_n \end{cases}$$

For any $\beta \in F(\alpha)$, we define $\phi_\beta : F(\alpha) \to F(\alpha)$ by $\phi_\beta(\gamma) = \beta\gamma$, $\forall \gamma \in F(\alpha)$. Then $\phi(\beta)$ is linear and we call ϕ_β the multiplication map associated with β. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of $F(\alpha)$ over F. Then

$$\phi_\beta \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M_\beta \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \text{ where } M_\beta \in F^{n\times n}.$$

The matrix M_β is called the matrix representation of β w.r.t. the basis $\{\alpha_1, \ldots, \alpha_n\}$. We know that the matrix representations of β w.r.t. two different bases are similar.

Definition 5.2.1. *Let $\beta \in F(\alpha)$ and M_β be a matrix representation of β w.r.t. some basis. We call* $\mathrm{Tr}(M_\beta)$ *the* trace *of β in $F(\alpha)$ over F, denoted by $\mathrm{Tr}_{F(\alpha)/F}(\beta)$ and call* $\det(M_\beta)$ *the* norm *of β in $F(\alpha)$ over F, denoted by $N_{F(\alpha)/F}(\beta)$.*

Remark: Since similar matrices have the same trace and norm, the above definitions of traces and norms are independent of bases.

Assume that $A, B \in F^{n\times n}$ are similar, i.e. $\exists$ invertible $P \in F^{n\times n}$ s.t. $A = P^{-1}BP$. Then

$$|\lambda I - A| = |\lambda I - P^{-1}BP| = |P^{-1}(\lambda I - B)P| = |\lambda I - B|.$$

So the characteristic polynomial of A and B are the same.
Write $|\lambda I - A| = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0 = (\lambda - \lambda_1)\cdots(\lambda - \lambda_n)$. Then we have

$$\begin{cases} \mathrm{Tr}(A) = \lambda_1 + \cdots + \lambda_n \\ \det(A) = \lambda_1 \cdots \lambda_n \end{cases}$$

So $\mathrm{Tr}(A)$ and $\det(A)$ are stable under similar transformations.

Theorem 5.2.2. *Let α be algebraic over F with the minimal polynomial $P = \sum_{i=0}^{n} P_i x^i \in F[x]$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be the distinct roots of P in $\bar{F}$, and $\sigma_i : F(\alpha) \to \bar{F}$ be the F-embedding defined by $\sigma_i(\alpha) = \alpha_i$. Then $\sigma_i(\beta') = (\sigma_i(\beta))'$ for any $\beta \in F(\alpha)$.*

Proof. It suffices to show that $\sigma_i(\alpha') = (\sigma_i(\alpha))'$. Let $P_0 = \sum_{i=0}^{n} P_i' x^i$ and $P_1 = \sum_{i=1}^{n} i P_i x^{i-1}$.
Then for any root α_i of P,

$$\alpha_i' = -\frac{P_0(\alpha_i)}{P_1(\alpha_i)} = Q(\alpha_i), \text{ where } Q \in F[x] \text{ and } \deg_x(Q) \le n-1.$$

Then for any $i \in \{1, 2, \ldots, n\}$, we have

$$\sigma_i(\alpha_1') = \sigma_i(Q(\alpha_1)) = Q(\sigma_i(\alpha_1)) = (\alpha_i)' = (\sigma_i(\alpha_1))'.$$

□

Proposition 5.2.3. *Let $(F, ')$ be a differential field of characteristic 0 and α be algebraic over F and $\alpha \neq 0$. Let $\beta_1, \beta_2 \in F(\alpha)$. Then*

1) $\mathrm{Tr}(\beta_1 + \beta_2) = \mathrm{Tr}(\beta_1) + \mathrm{Tr}(\beta_2)$;

2) $N(\beta_1\beta_2) = N(\beta_1)N(\beta_2)$;

3) $\frac{N(\alpha)'}{N(\alpha)} = \mathrm{Tr}(\frac{\alpha'}{\alpha})$.

Proof. We only show 3). Let $P = x^n + \sum_{i=0}^{n-1} P_i x^i \in F[x]$ be the minimal polynomial of α. Then the multiplication matrix of α w.r.t. the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is of the form

$$M_\alpha = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ -P_0 & -P_1 & -P_2 & \cdots & -P_{n-1} \end{pmatrix}.$$

Then $|xI - M_\alpha| = P_0 + P_1 x + \cdots + P_{n-1}x^{n-1} + x^n$. Then

$$\begin{aligned}\mathrm{Tr}(\alpha) &= -P_{n-1} = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)\\ N(\alpha) &= (-1)^n P_0 = \sigma_1(\alpha)\cdots\sigma_n(\alpha).\end{aligned}$$

In general,[1] we have $\forall \beta \in F(\alpha)$,

$$\begin{aligned}\mathrm{Tr}_{F(\alpha)/F}(\beta) &= \sigma_1(\beta) + \cdots + \sigma_n(\beta)\\ N_{F(\alpha)/F}(\beta) &= \sigma_1(\beta)\cdots\sigma_n(\beta).\end{aligned}$$

Then,

$$\frac{N(\alpha)'}{N(\alpha)} = \frac{\prod_{i=1}^{n}\sigma_i(\alpha)'}{\prod_{i=1}^{n}\sigma_i(\alpha)} = \sum_{i=1}^{n}\frac{(\sigma_i(\alpha))'}{\sigma_i(\alpha)} = \sum_{i=1}^{n}\frac{\sigma_i(\alpha')}{\sigma_i(\alpha)} = \sum_{i=1}^{n}\sigma_i(\frac{\alpha'}{\alpha}) = \mathrm{Tr}(\frac{\alpha'}{\alpha}).$$

□

Theorem 5.2.4 (Liouville's Theorem)**.** *Let $(F,')$ be a differential field of characteristic 0 and $f \in F$. If there exists an elementary extension $E = F(t_1, \ldots, t_n)$ with $C_E = C_F$ and $g \in E$ s.t. $f = g'$, then $\exists\, v \in F$, $u_1, \ldots, u_m \in F^* = F\backslash\{0\}$, $c_1, \ldots, c_m \in C_F$ s.t.*

$$f = v' + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}.$$

Proof. We proceed by induction on n. When $n = 0$, $E = F$ and the assertion holds by taking $v = g$ and $c_i = 0$ (for all $i = 1, \ldots, m$). Assume that the assertion holds for $n \le s-1$. We now consider the case $n = s$. Let $K = F(t_1)$. Then $E = K(t_2, \ldots, t_s)$, which is an $(s-1)$-tuple extension of K. We apply the hypothesis assumption to K and E.[2] Then there exist $\tilde{v} \in K$, $\tilde{u_1}, \ldots, \tilde{u_m} \in K\backslash\{0\}$, $\tilde{c_1}, \ldots, \tilde{c_m} \in C_K$, s.t.

$$f = \tilde{v}' + \sum_{i=1}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}}.$$

