Computational Differential Algebra
A Mini Introductory Course

William Sit[1]

The City College of The City University of New York

Theory of Singularities and Its Relation to
Arc Schema and Differential Algebra
L'université de Versailles Saint-Quentin-en-Yvelines
More Invariants from Arc Spaces Days
September 25–29, 2017

[1]Special thanks to Julien Sebag for the invitation.

Invertibility Modulo an Ideal

Invertible Initials and Saturation Ideal

Minimal Polynomials and Algorithms

Convention and Polynomial Rings

- In any commutative ring (**including the zero ring**), an element x is **multiplicatively invertible** if there exists an element y such that $xy = 1$. A **zero divisor** is a **non-zero** element x such that there is a non-zero y with $xy = 0$.
- Let $\mathcal{S}_0$ be an integral domain with quotient field $\mathcal{K}_0$. Let $\mathcal{S} := \mathcal{S}_0[x_1, \ldots, x_n]$, $\mathcal{K} := \mathcal{K}_0[x_1, \ldots, x_n]$ be polynomial rings.
- Let J be an ideal of $\mathcal{S}$, and let $J_{\mathcal{K}}$ be the ideal generated by J in $\mathcal{K}$. Let $V_J := \mathcal{K}/J_{\mathcal{K}}$, which is both a vector space over $\mathcal{K}_0$ and a ring—perhaps the zero ring, which happens if and only if $J \cap \mathcal{S}_0 \neq (0)$.
- Let $\eta : \mathcal{K} \longrightarrow V_J$ be the canonical quotient homomorphism.
- For any $F \in \mathcal{S}$, let $\eta_F : V_J \longrightarrow V_J$ denote the multiplication map by F, that is, $\eta_F(\eta(G)) = \eta(FG)$ for any $G \in \mathcal{K}$. Clearly η_F is a vector space endomorphism of V_J.

Invertibility Modulo An Ideal

Proposition 3.1

Let $F \in \mathcal{S}$. Then the following conditions are equivalent:

(a). η_F *is surjective.*

(b). $\eta(F)$ *is multiplicatively invertible in the ring* V_J.

(c). *There exist* $L \in \mathcal{S}_0$, $L \neq 0$ *and* $M \in \mathcal{S}$ *such that* $L \equiv MF \mod J$.

(d). $(J, F)_{\mathcal{S}} \cap \mathcal{S}_0 \neq (0)$ (*equivalently,* $(J, F)_{\mathcal{K}} = \mathcal{K}$).

- We say $F \in \mathcal{S}$ is **invertible modulo** J **over** $\mathcal{S}_0$ if any one (hence all) of the conditions (a) through (d) in Proposition 3.1 holds.

Proof of Proposition 3.1

- When V_J is the zero ring, conditions (a) through (d) are trivially satisfied by any F. So, assume V_J is not trivial.
- $(\mathrm{a}) \Rightarrow (\mathrm{b})$: When η_F is surjective, there exists $G \in \mathfrak{K}$ such that $\eta_F(\eta(G)) = \eta(1)$, that is, $\eta(F)\eta(G) = \eta(1)$.
- $(\mathrm{b}) \Rightarrow (\mathrm{c})$: If $\eta(F)$ is multiplicatively invertible, let its inverse be $\eta(G)$, where $G = N/D$, $N \in \mathfrak{s}, D \in \mathfrak{s}_0, D \neq 0$. We have $FG \equiv 1 \bmod J_{\mathfrak{K}}$ and hence $FG - 1 = \sum_{i=1}^{p} C_i A_i$ where $C_i = N_i/D_i$, $N_i \in \mathfrak{s}, D_i \in \mathfrak{s}_0, D_i \neq 0$ and $A_i \in J$. Then $L = D\prod_{i=1}^{p} D_i$ and $M = N\prod_{i=1}^{p} D_i$ satisfy (c).
- $(\mathrm{c}) \Rightarrow (\mathrm{d})$ is clear.
- $(\mathrm{d}) \Rightarrow (\mathrm{a})$: Let $L \in \mathfrak{s}_0$, $L \neq 0$, and $L = MF + \sum_{k=1}^{p} C_k A_k$, where $M, C_k \in \mathfrak{s}$ and $A_i \in J$. Since V_J is not trivial, $M \notin J$, $\eta(L) \neq 0$ and $\eta(1) = \eta(MF/L)$. Let $G \in \mathfrak{K}$. We have $\eta(G) = \eta(MFG/L) = \eta_F(\eta(MG/L))$ and hence η_F is surjective.

Three Corollaries on Invertibility

Corollary 3.2

Let $F \in \mathcal{S}$, and let $J \subseteq J'$ be two ideals of $\mathcal{S}$. If F is invertible modulo J, it is invertible modulo J'.

- The converse of Corollary 3.2 is false.

Corollary 3.3

Let $F, F_1, F_2 \in \mathcal{S}$. If $F = F_1 F_2$, then F is invertible J if and only if F_1, F_2 are.

Corollary 3.4

Let $\mathcal{S}'_0$ be an integral domain with quotient field $\mathcal{K}'_0$, $\mathcal{S}_0$ be a subdomain of $\mathcal{S}'_0$, and $x_1, \ldots, x_n$ be indeterminates over $\mathcal{K}'_0$. Let J be an ideal in $\mathcal{S} := \mathcal{S}_0[x_1, \ldots, x_n]$. If $F \in \mathcal{S}$ is invertible modulo J over $\mathcal{S}_0$, then $F \in \mathcal{S}' := \mathcal{S}'_0[x_1, \ldots, x_n]$ is invertible modulo $J_{\mathcal{S}'}$ over $\mathcal{S}'_0$.

General Set up for Triangular Sets

The following setting will be assumed.

- Let $\mathcal{S}_0$ be an integral domain, $\mathcal{K}_0$ its quotient field. Let $\mathcal{S} := \mathcal{S}_0[v_1, \ldots, v_p]$, $\mathcal{K} = \mathcal{K}_0[v_1, \ldots, v_p]$ be polynomial rings.
- Let $\mathbf{A}$: $A_1, \ldots, A_p$ be a subset of $\mathcal{S}_p$ in triangular form with respect to $v_1, \ldots, v_p$.
- For $1 \leqslant k \leqslant p$, let
  - $\mathcal{S}_k := \mathcal{S}_0[v_1, \ldots, v_k]$ and $\mathcal{K}_k := \mathcal{K}_0[v_1, \ldots, v_k]$,
  - $\mathbf{A}_k : A_1, \ldots, A_k$,
  - d_k be the degree of A_k in v_k,
  - $I_k \in \mathcal{S}_{k-1}$ be the initial of A_k with respect to v_k.

