Recall: Last week, we studied the notions of differential ranking, autoreduced set and characteristic set:

• A differential ranking \mathscr{R} is a total ordering on $\Theta(Y) := \{y_i^{(k)} : k \ge 0, 1 \le i \le n\}$ satisfying (1) $v < \delta(v)$ and (2) $v < u \Rightarrow \delta(v) < \delta(u)$. It is a well-ordering.

• Given $f \in K\{Y\}$, the leader/initial/rank/separant of f is denoted by $u_f, I_f, S_f, rk(f)$. A polynomial g is partially reduced w.r.t. f if no proper derivative of u_f appears in g; and in addition, if $\deg(g, u_f) < \deg(f, u_f)$, then g is reduced w.r.t f.

• An autoreduced set is a set $\mathcal{A} \subset K\{Y\}$ with each element reduced w.r.t. all the other elements. A characteristic set of a differential ieal I is an autoreduced set of lowest rank contained in I.

We start to introduce *pesudo-division* of differential polynomials:

Lemma 2.2.11. 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} (i.e., \tilde{F} is partially reduced w.r.t. each A_i),
- 2) the rank of \tilde{F} is not higher than that of F,

3)
$$\prod_{i=1}^{p} \mathbf{S}_{A_{i}}^{t_{i}} F \equiv \tilde{F} \mod [\mathcal{A}].$$

More precisely, $\prod_{i=1}^{p} S_{A_i}^{t_i} F - \tilde{F}$ 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 the maximal one among all such derivatives. 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

$$\delta^k(A) = S_A \delta^k(u_A) + T$$
 with T 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 $\geq v_F$. Then we have

$$S_A{}^l F = \sum_{i=0}^l J_i S_A{}^{l-i} (S_A v_F)^i \equiv \sum_{i=0}^l J_i S_A{}^{l-i} (-T)^i \mod (\delta^k(A)).$$

Clearly, $G = \sum_{i=0}^{l} J_i \mathbf{S}_A^{l-i} (-T)^i$ 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 $\prod_{i=1}^{p} \mathbf{S}_{A_i}^{k_i} G \equiv$

$$\tilde{G} \mod [\mathcal{A}]$$
. 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 A.

Let us recall the *pseudo reduction algorithm* in commutative algebra:

Let D be an integral domain and we consdier the polynomial ring D[v] (v is an indeterminate over D). Let $F, A \in D[v]$ be of respective degrees $d_F, d_A \ge 0$) and assume

$$A = I_{d_A} v^{d_A} + \dots + I_1 v + I_0$$

with $I_i \in D$. Let $e = \max\{d_F - d_A + 1, 0\}$. Then we can compute unique $Q, R \in D[v]$ with $\deg(R, v) < \deg(A, v)$ such that

$$I^e_{d_A}F = QA + R.$$

Theorem 2.2.12. 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 $\exists F_0 \in K\{y_1, \ldots, y_n\}$ (called the differential remainder of F w.r.t. \mathcal{A}) and $r_i, t_i \in \mathbb{N}$ s.t.

- 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) $\prod_{i=1}^{p} \mathbf{S}_{A_{i}}^{t_{i}} \mathbf{I}_{A_{i}}^{r_{i}} F \equiv F_{0} \mod [\mathcal{A}].$

Proof. Let \tilde{F} be the partial remainder of F with respect to \mathcal{A} and $\prod_{i=1}^{p} S_{A_i}^{t_i} F \equiv \tilde{F} \mod [\mathcal{A}]$. 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 $I_{A_p}^{r_p} \tilde{F} \equiv F_{p-1} \mod (A_p)$. 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 \mathcal{A}_{p-1} , A_p s.t. $I_{A_{p-1}}^{r_{p-1}} I_{A_p}^{r_p} \tilde{F} \equiv F_{p-2} \mod (A_{p-1}, A_p)$ and is not higher than \tilde{F} . Continuing in this way, we get F_0 satisfying the desired properties.

algorithm called the Bi

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 δ -rem (F, \mathcal{A}) , or $F \xrightarrow{}_{\mathcal{A}} F_0$.

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 $f \xrightarrow{\mathcal{A}} 0$, and $I_{A_1} f \in [\mathcal{A}]$.
- (2) Let $f = y'_1 + 1$ and $\mathcal{A} = A_1 = y_2 y_1^2$. $u_{A_1} = y_1$ and $S_{A_1} = 2y_2 y_1$. Clearly, f is not partially reduced with respect to \mathcal{A} . Note that $\delta(A_1) = 2y_2 y_1 y'_1 + y'_2 y_1^2$. The partial remainder of f with respect to \mathcal{A} is $2y_2 y_1 y'_2 y_1^2 = \tilde{f}$ and $S_{A_1} f \tilde{f} = A'_1 \in [\mathcal{A}]$.

