Recall $\Sigma \subseteq K\{y_1, \dots, y_n\}$: a finite set of nonzero δ-polys

- **basic set** of Σ: an autoreduced set $\mathcal{A} \subseteq \Sigma$ which is of lowest rank among all autoreduced sets contained in Σ.

- **Ritt-Wu's Well-ordering principle**

$$\begin{array}{cccccc}
\Sigma_0 = \Sigma & \subseteq & \Sigma_1 = \Sigma_0 \cup R_0 & \subseteq \cdots \subseteq & \Sigma_e = \Sigma_{e-1} \cup R_{e-1} \\
\mathcal{B}_0 = b.s.(\Sigma_0) & > & \mathcal{B}_1 = b.s.(\Sigma_1) & > \cdots > & \underline{\mathcal{B}_e = b.s.(\Sigma_e)} \\
R_0 \neq \phi & & R_1 \neq \phi & \cdots & R_e = \phi
\end{array}$$

$\mathcal{A} \triangleq \mathcal{B}_e$: the **characteristic set** of Σ. ($\mathcal{A} \subseteq [\Sigma]$ and $\delta\text{-rem}(\Sigma, \mathcal{A}) = \{0\}$)

Properties of $\mathcal{A}$:

① $\mathbb{V}(\mathcal{A}/H_{\mathcal{A}}) \subseteq \mathbb{V}(\Sigma) \subseteq \mathbb{V}(\mathcal{A})$;

② $\mathbb{V}(\Sigma) = \mathbb{V}(\mathcal{A}/H_{\mathcal{A}}) \cup \bigcup_{A \in \mathcal{A}} \left(\mathbb{V}(\Sigma, I_A) \cup \mathbb{V}(\Sigma, S_A) \right)$

($H_{\mathcal{A}} = \prod_{A \in \mathcal{A}} (I_A \cdot S_A)$, I_A, S_A: initial, separant of A)

- **Zero decomposition Theorem: Weak Form**

$$\mathbb{V}(\Sigma) = \bigcup_{j=1}^{l} \mathbb{V}(CS_j / H_{CS_j})$$
$$= \bigcup_{j=1}^{l} \mathbb{V}(\mathrm{sat}(CS_j))$$

CS_j: autoreduced set with $\delta\text{-rem}(\Sigma, CS_j) = \{0\}$.

& $CS_j \leq b.s.(\Sigma)$.

Question 1: Given an autoreduced set $\mathcal{A} \subseteq K\{y_1, \dots, y_n\}$

$\mathcal{A}$ is a char set of a prime δ-ideal $\Longleftrightarrow$?

- Lemma 5.2.1 (Rosenfeld's Lemma for $m=1$)

  If $f \in K\{y_1, \dots, y_n\}$ partially reduced w.r.t. $\mathcal{A}$,

  then $f \in [\mathcal{A}] : H_{\mathcal{A}}^{\infty} \Longleftrightarrow f \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$.

<u>Lemma 5.2.2</u> Let $\mathcal{A}$ be an autoreduced set in $K\{Y\}$ w.r.t. a ranking $\mathcal{R}$. Then $\mathcal{A}$ is a δ-characteristic set of a prime δ-ideal $\Longleftrightarrow$ $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ is a prime algebraic ideal in $K\{Y\}$ and $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ contains no nonzero element reduced w.r.t. $\mathcal{A}$.

(i.e., "reduced" in the differential sense.)

Proof. "$\Rightarrow$" Take a minimal subset $V \subseteq \Theta(Y)$ s.t. $\mathcal{A} \subseteq K[V]$.

Let $P_{\mathcal{A}} = \{ f \in K[V] \mid \exists\, m \in \mathbb{N} \text{ s.t. } H_{\mathcal{A}}^{m} \cdot f \in (\mathcal{A}) \}$.