Invertibility of Initials, Saturation Ideals

- We say **A has invertible initials with respect to** $v_1, \ldots, v_p$ **over** $\mathcal{S}_0$) if for $1 \leqslant k \leqslant p$, I_k is invertible modulo $(\mathbf{A}_{k-1}) := (A_1, \ldots, A_{k-1}) \subset S_{k-1} := \mathcal{S}_0[v_1, \ldots, v_{k-1}]$ over $\mathcal{S}_0$.
- Note $I_1 \neq 0$, $I_1 \in \mathcal{S}_0$**, so is invertible modulo** (0) **over** $\mathcal{S}_0$.
- Let $J \subset \mathcal{S} = \mathcal{S}_0[x_1, \ldots, x_n]$ be an ideal, and $H \in \mathcal{S}$. The **saturation of** J **by** H is the ideal

$$J : H^\infty := \{ F \in \mathcal{S} \mid H^m F \in J \text{ for some } m > 0 \}.$$

- Since $J : H^i \subseteq J : H^{i+1}$, the ideal $J : H^\infty = J : H^N$ for some $N \geqslant 1$ and hence $J : H^\infty$ is computable when generators of J are known.

Low Degree Polynomials in Saturation Ideals

Lemma 3.6

Let $\mathbf{A} : A_1, \ldots, A_p$ *be a triangular set as before and let* $I := I_1 \cdots I_p$. *Then* (a) *implies* (b), *where:*

(a). $\mathbf{A}$ *has invertible initials.*

(b). *If* $F \in (A_1, \ldots, A_p) : I^\infty$ *is such that for* $1 \leqslant k \leqslant p$, *the degree of* F *in* v_k *is* $< d_k$, *then* $F = 0$.

- We call $(\mathbf{A}) : I^\infty$ (in $\mathcal{S}$) the **saturation ideal of A with respect to its initials** and denote it by J_I if there is no possibility of confusion.

Proof of Lemma 3.6

- For $p = 1$. For some $e_1 \in \mathbb{N}$, $I_1^{e_1} F$ is divisible by A_1. Since $I_1 \in \mathcal{S}_0$ and $\deg_{v_1} F < d_1$, F must be zero.
- Assume Lemma proved for $1 \leqslant p \leqslant m$, let $p = m + 1$ and $H = I_1 \cdots I_m$.
- Then $I_{m+1}^h H^h F = \sum_{i=1}^{m+1} C_i A_i$ for some $h \in \mathbb{N}$, $C_i \in \mathcal{S}_{m+1}$.
- Let (e, Q_i, R_i) be a pseudo-division triple of C_i by A_{m+1} for $1 \leqslant i \leqslant m$, where $Q_i, R_i \in \mathcal{S}_{m+1}$. Comparing degree in v_{m+1}:
- $I_{m+1}^{e+h} H^h F - \sum_{i=1}^{m} R_i A_i = \left(I_{m+1}^e C_{m+1} + \sum_{i=1}^{m} Q_i A_i \right) A_{m+1} = 0.$
- For some $L \neq 0$, $L \in \mathcal{S}_0$, $M \in \mathcal{S}_m$, and $N \in (A_1, \ldots, A_m)$, by invertibility of I_{m+1}, $L = M I_{m+1} + N \in (A_1, \ldots, A_m, I_{m+1}) \cap \mathcal{S}_0$.
- Put $R_i' := M^{e+h} R_i$. Then $(L - N)^{e+h} H^h F = \sum_{i=1}^{m} R_i' A_i$.
- So $L^{e+h} F \in \mathcal{S}_{m+1} \cdot (A_1, \ldots, A_m) \colon H^\infty$.
- By induction applied to $v_1, \ldots, v_m$ over $\mathcal{S}_0' = \mathcal{S}_0[v_{m+1}]$ and $F' = L^{e+h} F$, we get $L^{e+h} F = 0$ and hence $F = 0$.

Computing in $V_{\mathbf{A}}$ and Minimal Polynomial

Corollary 3.9

Hypotheses as in Lemma 3.6(a). Let $\mathcal{K}_0$ be the quotient field of $\mathcal{S}_0$. Then $V_{\mathbf{A}} = \mathcal{K}_0[v_1, \ldots, v_p]/(\mathbf{A})$ is a non-trivial vector space over $\mathcal{K}_0$ with dimension $d = \prod_{k=1}^{p} d_k$. A $\mathcal{K}_0$-basis is

$$B_k = \{\, \eta_k(v_1^{e_1} \cdots v_k^{e_k}) \mid 0 \leqslant e_i < d_i \text{ for all } 1 \leqslant i \leqslant k \,\}. \quad (3.10)$$

Corollary 3.11

For any $F \in \mathcal{K} := \mathcal{K}_p$, we can compute $\eta(F) := \eta_p(F) \in V_{\mathbf{A}}$ in terms of the basis B_p with coefficients in $\mathcal{K}_0$.

- A **minimal polynomial of F modulo A over $\mathcal{S}_0$** is a non-zero polynomial $P \in \mathcal{S}_0[X]$ of minimal degree in X such that $\eta(P(F)) = 0$. Note that for some $L \neq 0$ in $\mathcal{S}_0$, $L \cdot P(F) \in (\mathbf{A})_{\mathcal{S}}$ and P, if it exists, is unique up to a non-zero factor in $\mathcal{S}_0$.

Proof of Corollary 3.9

- By Lemma 3.6, $(\mathbf{A}) : I^\infty \cap \mathcal{S}_0 = 0$. Hence $V_{\mathbf{A}}$ is non-trivial.
- Let $\eta_k : \mathcal{K}_k \longrightarrow \mathcal{K}_k/(\mathbf{A}_k)$ be the canonical homomorphism.
- Let $\sum C_j \eta_k(D_j) = 0$ be a linear dependence relation with $C_j \in \mathcal{K}_0$ and D_j being distinct monomials in $v_1, \ldots, v_k$ with degree in v_i less than d_i for $1 \leqslant i \leqslant k$.
- Clearing denominators, we get for some $F \in (\mathbf{A}_k)_{\mathcal{S}_k}$ and some non-zero $L \in \mathcal{S}_0$ such that $LC_j \in \mathcal{S}_0$ and $F = L \sum C_j D_j$.
- By Lemma 3.6, $F = 0$, so $LC_j = 0$ and hence $C_j = 0$. It thus suffices to prove by induction on k that B_k also generates $\mathcal{K}_k/(\mathbf{A}_k)$ as a vector space over $\mathcal{K}_0$.
- For $k = 0$, this is trivial. For $k \geqslant 1$, let $G \in \mathcal{K}_k = \mathcal{K}_{k-1}[v_k]$ be written as $\sum_{i=0} G_i v_k^i$ where $G_i \in \mathcal{K}_{k-1}$.

