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.

Overview

- The goal of this mini-course is to introduce the Ritt-Kolchin theory for differential polynomials.
- While adhering to Kolchin's exposition, these talks will concentrate on fundamental concepts in a fresh way with emphasis on the relationship between classical theory and the modern symbolic computation approach.
- The key problem to be explored is differential ideal membership, particularly about prime and radical differential ideals because of the Ritt-Raudenbush Basis Theorem.
- At the more advanced level, the algebraic meaning and relationship between the general and singular components of differential equations will be covered.

What the Course Will Cover

- basic algebraic set up: pseudo-division, triangular set, invertibility and regularity, decision problems;
- basic differential set up: rankings, reduction concepts for differential polynomial systems, characteristic sets;
- Rosenfeld Properties and coherence concepts; properties shared by differential polynomial ideals and algebraic polynomial ideals;
- Ritt-Raudenbush Basis Theorem and its role in the decomposition of radical differential ideals into primes.
- Advanced Theorems. Component Theorems. Low Power Theorem. Time permitting, Leading Coefficient Theorem. Irreducibility Theorem.
- Proofs or sketches of proofs, examples, and open problems.

What This Course Will Not Cover

- Positive characteristic differential field theory
- Advanced topics (systems of bounded order, leading coefficient theorem, Levi's Lemma, domination lemma)
- Differential Galois theory (strongly normal differential field extensions, parametric Picard-Vessiot theory)
- Differential algebraic geometry (differential algebraic groups, dimension theory, intersection theorem)
- Complexity theory in analysis of algorithms (bounds)
- Research in related topics (differential type and Rota-Baxter type algebras, integral-differential algebras, Model Theory, Painlevé transcendence, arithmetic differential geometry of Buium)

Calculus vs Differential Algebra

Gröbner Basis vs Characteristic Set

The Calculus Way vs Differential Algebra

- Consider the system of PDEs in $y(t,s)$ and $z(t,s)$:

$$\frac{\partial^2 y}{\partial t^2} = 0, \qquad \frac{\partial^2 z}{\partial t^2} = 0, \qquad \frac{\partial^2 z}{\partial t \partial s} + y = 0, \qquad \frac{\partial^2 y}{\partial s \partial t} + z = 0.$$

- **Integrating** the first two equations twice.

$$y(t,s) = c_0(s) + c_1(s)t, \qquad z(t,s) = d_0(t) + d_1(t)s.$$

- **Substituting** these into the remaining equations yields:

$$d_1'(t) + c_0(s) + c_1(s)t = 0, \qquad c_1'(s) + d_0(t) + d_1(t)s = 0.$$

- **By algebraic independence** of s and t, we see that $c_0(s), c_1(s), d_0(t), d_1(t)$ are all constants and hence all zero. So $y(t,s) = z(t,s) = 0$.
- We need all three highlighted steps.

Rewriting the PDEs Using Differential Polynomials

- A more general system of the previous example can be set up in the differential polynomial ring $\mathcal{R} = \mathcal{F}\{ y, z \}$ with $\Delta = \{ \delta_1, \delta_2 \}$ replacing $\frac{\partial}{\partial t}$ and $\frac{\partial}{\partial s}$.
- For any natural number $h > 0$, define four *linear* differential polynomials

$$f_1 := \delta_1^h y, \quad f_2 := \delta_2^h z, \quad f_3 := \delta_1 \delta_2^{h-1} z + y, \quad f_4 := \delta_1^{h-1} \delta_2 y + z.$$

- The previous example is when $h = 2$.

$$\frac{\partial^2 y}{\partial t^2} = 0, \qquad \frac{\partial^2 z}{\partial t^2} = 0, \qquad \frac{\partial^2 z}{\partial t \partial s} + y = 0, \qquad \frac{\partial^2 y}{\partial s \partial t} + z = 0.$$

Solving PDEs by Differential Elimination

- Again, for any natural number $h > 0$, define four *linear* differential polynomials

$$f_1 := \delta_1^h y, \quad f_2 := \delta_2^h z, \quad f_3 := \delta_1 \delta_2^{h-1} z + y, \quad f_4 := \delta_1^{h-1} \delta_2 y + z.$$

- Using differential elimination, the differential ideal generated by f_1, f_2, f_3, f_4 is easily seen to be $[y, z]$, since

$$y = f_3 - \delta_1 \delta_2^{h-1} f_4 + \delta_2^h f_1,$$

and similarly

$$z = f_4 - \delta_1^{h-1} \delta_2 f_3 + \delta_1^h f_2.$$

- No symbolic computation software I know can handle a literal "exponent" h. This example demonstrates arbitrary high order cancellation to produce a "**general solution**" $(0, 0)$.