Then we have $(\mathcal{A}) : H_{\mathcal{A}}^{\infty} = (P_{\mathcal{A}})_{K\{Y\}}$ and

$$P_{\mathcal{A}} = \left((\mathcal{A}) : H_{\mathcal{A}}^{\infty} \right) \cap K[V].$$

Indeed, $\forall\, f \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$, $\exists\, m \in \mathbb{N}$ s.t. $H_{\mathcal{A}}^{m} \cdot f = \sum_{A \in \mathcal{A}} C_A \cdot A$, $C_A \in K\{Y\}$

Rewrite f and C_A as δ-polys in $\Theta(Y) \setminus V$ with coefficients in $K[V]$, then $f = \sum_i f_i(V) \cdot M_i$ and $C_A = \sum_i C_{A,i}(V) \cdot M_i$ with M_i being distinct δ-monomials in $\Theta(Y) \setminus V$. Then we have

$H_{\mathcal{A}}^{m} \cdot f_i = \sum_{A \in \mathcal{A}} C_{A,i} \cdot A$, i.e., $f_i \in P_{\mathcal{A}}$. So $f \in (P_{\mathcal{A}})$ and $(\mathcal{A}) : H_{\mathcal{A}}^{\infty} = (P_{\mathcal{A}})_{K\{Y\}}$. Similarly, $P_{\mathcal{A}} \supseteq ((\mathcal{A}) : H_{\mathcal{A}}^{\infty}) \cap K[V]$ follows.

By Lemma 5.2.1, $\mathrm{Sat}(\mathcal{A}) \cap K[V] = \left((\mathcal{A}) : H_{\mathcal{A}}^{\infty} \right) \cap K[V] = P_{\mathcal{A}}$.

Since $\mathrm{sat}(\mathcal{A})$ is a prime δ-ideal, $P_{\mathcal{A}}$ is a prime ideal and consequently, $(\mathcal{A}) : H_{\mathcal{A}}^{\infty} = (P_{\mathcal{A}})_{K\{Y\}}$ is prime too.

Since $\mathcal{A}$ is a δ-characteristic set of $\mathrm{Sat}(\mathcal{A})$,

$(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ contains no nonzero polynomial reduced w.r.t. $\mathcal{A}$.

"$\Leftarrow$" We first show $\mathrm{sat}(\mathcal{A})$ is a prime δ-ideal.

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 $\exists\, m_1, m_2 \in \mathbb{N}$ s.t. $H_{\mathcal{A}}^{m_1} \cdot f_1 \equiv r_1 \mod [\mathcal{A}]$ and

$$H_{\mathcal{A}}^{m_2} \cdot f_2 \equiv r_2 \mod [\mathcal{A}].$$

$\Rightarrow r_1 r_2 \in \mathrm{sat}(\mathcal{A})$ and $r_1 r_2$ is partially reduced w.r.t. $\mathcal{A}$.

By Lemma 5.2.1, $r_1 r_2 \in (\mathcal{A}):H_{\mathcal{A}}^{\infty}$. Since $(\mathcal{A}):H_{\mathcal{A}}^{\infty}$ is prime, $r_1 \in (\mathcal{A}):H_{\mathcal{A}}^{\infty}$ or $r_2 \in (\mathcal{A}):H_{\mathcal{A}}^{\infty}$. So $f_1 \in \mathrm{sat}(\mathcal{A})$ or $f_2 \in \mathrm{sat}(\mathcal{A})$ and $\mathrm{sat}(\mathcal{A})$ is a prime δ-ideal.

It remains to show that $\mathcal{A}$ is a char set of $\mathrm{sat}(\mathcal{A})$. Let $f \in \mathrm{sat}(\mathcal{A})$ and $r = \delta\text{-rem}(f, \mathcal{A})$. Then by Lemma 5.2.1, $r \in (\mathcal{A}):H_{\mathcal{A}}^{\infty}$. Since $(\mathcal{A}):H_{\mathcal{A}}^{\infty}$ contains no nonzero poly reduced w.r.t. $\mathcal{A}$, $r=0$. Thus, $\mathcal{A}$ is a characteristic set of $\mathrm{sat}(\mathcal{A})$. 證.

<u>Remark</u> 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-char set of a prime δ-ideal

$\Leftrightarrow$ $\mathcal{A}$ is a char set of a prime algebraic ideal in $K[V]$.

($\mathcal{A}$ is a char set of $((\mathcal{A}):H_{\mathcal{A}}^{\infty})_{K[V]}$ which is prime.)

So we now reduce Question 1 (the problem of deciding whether an autoreduced set of δ-polys is a char set of a prime δ-ideal) to an algebraic problem.