Proof of Corollary 3.9, Continued

- Clearly, we have a natural embedding ι_k of $\mathcal{K}_0$-vector spaces from $\mathcal{K}_{k-1}/(\mathbf{A}_{k-1})$ into $\mathcal{K}_k/(\mathbf{A}_k)$.
- Since $\eta_k(G_i) = \iota_k(\eta_{k-1}(G_i))$, by the induction hypothesis, it suffices to show that for any $i \in \mathbb{N}$, $\eta_k(v_k^i)$ belongs to the subspace generated by B_k. Fix $i \in \mathbb{N}$.
- Let (e, Q_k, R_k) be a pseudo-remainder triple of v_k^i with respect to A_k over $\mathcal{S}_{k-1}$, so that $I_k^e v_k^i = Q_k A_k + R_k$.
- Since I_k is invertible respect to $(\mathbf{A}_{k-1})_{\mathcal{S}_{k-1}}$, there exist $M_k \in \mathcal{S}_{k-1}$, $N_k \in (\mathbf{A}_{k-1})_{\mathcal{S}_{k-1}}$, and $L_k \in \mathcal{S}_0$, $L_k \neq 0$ such that $L_k = M_k I_k + N_k$. Since $V_{\mathbf{A}_k} \neq 0$, it follows that $\eta_k(L_k) \neq 0$ and $\eta_k(v_k^i) = \eta_k((M_k/L_k)^e R_k)$. Since the degree in v_k of $(M_k/L_k)^e R_k$ is $< d_k$, the proof is completed by induction.

Proof That Maps η_k Are Computable

Corollary 3.11

For any $F \in \mathcal{K} := \mathcal{K}_p$, we can compute $\eta(F) := \eta_p(F) \in V_{\mathbf{A}}$ in terms of the basis B_p with coefficients in $\mathcal{K}_0$.

- Let $1 \leqslant k \leqslant p$. Since I_k is invertible respect to $(\mathbf{A}_{k-1})_{\mathcal{S}_{k-1}}$, by Proposition 3.1, $1 \in (A_1, \ldots, A_{k-1}, I_k)_{\mathcal{K}_{k-1}}$.
- We can compute an expression representing 1 as a $\mathcal{K}_{k-1}$-linear combination of $A_1, \ldots, A_{k-1}, I_k$.
- Clearing denominators (which are in $\mathcal{S}_0$), we can compute L_k, M_k, N_k with the properties as in the proof of Corollary 3.9.
- Pseudo-division allows us to replace any v_k^i occurring in F where $i \geqslant d_k$ by $(M_k/L_k)^e R_k$ (here e and R_k both depend also on i as well as k), which is a polynomial in K_k with degree in v_k is $< d_k$.
- Proceeding with this replacement inductively for $k = p, \ldots, 1$ eventually yields the representation for $\eta(F)$.

Computing a Minimal Polynomial

Corollary 3.12

Suppose $\mathbf{A}$ *has invertible initials and* $F \in \mathcal{S} = \mathcal{S}_p$. *Then we can compute a minimal polynomial of* F *modulo* $\mathbf{A}$ *over* $\mathcal{S}_0$.

- Let d be the dimension of the K_0 vector space $V_{\mathbf{A}}$.
- Then the elements $\eta(1), \eta(F), \ldots, \eta(F^d)$ must be linearly dependent over K_0.
- By Corollaries 3.9 and 3.11, such a dependence relation involving a minimal power $F^{d'}$ of F can be obtained by linear algebra.
- If $\sum_{i=0}^{d'} N_i \eta(F^i)/D_i = 0$, where $N_i, D_i \in \mathcal{S}_0, D_i \neq 0$, then clearing the denominators yields the polynomial $P(X)$ of degree d' satisfying the requirements.

Cyclic Vector, Remarks and Examples

- In the proof for Corollary 3.12, **if $d' = d$**, then $\eta(1)$ is a **cyclic vector** of the linear transformation $\eta_F : V_{\mathbf{A}} \to V_{\mathbf{A}}$, that is, $V_{\mathbf{A}}$ is generated over $\mathcal{K}_0$ by the linearly independent set of vectors: $\{\eta(1), \eta_F(\eta(1)), \ldots, \eta_F^{d-1}(\eta(1)\} = \{\eta(1), \eta(F), \ldots, \eta(F^{d-1})\}$. Relative to this basis, η_F is represented by a companion matrix (**with entries in $\mathcal{K}_0$**) whose characteristic polynomial $P(X)$ is a minimal polynomial for F modulo $\mathbf{A}$ over $\mathcal{K}_0$.
- **Corollaries 3.9 and 3.12 are false without A having invertible initials.** Let $\mathbf{A}$: $v_1, v_1 v_2$. Then $V_{\mathbf{A}} \cong K_0[v_2]$ is non-trivial and has infinite dimension over $\mathcal{K}_0$. The polynomial $F = v_2$ has no minimal polynomial and F is not invertible.
- **The converse of Corollary 3.9 is also false.** Let $\mathbf{A}$: $v_1, v_1 v_2^2 + v_2$. Then $V_{\mathbf{A}} \cong \mathcal{K}_0$ has dimension 1 but $\mathbf{A}$ does not have invertible initials.

Regularity of Initials

Invertibility vs Regularity

Zero-divisors Modulo Ideals

Regularity of Initials

- We say $F \in \mathcal{S}_p$ is **regular with respect to the triangular set $\mathbf{A}: A_1, \ldots, A_p$ and corresponding variables $v_1, \ldots, v_p$ over $\mathcal{S}_0$** (or that F is **regular w.r.t. $\mathbf{A}$**, or simply F is *regular*) if $((\mathbf{A}): I^\infty, F) \cap \mathcal{S}_0 \neq (0)$, where $I = I_1 \cdots I_p$ is the product of initials.

- We say **A has regular initials**, or **A** is a **regular chain with respect to $v_1, \ldots, v_p$ over $\mathcal{S}_0$** if for each k, $1 \leqslant k \leqslant p$, the initial I_k of A_k is regular w.r.t. $\mathbf{A}_{k-1}: A_1, \ldots, A_{k-1}$.

- The difference between regular and invertible for F is the use of the saturation ideal $(\mathbf{A}) : I^\infty$ rather than $(\mathbf{A})$. As will be seen, there is **practically** no difference in the two concepts for **initials of triangular sets**.

Practical Equivalence: Invertibility and Regularity

Theorem 3.16

Suppose A has invertible initials *and* $F \in \mathcal{S}_p$. *Then the following are equivalent:*

(a). *F is regular w.r.t.* $\mathbf{A}$ *over* $\mathcal{S}_0$.

(b). *F is invertible modulo* $(\mathbf{A})$ *over* $\mathcal{S}_0$.

(c). $\eta(F) \neq 0$ *and* $\eta(F)$ *is not a zero divisor.*

(d). η_F *is injective.*

(e). *Every pseudo-remainder of* $G \in (\mathbf{A})$: F^∞ *w.r.t.* $\mathbf{A}$ *is zero.*

(f). *For every minimal polynomial* $P(X)$ *of* F, $P(0) \neq 0$.

Equivalence for Triangular Sets

Corollary 3.17

Let $\mathbf{A}$ *be a triangular subset of* $\mathcal{S}_p$. *Then* $\mathbf{A}$ *has invertible initials if and only if* $\mathbf{A}$ *has regular initials.*

- Clearly, if $\mathbf{A}$ has invertible initials, it has regular initials. For each k, $1 \leqslant k \leqslant p$, we have $((\mathbf{A}_{k-1}), I_k)_{\mathcal{S}_{k-1}} \cap \mathcal{S}_0 \neq 0$ implies $((\mathbf{A}_{k-1}) : (I_1 \cdots I_k)^\infty, I_k)_{\mathcal{S}_{k-1}} \neq 0$.
- Conversely, suppose $\mathbf{A}$ has regular initials.
- Since $\mathbf{A}_1 : A_1$ has invertible initial, it follows from Theorem 3.16 that I_2 is invertible with respect to $\mathbf{A}_1$.
- By induction, $\mathbf{A}$ has invertible initials.

