An Equivalence Theorem for Regular Differential Chains

François Boulier
University of Lille, CRIStAL, France

CIMPA School: *Algebraic and Tropical Methods for Solving Differential Equations*

June 17, 2023

Overview

This talk aims at stating an equivalence theorem for regular differential chains

Regular differential chains are particular cases of regular chains, which are particular cases of triangular sets

We start with a triangular set A and investigate the properties of the ideal $(A) : I_A^\infty$ that it defines

$A = \{p_1, \ldots, p_r\}$ triangular set of $\mathscr{F}\{y_1, \ldots, y_n\}$

$x_1, \ldots, x_r$ leading variables/derivatives of the elements of A

$t_1, \ldots, t_m$ the other derivatives occuring in the elements of A

We view A as a triangular set of $\mathscr{F}[x_1, \ldots, x_r, t_1, \ldots, t_m]$

$i_1, \ldots, i_r$ the initials and $I_A = i_1 \cdots i_r$ their product

Example of triangular set

$$A \left\{ \begin{array}{lcl} (x_1 - t_1)\, x_3 - 1 & = & 0 \\ x_1\, x_2 - t_1 & = & 0 \\ (x_1 - t_2)\,(x_1 - t_1) & = & 0 \end{array} \right.$$

Here $I_A = x_1\,(x_1 - t_1)$

The Pseudoremainder by a Triangular Set

If f is a polynomial, denoting $x = x_k$,

$$f = f_e\, x^e + \cdots + f_1\, x + f_0 \qquad p_k = i_k\, x^{d_k} + \cdots + p_{k,1}\, x + p_{k,0}$$

Then there exist $q, g \in \mathscr{R}[x]$ with such that

$$i_k^{e-d_k+1}\, f = q\, p + g \quad (\deg(g, x) < d_k)$$

$g = \mathrm{prem}(f, p_k, x_k)$ is the pseudoremainder of f by p w.r.t. x_k

The Pseudoremainder by a Triangular Set

$\mathrm{prem}(f, p_k, x_k)$ is the pseudoremainder of f by p w.r.t. x_k

The Pseudoremainder by a Triangular Set

$\mathrm{prem}(f, p_k, x_k)$ is the pseudoremainder of f by p w.r.t. x_k

Def (pseudoremainder of f with respect to triangular set A)

$$\mathrm{prem}(f, A) \quad = \quad \begin{cases} \mathrm{prem}(f, p_1, x_1) & (r = 1) \\ \mathrm{prem}(\mathrm{prem}(f, p_r, x_r), A') & (A' = A \setminus \{p_r\}) \end{cases}$$

Note If $g = \mathrm{prem}(f, A)$ there exists a power product h of initials of A s.t.

$$h\,f \quad = \quad g \quad \mathrm{mod}\ (A)$$

The Pseudoremainder by a Triangular Set

Def (pseudoremainder of f with respect to triangular set A)

$$\operatorname{prem}(f, A) = \begin{cases} \operatorname{prem}(f, p_1, x_1) & (r = 1) \\ \operatorname{prem}(\operatorname{prem}(f, p_r, x_r), A') & (A' = A \setminus \{p_r\}) \end{cases}$$

Note If $g = \operatorname{prem}(f, A)$ there exists a power product h of initials of A s.t.

$$h\,f = g \mod (A)$$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

The Pseudoremainder by a Triangular Set

Def (pseudoremainder of f with respect to triangular set A)

$$\operatorname{prem}(f, A) = \begin{cases} \operatorname{prem}(f, p_1, x_1) & (r = 1) \\ \operatorname{prem}(\operatorname{prem}(f, p_r, x_r), A') & (A' = A \setminus \{p_r\}) \end{cases}$$

Note If $g = \operatorname{prem}(f, A)$ there exists a power product h of initials of A s.t.