Part II. Irreducible Ascending chains and Irreducible algebraic varieties

To distinguish notions between the differential and the algebraic cases, we call an autoreduced set in the poly ring $K[x_1, \dots, x_n]$ an ascending chain. And in $K[x_1, \dots, x_n]$, we only have elimination ranking which is also called variable ordering $\mathcal{R}: x_{i_1} < x_{i_2} < \dots < x_{i_n}$.

Let $\mathcal{A} = A_1, \dots, A_p$ be an ascending chain in $K[u_1, \dots, u_d, x_1, \dots, x_p]$ w.r.t. the ordering $u_1 < \dots < u_d < x_1 < \dots < x_p$ and $ld(A_i) = x_i$ for $i = 1, \dots, p$. Then $\mathcal{A}$ is of the form

$$\mathbb{A} := \begin{cases} A_1 = I_1(u_1,\dots,u_d)X_1^{m_1} + * X_1^{m_1-1} + \cdots + * X_1 + * ; \\ A_2 = I_2(u_1,\dots,u_d,x_1)X_2^{m_2} + * X_2^{m_2-1} + \cdots + * X_2 + * ; \\ \quad \vdots \\ A_p = I_p(u_1,\dots,u_d,x_1,\dots,x_{p-1})X_p^{m_p} + * X_p^{m_p-1} + \cdots + * X_p + * , \end{cases}$$

where $\deg(A_i, X_j) < m_j$ for all $i > j$.

We now introduce the notion of irreducible ascending chain:

<u>Def 5.2.3</u> (Irreducible ascending chain)

An ascending chain $\mathbb{A}$ is said to be irreducible if $\mathbb{A}$ possesses the following properties:

- Let $K_0 = K(u_1,\dots,u_d)$ be a purely transcendental extension field of K by adjoining $u_1,\dots,u_d$. A_1, considered as a poly in $K_0[x_1]$, is irreducible in $K_0[x_1]$. Take a solution y_1 of $A_1(x_1)=0$ and set $K_1 = K_0(y_1)$.

- $\tilde{A}_2 = A_2(u_1, \cdots, u_d, y_1, x_2) \in K_1[x_2]$ is irreducible.

  Take a solution y_2 of $\tilde{A}_2(x_2) = 0$ and set $K_2 = K_0(y_1, y_2)$.

- $\tilde{A}_3 = A_3(u_1, \cdots, u_d, y_1, y_2, x_3) \in K_2[x_3]$ is irreducible.

  Take a solution y_3 of $\tilde{A}_3(x_3) = 0$ and set $K_3 = K_0(y_1, y_2, y_3)$.

- Suppose that proceeding in the same manner, we get successively algebraic extensions $K_{i-1} = K_0(y_1, \cdots, y_{i-1})$ and irreducible polys $\tilde{A}_i = A_i(u_1, \cdots, u_d, y_1, \cdots, y_{i-1}, x_i) \in K_{i-1}[x_i]$ and a soluton y_i for $i = 1, \cdots, p$.

The obtained point $\tilde{y} = (u_1, \cdots, u_d, y_1, \cdots, y_p)$ is called a generic point of the irreducible ascending chain $\mathcal{A}$.

Note: The irreducibility of $\mathcal{A}$ could be determined mechanically relying on factorization algorithms on towers of algebraic extensions (eg. Trager algorithm) which we will not enter in the course.

<u>Lemma 5.2.4</u> Let $\mathcal{A}$ be an irreducible ascending chain with a generic point $\tilde{\eta}=(u_1,\dots,u_d,y_1,\dots,y_p)$, and $f\in K[u_1,\dots,u_d,x_1,\dots,x_p]$. Then

$$\underbrace{\mathrm{prem}(f,\mathcal{A})}_{\text{(i.e., pseudo-remainder of } f \text{ w.r.t. } \mathcal{A}\text{)}}=0 \iff f(\tilde{\eta})=0.$$

Furthermore, $\mathrm{asat}(\mathcal{A})=(\mathcal{A}):\underbrace{I_{\mathcal{A}}^{\infty}}$ is a prime ideal with $\mathcal{A}$ a characteristic set of it. ($I_{\mathcal{A}}^{\infty}$ is the multiplicative set generated by initials of $A\in\mathcal{A}$)

<u>Proof.</u> Let $\mathcal{A}_k=A_1,\dots,A_k$ $(1\le k\le p)$. Then $\mathcal{A}_k$ is an irreducible ascending chain in $K[u_1,\dots,u_d,x_1,\dots,x_k]$ with a generic point $\tilde{\eta}_k=(u_1,\dots,u_d,y_1,\dots,y_k)$. We shall prove by induction on k the following two claims:

$(C1_k)$ $I_k(\tilde{\eta}_{k-1})\neq 0$ for $I_k=\mathrm{init}(A_k)$.