Proof of Theorem 3.16: (a) $\Rightarrow$ (b)

To prove: F regular implies F invertible.

- Suppose F is regular. Let $L' \in \mathcal{S}_0$, $L' \neq 0$, $M' \in \mathcal{S}_p$ and $N' \in (\mathbf{A}) : I^\infty$ be such that $L' = M'F + N'$.
- Then $N' = L' - M'F$ and there exists some $e \in \mathbb{N}$ such that $I^e N' = I^e(L' - M'F) \in (\mathbf{A})$.
- Since $\mathbf{A}$ has invertible initials, let $L_k \in \mathcal{S}_0, M_k \in \mathcal{S}_{k-1}, N_k \in (\mathbf{A}_{k-1})$ be such that $L_k \neq 0$ and $L_k = M_k I_k + N_k$.
- $\prod_{k=1}^{p}(L_k - N_k)^e(L' - M'F) = \prod_{k=1}^{p}(M_k I_k)^e N' \in (\mathbf{A})$.
- Hence there exist $L \in \mathcal{S}_0$, $L \neq 0$, and $M \in \mathcal{S}_p$, $N \in (\mathbf{A})$ such that $L = MF + N$ and F is invertible.

Proof of Theorem 3.16: (b) $\Rightarrow$ (c)

To prove: F invertible implies $\eta(F) \neq 0$ and $\eta(F)$ is not a zero divisor.

- Suppose F is invertible. Let $L \in \mathcal{S}_0$, $L \neq 0$, and $M \in \mathcal{S}_p$, $N \in (\mathbf{A})$ be such that $L = MF + N$.
- Then $\eta(L) = \eta(MF)$.
- Since $V_{\mathbf{A}}$ is not trivial, $\eta(L) \neq 0$, and hence $\eta(F) \neq 0$.
- $\eta(MF/L) = \eta(1)$.
- Let $G \in K_0[v_1, \ldots, v_p]$ be such that $\eta(FG) = 0$.
- Then $\eta(G) = \eta(MFG/L) = 0$, showing that $\eta(F)$ cannot be a zero-divisor in $K_0[v_1, \ldots, v_p]/(\mathbf{A})$.

Proof of Theorem 3.16 (c) $\Rightarrow$ (d) $\Rightarrow$ (e)

To prove: $\eta(F) \neq 0$ and not a zero divisor implies η_F injective.

- For any $G \in \mathcal{K}_p$, $\eta_F(\eta(G)) = 0$ if and only if $\eta(F)\eta(G) = 0$.
- Since $\eta(F) \neq 0$ and not a zero divisor, $\eta(G) = 0$. So η_F is injective.

To prove: η_F injective implies every pseudo-remainder of $G \in (\mathbf{A}) : F^\infty$ with respect to A is zero.

- Let $G \in (\mathbf{A}) : F^\infty$. For some $e \in \mathbb{N}$, $F^e G \in (\mathbf{A})$.
- Let R_1 be a pseudo-remainder of G with respect to $\mathbf{A}$ and let $I_1^{e_1} \cdots I_p^{e_p} G = Q_1 A_1 + \cdots + Q_p A_p + R_1$.
- Then $F^e R_1 \in (\mathbf{A})$. Hence $\eta(F)^e \eta(R_1) = \eta_F^e(\eta(R_1)) = 0$.
- Since η_F is injective, we must have $\eta(R_1) = 0$.
- This means $LR_1 \in (\mathbf{A})$ for some non-zero $L \in \mathcal{S}_0$, and hence by Lemma 3.6, $R_1 = 0$.

Proof of Theorem 3.16: (e) $\Rightarrow$ (f)

To prove: If every pseudo-remainder of $G \in (\mathbf{A}) : F^\infty$ w.r.t. $\mathbf{A}$ is zero, then $P(0) \neq 0$ for every minimal polynomial P of F.

- Suppose there were a minimal polynomial $P(X) \in \mathcal{S}_0[X]$ of F but $P(0) = 0$.
- Write $P(X) = XQ(X)$. Since $\eta(FQ(F)) = 0$, there would exist a non-zero $L \in \mathcal{S}_0$ such that $G := LQ(F) \in (\mathbf{A}) : F^\infty$.
- Every pseudo-remainder R_1 of G w.r.t. $\mathbf{A}$ would be zero.
- In particular, by the invertibility of initials, there would exist a non-zero $L' \in \mathcal{S}_0$, $L' \neq 0$, such that $L'G \in (\mathbf{A})$.
- Thus $P'(X) := L'LQ(X)$ would be a polynomial satisfying $P'(\eta(F)) = \eta(P'(F)) = \eta(L'G) = 0$ but with a lower degree than $P(X)$, contradicting minimality in degree of P.

Proof of Theorem 3.16: (f) $\Rightarrow$ (a)

To prove: If $P(0) \neq 0$ for every minimal polynomial P of F over $\mathcal{S}_0$, then F is regular.

- By Corollary 3.12, there exists a minimal polynomial P for F.
- Let $P(X) = P(0) + XQ(X)$.
- Since $\eta(P(F)) = 0$, there exists a non-zero $L \in \mathcal{S}_0$ such that $LP(F) \in (\mathbf{A}) := (\mathbf{A})_{\mathcal{S}}$.
- Now both L and $P(0)$ are non-zero in $\mathcal{S}_0$, and $LP(0) = LP(F) - FQ(F)$ which is in $(\mathbf{A}, F)_{\mathcal{S}} \subseteq ((\mathbf{A}) : I^\infty), F)_{\mathcal{S}}$.
- So $((\mathbf{A}) : I^\infty, F) \cap \mathcal{S}_0 \neq (0)$ and F is regular.

Recap: Invertibility and Regularity

Theorem 3.16

Suppose A has invertible initials and $F \in \mathcal{S}_p$. Then the following are equivalent:

(a). F is regular w.r.t. $\mathbf{A}$ over $\mathcal{S}_0$.

(b). F is invertible modulo $(\mathbf{A})$ over $\mathcal{S}_0$.

(c). $\eta(F) \neq 0$ and $\eta(F)$ is not a zero divisor.

(d). η_F is injective.

(e). Every pseudo-remainder of $G \in (\mathbf{A})$: F^∞ w.r.t. $\mathbf{A}$ is zero.

(f). For every minimal polynomial $P(X)$ of F, $P(0) \neq 0$.