Linear Differential Ideals

- A **linear differential ideal** $\mathfrak{p}$ of $\mathcal{R} := \mathcal{F}\{z_1, \ldots, z_n\}$ is one that is generated by linear differential polynomials. Here, **linear** means all every **monomials in the derivatives of** $z_1, \ldots, z_n$ (that is, **differential monomials**) appears with at most degree 1.
- A linear differential ideal in $\mathcal{R}$ is always prime.
- **Example**: $\mathfrak{p} = [\delta_1^2 z - \delta_2 z, \quad \delta_1^3 z - \delta_2^2 z]$.
- In calculus notations, the system is for $z(x, y)$ satisfying

$$\frac{\partial^2 z}{\partial x^2} - \frac{\partial z}{\partial y} = 0, \qquad \frac{\partial^3 z}{\partial x^3} - \frac{\partial^2 z}{\partial y^2} = 0.$$

or

$$z_{xx} - z_y = 0, \qquad z_{xxx} - z_{yy} = 0.$$

- We cannot "solve" the system by direct integration.

Simple Rankings and Characteristic Sets

- Computing a **characteristic set** when $n = 1$ and $\mathcal{F} = \mathcal{C}$ is similar to computing a **Gröbner basis**. The set Δ plays the role of algebraic indeterminates. An **unmixed ranking** is analogous to a pure lex term ordering.
- Relative to an unmixed ranking where **every δ_1-derivative is higher than any δ_2-derivative**, a characteristic set of $\mathfrak{p} = [\delta_1^2 z - \delta_2 z, \quad \delta_1^3 z - \delta_2^2 z]$ is

$$\underline{\delta_1^2 z} - \delta_2 z, \quad \underline{\delta_1 \delta_2 z} - \delta_2^2 z, \quad \underline{\delta_2^3 z} - \delta_2^2 z,$$

  which has 3 elements.
- Relative to an unmixed ranking where **every δ_2-derivative is higher than any δ_1-derivative**, a characteristic set is

$$\underline{\delta_2 z} - \delta_1^2 z, \qquad \underline{\delta_1^4 z} - \delta_1^3 z.$$

- In either case, we obtain an linear ODE in z that we can integrate to find the general solution.

Differential Variety for $\mathfrak{p} = [\delta_2 z = \delta_1 z,\ \delta_1^4 z - \delta_1^3 z]$

- To find the general solution to $\mathfrak{p}$, **integrate** $\delta_1^4 z - \delta_1^3 z = 0$ three times with respect to δ_1.
- Writing $z = f(x, y)$ as a function in two variables, and $\delta_1 = \partial z/\partial x, \delta_2 = \partial z/\partial y$, we easily obtain first that $f(x, y) = c_1 x^2 + c_2 x + c_3 + c_4 e^x$**, where** c_1, c_2, c_3, c_4 **are undetermined functions of** y **alone**.
- **Substituting** this into the other equation and using the **linear independence** of $1, x, x^2, e^x$ over $\mathbb{Q}(y)$, we find that $c_1 = a, c_2 = b, c_3 = 2ay + c, c_4 = de^y$ with a, b, c, d arbitrary constants and obtain $f(x, y) = ax^2 + bx + c + 2ay + de^{x+y}$.
- The general solution depends only on (four) arbitrary functions of 0 variable (that is, constants). We say the **differential type** of $\mathfrak{p}$ is 0 and the **typical differential dimension** is 4.

The Algebraic Analog and Gröbner Basis

- The analogous algebraic ideal is $J = (x^2 - y, x^3 - y^2)$ in $\mathcal{C}[x, y]$, **which is not prime**: the polynomial $xy - y^2 \in J$ but not its factors.
- For the pure-lex term ordering with $x > y$, the Gröbner basis is $G_1 = \{ \underline{x^2} - y, \quad \underline{xy} - y^2, \quad \underline{y^3} - y^2 \}$. Compare this with:

$$\underline{\delta_1^2 z} - \delta_2 z, \quad \underline{\delta_1 \delta_2 z} - \delta_2^2 z, \quad \underline{\delta_2^3 z} - \delta_2^2 z.$$