Since

$$\mathbf{I}_{A_1}f - \mathbf{I}_{\tilde{f}}A_1 = y_2(2y_2y_1 - y_2'y_1^2) - (-y_2')y_2y_1^2 = 2y_2^2y_1$$

is reduced with respect to \mathcal{A} , $f \xrightarrow{\mathcal{A}} 2y_2^2y_1$ and $I_{A_1}S_{A_1}f - 2y_2^2y_1 = -y_2'A_1 + I_{A_1}A_1' \in [\mathcal{A}]$.

Theorem 2.2.13. Let \mathcal{A} be an autoreduced set of a proper differential ideal $I \subseteq K\{y_1, \ldots, y_n\}$. Then the following are equivalent:

- (1) \mathcal{A} is a characteristic set of I.
- (2) $\forall f \in I, \ \delta\text{-rem}(f, \mathcal{A}) = 0.$
- (3) I doesn't contain a nonzero differential polynomial reduced with respect to \mathcal{A} .

Proof. $(2) \Leftrightarrow (3)$ is obvious.

"(1) \Rightarrow (3)" Suppose $f \in I \setminus \{0\}$ is reduced with respect to $\mathcal{A} = A_1, \ldots, A_p$. Let $k \in \mathbb{N}$ be maximal such that $\operatorname{rk}(A_k) < \operatorname{rk}(f)$. Then A_1, \ldots, A_k, f is an autoreduced set lower than \mathcal{A} . (Here, in the case $\operatorname{rk}(f) < \operatorname{rk}(A_1)$, 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, $\operatorname{rk}(A_i) = \operatorname{rk}(B_i)$ and $A_k > B_k$, or (2) q > p and for $i \leq p$, $\operatorname{rk}(A_i) = \operatorname{rk}(B_i)$. Then either B_k or B_{p+1} is nonzero and reduced with respect to \mathcal{A} .

Remark: By Theorem 2.2.13, if $\mathcal{A} = A_1, \ldots, A_p$ is a characteristic set of $I \subseteq K\{Y\}$, then $I_{A_i}, S_{A_i} \notin I$ $(i = 1, \ldots, p)$.

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 2.2.14. Let \mathcal{A} be a characteristic set of a proper differential ideal $I \subseteq K\{Y\}$. Denote $H^{\infty}_{\mathcal{A}}$ to be the multiplicative set generated by initials and separants of elements in \mathcal{A} and set

$$\operatorname{sat}(\mathcal{A}) := [\mathcal{A}] : \operatorname{H}^{\infty}_{\mathcal{A}} = \{ f \in K\{Y\} \mid \exists M \in \operatorname{H}^{\infty}_{\mathcal{A}}, Mf \in [\mathcal{A}] \}.$$

Then $I \subseteq \operatorname{sat}(\mathcal{A})$. Furthermore, if I is prime, $I = \operatorname{sat}(\mathcal{A})$.

Proof. For each $f \in I$, by Theorem 2.2.13, δ -rem $(f, \mathcal{A}) = 0$. Thus, $\exists i_A, t_A \in \mathbb{N} (A \in \mathcal{A})$ s.t. $\prod_{A \in \mathcal{A}} I_A^{i_A} S_A^{t_A} f \in [\mathcal{A}].$ That is, $f \in \text{sat}(\mathcal{A}).$

Suppose I is prime. For each $f \in \text{sat}(\mathcal{A})$, $\exists i_A, t_A$ s.t. $\prod_{A \in \mathcal{A}} I_A^{i_A} S_A^{t_A} f \in [\mathcal{A}] \subseteq I$. Since I_A, S_A are not in $I, f \in I$ and $I = \text{sat}(\mathcal{A})$ follows. \Box

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 differential remainder of f w.r.t. \mathcal{A} . That is, g is reduced w.r.t. \mathcal{A} and there exist $i_k, j_k \in \mathbb{N}$ s.t. $I_{A_1}^{i_1} \cdots I_{A_p}^{j_p} S_{A_1}^{j_1} \cdots S_{A_p}^{j_p} f - g \in [\mathcal{A}]$.

2.3 The Ritt-Raudenbush basis theorem

In the end of section 2.1, we gave an example showing that a differential ideal in $K\{Y\}$ might not be differentially finitely generated. For example,

$$I = [y^2, (y')^2, \dots, (y^{(k)})^2, \dots]$$

and

$$J = [yy', y'y'', \dots, y^{(k)}y^{(k+1)}, \dots]$$

are not differentially finitely generated. But note that $\{I\} = \{y\}$ and $\{J\} = \{yy'\}$ are differentially finitely generated as radical differential ideals. In this section, we will show every radical differential ideal in $K\{Y\}$ is differentially finitely generated as radical differential ideals.