- Note, the image of F in $\mathcal{S}_0[v_1, \ldots, v_p]/(\mathbf{A})$ may be a zero divisor! Example, let $\mathcal{S}_0 = \mathbb{Q}[u]$, $\mathbf{A} : A_1 = uv$. Then $(\mathbf{A})_\mathcal{K} = (v)_\mathcal{K}$ and $(\mathbf{A})_\mathcal{S} = (uv)_\mathcal{S}$. The initial $I_1 = u$ is invertible modulo $(\mathbf{A})_\mathcal{K} = (v)_\mathcal{K}$ over $\mathcal{S}_0$, but its image is a zero divisor in $\mathcal{S}_0[v]/(\mathbf{A})$.

Remarks on Equivalences and Example

The equivalences in Theorem 3.16 do not always hold without the hypothesis that A has invertible initials.

- Let $\mathcal{S}_0 = \mathbb{Z}[u]$ and $A_1 = uv_1^2$, $A_2 = v_1v_2 - 1$ (so $p = 2$). Then $\mathbf{A}$: A_1, A_2 is triangular with respect to v_1, v_2 over $\mathcal{S}_0$.
- Let $F := v_1$. Its minimal polynomial (modulo $\mathbf{A}_1$) is uX^2. By Theorem 3.16 applied to $\mathbf{A}_1$ (which has invertible initial u), F **is *not* invertible modulo $(\mathbf{A}_1)$.**
- Since $F = I_2$, **A does not have invertible initials.**
- F **is invertible modulo $\mathbf{A}_{\mathcal{K}}$** since $1 = v_2F - A_2$.
- $V_{\mathbf{A}} = (0)$ since $0 \neq u = v_2^2A_1 - u(v_1v_2 + 1)A_2 \in (\mathbf{A}) \cap \mathcal{S}_0$.
- So η_F is (trivially) injective, and $\eta(F) = 0$ even though $F \notin (\mathbf{A})_{\mathcal{S}} = (u, A_2)$. So modulo $\mathbf{A}$ is $P_F(X) = 1$.
- The polynomial $G = uv_1 \in (\mathbf{A})\colon F^\infty$ has pseudo-remainder G.
- Thus (b), (d), and (f) do not imply (c) or (e).

Further Remark and Zero-divisors over $\mathcal{K}_0$ vs $\mathcal{S}_0$

- In the previous example, $\mathbf{A}_1 : u\, v_1^2$ has invertible initial u, but the product of the initials, namely u, is not invertible modulo $(\mathbf{A}_1)$ since its image in $V_{\mathbf{A}_1}$ is a (non-zero) zero-divisor.
- Let u, v_1, v_2, v_3 be indeterminates over $\mathbb{Q}$, $\mathcal{S}_0 = \mathbb{Q}[u]$ and
  - $A_1 = uv_1$ with $I_1 = u$;
  - $A_2 = u(v_1 + 1)v_2$ with $I_2 = u(v_1 + 1)$; and
  - $A_3 = (v_1 + 1)v_3 + u$ with $I_3 = v_1 + 1$.
- Since $u = I_2 - A_1$ and $u = u\, I_3 - A_1$, the triangular ordered set $\mathbf{A}$: A_1, A_2, A_3 has invertible initials w.r.t. v_1, v_2, v_3 over $\mathcal{S}_0$.
- The ideal $(\mathbf{A})$ in $K_0[v_1, v_2, v_3]$ is generated by $v_1, v_2, v_3 + u$. Thus $\eta(I_1), \eta(I_2), \eta(I_3)$ are non-zero, and they are not zero-divisors. However, the images of I_1, I_2, I_3 in $\mathcal{S}_0[v_1, v_2, v_3]/(\mathbf{A})$ are all zero-divisors.

Invertible Initials Equivalences

Decidability and Algorithms

Corollary 3.20

Let $\mathbf{A}$: $A_1, \ldots, A_p$ *be a triangular set with respect to* $v_1, \ldots, v_p$ *in* $\mathcal{S}_p$. *Let* $J_I := (A_1, \ldots, A_p) : I^\infty$ *be the saturation ideal of* $\mathbf{A}$ *with respect to initials. The following are equivalent:*[2]

(a). $\mathbf{A}$ *has invertible initials.*

(b). $F = 0$ *for any* $F \in J_I$ *for which its degree in* v_k *is* $< d_k$, *for all* k, $1 \leqslant k \leqslant p$.

(c). *Every pseudo-remainder* R_1 *of* $F \in J_I$ *with respect to* $\mathbf{A}$ *is zero.*

- (a) $\Rightarrow$ (b) has been proved in Lemma 3.6.
- (b) $\Rightarrow$ (c) is obvious since $R_1 \in J_I$ if F does.

[2] In the paper, this corollary was stated as (a) $\Longleftrightarrow$ (c).

Proof of Corollary 3.20: (c) implies (a)

- We show (a) by induction on p that $\mathbf{A}_p$ has invertible initials. When $p = 1$, I_1 is by definition invertible modulo (0).
- Suppose by induction, we have proved for $1 < p$, $\mathbf{A}_{p-1}$ has invertible initials. Let $F := I = I_1 \cdots I_p \in \mathcal{S}_{p-1}$.
- Let $G \in ((\mathbf{A}_{p-1}) : F^\infty)_{\mathcal{S}_{p-1}}$. Then $G \in J_I$.
- Let $R_{p-1}, \ldots, R_1$ be any PRS of G w.r.t. $\mathbf{A}_{p-1}$.
- Let $R_p = G$, which is the pseudo-remainder of G with respect to A_p since $G \in \mathbf{A}_{p-1}$ does not involve v_p. Hence $R_p, R_{p-1}, \ldots, R_1$ is a PRS of G w.r.t. $\mathbf{A}$.
- By hypothesis (c), $R_1 = 0$. By Theorem 3.16 applied to $\mathbf{A}_{p-1}$, F is invertible modulo $\mathbf{A}_{p-1}$. By Corollary 3.3, I_p is invertible modulo $\mathbf{A}_{p-1}$, and hence $\mathbf{A}$ has invertible initials.

Decidability of Invertibility and Effectiveness

Theorem 3.22

Suppose $\mathbf{A}$ *is triangular as before.*

(a). *The property that* $\mathbf{A}$ *has invertible initials is decidable.*

(b). *If* $\mathbf{A}$ *has invertible initials, and* $F \in \mathcal{S}_p$, *then the invertibility of* F *with respect to* $\mathbf{A}$ *is decidable.*

(b).1 *If* F *is invertible, we can compute a non-zero* $L \in \mathcal{S}_0$, $M \in \mathcal{S}_p$, *and* $N \in (\mathbf{A})$ *such that* $L = MF + N$.

(b).2 *If* F *is not invertible, we can compute a* $G \in \mathcal{S}_p$, *such that the degree of* G *in* v_k *is* $< d_k$ *for all* $1 \leqslant k \leqslant p$, $GF \in (\mathbf{A})$ *and* $G \notin (\mathbf{A})$.

- This result was due to Kandri Rody *et al.* [19, 9]. Part (b).1 can be solve by Gröbner basis methods. Part (b).2 will be needed in the prime decomposition of differential radical ideals.