Case 1: t_1 is algebraic over F with $[K : F] = r$.
Then there exist r F-embeddings $\sigma_j : F(t_1) \to \bar{F}$ $(j = 1, \ldots, r)$. Since $f \in F$, we have

$$\begin{aligned} f = \sigma_j(f) &= \sigma_j(\tilde{v}' + \sum_{i=1}^{m}\tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}}) = \sigma_j(\tilde{v})' + \sum_{i=1}^{m}\tilde{c_i}\sigma_j(\frac{\tilde{u_i}'}{\tilde{u_i}})\\ \Rightarrow rf &= \sum_{j=1}^{r}\sigma_j(\tilde{v})' + \sum_{i=1}^{m}\sum_{j=1}^{r}\tilde{c_i}\sigma_j(\frac{\tilde{u_i}'}{\tilde{u_i}}) = (\mathrm{Tr}(\tilde{v}))' + \sum_{i=1}^{m}\tilde{c_i}\frac{N(\tilde{u_i})'}{N(\tilde{u_i})}.\end{aligned}$$

Then

$$f = v' + \sum_{i=1}^{m} c_i\frac{u_i'}{u_i}, \text{ where } v = \frac{\mathrm{Tr}(\tilde{v})}{r} \in F,\ c_i = \frac{\tilde{c_i}}{r} \in C_F \text{ and } u_i = N(\tilde{u_i}) \in F^*.$$

Case 2: t_1 is transcendental over F.
If t_1 is either exponential or logarithmic over F, then

$$t_1' \in F[t_1], \quad f = \tilde{v}' + \sum_{i=1}^{m}\tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}},\ \tilde{v},\ \tilde{u_i} \in F(t_1).$$

[1] See Lang Algebra, P. 284-288, Proposition 5.6.
[2] Note that $F \subseteq K \subseteq E$ and $C_F = C_E$, thus $C_K = C_E$

W.L.O.G., we may assume that $\tilde{u_i} \in F[t_1]$ is irreducible and coprime to each other if $\tilde{u_i} \notin F$ (using the logarithmic derivative formula).

Claim 1: For any irreducible normal polynomial $P \in F[t_1]$, we have

1) $\mathrm{ord}_P(\tilde{v}) \geq 0$;

2) $\mathrm{ord}_P(\tilde{u_i}) = 0$ for $i = 1, \ldots, m$.

Proof of the Claim 1 1) Suppose that $\mathrm{ord}_P(\tilde{v}) < 0$. Then $\mathrm{ord}_P(\tilde{v}') = \mathrm{ord}_P(\tilde{v}) - 1$. Note that $\mathrm{ord}_P(f) = 0$ and

$$\mathrm{ord}_P(\frac{\tilde{u_i}'}{\tilde{u_i}}) = \begin{cases} \geq 0, & \mathrm{ord}_P(\tilde{u_i}) = 0 \\ -1, & \mathrm{ord}_P(\tilde{u_i}) \neq 0 \end{cases}$$

which implies that

$$\mathrm{ord}_P(\tilde{v}') = \mathrm{ord}_P(f - \sum_{i=1}^{m} \tilde{c_i} \frac{\tilde{u_i}'}{\tilde{u_i}}) \geq -1,$$

a contradiction. Thus, 1) is valid.
2) Suppose that $\mathrm{ord}_P(\tilde{u_i}) \neq 0$ for some $i \in \{1, \ldots, m\}$. Then $\mathrm{ord}_P(\tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}}) = -1$. By 1), we have $\mathrm{ord}_P(f - \tilde{v}') > -1$, but $\mathrm{ord}_P(\sum_{i=1}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}}) = -1$, a contradiction. Therefore, Claim 1 is proved.

Case 2.1: t_1 is logarithmic over F, i.e., $t_1' = \frac{u_0'}{u_0}$ for some $u_0 \in F$.
In this case, we first show that $t_1' \neq u'$ for any $u \in F$. If $t_1' = u'$ for some $u \in F$, then $(t_1 - u)' = 0$. $t_1 - u \in C_{F(t)} = C_F \Rightarrow t_1 \in F$, which contradicts the assumption that t_1 is transcendental over F. Then all the irreducible polynomials in $F[t_1]$ are normal by Proposition 5.1.12. By Claim 1, we have $\tilde{u_i} \in F$ for all $i = 1, \ldots, m$ and $\tilde{v} \in F[t_1]$. Since $f - \sum_{i=1}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}} \in F$, we have

$$\tilde{v} = c_0 t_1 + v, \text{ where } c_0 \in C_F \text{ and } v \in F.$$

Then

$$f = \tilde{v}' + \sum_{i=1}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}} = c_0\frac{u_0'}{u_0} + v' + \sum_{i=1}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}}.$$

Hence the assertion holds.

Case 2.2: t_1 is exponential over F, i.e., $t_1' = u_0' t_1$ for some $u_0 \in F$.
We first show that $\frac{t_1'}{t_1} \neq \frac{1}{l}\frac{a'}{a}$ for any $l \in \mathbb{N}\backslash\{0\}$ and $a \in F\backslash\{0\}$. If $\frac{t_1'}{t_1} = \frac{1}{l}\frac{a'}{a}$, then $(\frac{t_1^l}{a})' = 0$, so $\frac{t_1^l}{a} \in C_{F(t)} = C_F$, which contradicts the assumption that t_1 is transcendental over F. Then by Proposition 5.1.10, the only irreducible special polynomial in $F[t_1]$ is t_1. By Claim 1, we have $\tilde{v} \in F[t_1, t_1^{-1}]$ and at most one of $\tilde{u_i}$'s is equal to t_1, say $\tilde{u_1} = t_1$. Then

$$\sum_{i=1}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}} = \tilde{c_1}\frac{t_1'}{t_1} + \sum_{i=2}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}} = (\tilde{c_1}u_0)' + \sum_{i=2}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}} \in F.$$

Since $f \in F$, we have $\tilde{v}' = f - \sum_{i=1}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}} \in F$. We claim that $\tilde{v} \in F$. Suppose that $\tilde{v} = \sum_{-d \leq i \leq d} a_i t_1^i \notin F$. Then $\exists\ -d \leq i \leq d$ with $i \neq 0$ s.t. $a_i \neq 0$. Then

$$\tilde{v}' = \sum_{-d \leq i \leq d} (a_i' + i u_0' a_i) t_1^i.$$

Since $\tilde{v}' \in F$ and t_1 is transcendental over F, we have

$$a_i' + iu_0'a_i = 0 \Rightarrow u_0' = \frac{t_1'}{t_1} = -\frac{1}{i}\frac{a_i'}{a_i},$$

which is a contradiction. Hence $f = (\tilde{v} + \tilde{c_1}u_0)' + \sum_{i=2}^{m} \tilde{c_i}\frac{\tilde{u_i}'}{\tilde{u_i}}$, $\tilde{u_i} \in F$. This completes the proof.

□

Remark: There is a stronger version of Liouville's theorem saying that if f has an elementary integral in $E = F(t_1, \ldots, t_n)$, then $\exists\, v \in F$, $c_1, \ldots, c_m \in \bar{C_F}$, and $u_1, \ldots, u_m \in F(c_1, \ldots, c_m)$ s.t.

$$f = v' + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}.$$

See Bronstein's Book: Symbolic Integration (Theorem 5.5.3).
But we will consider complex functions which is defined over $\mathbb{C}$. And we knew that $\mathbb{C}$ is algebraically closed. So we can always assume that no new constants is needed to express the integral.