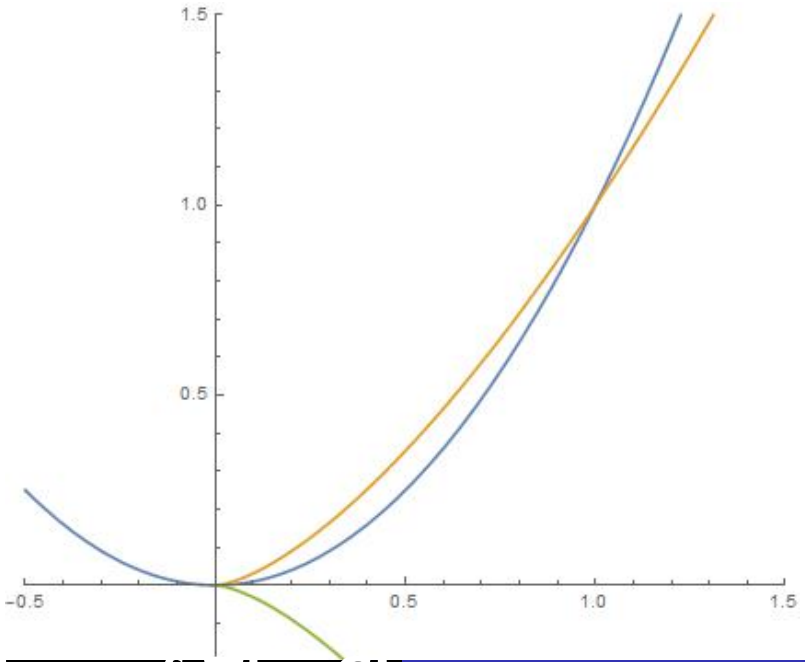
- For the pure-lex term ordering with $x < y$, the Gröbner basis is $G_2 = \{ \underline{y} - x^2, \quad \underline{x^4} - x^3 \}$ when $y > x$. Compare this with:

$$\underline{\delta_2 z} - \delta_1^2 z, \qquad \underline{\delta_1^4 z} - \delta_1^3 z.$$

- The algebraic variety consists of **four points** (counting multiplicity): (0,0), (0,0), (0,0), (1,1).

Similarity and Difference

- While the algebra (elimination) are similar between algebraic ideals and **linear** differential ideals **with constant coefficients**, the geometry is already very different. For non-linear differential ideals with coefficients from a differential field, the differential elimination process needs separate treatment.



Conventions and Notations

Differential Polynomials

Conventions and Notations

- All non-zero rings are **commutative, unitary, and contain** $\mathbb{Z}$. All fields have **characteristic zero**. All categories have a fixed finite or possibly countably infinite set of symbols $\Delta = \{ \delta_1, \ldots, \delta_m \}$, $m \in \mathbb{N}$ or $m = \aleph_0$, that **act on** the objects. For brevity and specificity, we use Δ-category, Δ-object, and Δ-morphisms. If $m = 0$, we may omit the prefix Δ.
- If Δ acts as **commutating derivations**, we may use the general adjectives **partial** and **differential** if $m \neq 0$, and **ordinary** and **differential** if $m = 1$, in place of the prefix Δ.
- For any Δ-object X, the subset of **constants**, which is again a Δ-object, is the set $X^\Delta := \{ x \in X \mid \delta x = 0 \ \forall \delta \in \Delta \}$.
- If $\mathcal{R}$ is a Δ-ring and $S \subseteq \mathcal{R}$, the **Δ-ideal generated by S** is denoted by $[S]$, and the **radical Δ-ideal generated by S** is denoted by $\{ S \}$ or $\sqrt{[S]}$.

Examples

- Any ring $\mathfrak{R}$ is a Δ-ring with $\delta a = 0$ for all $a \in \mathfrak{R}$ and all $\delta \in \Delta$.
- If $\mathbb{C}$ denotes the (differential) field of complex numbers, then $\mathfrak{F} = \mathbb{C}(\sin^2 x, \sin x \cos x)$ is an ordinary differential field with respect to the derivation $\delta = d/dx$ and $\mathfrak{F}^\Delta = \mathbb{C}$.
- If $\mathbf{k}$ is a field (or even just a ring), and X a finite or countably infinite set of symbols, the polynomial ring $\mathfrak{R} = \mathbf{k}[X]$ is a partial differential ring if $\Delta = \{ \partial/\partial x \mid x \in X \}$, and $\mathfrak{R}^\Delta = \mathbf{k}$.
- In case $\mathbf{k} = \mathbb{Z}$ and $X = \{ x \}$, the ideal $\mathfrak{a} = (2, 2x)$ of the δ-ring $\mathfrak{R} = \mathbb{Z}[x]$ is a proper δ-ideal, and the δ-ideal $[x] = \mathfrak{R}$.
- The ring $\mathbb{Z}[x, e^x]$ is δ-ring with $\delta = d/dx$ and (e^x) is a δ-ideal.