$$h\,f = g \mod (A)$$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

Prop If $g = 0$ then $f \in (A) : I_A^\infty$

The Pseudoremainder by a Triangular Set

Def (pseudoremainder of f with respect to triangular set A)

$$\operatorname{prem}(f, A) = \begin{cases} \operatorname{prem}(f, p_1, x_1) & (r = 1) \\ \operatorname{prem}(\operatorname{prem}(f, p_r, x_r), A') & (A' = A \setminus \{p_r\}) \end{cases}$$

Note If $g = \operatorname{prem}(f, A)$ there exists a power product h of initials of A s.t.

$$h f = g \mod (A)$$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Prop If $g = 0$ then $f \in (A) : I_A^\infty$

Example Assume $i_1^3\, i_2^7\, f = 0 \mod (A)$

The Pseudoremainder by a Triangular Set

Def (pseudoremainder of f with respect to triangular set A)

$$\mathrm{prem}(f, A) \quad = \quad \begin{cases} \mathrm{prem}(f, p_1, x_1) & (r = 1) \\ \mathrm{prem}(\mathrm{prem}(f, p_r, x_r), A') & (A' = A \setminus \{p_r\}) \end{cases}$$

Note If $g = \mathrm{prem}(f, A)$ there exists a power product h of initials of A s.t.

$$h\,f \quad = \quad g \quad \mathrm{mod}\ (A)$$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ \ I_A^d\, f \in (A)\}$

Prop If $g = 0$ then $f \in (A) : I_A^\infty$

Example Assume $i_1^3\, i_2^7\, f = 0 \mod (A)$
Then $i_1^7\, i_2^7\, f = I_A^7\, f = 0 \mod (A)$

The Pseudoremainder by a Triangular Set

Def (pseudoremainder of f with respect to triangular set A)

$$\operatorname{prem}(f, A) = \begin{cases} \operatorname{prem}(f, p_1, x_1) & (r = 1) \\ \operatorname{prem}(\operatorname{prem}(f, p_r, x_r), A') & (A' = A \setminus \{p_r\}) \end{cases}$$

Note If $g = \operatorname{prem}(f, A)$ there exists a power product h of initials of A s.t.

$$h\,f = g \mod (A)$$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

Prop If $g = 0$ then $f \in (A) : I_A^\infty$

Example Assume $i_1^3\, i_2^7\, f = 0 \mod (A)$
Then $i_1^7\, i_2^7\, f = I_A^7\, f = 0 \mod (A)$
Then $f \in (A) : I_A^\infty$

Relationship with $A = 0,\ I_A \neq 0$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Prop If $f \in (A) : I_A^\infty$ then f vanishes at every zero of

$$A = 0, \qquad I_A \neq 0.$$

Relationship with $A = 0, \ I_A \neq 0$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0, \ I_A^d \, f \in (A)\}$

Prop If $f \in (A) : I_A^\infty$ then f vanishes at every zero of

$$A = 0 \,, \qquad I_A \neq 0 \,.$$

Proof Assume $f \in (A) : I_A^\infty$ i.e. there exist polynomials q_i and a power product h of initials of elements of A such that

$$h\,f = q_1\,p_1 + \cdots + q_r\,p_r$$

If $p_1 = \cdots = p_r = 0$ and $h \neq 0$ then $f = 0$

Conversely In most contexts, when solving a triangular system, we are supposed to seek solutions which annihilate A but not I_A

Possibly Empty Solution Set

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

It may happen $1 \in (A) : I_A^\infty$ i.e. that the following system has no solution

$$A = 0\,, \qquad I_A \neq 0\,.$$

Consider the triangular system

$$A \begin{cases} (x_1 - t_1)\, x_3 - 1 & = & 0 \\ x_1\, x_2 - 1 & = & 0 \\ x_1\,(x_1 - t_1) & = & 0 \end{cases}$$

Possibly Empty Solution Set

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

It may happen $1 \in (A) : I_A^\infty$ i.e. that the following system has no solution

$$A = 0, \qquad I_A \neq 0.$$

Consider the triangular system

$$A \begin{cases} (x_1 - t_1)\, x_3 - 1 & = & 0 \\ x_1\, x_2 - 1 & = & 0 \\ x_1\, (x_1 - t_1) & = & 0 \end{cases}$$