Applications of Liouville's Theorem

We can now show that

$$\exp(x^2),\ \frac{1}{\log(x)},\ \frac{\exp(x)}{x},\ \exp(\exp(x)),\ \log(\log(x))$$

have no elementary integral.

Example 1: $f = \exp(x^2)$ has no elementary integral.
Let $F = \mathbb{C}(x)(f)$, which is elementary over $\mathbb{C}(x)$. Note that f is transcendental over $\mathbb{C}(x)$. If f has an elementary integral, then $\exists\, v \in F$, $c_1, \ldots, c_m \in C_F = \mathbb{C}$, and $u_1, \ldots, u_m \in F$ s.t.

$$f = v' + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}.$$

By the order estimate, we have, for all irreducible normal $P \in \mathbb{C}(x)[f]$, $\mathrm{ord}_P(v) \geq 0$ and $\mathrm{ord}_P(u_i) = 0$. Then $v \in \mathbb{C}(x)[f, f^{-1}]$ and at most one of u_i's is equal to f. Since $\deg_f(f - \sum_{i=1}^{m} c_i\frac{u_i'}{u_i}) = 1$, we have $v = af + b$, where $a, b \in \mathbb{C}(x)$ and $a \neq 0$. Then $f = (af)' = (a' + 2xa)f$, which implies $1 = a' + 2xa$. By the order estimate, we have shown that the equation $1 = y' + 2xy$ has no solution in $\mathbb{C}(x)$. So $f = \exp(x^2)$ has no elementary integral.

Example 2: $f = \frac{1}{\log(x)}$ has no elementary integral.
Let $F = \mathbb{C}(x)(t)$, with $t = \log(x)$, which is transcendental over $\mathbb{C}(x)$. If f has an elementary integral over F, then $\exists\, v \in F$, $u_1, \ldots, u_m \in F\backslash\{0\}$, and $c_1, \ldots, c_m \in \mathbb{C}$ s.t.

$$\frac{1}{t} = v' + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}.$$

By the order estimate, we can show that $\mathrm{ord}_P(v) \geq 0$ and $u_i = t$ or $\mathrm{ord}_P(u_i) = 0$ for any irreducible normal polynomial $P \in \mathbb{C}(x)[t]$. In fact, if $P \neq t$, then

$$\mathrm{ord}_P(v') = \begin{cases} \geq 0, & \mathrm{ord}_P(v) \geq 0 \\ < -1, & \mathrm{ord}_P(v) < 0 \end{cases}.$$

But $\mathrm{ord}_P(\frac{1}{t} - \sum_{i=1}^{m} c_i \frac{u_i'}{u_i})$ is either ≥ 0 or -1. Then we have $\mathrm{ord}_P(v) \geq 0$. If $\mathrm{ord}_P(u_i) \neq 0$ for some $i \in \{1, \ldots, m\}$, then $\mathrm{ord}_P(\frac{1}{t} - \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}) = -1$, contradicts with $\mathrm{ord}_P(v') \geq 0$. Then $\mathrm{ord}_P(u_i) = 0$ for all $i \in \{1, \ldots, m\}$. If $P = t$, then $\mathrm{ord}_P(\frac{1}{t}) = -1$, which implies that $u_i = t$ for some i. Then

$$\frac{1}{t} = v' + c_i \frac{t'}{t} + \sum_{\substack{j=1 \\ j \neq i}}^{m} c_j \frac{u_j'}{u_j}, \ c_i \in \mathbb{C}.$$

Thus, $1 = c_i t' = c_i \frac{1}{x}$, which is a contradiction.

Chapter 6

Algorithms and open problems in differential algebra

6.1 Well-ordering theorem for differential polynomials

Let (K, δ) be a differential field of characteristic 0 and consider the differential polynomial ring $K\{Y\} \triangleq K\{y_1, \ldots, y_n\}$. We have introduced the theory of differential characteristic sets in Section 2.1, in this section we focus on the computational aspects.

We now come to the well-ordering of a (finite) differential polynomial set $\Sigma \subseteq K\{Y\}$. Fix a ranking $\mathscr{R}$ on $K\{Y\}$.

Definition 6.1.1. *An autoreduced set of lowest rank among all autoreduced sets belonging to* Σ *(i.e. each element belongs to* Σ*) is called a* basic set *of* Σ.

Lemma 6.1.2. *Let* Σ *be a finite set of nonzero* δ*-polynomials in* $K\{Y\}$. *Then* Σ *necessarily has basic sets and there is a mechanical method in getting such a basic set in a finite number of steps.*

Proof. As Σ is finite, the existence of basic sets is evident. So the problem reduces to a mechanical generation of such a set. To show this, first choose $A_1 \in \Sigma$ of lowest rank. Let $\Sigma_1 = \{f \in \Sigma \mid f \text{ is reduced w.r.t. } A_1\}$. If $\Sigma_1 = \emptyset$, then output A_1. Otherwise, choose $A_2 \in \Sigma_1$ of lowest rank. Then A_1, A_2 is autoreduced. Let $\Sigma_2 = \{f \in \Sigma \mid f \text{ is reduced w.r.t. } A_1, A_2\}$. If $\Sigma_2 = \emptyset$, A_1, A_2 is a basic set of Σ. Otherwise, choose $A_3 \in \Sigma_2$ of lowest rank and proceed as before. As $A_1, A_2, A_3 \ldots$ constitute an autoreduced set, we have to stop in a finite number of steps and finally get a basic set in a mechanical manner. □

Lemma 6.1.3. *Let* Σ *be a finite set of nonzero* δ*-polynomials with a basic set* $\mathcal{A} : A_1, A_2, \ldots, A_p$ *of which* $A_1 \notin K$. *Let* B *be a nonzero* δ*-polynomial reduced w.r.t.* $\mathcal{A}$. *Then the set* $\Sigma_1 = \Sigma \cup \{B\}$ *will have a basic set of rank lower than that of* $\mathcal{A}$.

