Recall: Let (K,δ) be a diff field of char 0 and $(E,\delta)\supseteq(K,\delta)$ diff closed.

Ritt-Raudenbush Basis Theorem $K\{y_1,\cdots,y_n\}$ is Ritt-Noetherian. So every radical δ-ideal is finitely generated (as a radical δ-ideal).

Cor. Let $I \subsetneqq K\{y_1,\cdots,y_n\}$ be a radical δ-ideal. Then $\exists$ finitely many prime δ-ideals $P_1,\cdots,P_l$ s.t. $I=\bigcap_{i=1}^{l} P_i$. $(*)$

If $(*)$ is irredundant (i.e., $\forall i$, $\bigcap_{j\neq i} P_j \not\subseteq P_i$), the set of prime ideals in $(*)$ is unique and each P_i is called prime components of I.

A diff variety $V\subseteq E^n$ over K is of the form

$$V=\mathbb{V}(f_1,\cdots,f_m)=\{\eta\in E^n \mid f_i(\eta)=0,\ i=1,\cdots,m\} \text{ for some } f_i\in K\{y_1,\cdots,y_n\}.$$

($V=\mathbb{V}(S)=\mathbb{V}([S])=\mathbb{V}(\{S\})=\mathbb{V}(f_1,\cdots,f_m)$, where $\{S\}=\{f_1,\cdots,f_m\}$ guaranteed by the Ritt-Raudenbush Basis theorem).

We have two inclusion-reversing maps as follows:

$$\mathbb{I}: \{\delta\text{-varieties in } E^n \text{ over } K\} \longrightarrow \{\text{radical } \delta\text{-ideals in } K\{y_1,\cdots,y_n\}\}$$
$$V \qquad\qquad\qquad\qquad \mathbb{I}(V)$$

and

$$\mathbb{V}: \{\text{radical } \delta\text{-ideals in } K\{y_1,\cdots,y_n\}\} \longrightarrow \{\delta\text{-varieties in } E^n \text{ over } K\}$$
$$I \qquad\qquad\qquad\qquad \mathbb{V}(I)$$

Cor 3.1.2 $\quad \mathbb{V}(\mathbb{I}(V))=V$.

§3.2 Differential Nullstellensatz

The Hilbert Nullstellensatz in algebraic geometry has two forms:

Theorem (Weak Nullstellensatz)

Let $F\subseteq K[x_1,\cdots,x_n]$. Then $\mathcal{V}(F)=\{\eta\in\overline{K}^n \mid F(\eta)=0\}=\phi \Leftrightarrow 1\in(F)$.

Theorem (Strong Nullstellensatz)

Let $F \subseteq K[x_1, \cdots, x_n]$ and $f \in K[x_1, \cdots, x_n]$. If $f|_{V(F)} \equiv 0$, then
$$f \in \sqrt{(F)}.$$

We have differential versions of Hilbert Nullstellensatz in differential algebra.

Theorem 3.2.1 (Weak Differential Nullstellensatz)

Let $F \subseteq K\{Y_1, \cdots, Y_n\}$ and $(E, \delta) \supseteq (K, \delta)$ a diff closed field.
Then $\mathbb{V}(F) = \{\eta \in E^n \mid F(\eta) = 0\} = \phi \iff 1 \in [F]$.

Proof. It suffices to show that if $[F] \neq K\{Y_1, \cdots, Y_n\}$, then $\exists\ \eta \in E^n$ s.t. $f(\eta) = 0$ for all $f \in F$.

Since $1 \notin [F]$, $\sqrt{[F]} \neq K\{Y_1, \cdots, Y_n\}$. Let $\sqrt{[F]} = \bigcap_{i=1}^{l} P_i$ be the minimal prime decomposition. Let $M = \mathrm{Frac}(K\{Y_1, \cdots, Y_n\}/P_1)$. Then M is a δ-extention field of K and $(\bar{Y}_1, \cdots, \bar{Y}_n) \in M^n$ is a generic zero of P_1. $F \subseteq P_1$ implies that $(\bar{Y}_1, \cdots, \bar{Y}_n)$ is a δ-zero of F. Since $E \supseteq K$ is diff closed, there exists $\eta = (\eta_1, \cdots, \eta_n) \in E^n$ s.t. $\forall\ f \in F$, $f(\eta) = 0$. ☒.