Definition 2.3.1. A differential ring is called **Ritt-Noetherian** if the set of radical differential ideals satisfies the ascending chain condition (ACC).

Lemma 2.3.2. 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., $\{a_1\} \subsetneq \{a_1, a_2\} \subsetneqq \cdots \subsetneqq \{a_1, a_2, \dots, a_p\} \gneqq \cdots$. " \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

"⇐" 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 $j \in \mathbb{N}$.

Lemma 2.3.3. Let R be a differential ring with $\mathbb{Q} \subset \mathbb{R}$. Let $S \subset \mathbb{R}$ be a subset and $a \in \mathbb{R}$ such that the radical differential ideal $\{S, a\}$ has a finite set of generators as a radical differential ideal. Then, there exists $s_1, \ldots, s_p \in S$ such that $\{S, a\} = \{s_1, \ldots, s_p, a\}$.

Proof. By hypothesis, $\exists h_1, \ldots, h_l$ s.t. $\{a, S\} = \{h_1, \ldots, h_l\}$. For each $i, h_i \in \{a, S\} \Rightarrow \exists m_i$ s.t. $h_i^{m_i} \in [a, S]$. So $\exists s_1, \ldots, s_p \in S$ s.t. for each $i, h_i^{m_i} \in [a, s_1, \ldots, s_p]$. Thus, $h_i \in \{a, s_1, \ldots, s_p\} \subset \{a, S\} \Rightarrow \{h_1, \ldots, h_l\} \subseteq \{a, s_1, \ldots, s_p\} \subseteq \{a, S\}$.

Theorem 2.3.4. 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 2.3.2, 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.

<u>Proof of the claim.</u> Suppose the contrary, then $\exists a, b \in K\{y_1, \ldots, y_n\}$ s.t. $a, b \notin J$ but $ab \in J$. Since $\{a, J\} \supseteq J$ and $\{b, J\} \supseteq J$, $\{a, J\}$ and $\{b, J\}$ are finitely generated as radical differential ideals. Then by Lemma 2.3.3, $\exists f_1, \ldots, f_s, g_1, \ldots, g_t \in J$ s.t. $\{a, J\} = \{a, f_1, \ldots, f_s\}$ and $\{b, J\} = \{b, g_1, \ldots, g_t\}$. Hence,

$$J^{2} \subseteq \{a, J\} \cdot \{b, J\} = \{a, f_{1}, \dots, f_{s}\} \cdot \{b, g_{1}, \dots, g_{t}\}$$
$$\subseteq \{ab, ag_{j}, bf_{i}, f_{i}g_{j} : 1 \le i \le s, 1 \le j \le t\} \triangleq P$$
$$\subseteq J.$$

For each $f \in J$, $f^2 \in J^2 \subseteq P \Rightarrow f \in P \Rightarrow J = P = \{ab, ag_j, bf_i, f_ig_j : 1 \le i \le s, 1 \le j \le t\}$, contradicting the hypothesis that J is not finitely generated. The claim thus is proved.

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 $I \triangleq \prod_{i=1}^{p} I_{A_i}, S \triangleq \prod_{i=1}^{p} S_{A_i}$. Since J is prime, $J = \operatorname{sat}(\mathcal{A}) = [\mathcal{A}] : H^{\infty}_{\mathcal{A}} \subseteq \{\mathcal{A}\}$: (IS). Since $I_{A_i}, S_{A_i} \notin J$ for each i, IS $\notin J$. Thus $\{J, IS\}$ is finitely generated as a radical differential ideal. That is, $\exists h_1, \ldots, h_l \in J$ s.t. $\{J, IS\} = \{h_1, \ldots, h_l, IS\}$. Thus,

$$J^{2} \subseteq J \cdot \{J, \mathrm{IS}\} = J \cdot \{h_{1}, \dots, h_{l}, \mathrm{IS}\}$$
$$\subseteq \{h_{1}, \dots, h_{l}, \mathcal{A}\} (\text{for } \mathrm{IS} \cdot J \subseteq \{\mathcal{A}\})$$
$$\subseteq J.$$

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.

Theorem 2.3.5. Let R be a differential ring which is Ritt-Noetherian and $\mathbb{Q} \subseteq R$. Then for every radical differential ideal $I \subsetneq R$, 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 $U = \{I \mid I \subsetneqq K\{y_1, \ldots, y_n\}$ 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 U. By Zorn's lemma, U has a maximal element $J \in U$. Clearly, J is not prime. So $\exists a, b \notin J$ but $ab \in J$. Thus, $\{J, a\} \gneqq J$ and $\{J, b\} \gneqq J$. 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.

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

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 $J \in U$. So the first statement is valid.

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

Corollary 2.3.6. Every proper radical differential ideal $I \subsetneq K\{y_1, \ldots, y_n\}$ (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.

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