$(C2_k)$ If $R_k\in K[u_1,\dots,u_d,x_1,\dots,x_k]$ is reduced w.r.t. $\mathcal{A}_k$ and $R_k(\tilde{\eta}_k)=0$, then $R_k\equiv 0$.

First note that $(C1_k)$ is a consequence of $(C2_{k-1})$.

Since $(C1_1)$ is obviously true, it suffices to prove $(C2_k)$ by induction on k.

For $k=1$, if R_1 is reduced w.r.t. $\mathcal{A}_1 := A_1$, then

$\deg(R_1, x_1) < m_1 = \deg(A_1, x_1)$. But $R_1(\eta_1) = 0$, so

$A_1 \mid R_1$, thus $R_1 \equiv 0$ follows.

Suppose $(C2_{k-1})$ has been proved. Consider any $R_k \in K[u_1, \dots, u_d, x_1, \dots, x_k]$ reduced w.r.t. $\mathcal{A}_k$ and $R_k(\tilde{\eta}_k) = 0$.

Rewrite R_k as a poly in x_k, then

$$R_k = S_0 x_k^r + S_1 x_k^{r-1} + \dots + S_r \quad \text{with } S_i \in K[u_1, \dots, u_d, x_1, \dots, x_{k-1}]$$

and $r < m_k = \deg(A_k, x_k)$. Since R_k is reduced w.r.t. $\mathcal{A}_k$, each S_i is reduced w.r.t. $\mathcal{A}_{k-1}$.

Since $R_k(\tilde{\eta}_k) = 0 = S_0(\tilde{\eta}_{k-1})\eta_k^r + S_1(\tilde{\eta}_{k-1})\eta_k^{r-1} + \dots + S_r(\tilde{\eta}_{k-1})$ and $r < m_k$, we have $S_i(\tilde{\eta}_{k-1}) = 0$ for each i.

By induction hypothesis $(C2_{k-1})$, $S_i \equiv 0$, $i = 0, \dots, r$.

Thus, $R_k \equiv 0$. By induction, $(C2_k)$ and $(C1)_k$ are proved.

"$\Rightarrow$" If $\operatorname{prem}(f, \mathcal{A}) = 0$, $\exists\, l_i \in \mathbb{N}$ s.t.

$$I_1^{l_1} \cdots I_p^{l_p} f \in (\mathcal{A}).$$

Since each $A_i(\tilde{y}) = 0$ and $I_i(\tilde{y}) \neq 0$ $(i = 1, \ldots, p)$,

$f(\tilde{y}) = 0$.

"$\Leftarrow$" Conversely, Sps $f(\tilde{y}) = 0$. Let $r = \operatorname{prem}(f, \mathcal{A})$.

Then $r(\tilde{y}) = 0$. By $(C2_p)$, $r \equiv 0$, i.e., $f \in \operatorname{asat}(\mathcal{A})$.

So $\operatorname{asat}(\mathcal{A}) = \{ f \in K[u_1, \ldots, x_p] \mid f(\tilde{y}) = 0 \}$ follows.

Thus, $\underset{((\mathcal{A}) : I_{\mathcal{A}}^{\infty})}{\overset{\parallel}{\operatorname{asat}(\mathcal{A})}}$ is a prime ideal with $\mathcal{A}$ a characteristic set. ☒.

In the following, we shall give another characterization of the irreducibility of ascending chains.

Assume now $\mathcal{A} : A_1, \ldots, A_p$ is not irreducible. Then $\exists\, k$ s.t. $\mathcal{A}_{k-1} = A_1, \ldots, A_{k-1}$ is irreducible with a generic point $\tilde{y}_{k-1} = (u_1, \ldots, u_d, y_1, \ldots, y_{k-1})$ and

$\tilde{A}_k \in K(\tilde{\eta}_{k-1})[X_k]$ is reducible with

$$\tilde{A}_k = g_1 g_2 \cdots g_h$$

where each $g_i \in K(\tilde{\eta}_{k-1})[X_k]$ 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

$$\tilde{D} \cdot \tilde{A}_k = \tilde{G}_1 \cdot \cdots \cdot \tilde{G}_h ,$$

where $D \in K[u_1, \dots, u_d, x_1, \dots, x_{k-1}]$, $G_i \in K[u_1, \dots, u_d, x_1, \dots, x_k]$ and $\tilde{D} = D(\tilde{\eta}_{k-1})$ and $\tilde{G}_i = G_i(\tilde{\eta}_{k-1}, X_k)$.