Proof of Theorem 3.22

- **We prove (a) and simultaneously (b) in the special case when A is $\mathbf{A}_k$ and $F = I_k$, by induction on k, $k = 1, \ldots, p$.**
- For $k = 1$, $\mathbf{A}_1$ always has invertible initial and for $F = I_1$, we may take $L = I_1, M = 1, N = 0$. Then $L = MF + N$.
- For $2 \leqslant k < p$, assume that the above holds for $j \leqslant k - 1$. We are done if $\mathbf{A}_{k-1}$ does not have invertible initials. So suppose $\mathbf{A}_{k-1}$ has invertible initials.
- By Corollary 3.12, we can compute a minimal polynomial $P_k(X) = P_k(0) + XQ_k(X)$ of $F = I_k$ with respect to $\mathbf{A}_{k-1}$ and $L_k \neq 0$, $L_k \in \mathfrak{s}_0$ such that $L_k P_k(I_k) \in (\mathbf{A}_{k-1})$.
- (b).**1**: If $P_k(0) \neq 0$, then I_k is invertible with respect to $\mathbf{A}_{k-1}$ by Theorem 3.16, and we may take $L = L_k P_k(0)$, $M = -L_k Q_k(I_k)$ and $N = L_k P_k(I_k)$. Then $L = MF + N$.

Proof Continues: Case $P_k(0) = 0$

- (b).**2**: If $P_k(0) = 0$, let $V_{k-1} = \{ v_1, \ldots, v_{k-1} \}$ and let $I_1^{e_1} \cdots I_{k-1}^{e_{k-1}} Q_k(I_k) = \sum_{j=1}^{k-1} Q_j' A_j + G_k$ be the result of a pseudo-division of $Q_k(I_k)$ by $\mathbf{A}_{k-1}$ with G_k a pseudo-remainder of $Q_k(I_k)$ w.r.t. $\mathbf{A}_{k-1}$.
- Now $G_k \notin (\mathbf{A}_{k-1})$, for otherwise, we would have $I_1^{e_1} \cdots I_{k-1}^{e_{k-1}} Q_k(I_k) \in (\mathbf{A}_{k-1})$; the invertibility of initials of $\mathbf{A}_{k-1}$ would imply that there be a non-zero $L' \in \mathcal{S}_0$ (explicitly, $L' = \prod_{j=1}^{k-1} (L_j P_j(0))^{e_j}$) such that $L' Q_k(I_k) \in (\mathbf{A}_{k-1})$; and this would contradict the minimality of $P_k(X)$.
- Now $G = L_k G_k$ has the property we need for I_k, that is, $G \notin (\mathbf{A}_{k-1})$ and

$$G I_k = L_k I_k G_k \equiv L_k I_k I_1^{e_1} \cdots I_{k-1}^{e_{k-1}} Q_k(I_k) \equiv 0 \bmod (\mathbf{A}_{k-1}).$$

- This completes the induction and proves (a). The proof for (b) for a general $F \in \mathcal{S}_p$ is similar (append $A_{p+1} = F v_{p+1}$, for example).

Invertibility of Separants

Separable Ring Extensions and Ideals

Kolchin's Lemma 13

Invertibility of Separants

- Let $\mathbf{A}$: $A_1, \ldots, A_p$ be triangular w.r.t. $v_1, \ldots, v_p$ over $\mathcal{S}_0$.
- The **separant** of A_k w.r.t. v_k is $S_k = \partial A_k / \partial v_k$.
- We denote **the product of separants** of $\mathbf{A}$ by S, and let $H = IS$.
- We say $\mathbf{A}$ **has invertible separants w.r.t.** $v_1, \ldots, v_p$ **over** $\mathcal{S}_0$ if for $1 \leqslant k \leqslant p$, S_k is invertible modulo $(\mathbf{A}_k)$ over $\mathcal{S}_0$ w.r.t $v_1, \ldots, v_k$ for $1 \leqslant k \leqslant p$.

Corollary 3.25

Let $\mathbf{A}$ *be triangular as before and suppose* $\mathbf{A}$ *has invertible initials. Then the property that* $\mathbf{A}$ *has invertible separants is decidable.*

Example of Non-Invertible Separants

- Consider a previous example: $p = 2$, $\mathcal{S}_0 = \mathbb{Z}[u]$ (u an indeterminate), $\mathbf{A} : A_1 := uv_1^2, A_2 := v_1 v_2 - 1$.
- The separant $S_1 = 2uv_1$ is not invertible modulo $(\mathbf{A}_1)$, but the separant $S_2 = v_1$ is invertible modulo $(\mathbf{A})$ since $1 = v_2 v_1 - A_2$.
- The same polynomial v_1, as the initial I_2, on the other hand, is not invertible modulo $(\mathbf{A}_1)$.
- $\mathbf{A}$ has neither invertible initials nor separants, but *all* initials and separants *are* invertible modulo $(\mathbf{A})$ over $\mathcal{S}_0$.

Kolchin's Notion of Separable Ring Extensions

- For a ring $\mathcal{K}$, $\mathcal{K}$ is **separable** over a subring S_0 if either $\mathcal{K} = (0)$, or $\mathcal{K} \neq (0)$ **and has the three properties**:
  - (a). $\mathcal{K}$ has no non-zero nilpotent elements;
  - (b). for every non-zero $L \in \mathcal{S}_0$ and non-zero $G \in \mathcal{K}$, $LG \neq 0$;
  - (c). either $\mathcal{K}$ has characteristic 0, or has characteristic $p \neq 0$ and $\mathcal{K}^p$ and $\mathcal{S}_0$ are linearly disjoint over $\mathcal{S}_0^p$.
- (b) implies that $\mathcal{S}_0$ is an integral domain.
- The separable relation is transitive for rings $\mathcal{S}_0 \subset \mathcal{S}_1 \subset \mathcal{S}_2$.
- An $\mathcal{S}_0$-algebra $\mathcal{K}$ that is an integral domain is separable over $\mathcal{S}_0$.
- An $\mathcal{S}_0$-algebra $\mathcal{R}$ that is a local ring (but not a field) is not separable over $\mathcal{S}_0$ since its maximal ideal $\neq (0)$ but is the radical (of (0)).

Kolchin's Notion of a Separable Ideal

- An ideal J of $\mathcal{K}$ is **separable** over $\mathcal{S}_0$ if $\eta(\mathcal{K})$ is separable over $\eta(\mathcal{S}_0)$, where $\eta : \mathcal{K} \to \mathcal{K}/J$ is the canonical homomorphism, that is, $\mathcal{K}/J$ is separable over $(\mathcal{S}_0 + J)/J \cong \mathcal{S}_0/(J \cap \mathcal{S}_0)$.
- So $J \subseteq \mathcal{K}$ is separable over $\mathcal{S}_0$ if either $J = \mathcal{K}$, or J is a proper ideal of $\mathcal{K}$ and
  - (a). J is a radical ideal;
  - (b). for every $L \in \mathcal{S}_0$ and $L \notin J$, and every $G \in \mathcal{K}$ and $G \notin J$, $LG \notin J$ (in particular $J \cap \mathcal{S}_0$ is a prime ideal). Alternatively, $\eta_L : \mathcal{K}/J \to \mathcal{K}/J$, the multiplication map by $\eta(L)$ defined by $\eta_L(\eta(G)) = \eta(LG)$ is injective for every $L \in \mathcal{S}_0 \backslash (J \cap \mathcal{S}_0)$.
  - (c). Although $\mathcal{K}/J$ may have non-zero characteristic when K has characteristic zero, in most cases, it has characteristic zero in this talk.