Differential Indeterminates and Notations

- We use $\Theta = M(\Delta)$ to denote the **free multiplicative monoid generated by** Δ. An element $\theta \in \Theta$ is called a **derivative operator** and has the form $\theta = \delta_1^{e_1} \cdots \delta_m^{e_m}$, where $e_1, \cdots, e_m \in \mathbb{N}$. The **order** of θ is $\operatorname{ord} \theta := e_1 + \cdots + e_m$. For $s \in \mathbb{N}$, $\Theta(s)$ is the set of derivative operators of order $\leqslant s$.
- For any Δ-object X, Θ acts on X by $\theta x = \delta_1^{e_1} \cdots \delta_m^{e_m} x$, $x \in X$.
- Let $n \in \mathbb{N}$ or $n = \aleph_0$. Let $\Theta Y = \{ y_{\theta,j} \}_{1 \leqslant j \leqslant n, \theta \in \Theta}$ be a family of symbols. The set Δ acts on ΘY by $\delta(y_{\theta,j}) = y_{\delta\theta,j}$, making ΘY a Δ-set. We call $y_j := y_{1,j}$ a **differential indeterminate**, and $\theta y_j := y_{\theta,j}$ a **(partia) derivative** (of y_j).
- The **order of a derivative** $u = \theta y_j$ is $\operatorname{ord} u := \operatorname{ord} \theta$.

Differential Polynomials and Notations

- Let $\mathcal{F}$ be a partial differential ring. The action of Δ on ΘY induces a unique action of Δ **as commutating derivations** on the polynomial ring $\mathcal{F}[\Theta Y]$, extending the Δ action on $\mathcal{F}$ and ΘY. The resulting Δ-ring $\mathcal{R}$ is denoted by $\mathcal{F}\{y_1, \cdots, y_n\}$ or $\mathcal{F}\{y_1, \cdots, y_n\}_\Delta$ and called the **differential polynomial ring in n differential indeterminates** $y_1, \cdots, y_n$.
- A **differential monomial** M is a finite power product of derivatives: $M = \prod_k (u_k)^{e_k}$, where $u_k := \theta_k y_{j_k}$ are usually distinct, but θ_k (or j_k) need not be distinct as k varies. The **order** of M is $\operatorname{ord} M := \max_k \operatorname{ord} \theta_k$.
- A **differential polynomial** or **Δ-polynomial** A is a finite linear combination $A = \sum_M a_M M$ of differential monomials M with coefficients a_M in $\mathcal{F}$. The **order** of A is $\operatorname{ord} A = \max_M \operatorname{ord} M$. Throughout, A could be a polynomial if either $m = 0$ ($\Delta = \emptyset$, the **algebraic case**) or $\operatorname{ord} A = 0$.

Polynomial Divisions

Ideal Membership as Simplification

Pseudo-Divisions and Triangular Sets

Divisions and Order in Multivariate Polynomials

- Let $\mathcal{K} = \mathcal{K}_0[v_1, \ldots, v_p]$, where $\mathcal{K}_0$ is a field. We have two types of division processes.
- **Normal division** proceeds by elimination of the **highest monomial** appearing in the dividend that is divisible by that in the divisor. Computation can be done using **rewriting rules** based on an **ordered monomial basis**, as in Gröbner basis computations.
- **Pseudo-division**, as done in the characteristic set methods, **chooses a main variable**, say v_p and view polynomials as univariate polynomials in v_p with coefficients now in a field $\mathcal{K}_0(v_1, \ldots, v_{p-1})$, and proceed to divide normally and afterwards clearing denominators in $\mathcal{K}_0(v_1, \ldots, v_{p-1})$.
- In repeated pseudo-division using different main variables, we need **an ordering of the main variables chosen**.