Rewrite $D \cdot A_k - G_1 \cdots G_h$ as a poly in X_k, then

$$D \cdot A_k - G_1 \cdots G_h = \sum_i B_i(u_1, \dots, u_d, x_1, \dots, x_{k-1}) \cdot X_k^i .$$

Then $\tilde{D} \cdot \tilde{A}_k - \tilde{G}_1 \cdots \tilde{G}_h = 0 = \sum_i B_i(\tilde{\eta}_{k-1}) \cdot X_k^i$.

$\Rightarrow \forall i, \quad B_i(\tilde{\eta}_{k-1}) = 0$ i.e., $B_i \in \mathrm{asat}(\mathcal{A}_{k-1})$.

So $\exists\, r_{i,1}, \dots, r_{i,k-1}$ s.t. $I_1^{r_{i,1}} \cdots I_{k-1}^{r_{i,k-1}} \cdot B_i \in (\mathcal{A}_{k-1})$.

Let $r_j = \max_i \{r_{i,j}\}$ for $j = 1, \dots, k-1$, then

$$I_1^{r_1}\cdots I_{k-1}^{r_{k-1}}(DA_k - G_1\cdots G_h) \in (\mathcal{A}_{k-1}).$$

Let $D' = I_1^{r_1}\cdots I_{k-1}^{r_{k-1}} D$ and $G_1' = I_1^{r_1}\cdots I_{k-1}^{r_{k-1}} G_1$, $G_i' = G_i$, $(i=2,\dots,h)$.

Then $D'A_k - G_1'G_2'\cdots G_h' \in (\mathcal{A}_{k-1})$.

By performing reductions for D' and each G_i w.r.t. $A_{k-1}, A_{k-2}, \dots, A_1$ in turn when necessary, we may assume D' and each G_i' are reduced w.r.t. $\mathcal{A}_{k-1}$.

(If D' or some G_i' is not reduced w.r.t. $\mathcal{A}_{k-1}$, say not reduced w.r.t. A_{k-1}, the perform reduction for D' and each G_i' w.r.t. A_{k-1}, then $\exists\, e_0, e_1, \dots, e_h \in \mathbb{N}$ s.t.

$$I_{k-1}^{e_0} \cdot D' \equiv D_1 \mod (A_{k-1}), \quad I_{k-1}^{e_i} \cdot G_i' = G_{i,1} \mod (A_{k-1})$$

Let $e = \max\{e_0, \sum e_i\}$. Then $\underbrace{I_{k-1}^{e-e_0} \cdot D_1}_{\text{new } D'} A_k - \underbrace{I_{k-1}^{e-\sum e_i} G_{1,1}}_{\text{new } G_1'} G_{2,1} \cdots G_{h,1} \in (\mathcal{A}_{k-1})$ reduced w.r.t. A_{k-1}

In this way, we shall get D' & G_i' reduced w.r.t. $\mathcal{A}_{k-1}$.)

✡ ✡ ✡

Thus, we have the following lemma:

<u>Lemma 5.2.6</u> Given an autoreduced set $\mathcal{A} = A_1, \dots, A_p$, if $\mathcal{A}$ is reducible, then $\exists\, k$ $(1 \le k \le p)$ and polynomials $D \in K[u_1, \dots, u_d, x_1, \dots, x_{k-1}]$,

$G_i \in K[u_1, \cdots, u_d, x_1, \cdots, x_k]$ $(i=1, \cdots, h \geq 2)$ with $\deg(G_i, x_k) > 0$,
D and G_i are reduced w.r.t. $\mathcal{A}_k$ such that

$$\mathcal{A}_{k-1} = A_1, \cdots, A_{k-1} \text{ is irreducible}$$

and $D \cdot A_k \equiv G_1 G_2 \cdots G_h \mod (\mathcal{A}_{k-1})$

Thus, $\mathbb{W}(\mathcal{A}/I_{\mathcal{A}}) = \mathbb{W}(\mathcal{A}, D/I_{\mathcal{A}}) \cup \bigcup_{i=1}^{h} \mathbb{W}(\mathcal{A} \setminus \{A_k\}, G_i / I_{\mathcal{A}} D)$ $(*)$

where $I_{\mathcal{A}} = \prod_{i=1}^{p} I_{A_i}$.