Kolchin's vs Contemporary Notions

- A triangular set **A** is **autoreduced** if $\deg_{v_j} A_k < d_j$ for all $1 \leqslant j < k \leqslant p$.
- When **A** has both invertible initials and invertible separants, it is called **separable** by Sadik [37], and **A** is said to be a **squarefree regular chain** by Boulier [8].
- When **A** is in addition autoreduced, **A** is said to be **satured** by Bouziane *et al.* [9].

Kolchin's Lemma 13

Lemma 13 (Kolchin [24, p. 36])
Suppose **A** has invertible initials and separants and is autoreduced. Then

(a). the ideal J_I of $\mathcal{S}$ is separable over $\mathcal{S}_0$, and

(b). $F = 0$ for any $F \in J_I$ for which its degree in v_k is $< d_k$, for all k, $1 \leqslant k \leqslant p$.

- The Lemma provides the theoretical basis of the Ritt-Kolchin decomposition algorithm using factorization over algebraic extensions.
- More importantly, it shows that, under these hypothesis, J_I **is radical**. With further hypothesis, we have $J_I = (\mathbf{A}) : H^\infty$.

Contemporary References on Invertibility

- Sadik [37] observed that the proof of Kolchin's Lemma 13(b) works equally well for triangular sets with invertible initials (as proved in Lemma 3.6) and indeed the two properties are equivalent (as shown in Corollary 3.20).
- That J_I is radical and $J_I = J_H$ (under additional hypothesis) are pointed out by Hubert [18, Proposition 3.3], and Sadik[37, Corollary 2.1.1].
- Bouziane *et al.* and Sadik used the properties to compute the dimension of $J_I = (\mathbf{A}) : I^\infty$.
- Hubert developed similar algorithms using properties of Gröbner basis of zero-dimensional polynomial ideals.
- Boulier (LIFL-2001-09, Theorem 4) gave a proof that does not involve dimension, but appeals to **Lazard's Lemma**: $J_S := (\mathbf{A}) : S^\infty$ is radical.
- These authors extended their results to the differential case.

Rankings on Derivatives

Comparative Rank

Autoreduced Sets

Rankings on Derivatives

- A **ranking** is a total ordering $\preceq$ on the set ΘY of derivatives such that for all $u, v \in \Theta Y$ and $\delta \in \Delta$, we have
$$u \preceq \delta u \quad \text{and} \quad u \preceq v \Rightarrow \delta u \preceq \delta v.$$
- A ranking is **orderly** if $\operatorname{ord} u < \operatorname{ord} v \Rightarrow u \prec v$.
- A ranking is **unmixed** if for every $(i, j), 1 \leqslant i, j \leqslant n$ and every $\theta \in \Theta$,
$$y_i \prec y_j \Rightarrow \theta y_i \prec y_j.$$
- A ranking is **integrated** if for every pair of derivatives $(\theta y_i, \lambda y_j)$, there is a $\rho \in \Theta$ such that $\rho\theta y_i \succ \lambda y_j$. Equivalently, if for every i, there is a $\rho \in \Theta$ such that $\rho y_i \succ y_j$ for all $j \neq i$.
- A ranking is **sequential** if every derivative θy_i has only finitely many derivatives $u \prec \theta y_j$.

Lexicographically-induced Rankings

- **A sequential ranking is always integrated** and **an orderly ranking is always sequential**. An unmixed ranking ($n > 1$) cannot be integrated.
- Rankings are usually given via an embedding $\varphi\colon \Theta Y \longrightarrow \mathbb{R}^s$.
- The set $\mathbb{R}^s$ may be ordered lexicographically: for two s-tuples $(a_1, \cdots, a_s)$ and $(b_1, \cdots, b_s)$ in $\mathbb{R}^s$, we say $(a_1, \cdots, a_s) <_{lex} (b_1, \cdots, b_s)$ if there exists some r, $1 \leqslant r \leqslant s$ such that $a_i = b_i$ for $1 \leqslant i < r$ and $a_r < b_r$.
- This lexicographic order on $\mathbb{R}^s$ induces a ranking on ΘY via φ: that is, $u \prec v$ if $\varphi(u) <_{lex} \varphi(v)$. We say loosely that the ranking $\preceq$ is **lexicographic w.r.t. the s-tuple $\varphi(u)$**.

Examples of Rankings

- Let $u = \delta_1^{e_1} \cdots \delta_m^{e_m} y_j$ be a typical derivative.
- The lexicographical order with respect to the $(m+1)$-tuple $(\operatorname{ord} \mathbf{u}, j, e_1, \cdots, e_{m-1})$ induces an **orderly** ranking on ΘY.
- The lexicographical order with respect to $(\mathbf{j}, \operatorname{ord} u, e_1, \cdots, e_{m-1})$ is **unmixed**.
- Let $m = 2, n = 1$ and order the set ΘY lexicographically with respect to the tuple $(2e_1 + e_2, e_1)$. Then $\delta_2^2 y \prec \delta_1 y$ since $(2, 0) <_{lex} (2, 1)$. This ranking is **not orderly** but is **sequential**, hence also **integrated**.
- If $m = n = 1$, there is only one ranking, which is orderly:

$$y \prec y' \prec y^{(2)} \prec \cdots .$$

Dickson's Lemma

Dickson's Lemma. *Any union of cones in $\mathbb{N}^m$ is a finite union of cones.*

- Dickson's Lemma is a result on the **product order of $\mathbb{N}^m$**.
- The product order is the partial order defined by $(a_1, \ldots, a_m) \leqslant (b_1, \ldots, b_m)$ if $a_i \leqslant b_i$ for all i, $1 \leqslant i \leqslant m$.
- Given a lattice point $p \in \mathbb{N}^m$, let C_p be the translate $p + \mathbb{N}^m$ (the **cone based at p**). If $q \in C_p$, we also say p **divides** q ($q \geqslant p$ in the product order—division in the sense of associated monomials in m variables).

One Equivalent Form of Dickson's Lemma

Lemma-A. *In any infinite sequence of points* $p_1, p_2, \cdots \in \mathbb{N}^m$, *there is a subsequence* $p_{k_1}, p_{k_2}, \ldots$ *such that* p_{k_i} *divides* $p_{k_{i+1}}$ $(p_{k_i} \leqslant p_{k_{i+1}})$.

- Suppose first $m = 1$. The conclusion is clear if some number occurs infinitely often in the sequence.
- Otherwise, every number occurs only a finite number of times and there will be an infinite (strictly) increasing subsequence.
- The case for $m > 1$ then follows by induction (getting non-decreasing subsequences one coordinate at a time).
- Claim: **Lemma-A** $\Longleftrightarrow$ **Dickson's Lemma.**

Lemma-A $\Rightarrow$ Dickson's Lemma

Lemma-A $\Rightarrow$ Dickson's Lemma.