Theorem 3.2.2 (Differential Nullstellensatz).

- Let $F \subseteq K\{Y_1, \cdots, Y_n\}$ and $f \in K\{Y_1, \cdots, Y_n\}$. If f vanishes at every δ-zero of F in E^n, then $f \in \{F\}$.
- $\mathbb{I}(\mathbb{V}(F)) = \{F\}$.

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

Introduce a new δ-indeterminate t and consider the new diff poly set $F, 1 - ft$ in $K\{Y_1, \cdots, Y_n, t\}$. Since f vanishes

at every δ-zero in E^n of F, $\mathbb{V}(F, 1-ft) \subseteq E^{n+1}$ is the emptyset.
By the weak differential Nullstellensatz, $1 \in [F, 1-ft] \subseteq K\{y_1, \cdots, y_n, t\}$.
Hence, $\exists\, A_i, B_i \in K\{y_1, \cdots, y_n, t\}$ 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

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

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

<u>Remark</u> 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 Cor 3.1.2 show that the two maps $\mathbb{I}$ and $\mathbb{V}$ are bijections.

<u>Theorem 3.2.3</u> The maps $V \longrightarrow \mathbb{I}(V)$ and $I \rightarrow \mathbb{V}(I)$ define inclusion reversing bijections between the set of all δ-varieties in E^n over K and the set of all radical δ-ideals in $K\{y_1, \cdots, y_n\}$.

Def 3.2.4 Let $V \subseteq E^n$ be a δ-variety. Then the δ-ring

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

is called the differential coordinate ring of V.
(Since for any $a \in V$, $\bar{f_1} = \bar{f_2}$ implies that $f_1(a) = f_2(a)$. So $K\{V\}$ could be regarded as a ring of differential functions on V.)

$W \subseteq E^n$ is called a δ-subvariety of V if $W \subseteq V$ and W is a δ-variety in E^n. (Assume all δ-varieties are over K unless otherwise indicated)

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

Cor 3.2.5 Let $V \subseteq E^n$ be a δ-variety. The map

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

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

Remark. (Effective Hilbert Nullstellensatz and Effective differential Nullstellensatz)

Effective Nullstellensatz

Let $p_1, \cdots, p_m \in \mathbb{C}[x_1, \cdots, x_n] = \mathbb{C}[X]$ have degree at most $D \geq 1$. If $p_1, \cdots, p_m$ have no common zero in $\mathbb{C}^n$, then there are poly $A_1, \cdots, A_m \in \mathbb{C}[X]$ of degree bounded by $B(D, n, m)$ s.t.

$$1 = A_1 p_1 + \cdots + A_m p_m.$$

(If such a degree bound $B(D, n, m)$ for A_i exists, to decide whether $p_1 = \cdots = p_m = 0$ has a zero is reduced to solve linear equations.)

- $\deg(A_i) \leq 2(2D)^{2^{n-1}}$ (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)
- $\deg(A_i p_i) \leq \begin{cases} d_1 d_2 \cdots d_m & \text{if } m \leq n \\ d_1 \cdots d_{n-1} d_m & \text{if } m > n > 1 \\ d_1 + d_m - 1 & \text{if } m > n = 1. \end{cases}$ (Kollar, J. Amer. Math. Soc., 1988)

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

Subsequent work on sharper bounds or new proofs.

Effective Differential Nullstellensatz

If $F_1, \cdots, F_k \in K\{Y_1, \cdots, Y_n\}$ have no common δ-zeros in E^n, then $\exists\ s \in \mathbb{N}$ and $A_{ij} \in K\{Y_1, \cdots, Y_n\}$ 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 # diff variables n.