Ideal Membership Testing

- We replace $\mathcal{K}_0$ by an integral domain $\mathcal{S}_0$.
- Repeated division of F by a sequence of divisors $A_1, \ldots, A_k$, produces:

$$LF = Q_1 A_1 + \cdots + Q_k A_k + R$$

  where $L, Q_1, \ldots, Q_k, R \in \mathcal{S}_0[v_1, \ldots, , v_p]$ and $L \neq 0$.
- In repeated divisions, the final **pseudo-remainder** R (or **remainder** R if $L = 1$) depends on the division steps used.
- "remainder = zero" is a sufficient condition for membership of F in $(A_1, \ldots, A_k)$, but "pseudo-remainder = 0" only suffices to show membership of F in $(A_1, \ldots, A_k) : L$.
- **Division by a Gröbner Basis and Characteristic Set makes $R = 0$ a necessary condition.**
- The remainder (or pseudo-remainder) R is a simplification of F for membership problems.

Algebra Review: Triangular Sets and Notations

- A subset **A** of differential polynomials is **triangular** if its elements can be rearranged as $A_1, A_2, \ldots, A_k, \ldots$ such that each A_k involves at least one derivative $\theta_k y_{j_k}$ which does not appear in $A_1, \ldots, A_{k-1}$ (in particular, $A_1 \notin \mathcal{F}$). When such a rearrangement **and** derivatives are chosen, we write $\mathbf{A}: A_1, \ldots, A_k, \ldots$ (as an **ordered set**, instead of as a set $\mathbf{A} = \{A_1, \ldots, A_k, \ldots\}$) and say **A** is in **triangular form with respect to**, or **with main derivatives**, $\theta_1 y_{j_1}, \ldots, \theta_k y_{j_k}, \ldots$.
- Contrary to other definitions, at this time, **we do not require an ordering $\preceq$ of the derivatives** ΘY (nor of the Δ-indeterminates $y_1, \ldots, y_n$) be given, nor if $\preceq$ is given, that the ordering on A be compatible with $\preceq$, and even if it is, we do not require that the main derivative $\theta_k y_{j_k}$ of A_k be the highest derivative (called **leader**) in A_k relative to $\preceq$.

Examples of Triangular Sets

- Let $A_1 = \delta^2 y_2 + y_2$, $A_2 = \delta^2 y_2 + y_2^2 + y_3$, $A_3 = \delta^2 y_2 + y_1$ in $\mathcal{F}\{ y_1, y_2 \}_\delta$. Then the ordered set $\mathbf{A}$: A_1, A_2, A_3 is in triangular form with respect to y_2, y_3, y_1. The ordered set $\mathbf{A}$ is also in triangular form with main derivatives $\delta^2 y_2, y_3, y_1$. However, the re-ordered set $\mathbf{A}$: A_2, A_1, A_3 is *not* in triangular form.
- If we replace $\delta^2 y_2$ by y_4 and view $\mathbf{A} \subset \mathcal{F}[y_1, y_2, y_3, y_4]$ (that is as polynomials), and order the variables by $y_1 \prec y_2 \prec y_3 \prec y_4$, then the highest derivative (leader) for A_k (called its **main variable** in the algebraic case) is y_4 for all k, and the ordered set $\mathbf{A}$: A_1, A_2, A_3 is not triangular in the sense of say Aubry et. al. (the main variable of A_k must not appear in $A_1, \ldots, A_{k-1}$).
- Note, by definition, the main derivatives of a triangular set must be distinct even if the leaders are not.

Pseudo-division and Notations

- Let $\mathcal{S}_0$ be an integral domain, and v an indeterminate over $\mathcal{S}_0$. Let F, A be two polynomials in $\mathcal{S}_0[v]$ of respective non-zero degrees d_F and d_A. Let $e = \max(d_F - d_A + 1, 0)$.
- Write $A = I_{d_A} v^{d_A} + \cdots + I_1 v + I_0 \neq 0$, where $I_k \in \mathcal{S}_0$ for all k.
- We can compute unique polynomials $Q, R \in \mathcal{S}_0[v]$ such that

$$I_{d_A}^e F = QA + R, \quad \text{and } \deg(R) < \deg(A). \tag{2.5}$$

- The leading coefficient $I_{d_A} \in \mathcal{S}_0$ of A is called the **initial** of A **with respect to the variable** v. The unique polynomial $Q = Q(F, A, \mathcal{S}_0, v)$ is called the **pseudo-quotient** and $R = R(F, A, \mathcal{S}_0, v)$, the **pseudo-remainder** of F **with respect to** A. We will call $e = E(F, A, \mathcal{S}_0, v)$ the **pseudo-exponent**. **Any triple** (e, Q, R) that satisfies Eq.(2.5) will be called a **pseudo-division triple** of F by A over $\mathcal{S}_0$ with respect to v.