Proof. If $B \in K$, then B is a basic set of Σ_1 of rank lower than that of $\mathcal{A}$. Otherwise, there exists i such that $\mathrm{rk}(B) < \mathrm{rk}(A_i)$ and $\mathrm{rk}(B) > \mathrm{rk}(A_{i-1})$. Since B is reduced w.r.t. each A_j, we obtain $A_1, \ldots, A_{i-1}, B$ is an autoreduced set in Σ_1 of rank lower than $\mathcal{A}$. The basic set of Σ_1 will have therefore a fortiori a rank lower than that of $\mathcal{A}$. □

Let Σ be a finite set of δ-polynomials in $K\{Y\}$. Set $\Sigma_1 = \Sigma$. By Lemma 6.1.2, Σ_1 has a basic set, say $\mathcal{A}_1$. Let $R_1 = \{\delta\text{-rem}(f, \mathcal{A}_1) \mid f \in \Sigma_1 \backslash \mathcal{A}_1\} \backslash \{0\}$. If $R_1 = \emptyset$, ouput $\mathcal{A}_1$. If $R_1 \neq \emptyset$, set $\Sigma_2 = \Sigma_1 \cup R_1$ and Σ_2 has a basic set, say $\mathcal{A}_2$. By Lemma 6.1.3, $\mathcal{A}_2$ is of lower rank than $\mathcal{A}_1$. If $R_2 = \emptyset$, output $\mathcal{A}_2$. Otherwise, we can proceed as before. In this way we shall get a sequence of sets

of δ-polynomials $\Sigma_1 \subseteq \Sigma_2 \subseteq \cdots$ with corresponding basic sets $\mathcal{A}_1, \mathcal{A}_2, \ldots$ having decreasing ranks. Thus, such a sequence can have only a finite number of terms. In other words, if Σ_q is the last one of such a sequence with a basic set $\mathcal{A}_q$, then $R_q = \emptyset$, i.e., $\forall\, f \in \Sigma_q$, $\delta\text{-rem}(f, \mathcal{A}_q) = 0$. Output $\mathcal{A}_q$.

$$\begin{array}{ccccccc} \Sigma_1 = \Sigma & \subseteq & \Sigma_2 = \Sigma_1 \cup R_1 & \subseteq & \cdots & \subseteq & \Sigma_q = \Sigma_{q-1} \cup R_{q-1} \\ \mathcal{A}_1 & > & \mathcal{A}_2 & > & \cdots & > & \mathcal{A}_q \\ R_1 \neq \emptyset & & R_2 \neq \emptyset & & \cdots & & R_q = \emptyset \end{array} \tag{6.1}$$

Definition 6.1.4. *The above $\mathcal{A}_q$ is called a* characteristic set *of the finite δ-polynomial set Σ.*

Theorem 6.1.5 (Well-ordering Principle)**.** *Given a finite δ-polynomial set $\Sigma \subseteq K\{y_1, \ldots, y_n\}$, there is an algorithm to obtain a characteristic set $\mathcal{A}$ of Σ after mechanically a finite number of steps. Moreover, we have*

$$\mathbb{V}(\mathcal{A}/\mathrm{H}_{\mathcal{A}}) \subseteq \mathbb{V}(\Sigma) \subseteq \mathbb{V}(\mathcal{A}),$$

and

$$\mathbb{V}(\Sigma) = \mathbb{V}(\mathcal{A}/\mathrm{H}_{\mathcal{A}}) \cup \cup_{A\in\mathcal{A}}\big(\mathbb{V}(\Sigma, \mathrm{I}_A) \cup \mathbb{V}(\Sigma, \mathrm{S}_A)\big).^1$$

Proof. The first assertion has been shown above the scheme. Note that $R_k \subseteq [\Sigma_k]$ for each k, so $\mathbb{V}(\Sigma_k) = \mathbb{V}(\Sigma_{k+1})$ and thus, $\mathbb{V}(\Sigma_1) = \mathbb{V}(\Sigma_2) = \cdots = \mathbb{V}(\Sigma_q) = \mathbb{V}(\Sigma)$. On the other hand, since $\delta\text{-rem}(f, \mathcal{A}_q) = 0$ for all $f \in \Sigma_q$, $\exists\, i_A, s_A \in \mathbb{N}$ s.t. $\prod_{A\in\mathcal{A}_q} \mathrm{I}_A^{i_A}\mathrm{S}_A^{s_A} f \in [\mathcal{A}_q]$. It follows that any δ-zero of $\mathcal{A}_q$, which doesn't annul $\mathrm{H}_{\mathcal{A}}$, is necessarily also a δ-zero of Σ_q and thus a δ-zero of Σ. □

Remark: Each newly obtained δ-polynomial set $\Sigma \cup \{\mathrm{I}_A\}$ or $\Sigma \cup \{\mathrm{S}_A\}$ has basic sets of rank lower than that of Σ. $\Sigma_q \cup \{\mathrm{I}_A\}$ (or $\cup\{\mathrm{S}_A\}$) has basic sets of rank lower than that of Σ_q and $\mathbb{V}(\Sigma_q, \mathrm{I}_A) = \mathbb{V}(\Sigma, \mathrm{I}_A)$. Continuing the above procedure for $\Sigma_q \cup \{\mathrm{I}_A\}$ or $\Sigma_q \cup \{\mathrm{S}_A\}$ and also for the new δ-polynomial sets obtained, since the basic sets are strictly decreasing, this procedure has to end in a finite number of steps and so we get the following.

Zero Decomposition Theorem (Weak Form)
There is an algorithmic procedure which permits us to give for Σ a decomposition of the form

$$\mathbb{V}(\Sigma) = \cup_k \mathbb{V}(\mathcal{B}_k/\mathrm{H}_{\mathcal{B}_k}),$$

where $\mathcal{B}_k$ is a characteristic set for some δ-polynomial set.

Example: Let $f = y_1' + 1$ and $g = y_1 + y_2'$ in $\mathbb{Q}(t)\{y_1, y_2\}$.
(1) Consider the elimination ranking $\mathscr{R}_1$ with $y_1 > y_2$. We compute a characteristic set of the set $\Sigma = \{f, g\}$ following the scheme (6.1). Let $\Sigma_1 = \Sigma$. A basic set of Σ_1 is $\mathcal{A}_1 := g$. Compute $r_1 \triangleq \delta\text{-rem}(f, \mathcal{A}_1) = f - g' = 1 - y_2''$. So $R_1 = \{r_1\}$. Let $\Sigma_2 = \Sigma \cup \{r_1\} = \{f, g, r_1\}$. A basic set of Σ_2 is $\mathcal{A}_2 := r_1, g$. Compute $r_2 \triangleq \delta\text{-rem}(f, \mathcal{A}_2) = 0$. So $R_2 = \emptyset$ and a characteristic set of Σ is $\mathcal{A}_2 = r_1, g$.
(2) Consider the orderly ranking $\mathscr{R}_2$ with $y_1 > y_2$. Let $\Sigma_1 = \Sigma$. A basic set of Σ_1 is $\mathcal{A}_1 = g, f$. So $R_1 = \emptyset$ and a characteristic set of Σ w.r.t. $\mathscr{R}_2$ is $\mathcal{A} = g, f$.

6.2 Differential Decomposition Theorems/Algorithms

In this section, we shall consider the main decomposition problem in differential algebra and give a partial answer to it:

[1] $\mathrm{H}_{\mathcal{A}} = \prod_{A\in\mathcal{A}} \mathrm{I}_A\mathrm{S}_A$, $\mathbb{V}(\mathcal{A}/\mathrm{H}_{\mathcal{A}}) = \{\eta \in \bar{K}^n \mid \mathcal{A}(\eta) = 0 \text{ and } \mathrm{H}_{\mathcal{A}}(\eta) \neq 0\}$.