- Let P be a union of cones and let p_1 be in P.
- If possible, let p_2 be an element of $P \setminus C_{p_1}$.
- In general, if possible, let p_k be an element of the complement in P of the union of the cones at $p_1, \ldots, p_{k-1}$.
- If this process stops, then P is a finite union of cones.
- If not, we obtain an infinite sequence where no member is in the union of the cones of earlier members. This contradicts Lemma-A.

Dickson's Lemma $\Rightarrow$ Lemma-A

- Let P be the union of the cones at p_k, $k = 1, 2, \ldots$.
- Then P is the union of a finite number of cones by Dickson's Lemma, and one of them must contain an infinite subsequence of the given one.
- Let the base of this cone be p_{k_0}.
- If all elements in the subsequence are equal to p_{k_0}, we are done.
- Otherwise repeat the argument for the subsequence (after removing a finite number of duplicates of p_{k_0} if needed, or including them all as the start of the next subsequence) to get $p_{k_1} > p_{k_0}$.

Dickson's Lemma $\Rightarrow$ Hilbert Basis Theorem

- Fix a term-ordering. The set of Gröbner ranks (leading monomials) of all elements in the polynomial ideal I corresponds to a union P of cones in $\mathbb{N}^m$, which is a finite union of cones. Let the bases of these cones correspond to the Gröbner ranks of $G_1, \ldots, G_s$, with $G_i \in I$. Then I is generated by $G_1, \ldots, G_s$. Indeed, **the G_i form a Gröbner basis**: Let $F \in I$. Performing successive Gröbner reductions yields a relation of the form:

$$F = Q_1 G_1 + \cdots + Q_s G_s + R$$

where R is Gröbner-reduced with respect to every G_i. If $R \neq 0$, since $R \in I$, the Gröbner rank of R would correspond to a point in P, which would mean that R is not Gröbner-reduced with respect to some G_i. This contradiction shows that $R = 0$ and hence I is generated by $G_1, \ldots, G_s$, which is a Gröbner basis since every $F \in J$ Gröbner-reduces to zero.

Corollary 4.4

Every ranking is a well-ordering on ΘY

- Let $m \geqslant 1$ and let R be the polynomial ring $K[x_1, \cdots, x_m]$ over a field K, and let N be a free R-module on n generators $z_1, \ldots, z_n$.
- As a vector space over K, N has a basis
$$B = \{\, x_1^{d_1} \cdots x_m^{d_m} z_i \mid (d_1, \ldots, d_m) \in \mathbb{N}^m, 1 \leqslant j \leqslant n \,\}.$$
- A monomial ordering on B corresponds to a ranking on ΘY with $m = \mathrm{Card}(\Delta)$ and $n = \mathrm{Card}(Y)$.
- The monomial ordering on B is degree-compatible if and only if the corresponding ranking is orderly.
- When $\Delta = \emptyset$, a ranking is an ordering of the indeterminates $y_1, \cdots, y_n$ only and not a monomial ordering.

An Open Problem on Rankings

Open Problem 4.7

Characterize the set of all rankings on ΘY.

- Let $(a_{i,j})$ be an $m \times s$ matrix in $\mathbb{R}^{ms}$, such that on each row i, the first non-zero entry is positive. Then the lexicographic order on $\mathbb{R}^s$ with respect to the s-tuple

$$\left(\sum_{i=1}^{m} a_{i,1} e_i, \ldots, \sum_{i=1}^{m} a_{i,s} e_i \right)$$

induces a ranking on Θy when $Y = \{ y \}$ $(n = 1)$. Conversely every ranking on Θy can be obtained this way.
See Kolchin [24, Ex. 1, 2; p. 53] and Robbiano [34].

- For $n > 1$, Carrá-Ferro & Sit [13] has a structural theorem and an algorithm to construct rankings in terms of generalized Dedekind cuts and weight vectors. See also Rust & Reid [36].

Basic Notions on Differential Polynomials

- We now assume that a ranking $\preceq$ is fixed and given on ΘY.
- For any $v \in \Theta Y$, let $\mathcal{R} = \mathcal{F}\{y_1, \ldots, y_n\}$ and

$$\begin{aligned} \mathcal{R}_{[v]} &= \mathcal{F}[\{u \in \Theta Y \mid u \preceq v\}] \\ \mathcal{R}_{[v)} &= \mathcal{F}[\{u \in \Theta Y \mid u \prec v\}] \end{aligned}$$

- The **leader** of a differential polynomial $A \in \mathcal{R}$ **(always assuming $A \notin \mathcal{F}$)** is the highest ranked derivative u_A appearing in A. Then $d = \deg_{u_A} A > 0$.
- We often write A as a univariate polynomial in u_A, thus:

$$A = I_d u_A^d + I_{d-1} u_A^{d-1} + \cdots + I_0, \tag{4.9}$$

where $I_d, \ldots, I_0 \in \mathcal{R}_{(u_A)}$ and the **initial** $I_A := I_d \neq 0$.

- The **separant** S_A of A is $\frac{\partial A}{\partial u_A}$.
- The **rank** of A is the pair $(u_A, \deg_{u_A} A)$.

Comparing Differential Polynomials (DP)

- We extend a ranking $\preceq$ on ΘY to a **pre-order** on $\mathcal{R}\backslash\mathcal{F}$ (**that is, a reflexive and transitive relation**) by the lexicographic order on the ranks of DPs.
- Thus, $A \preceq B$ if either $u_A \prec u_B$ or $v := u_A = u_B$ and $\deg_v A \leqslant \deg_v B$.
- We further extend $\preceq$ to $\mathcal{R}$ by letting all elements of $\mathcal{F}$ have the same rank, which is less than the rank of every $A \in \mathcal{R}\backslash\mathcal{F}$. This can be done by extending the ranking to $\Theta Y \cup \mathcal{F}$, defining $a \prec v$ for any $v \in \Theta Y$, and $a \in \mathcal{F}$, and defining the rank of $a \in \mathcal{F}$ to be $(1, 0)$.
- For any ranking and any $A \in \mathcal{R}$, we have $I_A \prec A$ and $S_A \prec A$.

Example Comparing Rank of DPs

- Let $m = 1$ and $n = 2$. Denoting the differential indeterminates by w and z, there is a unique orderly ranking on $\mathcal{F}\{w, z\}$ such that $w < z$.
- Using the prime notation for differentiation, let

$$A = (w' + w^3)(z''')^2 + w^2 z''' - 3w^2(z')^3 z''.$$

- We have $u_A = z'''$, $I_A = w' + w^3$ and $S_A = 2(w' + w^3)z''' + w^2$.
- The rank of A is $(z''', 2)$. Both I_A and S_A are of lower rank than A.
- If $m = 0$, then $w^3 z^2$ and $w^2 z^2$ both have the same rank $(z, 2)$.