Proof. The first part follows from the discussion before the lemma. It remains to show $(*)$ holds.

Note that $\forall\, \xi \in \mathbb{W}(\mathcal{A}/I_{\mathcal{A}})$, $\exists\, i$, $G_i(\xi) = 0$,

So either $\xi \in \mathbb{W}(\mathcal{A}, D/I_{\mathcal{A}})$ or $\xi \in \mathbb{W}(\mathcal{A} \setminus \{A_k\}, G_i / I_{\mathcal{A}} \cdot D)$.

On the other hand, $\mathbb{W}(\mathcal{A}, D/I_{\mathcal{A}}) \subseteq \mathbb{W}(\mathcal{A}/I_{\mathcal{A}})$

and for each i, if $\xi \in \mathbb{W}(\mathcal{A} \setminus \{A_k\}, G_i / I_{\mathcal{A}} D)$,

$$\mathcal{A}_{k-1}(\xi) = 0 \;\&\; G_i(\xi) = 0 \Rightarrow D(\xi) \cdot A_k(\xi) = 0 \xRightarrow{D(\xi) \neq 0} A_k(\xi) = 0$$

$$\Rightarrow \mathcal{A}_k(\xi) = 0.$$

Thus, $\mathbb{V}(\mathcal{A}/I_{\mathcal{A}}) = \mathbb{V}(\mathcal{A}, D/I_{\mathcal{A}}) \cup \bigcup_{i=1}^{h} \mathbb{V}(\mathcal{A}\setminus\{A_i\}, G_i/I_{A_i D})$.

<u>Corollary 5.2.7</u> For an ascending chain $\mathcal{A} \subseteq K[X][\xi]$ to be a char set of a prime ideal $\Leftrightarrow$ $\mathcal{A}$ is irreducible.

Part III. Irreducible decomposition for diff varieties

Let $\mathcal{A} = A_1, \cdots, A_p$ be an autoreduced set in $K\{y_1, \cdots, y_n\}$

By Lemma 5.2.2, $\mathcal{A}$ is a δ-char set of a prime δ-ideal $\Longleftrightarrow$ $\mathcal{A}$ is a char set of a prime ideal in $K[X]$ $\left(\begin{array}{l} X \subseteq \Theta(Y) \ \& \\ \mathcal{A} \subseteq K[X] \end{array} \right)$

We now introduce the notion of δ-irreducible autoreduced sets.

<u>Definition 5.2.8</u> An autoreduced set $\mathcal{A} = A_1, \cdots, A_p$ is called δ-irreducible if for $\forall k$ $(1 \leq k \leq p)$, there cannot exist any relation of the form

$$D_k \cdot A_k \equiv G_{k,1} \cdot G_{k,2} \mod [\mathcal{A}_{k-1}]$$

in which $G_{k,1}$ and $G_{k,2}$ are δ-polys having the same leader as A_k and reduced w.r.t. $\mathcal{A}_k$, while D_k is some δ-poly of lower leader than A_k and reduced w.r.t. $\mathcal{A}_{k-1}$.

In the contrary case, we say that $\mathcal{A}$ is δ-reducible.

To an autoreduced set $\mathcal{A} = A_1, \dots, A_p$ ($\subseteq K\{Y\}$) w.r.t. R, we associate an ascending chain $\mathcal{A}^a = A_1, \dots, A_p$ considered as algebraic poly in $K[\Theta(Y)]$ w.r.t. a variable ordering with

- $\Theta(Y) \setminus \Theta(ld(\mathcal{A})) < \Theta(ld(\mathcal{A}))$
- $ld(A_1) < ld(A_2) < \dots < ld(A_p)$

and the ordering of $\Theta(ld(\mathcal{A}))$ is induced by R.