Decomposition Problem: Given a finite subset $\Sigma \subseteq K\{Y\}$, decompose the radical δ-ideal $\{\Sigma\}$ into an irredundant intersection of prime δ-ideals: $\{\Sigma\} = P_1 \cap P_2 \cap \cdots \cap P_r$.

Since a prime δ-ideal P is completely determined by its characteristic set $\mathcal{A}$ (i.e., $P = \mathrm{sat}(\mathcal{A})$), the above decomposition problem can be separated into the following two problems:

Problem 1: Given Σ, to find a finite set Λ of autoreduced sets of $K\{Y\}$, each of which is a characteristic set of a prime δ-ideal containing Σ, such that Λ contains a characteristic set of each component of $\{\Sigma\}$. That is, $\{\Sigma\} = \mathrm{sat}(\mathcal{B}_1) \cap \cdots \cap \mathrm{sat}(\mathcal{B}_l)$ with $\Lambda = \{\mathcal{B}_1, \ldots, \mathcal{B}_l\}$.

Problem 2: Given an aotureduced set $\mathcal{A}$ of $K\{Y\}$, to determine whether or not $\mathcal{A}$ is a characteristic set of a component of $\{\Sigma\}$.

Problem 2': Given that $\mathcal{A}$ and $\mathcal{B}$ are characteristic sets of the prime δ-ideals P and Q respectively, to determine whether or not $P \subseteq Q$.

$$\begin{aligned} \text{Decomposition Problem} &= \text{Problem 1} + \text{Problem 2} \\ &= \text{Problem 1} + \text{Problem 2'} \end{aligned}$$

Remark:

① Problem 1 has been solved (Ritt-Kolchin decomposition Algorithm)

② Problem 2 in the general case is still not solved, and we have a complete answer for the case when Σ consists of a single δ-polynomial given by Ritt's component theorem and the low power theorem.

③ Although it is trivial to decide whether $P = Q$, Problem 2' is currently open, even for the special case below:

Ritt's problem Given $A \in K\{y_1, \ldots, y_n\}$ irreducible with $A(0, \ldots, 0) = 0$, decide whether $(0, \ldots, 0)$ is a zero of $\mathrm{sat}(A)$, or equivalently, whether $\mathrm{sat}(A) \subseteq [y_1, \ldots, y_n]$.

In this section, we shall focus on a solution of Problem 1.

Question: Given an autoreduced set $\mathcal{A} \subseteq K\{Y\}$, give a necessary and sufficient condition for $\mathcal{A}$ to be a characteristic set of a prime δ-ideal $P \subseteq K\{Y\}$.

Lemma 6.2.1 (Rosenfeld's lemma in ordinary differential case)**.** *Let $\mathcal{A} = A_1, \ldots, A_p$ be an autoreduced set in $K\{Y\}$ w.r.t. a ranking and $f \in K\{Y\}$ be partially reduced w.r.t. $\mathcal{A}$. Then*

$$f \in \mathrm{sat}(\mathcal{A}) = [\mathcal{A}] : \mathrm{H}_{\mathcal{A}}^{\infty} \Leftrightarrow f \in (\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}.$$

Proof. "$\Leftarrow$" Trivial.

"$\Rightarrow$" Suppose $f \in \mathrm{sat}(\mathcal{A})$. Then $\exists\, m \in \mathbb{N}$ and $c_{ij} \in K\{Y\}$ s.t.

$$\mathrm{H}_{\mathcal{A}}^{m} f = \sum_{i=1}^{p} c_{i0} A_i + \sum_{i=1}^{p} \sum_{j=1}^{k_i} c_{ij} A_i^{(j)}. \quad (*)$$

Note that for $j \geq 1$, $A_i^{(j)} = \mathrm{S}_{A_i} \cdot \delta^j(u_{A_i}) + T_{ij}$ for some $T_{ij} \in K\{Y\}$ free of $\delta^j(u_{A_i})$. Let $\Phi = \{\delta^j(u_{A_i}) \mid c_{ij} \neq 0, j \geq 1, i = 1, \ldots, p\}$. If $\Phi \neq \emptyset$, take the greatest $v = \delta^j(u_{A_i})$ in Φ and substitute $\delta^j(u_{A_i}) = -\frac{T_{ij}}{\mathrm{S}_{A_i}}$ at both sides of $(*)$ and set $\Phi = \Phi \backslash \{v\}$. Continue this process and successively substitute $\delta^j(u_{A_i}) = -\frac{T_{ij}}{\mathrm{S}_{A_i}}$ into $(*)$ for all $\delta^j(u_{A_i})$ in Φ. Clearing denominators by multiplying a power product $\mathrm{S}_{\mathcal{A}}^{l}$ of S_{A_i} at both sides of the obtained equality, we have

$$\mathrm{S}_{\mathcal{A}}^{l} \cdot \mathrm{H}_{\mathcal{A}}^{m} f = \sum_{i=1}^{p} \bar{c_{i_0}} A_i, \text{ where } \bar{c_{i_0}} \in K\{Y\}.$$

Thus, $f \in (\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}$. □

Lemma 6.2.2. *Let $\mathcal{A}$ be an autoreduced set in $K\{Y\}$ w.r.t. a ranking $\mathscr{R}$. Then $\mathcal{A}$ is a δ-characteristic set of a prime δ-ideal if and only if $(\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}$ is a prime algebraic ideal in $K\{Y\}$ and $(\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}$ contains no nonzero element reduced w.r.t. $\mathcal{A}$.*

Proof. "⇒" Take a smallest finite subset $V \subseteq \Theta(Y)$ such that $\mathcal{A} \subseteq K[V]$. Let $I_{\mathcal{A}} = \{f \in K[V] \mid \exists\, m \in \mathbb{N} \text{ s.t. } \mathrm{H}_{\mathcal{A}}^{m} f \in (\mathcal{A})\}$. Then we have $(\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty} = (I_{\mathcal{A}})_{K\{Y\}}$ and $I_{\mathcal{A}} = ((\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}) \cap K[V]$.[2] By Lemma 6.2.1, $\mathrm{sat}(\mathcal{A}) \cap K[V] = ((\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}) \cap K[V] = I_{\mathcal{A}}$. So $I_{\mathcal{A}}$ is a prime ideal and consequently, $(\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty} = (I_{\mathcal{A}})_{K\{Y\}}$ is prime too. Since $\mathcal{A}$ is a characteristic set of $\mathrm{sat}(\mathcal{A})$, $(\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}$ contains no nonzero δ-polynomial reduced w.r.t. $\mathcal{A}$.

"⇐" To show ① $\mathrm{sat}(\mathcal{A})$ is prime and ② $\mathcal{A}$ is a characteristic set of $\mathrm{sat}(\mathcal{A})$.

① Given $f_1, f_2 \in K\{Y\}$ with $f_1 f_2 \in \mathrm{sat}(\mathcal{A})$. Let $r_i = \delta\text{-rem}(f_i, \mathcal{A})$. Then $\mathrm{H}_{\mathcal{A}}^{m_i} f_i \equiv r_i \bmod [\mathcal{A}] \Rightarrow r_1 r_2 \in \mathrm{sat}(\mathcal{A})$ partially reduced w.r.t. $\mathcal{A} \Rightarrow$ By Lemma 6.2.1, $r_1 \in (\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}$ or $r_2 \in (\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}$. Thus, $f_1 \in \mathrm{sat}(\mathcal{A})$ or $f_2 \in \mathrm{sat}(\mathcal{A})$.