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

Focus on the ordinary diff case:

- $s \leq A(9, \max\{n, h, d\})$ $\left(A(\cdot,\cdot) \text{ Ackermann function } \begin{cases} A(0,n) = n+1 \\ A(m+1, 0) = A(m, 1) \\ A(m+1, n+1) = A(m, A(m+1, n)) \end{cases} \right)$

  (Golubitsky, J. Algebra, 2009)

- K: constant diff 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)

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

  (Ovchinnikov, Arxiv:1610.~~0422v6,~~ 2018)

Example: $F = \{Y_1^2, Y_1 - Y_2^2, \cdots, Y_{n-1} - Y_n^2, 1 - Y_n'\}$ $\mathbb{V}(F) = \phi$.

$1 \notin (F, \cdots, F^{(2^n - 1)})$ and $1 \in (F, \cdots, F^{(2^n)})$.

So $s \leq 2^n$.

§3.3 Irreducible decomposition of differential varieties

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

Lemma 3.3.1 A δ-variety V is irreducible $\Leftrightarrow \mathbb{I}(V) \subseteq K\{y_1, \cdots, y_n\}$ 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 irr $\Rightarrow$ $\mathbb{V}(\mathbb{I}(V), f) = V$ 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, $\exists\, f_i \in \mathbb{I}(V_i) \setminus \mathbb{I}(V)$, $i = 1, 2$, but $f_1 f_2 \in \mathbb{I}(V_1) \cap \mathbb{I}(V_2) = \mathbb{I}(V)$ $\rightarrow\leftarrow$.

If $\mathbb{I}(V_1) \subseteq \mathbb{I}(V)$, then $V = V_1$; and in the other case, $V = V_2$. $\boxtimes$.

Theorem 3.3.2. Any δ-variety V is a finite union of irreducible δ-varieties, i.e., $V = \bigcup_{i=1}^{l} V_i$ w/ V_i irreducible δ-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 $V_i \nsubseteq \bigcup_{j \neq i} V_j$, $\forall\, i$), then the set $\{\underline{V_1, \cdots, V_l}\}$ is unique for V.
irreducible components of V

Proof. By Theorem 2.2.4 and Corollary 2.2.5,

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

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

<u>Uniqueness</u>: 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 $i=1,\dots,l$. ☒.

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

<u>Components of a single Algebraic differential Equation</u> $K\{Y\}=K\{y_1,\dots,y_n\}$.

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

<u>Example</u> Let $A=y''^2-y\in K\{y\}$. Then $A'=2y''y^{(3)}-y'$,

$$A''=2y''y^{(4)}+2(y^{(3)})^2-y'',\quad A^{(3)}=2y''y^{(5)}+6y^{(3)}y^{(4)}-y^{(3)}.$$

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

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

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

Let $P_1 = \{A\} : S_A = \{ f \in K\{Y\} \mid S_A f \in \{A\}$.

Lemma 3.3.3 1) P_1 is prime.

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

Proof. 1) Let $fg \in P_1$ w/ $f, g \in K\{Y\}$. 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.

$$S_A^a f \equiv f_1 \mod [A]$$

and $\quad S_A^b g \equiv g_1 \mod [A]$.

$$\Rightarrow S_A^{a+b+1} fg \equiv S_A f_1 g_1 \mod [A].$$

Since $fg \in P_1 = \{A\} : S_A$, $S_A f_1 g_1 \in \{A\}$. Thus, $\exists\, l \in \mathbb{N}$ s.t.

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

Recall that for $k \geq 1$, $A^{(k)} = S_A y_p^{(h+k)} + T_k$ w/ T_k free of $y_p^{(h+k)}$.
Note that S_A, f_1, g_1 are free from $y_p^{(h+1)}, \cdots, y_p^{(h+q)}$.
Now replace $y_p^{(h+k)}$ by $-\frac{T_k}{S_A}$ for $k = 1, \cdots, q$ at both sides of $(*)$, then we have

$$(S_A f_1 g_1)^l = \overline{M} \cdot A \quad \text{where } \overline{M} = M \Big|_{y_p^{(h+k)} = -\frac{T_k}{S_A}}.$$

Clearing fractions, we have

$$S_A^t (f_1 g_1)^l = N \cdot A.$$

Since A is irreducible and $A \nmid S_A$, $A \mid f_1 g_1$ and thus $A \mid f_1$ or $A \mid g_1$. Suppose that $A \mid f_1$. Then $S_A^a f \in \{A\}$ and it follows that $f \in \{A\} : S_A = P_1$ and P_1 is prime. $\square$.