Some Remarks on Pseudo-Division

- $R(F, A, \mathcal{S}_0, v)$ is often simply written as $\operatorname{prem}(F, A)$. We emphasize the coefficient ring $\mathcal{S}_0$ and the univariate variable v.
- In general, $E(F, A, \mathcal{S}_0, v)$ need not be the least exponent among triples. For example, $E(A, A, \mathcal{S}_0, v) = 1$, not 0.
- The uniqueness of Q, R are subject to the predefined e.
- A triple (e, Q, R) can be easily computed (see Algorithm R, p. 369 of Knuth [22], or Cox et al. [15, Ch. 6,Sec. 5: Wu Method]).
- When A is linear in v, $E(F, A, \mathcal{S}_0, v) = \deg F$. To get Q and R, solve for v in $A = 0$, substitute the result for v in F and multiply by $I_1^{\deg F}$.
- More generally, one can divide F by A in $\mathcal{K}_0[v]$, where $\mathcal{K}_0$ is the quotient field of $\mathcal{S}_0$, and clear denominators.

Example Illustrating Pseudo-Division Algorithm

- In $\mathbb{Z}[v]$, let $F = 5v^2 + 3v$ and $A = 2v$. $I_A = 2$.
- Performing pseudo-division of F by A, we have first $2F = 10v^2 + 6v = 5v(2v) + 6v = 5v \cdot A + 6v$.
- Then pseudo-dividing $6v$ by A, we have $4F = 10v \cdot A + 6(2v) + 0 = (10v + 6)A + 0$.
- So $Q(F, A, \mathbb{Z}, v) = 10v + 6$, $R(F, A, \mathbb{Z}, v) = 0$ and $E(F, A, \mathbb{Z}, v) = 2 = \deg F$.
- Note that we could also have $2F = (5v + 3)A + 0$. Thus $(2, 10v + 6, 0)$ and $(1, 5v + 3, 0)$ are both pseudo-division triples of F by A over $\mathbb{Z}$ with respect to v.
- For **simultaneous pseudo-divisions of several polynomials** $F_1, \cdots, F_q$ by A, we can obtain a pseudo-division triple (e, Q_i, R_i) of F_i for each i with a **common exponent** e since the initial of A does not involve v.

Iterated Pseudo-Division by Sequence of Divisors

- Let $\mathcal{S}_0$ be an integral domain, and let $\mathcal{S} = \mathcal{S}_0[v_1, \ldots, v_p]$ be the polynomial ring over $\mathcal{S}_0$.
- Let $F \in \mathcal{S}$ and let $\mathbf{A}$: $A_1, \ldots, A_p$ be an (ordered) subset of $\mathcal{S}$ in triangular form with respect to $v_1, \ldots, v_p$.
- For $1 \leqslant k \leqslant p$, let d_k be the degree of A_k in v_k and let I_k be the initial of A_k with respect to v_k.
- Note that $A_k, \ldots, A_p$ is an (ordered) subset of $\mathcal{S}_0[v_1, \ldots, v_{k-1}][v_k, \ldots, v_p]$ triangular with respect to $v_k, \ldots, v_p$ over $\mathcal{S}_0[v_1, \ldots, v_{k-1}]$.

Iterated Pseudo-Division: Proposition 2.9

Proposition 2.9

We can compute, for each k, $1 \leqslant k \leqslant p$, *a natural number* e_k, *and polynomials* $R_k, Q_{k,k}, \ldots, Q_{k,p} \in \mathcal{S}$

$$I_k^{e_k} \cdots I_p^{e_p} F = Q_{k,k} \cdot A_k + \cdots + Q_{k,p} \cdot A_p + R_k, \qquad (2.9)$$

and $\deg_{v_j} R_k < d_j$ *for* $k \leqslant j \leqslant p$.