② $\forall f \in \mathrm{sat}(\mathcal{A})$, suppose $r = \delta\text{-rem}(f, \mathcal{A})$. Then $r \in (\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}$ by Lemma 6.2.1. Since r is reduced w.r.t. $\mathcal{A}$, $r = 0$. Thus, $\mathcal{A}$ is a δ-characteristic set of $\mathrm{sat}(\mathcal{A})$. □

Remark 6.2.3. *Given an autoreduced set $\mathcal{A} \subseteq K\{Y\}$, denote V to be the set of all derivatives appearing effectively in $\mathcal{A}$. By the proof of Lemma 6.2.2,*

> *$\mathcal{A}$ is a δ-characteristic set of a prime δ-ideal*
> *$\Leftrightarrow$ In $K[V]$, $\mathcal{A}$ is an algebraic characteristic set of $I_{\mathcal{A}}$ and $I_{\mathcal{A}}$ is prime.*

So the question has been reduced to an algebraic one. Below, we follow Wu's constructive theory for irreducible ascending chains.

Algebraic Case: Let $\mathcal{A} = A_1, \ldots, A_p \subseteq K[u_1, \ldots, u_d, x_1, \ldots, x_p]$ be an ascending chain (i.e., an autoreduced set with all elements of order 0) w.r.t. the ranking $u_1 < \cdots < u_d < x_1 < \cdots < x_p$ and $\mathrm{ld}(A_i) = y_i$.

$$\mathcal{A} \begin{cases} A_1 = I_1(u_1, \ldots, u_d) x_1^{m_1} + *x_1^{m_1-1} + \cdots + *x_1 + *; \\ A_2 = I_2(u_1, \ldots, u_d, x_1) x_2^{m_2} + *x_2^{m_2-1} + \cdots + *; \\ \quad \cdots \\ A_p = I_p(u_1, \ldots, u_d, x_1, \ldots, x_{p-1}) x_p^{m_p} + *x_p^{m_p-1} + \cdots + *. \end{cases} \quad \text{degree } (A_i, x_j) < m_j \text{ for } j < i.$$

Definition 6.2.4 (Irreducible ascending chain)**.** *$\mathcal{A} : A_1, \ldots, A_p$ is said to* irreducible *if $\mathcal{A}$ possesses the following properties:*

- *Let $K_0 = K(u_1, \ldots, u_d)$ be transcendental extension field of K adjoining $u_1, \ldots, u_d$. Then A_1, as a polynomial $\tilde{A}_1$ in $K_0[x_1]$, is irreducible in $K_0[x_1]$. Take a solution η_1 of $\tilde{A}_1(x_1) = 0$ and set $K_1 = K_0(\eta_1)$.*

[2] Indeed, for all $f \in (\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}$, $\exists\, c_A \in K\{Y\}$ s.t. $\mathrm{H}_{\mathcal{A}}^{m} f = \sum_{A \in \mathcal{A}} c_A \cdot A$. Rewrite f and each c_A as δ-polynomials in $\Theta(Y)\backslash V$ with coefficients in $K[V]$, then $f = \sum_i f_i(V) M_i$ and $c_A = \sum_i c_{A_i}(V) M_i$ with M_i being distinct δ-monomials in $\Theta(Y)\backslash V$. Then $\mathrm{H}_{\mathcal{A}}^{m} f_i = \sum_{A \in \mathcal{A}} c_{A_i} \cdot A$ in $K[V]$. Thus, $f_i \in I_{\mathcal{A}}$ and $(\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty} = (I_{\mathcal{A}})_{K\{Y\}}$. Similarly, $I_{\mathcal{A}} = ((\mathcal{A}) : \mathrm{H}_{\mathcal{A}}^{\infty}) \cap K[V]$.

- $\tilde{A_2} = A_2(u_1, \ldots, u_d, \eta_1, x_2) \in K_1[x_2]$ *is irreducible. Take a solution* η_2 *of* $\tilde{A_2}(x_2) = 0$ *and set* $K_2 = K_1(\eta_2)$.
- $\tilde{A_3} = A_3(u_1, \ldots, u_d, \eta_1, \eta_2, x_3) \in K_2[x_3]$ *is irreducible. Take a solution* η_3 *of* $\tilde{A_3}(x_3) = 0$ *and set* $K_3 = K_2(\eta_3)$.
- *Suppose that proceeding in the same manner, we get successively algebraic extensions* $K_i = K_{i-1}(\eta_i)$, *polynomial* $\tilde{A_i} = A_i(u_1, \ldots, u_d, \eta_1, \ldots, \eta_{i-1}, x_i)$ *is irreducible in* $K_{i-1}[x_i]$.

The obtained point $\tilde{\eta} = (u_1, \ldots, u_d, \eta_1, \ldots, \eta_p)$ *is called a* generic point *of the irreducible* $\mathcal{A}$.

Note: The irreducibility of $\mathcal{A}$ could be determined mechanically relying on factorization algorithms on towers of algebraic extensions.

Lemma 6.2.5. *If the ascending chain* $\mathcal{A}$ *is irreducible with a generic point* $\tilde{\eta} = (u_1, \ldots, u_d, \eta_1, \ldots, \eta_p)$, *then*

$$\text{prem}(f, \mathcal{A}) = 0 \Leftrightarrow f(\tilde{\eta}) = 0.$$

Furthermore, $\text{asat}(\mathcal{A}) = (\mathcal{A}) : \text{I}_{\mathcal{A}}^{\infty}$ *is a prime ideal with* $\mathcal{A}$ *a characteristic set of it.*[3]

Proof. Let $\mathcal{A}_k = A_1, \ldots, A_k$ $(1 \leq k \leq p)$. Then $\mathcal{A}_k$ is irreducible in $K[u_1, \ldots, u_d, x_1, \ldots, x_k]$ with a generic point $\tilde{\eta_k} = (u_1, \ldots, u_d, \eta_1, \ldots, \eta_k)$. We shall prove by induction on k the following two assertions:

(1_k) $I_k(\tilde{\eta_{k-1}}) \neq 0$ for $I_k = \text{init}(A_k)$.

(2_k) If $R_k \in K[u_1, \ldots, u_d, x_1, \ldots, x_k]$ is reduced w.r.t. $\mathcal{A}_k$ and $R_k(\tilde{\eta_k}) = 0$, then $R_k \equiv 0$.