Theorem 5.2.9 (Irreducibility Theorem)

For an autoreduced set $\mathcal{A} \subseteq K\{Y\}$ to be a char set of a prime δ-ideal, it is necessary and sufficient that $\mathcal{A}$ be δ-irreducible.

proof. It suffices to show $\mathcal{A}$ is δ-reducible $\Leftrightarrow$ $\mathcal{A}^a$ is reducible.

"$\Leftarrow$" ✓

"$\Rightarrow$" Sps $\mathcal{A}$ is δ-reducible. Then $\exists\, 1 \le k \le p$, $\mathcal{A}_{k-1}$ is δ-irr & $\exists\, D, G_1, G_2 \in K\{Y\}$ with $ld(D) < ld(A_k)$, $ld(G_i) = ld(A_k)$ D, G_1, G_2 reduced w.r.t. $\mathcal{A}_k$ s.t.

$$D A_k = G_1 G_2 + \sum_j \sum_{i=1}^{k-1} C_{ij} A_i^{(j)}. \quad (*)$$

If $\exists\, j > 0$ in $(*)$ s.t. $C_{ij} \ne 0$, take $v = \max_{i,j} \{ ld(A_i^{(j)}) \mid C_{ij} \ne 0, j>0 \}$, say $v = ld(A_{i_0}^{(j_0)})$. Since $A_{i_0}^{(j_0)} = S_{A_{i_0}} \cdot v + T$, substitute $v = -\frac{T}{S_{A_{i_0}}}$

into both sides of (*) and clearing denominators, we get an identity still of the form (*) with $C_{i_0 j_0} A_{i_0}^{(j_0)}$ removed. Proceeding in the same manner, we will finally remove all such terms and arrive an identity $D \cdot A_k = G_1 G_2 + \sum_j \tilde{C}_{i0} A_i$.
So $\mathcal{A}^a$ is reducible. $\boxtimes$.

<u>Theorem 5.2.10</u> (Zero Decomposition Theorem: Strong Form)
There is an algorithmic procedure which permits to detect whether $\mathbb{W}(\Sigma) = \phi$ for any finite subset $\Sigma \subseteq K\{Y\} \setminus \{0\}$, and in the nonempty case, to decompose $\mathbb{W}(\Sigma)$ in the following form:

$$\mathbb{W}(\Sigma) = \bigcup_{i=1}^{l} \mathbb{W}(\mathcal{A}_i / R_i), \qquad (1)$$

in which each $\mathcal{A}_i$ is a δ-irreducible autoreduced set and $0 \neq R_i = \delta\text{-rem}(H_{\mathcal{A}_i} \cdot G_i, \mathcal{A}_i)$ for some nonzero δpoly G_i.

<u>Proof.</u> By the zero decomposition theorem (weak form), we can compute a finite number of autoreduced sets CS_j s.t.

$$\mathbb{W}(\Sigma) = \bigcup_{j=1}^{l} \mathbb{W}(CS_j / H_{CS_j}), \quad (2)$$

where $\delta\text{-rem}(\Sigma, CS_j) = \{0\}$ and $CS_j \leq b.s.(\Sigma)$.

If for $\forall j$, $CS_j = a \in K$ or δ-rem$(H_{CS_j}, CS_j) = 0$, $\mathbb{W}(\Sigma) = \phi$.

If all the CS_j are δ-irreducible, form $R_j := \delta\text{-rem}(H_{CS_j}, CS_j)$, by the reduction formula, $\mathbb{W}(CS_j / H_{CS_j}) = \mathbb{W}(CS_j / R_j)$ and a decomposition of the form (1) is obtained.

Suppose $\exists$ some $CS_j = C_1, \cdots, C_r$ is δ-reducible. Then $\exists\, k\ (1 \le k \le r)$ s.t. $CS_{j,k-1} = C_1, \cdots, C_{k-1}$ is δ-irreducible and $\exists\, D, G_1, G_2 \in K\{Y\}$ reduced w.r.t. $CS_{j,k-1}$ with $ld(D) < ld(C_k)$ and $ld(G_i) = ld(C_k)$ satisfying

$$D \cdot C_k = G_1 \cdot G_2 \mod [CS_{j,k-1}].$$

Let $\hat{CS_j} = CS_j \setminus \{C_k\}$. It is clear that

$$\mathbb{W}(CS_j / H_{CS_j}) = \mathbb{W}(CS_j, D / H_{CS_j}) \cup \mathbb{W}(\hat{CS_j}, G_1 / D \cdot H_{CS_j}) \cup \mathbb{W}(\hat{CS_j}, G_2 / D \cdot H_{CS_j}). \quad (3)$$

By lemma 5.1.2, a basic set of $\begin{cases} CS_j \cup \{D\} \\ \hat{CS_j} \cup \{G_1\} \\ \hat{CS_j} \cup \{G_2\} \end{cases}$ is of lower rank than CS_j.