- Note for $k = 1$, with $Q_j = Q_{1,j}$, we have:

$$I_1^{e_1} \cdots I_p^{e_p} F = Q_1 \cdot A_1 + \cdots + Q_p \cdot A_p + R_1, \qquad (2.10)$$

- **If** $d_j = 1$ **for every** j**, then** $R_k \in \mathcal{S}_0[v_1, \ldots, v_{k-1}]$ **for every** k**; in particular,** $R_1 \in \mathcal{S}_0$**.**
- Proposition 2.9 is a revision of Proposition 2.9 in the paper. Eq. (2.9) is Eq. (2.10) applied to the triangular set $A_k, \ldots, A_p$.

Constructive Proof For Proposition 2.9

- Let $V = \{ v_1, \ldots, v_p \}$. For $1 \leqslant j \leqslant p$, let $V_j = V \backslash \{ v_j \}$.
- Let $R_{p+1} = F$. Inductively, for $p \geqslant k \geqslant 1$, let (e_k, Q'_k, R_k) be a pseudo-division triple for R_{k+1} by A_k over $\mathcal{S}_0[V_k]$ w.r.t. v_k.
- So $\deg_{v_j} Q'_k \leqslant \deg_{v_j} R_{k+1}$ for $k+1 \leqslant j \leqslant p$ and $I_k^{e_k} R_{k+1} = Q'_k A_k + R_k$ and $\deg_{v_k} R_k < d_k$.
- Inductively, if $\deg_{v_j} R_{k+1} < d_j$ for $k+1 \leqslant j \leqslant p$, then $\deg_{v_j} R_k < d_j$ for $k \leqslant j \leqslant p$.
- For $k \leqslant j \leqslant p$, let $Q_{k,j} = Q'_j \prod_{i=k}^{j-1} I_i^{e_i} = I_k^{e_k} \cdots I_{j-1}^{e_{j-1}} Q'_j$. Then

$$\begin{aligned}
I_k^{e_k} \cdots I_p^{e_p} R_{p+1} &= I_k^{e_k} \cdots I_{p-1}^{e_{p-1}} (Q'_p A_p + R_p) \\
&= Q_{k,p} A_p + I_k^{e_k} \cdots I_{p-1}^{e_{p-1}} R_p \\
&= Q_{k,p} A_p + I_k^{e_k} \cdots I_{p-2}^{e_{p-2}} (Q'_{p-1} A_{p-1} + R_{p-1}) \\
&= Q_{k,p} A_p + Q_{k,p-1} A_{p-1} + I_k^{e_k} \cdots I_{p-2}^{e_{p-2}} R_{p-1} \\
&= Q_{k,p} A_p + Q_{k,p-1} A_{p-1} + \cdots + Q_{k,k} A_k + R_k,
\end{aligned}$$

There is nothing unique in Eq.(2.10)

- We have $I_k^{e_k} \cdots I_p^{e_p} F \in (\mathbf{A})_{\mathcal{S}}$ **if and only** $R_k \in (\mathbf{A})_{\mathcal{S}}$. However, R_1 **need not be 0 even if** $F \in (\mathbf{A})_{\mathcal{S}}$.
- Let's "divide" (using repeated subtractions) 3275 by 15 and 10 in two ways.
- **First way**:

  (a). 3275 = 200*15 + 275
  (b). 275 = 20*10 + 75
  (c). 75 = 5*15 + 0

- **Second way**:

  (a). 3275 = 300*10 + 275
  (b). 275 = 10*15 + 125
  (c). 125 = 10*10 + 25
  (d). 25 = 2*10 + 5

Comments on Iterated Pseudo-Division Algorithm

- **A pseudo-remainder sequence (PRS) for F w.r.t. A** is a successive sequence of pseudo-remainders $R_p, \ldots, R_1$ as constructed in the proof, starting with $R_{p+1} = F$. **A pseudo-remainder of F w.r.t. A** is *any* R_1 satisfying the property in Eq. (2.10) for some $Q_1, \ldots, Q_p \in \mathcal{S}_p$ and some $e_1, \ldots, e_p \in \mathbb{N}$, as the last pseudo-remainder in a sequence.
- One choice of a PRS is to use $E(R_{k+1}, A_k, \mathcal{S}_0[V_k], v_k)$ for the k-th pseudo-exponent at each stage, resulting in **the default PRS**, and R_1 as **the default pseudo-remainder**.
- The exponent e_k in Eq.(2.10) do not just depend on F and the degree d_k, but also on the degrees of R_{k+1} and of I_{k+1}.
- In theory, it is easier to deal coefficients in a field, but computing in the quotient field of an integral domain is far more expensive than computing in the integral domain.

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 $\mathcal{S}'_0$.