First note that (1_k) is a consequence of (2_{k-1}). And (1_1) is trivial. So it suffices to prove (2_k) by induction on k. For $k = 1$, if R_1 is reduced w.r.t. $\mathcal{A}_1 = A_1$, then $\deg(R_1, x_1) < m_1$. But $R_1(\tilde{\eta_1}) = 0$ $\Rightarrow A_1 \mid R_1 \Rightarrow R_1 \equiv 0$. Suppose (2_{k-1}) has been proved. Consider any $R_k \in K[u_1, \ldots, u_d, x_1, \ldots, x_k]$ reduced w.r.t. $\mathcal{A}_k$ and $R_k(\tilde{\eta_k}) = 0$. Rewrite R_k as a polynomial in x_k, then $R_k = s_0 x_k^r + s_1 x_k^{r-1} + \cdots +$ s_r for $s_i \in K[u_1, \ldots, u_d, x_1, \ldots, x_{k-1}]$ and $r < m_k$. Since R_k is reduced w.r.t. $\mathcal{A}_k$, each s_i is reduced w.r.t. $\mathcal{A}_{k-1}$. Since $R_k(\tilde{\eta_k}) = 0 = \tilde{s_0}\eta_k^r + \tilde{s_1}\eta_k^{r-1} + \cdots + \tilde{s_r}$ with $\tilde{s_i} = s_i(u_1, \ldots, u_d, \eta_1, \ldots, \eta_{k-1})$, $r < m_k \Rightarrow \tilde{s_i} = 0 \; \forall i = 0, \ldots, r$. By induction hypothesis on (2_{k-1}), $s_i \equiv 0 \Rightarrow R_k \equiv 0$, which completes the proof of (2_k). Thus, by induction (1_k) and (2_k) are proved.

If $\text{prem}(f, \mathcal{A}) = 0$, $I_1^{l_1} \cdots I_p^{l_p} f \in (\mathcal{A}) \Rightarrow f(\tilde{\eta}) = 0$ by (1). Given f with $f(\tilde{\eta}) = 0$, $r = \text{prem}(f, \mathcal{A})$ $\Rightarrow r(\tilde{\eta}) = 0 \Rightarrow r = 0$ by (2). Thus, $\text{prem}(f, \mathcal{A}) = 0 \Leftrightarrow f(\tilde{\eta}) = 0$.

Clearly, $\text{asat}(\mathcal{A}) = \{f \in K[u_1, \ldots, u_d, x_1, \ldots, x_p] \mid f(\tilde{\eta}) = 0\}$. Thus, $\text{asat}(\mathcal{A})$ is prime and $\mathcal{A}$ is a characteristic set of $\text{asat}(\mathcal{A})$. □

Another characterization of irreducibility of ascending sets:

Consider now $\mathcal{A} : A_1, \ldots, A_p$ not necessarily irreducible. Suppose $\exists\, k$ s.t. $\mathcal{A}_{k-1} := A_1, \ldots, A_{k-1}$ is irreducible with a generic point $\tilde{\eta_{k-1}} = (u_1, \ldots, u_d, \eta_1, \ldots, \eta_{k-1})$ and $\tilde{A_k} \in K_{k-1}[x_k]$ is reducible with

$$\tilde{A_k} = g_1 \cdots g_h$$

in which each $g_i \in K_{k-1}[x_k]$ is irreducible and $h \geq 2$. Since the denominators of coefficients of g_i are polynomials in $\tilde{\eta_{k-1}}$, by multiplying a common multiple of the denominators, we get

$$\tilde{D}\tilde{A_k} = \tilde{G_1} \cdots \tilde{G_h}$$

[3]Remark: $\text{prem}(f, \mathcal{A})$ $(= \delta\text{-rem}(f, \mathcal{A}))$ obtained only by performing the proof of Theorem 2.1.12.

in which $D \in K[u_1, \ldots, u_d, x_1, \ldots, x_{k-1}]$, $G_i \in K[u_1, \ldots, u_d, x_1, \ldots, x_k]$ and $\tilde{G_i} = G_i(\eta_{k-1}^{\sim})$. We may also assume D and G_i are reduced w.r.t. $\mathcal{A}_k$.

Write $DA_k - G_1 \cdots G_h = \sum_i B_i x_k^i$ with $B_i \in K[u_1, \ldots, u_d, x_1, \ldots, x_{k-1}]$. Then

$$\sum_i B_i(\eta_{k-1}^{\sim})x_k^i = 0 \Rightarrow B_i \in \mathrm{asat}(\mathcal{A}_{k-1}) \Rightarrow I_1^{r_{i,1}} \cdots I_{k-1}^{r_{i,k-1}} B_i \in (\mathcal{A}_{k-1})$$
$$\Rightarrow I_1^{s_1} \cdots I_{k-1}^{s_{k-1}}(DA_k - G_1 \cdots G_h) \in (A_1, \ldots, A_k) \text{ where } s_j = \max_i\{r_{i,j}\}.$$

Lemma 6.2.6. *Given an autoreduced set $\mathcal{A} = A_1, \ldots, A_p$, if $\mathcal{A}$ is reducible, then $\exists\, k$ $(1 \le k \le p)$ and some $D \in K[u_1, \ldots, u_d, x_1, \ldots, x_{k-1}]$ and $G_i \in K[u_1, \ldots, u_d, x_1, \ldots, x_k]$ s.t. $\mathcal{A}_{k-1} = A_1, \ldots, A_{k-1}$ is irreducible and*

$$DA_k \equiv G_1 G_2 \cdots G_h \bmod (\mathcal{A}_{k-1})$$

where D is reduced w.r.t. $\mathcal{A}_{k-1}$ and $\deg(G_i, x_k) > 0$. Thus,

$$\mathrm{Zero}(\mathcal{A}/\mathrm{I}_{\mathcal{A}}) = \mathrm{Zero}(\mathcal{A}, D/\mathrm{I}_{\mathcal{A}}) \cup \mathrm{Zero}(\mathcal{B}_1/\mathrm{I}_{\mathcal{A}} \cdot D) \cup \cdots \cup \mathrm{Zero}(\mathcal{B}_h/\mathrm{I}_{\mathcal{A}} \cdot D),^4$$

where $\mathcal{B}_i$ is obtained from $\mathcal{A}$ by replacing A_k by G_i.

Return to the differential case: Fix a ranking $\mathscr{R}$ on $K\{Y\}$. Given a finite subset $\Sigma \subseteq K\{Y\}$, mechanical procedures to decompose $\mathbb{V}(\Sigma)$:

Step 1: Apply well-ordering principle to Σ:

$$\mathbb{V}(\Sigma) = \mathbb{V}(\mathcal{A}/\mathrm{H}_{\mathcal{A}}) \cup \cup_{A \in \mathcal{A}}\big(\mathbb{V}(\Sigma, \mathrm{I}_A) \cup \mathbb{V}(\Sigma, \mathrm{S}_A)\big)$$
$$= \cdots = \cup_k \mathbb{V}(\mathcal{B}_k/J_k).$$

