Recall the concept of differential variety and the differential Nullstellensatz theorem:

Let (K,δ) be a differential field of characteristic 0 and $(E,\delta)\supset(K,\delta)$ is a differentially closed field. Consider the differental polynomial ring $K\{\mathbb{Y}\}=K\{y_1,\ldots,y_n\}$ and the affine space E^n.

- A differential variety V is the set of differential zeros of some differential polynomial set $\Sigma\subset K\{\mathbb{Y}\}$ rational over E. That is, $V=\mathbb{V}(\Sigma)\triangleq\{\eta\in E^n \mid f(\eta)=0,\forall f\in\Sigma\}$.

  Basic operations: $\mathbb{V}(\Sigma_1\cdot\Sigma_2)=\mathbb{V}(\Sigma_1)\cup\mathbb{V}(\Sigma_2)$; $\mathbb{V}(I\cdot J)=\mathbb{V}(I)\cup\mathbb{V}(J)=\mathbb{V}(I\cap J)$;
  $\mathbb{I}(V_1\cup V_2)=\mathbb{I}(V_1)\cap\mathbb{I}(V_2)$

- The **Ritt-Raudenbush basis theorem** guarantees that each differential variety can be defined by a finite set of differential polynomials. (Indeed, $\exists\, f_1,\ldots,f_s\in\Sigma$ s.t. $\{\Sigma\}=\{f_1,\ldots,f_s\}$. So $V=\mathbb{V}(\Sigma)=\mathbb{V}(\{\Sigma\})=\mathbb{V}(\{f_1,\ldots,f_s\})=\mathbb{V}(f_1,\ldots,f_s)$.)

  We have two maps between the set of δ-K-varieties and the set of radical δ-ideals in $K\{Y\}$:

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

  and

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

- **Differential Nullstellensatz**: $\mathbb{I}(\mathbb{V}(F))=\{F\}$. In particular, $\mathbb{V}(F)=\emptyset\Longleftrightarrow 1\in[F]$.

  Consequently, $\mathbb{I}$ and $\mathbb{V}$ are inclusion reversing bijective maps.

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. Otherwise, it is said to be reducible.

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 $f_1f_2\in\mathbb{I}(V_1)\cap\mathbb{I}(V_2)=\mathbb{I}(V)$, 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 2.3.5 and Corollary 2.3.6,

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

So $V = \mathbb{V}(\mathbb{I}(V)) = \mathbb{V}(\bigcap_{j=1}^{l} P_j) = \bigcup_{j=1}^{l} \mathbb{V}(P_j)$ 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 maximal irreducible differential subvarieties contained in V.

Irreducible components of a single Algebraic differential equation

Let $A \in K\{Y\} \backslash K$ be algebraically irreducible (i.e., not the product of two differential polynomials in $K\{Y\} \backslash K$). Unlike the algebraic case, $\mathbb{V}(A)$ might be a reducible differential variety:

Example: (1) Let $A = (y')^2 - 4y \in K\{y\}$. Note that $A' = 2y'(y''-2)$. So $\mathbb{V}(A) = \mathbb{V}(y) \cup \mathbb{V}(A, y''-2)$.

(2) Let $A = y''^2 - y \in K\{y\}$. Then $A' = 2y''y^{(3)} - y', A'' = 2y''y^{(4)} + 2(y^{(3)})^2 - y''$, $A^{(3)} = 2y''y^{(5)} + 6y^{(3)}y^{(4)} - y^{(3)}$. An easy calculation shows that

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

So $\mathbb{V}(A) = \mathbb{V}(A, y'') \cup \mathbb{V}(A, 4y^{(3)}y^{(5)} - 12(y^{(4)})^2 + 8y^{(4)} - 1)$.

In the following, we study the prime decomposition of the radical differential ideal $\{A\}$ (or equivalently, the irreducible decomposition of the variety $\mathbb{V}(A)$).

Fix an arbitrary differential ranking $\mathscr{R}$ on $\Theta(Y)$. Let $\mathrm{ld}(A) = y_p^{(h)}$ for some $p \in \{1, \ldots, n\}$ and $h \in \mathbb{N}$, and take the separant S_A of A under $\mathscr{R}$.

Definition. 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 $\mathrm{ord}(A) = \max_i\{\mathrm{ord}(A, y_i)\}$.

Lemma 3.3.3. *Let* $P_1 = \{A\} : \mathrm{S}_A = \{f \in K\{Y\} \mid \mathrm{S}_A f \in \{A\}\}$. *Then*

1) P_1 *is prime.*

2) *For a differential polynomial* $F \in K\{Y\}$, *we have* $F \in P_1$ *if and only if* δ-*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 $f, g \in K\{Y\}$ with $fg \in P_1$. 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.

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

So $\mathrm{S}_A^{a+b+1} fg \equiv\ S_A f_1 g_1 \bmod [A]$. 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.

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

We now show q can be taken 0 in $(*)$. Assume $q > 0$. 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 $y_p^{(h+1)}, \ldots, y_p^{(h+q)}$. If $q > 0$, by replacing $y_p^{(h+k)}$ by $-\frac{T_k}{\mathrm{S}_A}$ for $k = 1, \ldots, q$ at both sides of $(*)$, we have

$$(\mathrm{S}_A f_1 g_1)^l = \overline{M} \cdot A, \text{ where } \overline{M} = M\mid_{y_p^{(h+k)} = -\frac{T_A}{\mathrm{S}_A},\ k=1,\ldots,q}.$$

Clearing fractions by multiplying a power of S_A, we have

$$\mathrm{S}_A^t (f_1 g_1)^l = N \cdot A$$

for some $N \in K\{Y\}$. Since A is irreducible and $A \nmid \mathrm{S}_A$, $A|(f_1 g_1)$ and thus $A|f_1$ or $A|g_1$. Suppose that $A|f_1$. Then $\mathrm{S}_A^a f \in \{A\}$ and it follows that $f \in \{A\} : \mathrm{S}_A = P_1$. Thus, P_1 is prime.