Applying the weak form of zero decomposition theorem to each member of (3), we can replace $\mathbb{W}(CS_j / H_{CS_j})$ by a finite union of $\mathbb{W}(CS' / (H_{CS'} D'))$ with each autoreduced set CS' is of lower rank than CS_j.

perform the above procedures for each δ-reducible autoreduced set CS_j in (2), we shall get a decomposition still of the form (2) with each δ-reducible CS_j being replaced by new autoreduced sets of lower rank than CS_j. If in the new form there are δ-reducible autoreduced sets, we perform the above procedures to replace them by autoreduced sets of lower rank. Repeat this process recursively, and this recursive process will finally terminate. For otherwise, we shall get a strictly decreasing sequence of autoreduced sets, a contradiction. Finally, we will get a decomposition

$$\mathbb{W}(\Sigma) = \bigcup_{j=1}^{l} \mathbb{W}(\mathcal{A}_j / H_{\mathcal{A}_j} D_j), \qquad (4)$$

where all the $\mathcal{A}_j$ are δ-irreducible and $D_j \in K\{Y\} \setminus \{0\}$.

Let $R_j = \delta\text{-rem}(H_{\mathcal{A}_j} D_j, \mathcal{A}_j)$. Then by the reduction formula, $\mathbb{W}(\mathcal{A}_j / H_{\mathcal{A}_j} D_j) = \mathbb{W}(\mathcal{A}_j / R_j)$.

If $R_j = 0$, $\mathbb{W}(\mathcal{A}_j / H_{\mathcal{A}_j} D_j) = \phi$ and we can omit such a term from (4). Thus, a decomposition of the form (1) is obtained.

<u>Theorem 5.2.11 (δ-Variety decomposition theorem)</u>

There is an algorithmic procedure to give a decomposition of $\mathbb{V}(\Sigma)$ for any finite set of δ-polys $\Sigma \subseteq K\{y\}$ into a finite union of irreducible δ-varieties:

$$\mathbb{V}(\Sigma) = \bigcup_{i=1}^{l} \mathbb{V}(\mathrm{sat}(\mathcal{A}_i))$$

where $\mathcal{A}_i$ are δ-irr autoreduced sets.

<u>Proof.</u> By Theorem 5.2.10, a finite number of δ-irr autoreduced sets $\mathcal{A}_1, \dots, \mathcal{A}_l$ can be computed s.t. $\mathbb{V}(\Sigma) = \bigcup_{i=1}^{l} \mathbb{V}(\mathcal{A}_i / R_i)$ with $0 \neq R_i = \delta\text{-rem}(H_{\mathcal{A}_i} D_i, \mathcal{A}_i)$.

Note that for $\forall i$, $\mathbb{V}(\mathcal{A}_i / R_i) = \mathbb{V}(\mathcal{A}_i / (H_{\mathcal{A}_i} D_i))$
$\subseteq \mathbb{V}(\mathrm{sat}(\mathcal{A}_i))$, so $\mathbb{V}(\Sigma) \subseteq \bigcup_{i=1}^{l} \mathbb{V}(\mathrm{sat}(\mathcal{A}_i))$.

Take a generic point ξ of $\mathrm{sat}(\mathcal{A}_i)$, then $\mathcal{A}_i(\xi) = 0$ and $R_i(\xi) \neq 0$. So $\xi \in \mathbb{V}(\mathcal{A}_i / R_i) \subseteq \mathbb{V}(\Sigma)$.
Thus, $\mathbb{V}(\mathrm{sat}(\mathcal{A}_i)) \subseteq \mathbb{V}(\Sigma)$ for $\forall i$ and $\bigcup_i \mathbb{V}(\mathrm{sat}(\mathcal{A}_i)) = \mathbb{V}(\Sigma)$ follows. 証.