Step 2: Consider $\mathbb{V}(\mathcal{B}_k/J_k)$. If $\mathcal{B}_k$ is reducible, then regard $\mathcal{B}_k$ as an algebraic ascending chain in $K[V]$ w.r.t. the ordering induced by $\mathscr{R}$. Then at stage i, $\mathcal{B}_{k,i-1} = B_{k,1}, \ldots, B_{k,i-1}$ is irreducible and

$$DB_{k,i} \equiv G_1 \cdots G_h \bmod (\mathcal{B}_{k,i-1}),$$

where D is reduced w.r.t. $\mathcal{B}_{k,i-1}$ and each G_j has the same leader as $B_{k,i}$. Thus,

$$\mathbb{V}(\mathcal{B}_k/J_k) = \mathbb{V}(\mathcal{B}_k, D/J_k) \cup \cup_{k=1}^h \mathbb{V}(\hat{\mathcal{B}_{k,j}}/D \cdot J_k)$$
$$\cdots = \cup_j \mathbb{V}(\mathcal{C}_{k,j}/\mathrm{H}_{\mathcal{C}_{k,j}}).$$

Here, $\hat{\mathcal{B}_{k,j}}$ is obtained by replacing $B_{k,i}$ by G_j. Continue this procedure until we get the following

Zero Decomposition Theorem (Strong Form)

There is an algorithmic procedure which allows us to give for any finite Σ a decomposition of the form

$$\mathbb{V}(\Sigma) = \cup_k \mathbb{V}(\mathrm{IRR}_k/J_k \cdot G_k),$$

where IRR_k is a d-irreducible autoreduced set and $J_k = \mathrm{H}_{\mathrm{IRR}_k}$.

Differential decomposition Theorem

$\mathbb{V}(\Sigma) = \cup_k \mathbb{V}(\mathrm{sat}(\mathrm{IRR}_k))$, or equivalently, $\{\Sigma\} = \cap_k \mathrm{sat}(\mathrm{IRR}_k)$.

Recent Algorithms:

① Regular decomposition: $\{\Sigma\} = ([\mathcal{A}_1] : \mathrm{H}_{Q_1}^{\infty}) \cap \cdots \cap ([\mathcal{A}_m] : \mathrm{H}_{Q_m}^{\infty})$.

[4] Zero$(*)$ means an algebraic variety.

② (Factorization-free) Characterizable decomposition: $\{\Sigma\} = \mathrm{sat}(\mathcal{A}_1) \cap \cdots \cap \mathrm{sat}(\mathcal{A}_l)$, with $\mathcal{A}_i$ being a characteristic set of $\mathrm{sat}(\mathcal{A}_i)$.

③ Rosenfeld-Gröbner algorithm/Maple.

Application (Mechanical Theorem Proving)
Example: Kepler's Laws $\Longrightarrow$ Newton's Gravitation Laws

$$\underset{\text{Kepler's Laws}}{\overset{\text{(In polar coordinates)}}{}} \begin{cases} (K_1)\ r = \dfrac{p}{1 - e\cos(\theta)} \\ (K_2)\ r^2\theta' = h \end{cases} \Longrightarrow \quad \begin{cases} r = p + ex \\ p' = e' = 0 \\ xy' - x'y = h \\ h' = 0 \end{cases} \text{(In rectangular coordinates)}$$

Here, p, e, h are constants.

$$\underset{\text{Newton's Laws}}{\overset{\text{(In polar coordinates)}}{}} \begin{cases} (N_1)\ a = \dfrac{\text{Const}}{r^2} \\ (N_2)\ (x'', y'') = -\text{Const} \cdot (-x, -y) \end{cases} \Longrightarrow \quad \begin{cases} \big((x'')^2 + (y'')^2\big)r^4 = k \\ k' = 0 \\ x''y - xy'' = 0 \end{cases} \text{(In rectangular coordinates)}$$

$$\mathrm{HYP} = \{r - p - ex, p', e', xy' - x'y - h, h', \big((x'')^2 + (y'')^2\big)r^4 - k\}.$$
$$\mathrm{Conc} = \{k', x''y - xy''\}.$$

To show $\mathrm{HYP} = 0 \xrightarrow[\text{condition } J \neq 0]{\text{under non-degenerate}} \mathrm{Conc} = 0$.
Rename variables $(p, e, r, x, y, h, k) = (x_{21}, x_{22}, x_{31}, x_{32}, x_{33}, x_{51}, x_{52})$ and take the elimination ranking with $x_{21} < x_{22} < x_{31} < x_{32} < x_{33} < x_{51} < x_{52}$. Use the well-ordering principle with selecting "weak" basic set (not necessarily autoreduced, but initials and separants are partially reduced).

$$\mathrm{HYP} \begin{cases} r = p + ex \\ p' = 0 \\ e' = 0 \\ xy' - x'y = h \\ h' = 0 \\ r^2 = x^2 + y^2 \\ \big((x'')^2 + (y'')^2\big)r^4 = k \end{cases} \Longrightarrow \Sigma_1 \begin{cases} x'_{21} = F_1 \\ x'_{22} = F_2 \\ x_{21} + x_{22}x_{32} - x_{31} = F_3 \\ x_{32}x'_{33} - x'_{32}x_{33} - x_{51} = F_4 \\ x'_{51} = F_5 \\ x^2_{32} + x^2_{33} - x^2_{31} = F_6 \\ x''^2_{32}x^4_{31} + x''^2_{33}x^4_{31} - x_{52} = F_7 \end{cases}$$

$\Sigma_1 = \{F_1, F_2, \ldots, F_7\}$.
$\mathcal{A}_1 = F_1, F_2, F_3, F_6, F_4, F_7$.
$r_1 = \delta\text{-rem}(F_5, \mathcal{A}_1) = 4x_{21}\big((x^3_{31}x^2_{22} - x^3_{31} + 2x^2_{31}x_{21} - x_{31}x^2_{21})x''_{31} + x_{31}x_{21}(x'_{31})^2 - x'^2_{31}x^2_{21}\big)$.
$\Sigma_2 = \Sigma_1 \cup \{r_1\}$.
$\mathcal{A}_2 = \{F_1, F_2, r_1, F_3, F_4, F_6, F_7\}$.
$R_2 = \emptyset$.
So $\mathcal{A} = \mathcal{A}_2$.

$$\begin{cases} \delta\text{-rem}(x'_{52}, \mathcal{A}) = 0 \text{ with } h_1 = -128x^8_{33}x^8_{22}x^2_{21} \\ \delta\text{-rem}(x''_{32}x_{33} - x_{32}x''_{33}, \mathcal{A}) = 0 \text{ with } h_2 = 16x^3_{33}x^3_{22}x_{21}. \end{cases}$$

So $\mathbb{V}(\mathrm{HYP}/\mathrm{H}_{\mathrm{HYP}}) \subseteq \mathbb{V}(\mathrm{Conc})$.
Note that $\mathrm{H}_{\mathrm{HYP}} = 4x_{21}(x^3_{31}x^2_{22} - x^3_{31} + 2x^2_{31}x_{21} - x_{31}x^2_{21})x_{33}x_{22} \xrightarrow{F_3} 4x_{21}x_{31}x^3_{22}x^3_{33}$.
Non-degenrate elliptic orbits $\Longrightarrow x_{21} = p \neq 0, x_{31} = r \neq 0, x_{22} = e \neq 0, x_{33} = y \neq 0$.
Thus, Kepler's Laws (K_1) and (K_2) $\Longrightarrow$ (N_1) and (N_2).