2) If $\delta\text{-rem}(F, A) = 0$, then $F \in \mathrm{sat}(A) = [A] : \mathrm{S}_A^\infty \subseteq \{A\} : \mathrm{S}_A = P_1$.

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 $\delta\text{-rem}(F, A) = 0$.

□

Remark. By Lemma 3.3.4, $P_1 = \{A\} : \mathrm{S}_A = \mathrm{sat}(A) = [A] : \mathrm{S}_A^\infty$ and A is a characteristic set of P_1 under the ranking $\mathscr{R}$.

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

Proof. Clearly, $\{A\} \subseteq P_1 \cap \{A, \mathrm{S}_A\}$. Suppose $f \in P_1 \cap \{A, \mathrm{S}_A\}$, we need to show $f \in \{A\}$. Since $f \in \{A, \mathrm{S}_A\}$, $\exists\, l \in \mathbb{N}$, $f^l = T_1 + T_2$ for $T_1 \in [A], T_2 \in [\mathrm{S}_A]$. $f \in P_1 \Rightarrow \mathrm{S}_A f \in \{A\} \Rightarrow \delta^k(\mathrm{S}_A) f \in \{A\}$ for each $k \in \mathbb{N}$. 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 $\{A\} = P_1 \cap \cdots \cap P_r$ is the minimal prime decomposition of $\{A\}$.

<u>Claim</u> 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 $\{A, \mathrm{S}_A\} \subseteq P_2, \ldots, P_r$, $\mathrm{S}_A \in P_2, \ldots, P_r$. $\mathrm{S} \in P_2, \ldots, P_r$ follows from the fact that $\{P_1, \ldots, P_r\}$ are the unique irreducible components of $\{A\}$. □

Remark: A is a differential characteristic set of $P_1 = \{A\} : \mathrm{S}_A = \{A\} : \mathrm{S} = \mathrm{sat}(A)$ (S is the separant of A under some 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: Let $n = 1$ and $A = (y')^2 - 4y$. Clearly, $\mathrm{S}_A = 2y'$ and $\{A, \mathrm{S}_A\} = \{(y')^2 - 4y, 2y'\} = [y]$. Since $A' = 2y'(y'' - 2)$, $y'' - 2 \in \{A\} : \mathrm{S}_A$ and $y'' - 2 \notin [y]$. Note that for each $f \in \{A\} : \mathrm{S}_A$, if $f_1 = \delta\text{-rem}(f, y'' - 2)$, then $f_1 \in \{A\} : \mathrm{S}_A$ and $A|f_1$ follows. Thus, $\{A\} : \mathrm{S}_A = [(y')^2 - 4y, y'' - 2]$ is the general component of A and $[y]$ is the singular component of A.

Let us solve $(y')^2 - 4y = 0$ over $K = (\mathbb{R}(x), \frac{\mathrm{d}}{\mathrm{d}x})$: Note that $\frac{\mathrm{d}y}{\mathrm{d}x} = \pm 2\sqrt{y} \Rightarrow \frac{\mathrm{d}y}{2\sqrt{y}} = \pm \mathrm{d}x \Rightarrow \sqrt{y} = \pm x + c$. So $y = (x + c)^2$ (c an arbitrary constant) or $y = 0$. Here $[(y')^2 - 4y, y'' - 2]$ defines the "general solution" $(x + c)^2$ and y defines the "singular solution" of A.

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: Let $A = (y')^2 - y^3 \in K\{y\}$. $\mathrm{S}_A = 2y'$. 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, if $K = (\mathbb{C}(t), \frac{\mathrm{d}}{\mathrm{d}t})$, $\eta_c = \frac{1}{4(t+c)^2}$ 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, we have the following result.

Theorem 3.3.5. ***(Ritt's component theorem)*** *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 $\mathrm{ord}(B_i) < \mathrm{ord}(A)$.

Let $A \in K\{Y\}$ be an algebraically irreducible differential polynomial. Ritt's component theorem calims that there exists irreducible differential polynomials $B_1, \ldots, B_s$ of order lower than the order of A such that the general component of $B_1, \ldots, B_s$ are the singluar components of $\mathbb{V}(A)$. Let B be an irreducible differential polynomial such that A belongs to the general component of B.

Problem. Can we determine whether $\mathrm{sat}(B)$ is a prime component of A?

Yes, the low power theorem gives a necessary and sufficient condition for the general component of B to be a prime component of A. For this, we need the *preparation congruence for A w.r.t. B*, which is to write $\mathrm{S}_B A$ as a differential polnomial in B with coefficients that are differential polynomials in $K\{Y\}$ not contained in $\mathrm{sat}(B)$.

The Low Power Theorem (Ritt, 1936) The general component of B is a component of A if and only if the preparation congruence for A w.r.t. B contains a term cB^k, free of proper derivatives of B, which considered as a differential polynomial in B, has lower degree than any other term.

Example. $[y]$ is a singular component of $y'y'' - y$, but not for $(y')^2 - y^3, yy''' - y''$ and $y''y''' - y^2$.

Chapter 4

Extensions of differential fields

4.1 Extensions of derivations

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 $\frac{\mathrm{d}}{\mathrm{d}x}(\sum_{i=0}^{l} r_i x^i) = \sum_{i=1}^{l} i r_i x^{i-1}$. Of course, $\frac{\mathrm{d}}{\mathrm{d}x}$ does not extend δ.

Lemma 4.1.1. *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 4.1.2. *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.*