2) If $\delta\text{-Rem}(F,A)=0$, then $F\in \mathrm{Sat}(A)=[A]:S_A^{\infty}\subseteq \{A\}:S_A=P_1$.
Conversely, Let $F\in P_1$, then $S_AF\in\{A\}$.
Let R be the partial remainder of F w.r.t. A, then
$$S_A^m F \equiv R \mod [A].$$
$S_AF\in\{A\} \Rightarrow S_AR\in\{A\}$.
$\Rightarrow \exists\, l\in\mathbb{N}$ s.t. $(S_AR)^l = MA+M_1A'+\cdots+M_tA^{(t)}$.
By the procedure in 1), we can show $A\mid R$. So $\delta\text{-rem}(F,A)=0$. ☒.

<u>Prop 3.3.4</u> $\{A\}=P_1\cap\{A,S_A\}$.
proof. Clearly, $\{A\}\subseteq P_1\cap\{A,S_A\}$.
Suppose $f\in P_1\cap\{A,S_A\}$, it suffices to show $f\in\{A\}$.
Since $f\in\{A,S_A\}$, $\exists\, l\in\mathbb{N}$, $f^l=T_1+T_2$ for $T_1\in[A]$, $T_2\in[S_A]$.
$f\in P_1 \Rightarrow S_Af\in\{A\} \Rightarrow \delta^k(S_A)f\in\{A\}$
So $f^{l+1}\in\{A\}$ and $f\in\{A\}$ follows. ☒.

Let $\{A,S_A\}=Q_1\cap\cdots\cap Q_t$ be the minimal prime decomposition of $\{A,S_A\}$. Then $\{A\}=P_1\cap Q_1\cap\cdots\cap Q_t$. Suppressing those Q_i with $P_1\subseteq Q_i$ and denote the left Q_i's by $P_2,\cdots,P_r$. Then
<u>$\{A\}=P_1\cap\cdots\cap P_r$</u> is the minimal prime decomposition of $\{A\}$.

<u>Claim</u> For each separant S of A any arbitrary ranking,
$$S\notin P_1=\{A\}:S_A \text{ and } S\in P_2,\cdots,P_r.$$
<u>proof.</u> $S\notin P_1$ follows from Lemma 3.3.3 and the fact $A\nmid S$.
Since $\{A,S_A\}\subseteq P_2,\cdots,P_r$, $S_A\in P_2,\cdots,P_r$.

$S \in P_2, \cdots, P_r$ follows from the fact that $\{P_1, \cdots, P_r\}$ are the unique irreducible components of $\{A\}$. ☒.

Remark: A is the δ-characteristic set of $P_1 = \{A\} : S_A = \{A\} : S = \text{sat}(A)$.
(S is the separant of A under any other ranking)
P_1 or $\mathbb{V}(P_1)$ is called the general component of $A = 0$.
$P_2, \cdots, P_r$ are called singular components of $A = 0$.

Def. A δ-zero $\eta \in E^n$ of A is called a nonsingular zero if $\exists$ a separant S of A s.t. $S(\eta) \neq 0$. And if $S(\eta) = 0$ for all separants of A, η is called a singular solution/zero of $A = 0$
Nonsingular zeros belong to general component of A, but general component of A may contain singular solutions of A.

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

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

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

Theorem 3.3.5 Let $A \in K\{y_1, \cdots, y_n\}$ be a δ-poly not in K.
Let $\{A\} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ be the minimal prime decomposition of $\{A\}$, then $\exists\, B_i \in K\{y_1, \cdots, y_n\}$ irreducible s.t. $\mathfrak{p}_i = \mathrm{sat}(B_i)$, $i = 1, \cdots, r$.
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 $\mathrm{ord}(B_i) < \mathrm{ord}(A)$.