Possibly Empty Solution Set

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

It may happen $1 \in (A) : I_A^\infty$ i.e. that the following system has no solution

$$A = 0\,, \qquad I_A \neq 0\,.$$

Consider the triangular system

$$A \left\{ \begin{array}{rcl} (x_1 - t_1)\, x_3 - 1 & = & 0 \\ x_1\, x_2 - 1 & = & 0 \\ x_1\, (x_1 - t_1) & = & 0 \end{array} \right.$$

A is not a Basis of $(A) : I_A^\infty$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

$$A \left\{ \begin{array}{lcl} t_1\, {x_3}^2 - x_2^2 - t_1 & = & 0 \\ {x_2}^3 - t_1^2 & = & 0 \\ x_1 & = & 0 \end{array} \right.$$

A Gröbner basis of $(A) : I_A^\infty$ can be computed by the Rabinovitch trick

$$(A) : I_A^\infty \;=\; (A,\ I_A\, z - 1) \cap \mathscr{R} \;=\; \begin{array}{r} (x_1, \\ x_2^3 - t_1^2, \\ t_1^2\, x_3^2 - x_2^2 - t_1, \\ t_1\, x_2\, x_3^2 - t_1 - x_2, \\ x_2^2\, x_3^2 - t_1\, x_3^2 - x_2 + 1)\,. \end{array}$$

Where is Charlie?

A is not a Basis of $(A) : I_A^\infty$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

$$A \begin{cases} t_1\, {x_3}^2 - x_2^2 - t_1 & = & 0 \\ {x_2}^3 - t_1^2 & = & 0 \\ x_1 & = & 0 \end{cases}$$

A Gröbner basis of $(A) : I_A^\infty$ can be computed by the Rabinovitch trick

$$(A) : I_A^\infty \;=\; (A,\ I_A\, z - 1) \cap \mathscr{R} \;=\; \begin{aligned}(x_1,\\ x_2^3 - t_1^2,\\ t_1^2\, x_3^2 - x_2^2 - t_1,\\ t_1\, x_2\, x_3^2 - t_1 - x_2,\\ x_2^2\, x_3^2 - t_1\, x_3^2 - x_2 + \boxed{1}\,).\end{aligned}$$

Actually,

$$(A) \;=\; (A) : I_A^\infty \cap (x_2,\ x_1,\ t_1)\,.$$

A is not a Basis of $(A) : I_A^\infty$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

$$A \left\{ \begin{array}{lcl} t_1\, {x_3}^2 - x_2^2 - t_1 & = & 0 \\ {x_2}^3 - t_1^2 & = & 0 \\ x_1 & = & 0 \end{array} \right.$$

A Gröbner basis of $(A) : I_A^\infty$ can be computed by the Rabinovitch trick

$$(A) : I_A^\infty \;=\; (A,\, I_A\, z - 1) \cap \mathscr{R} \;=\; \begin{array}{r} (x_1, \\ x_2^3 - t_1^2, \\ t_1^2\, x_3^2 - x_2^2 - t_1, \\ t_1\, x_2\, x_3^2 - t_1 - x_2, \\ x_2^2\, x_3^2 - t_1\, x_3^2 - x_2 + \boxed{1}). \end{array}$$

Remark Looking at triangular sets, it is not obvious that

$$(A) : I_A^\infty \;\not\subset\; (x_2,\ x_1,\ t_1)\,.$$

A is not a Basis of $(A) : I_A^\infty$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

$$A \left\{ \begin{array}{lcl} t_1\, {x_3}^2 - x_2^2 - t_1 & = & 0 \\ {x_2}^3 - t_1^2 & = & 0 \\ x_1 & = & 0 \end{array} \right.$$

A Gröbner basis of $(A) : I_A^\infty$ can be computed by the Rabinovitch trick

$$(A) : I_A^\infty \;=\; (A,\, I_A\, z - 1) \cap \mathscr{R} \;=\; \begin{array}{r} (x_1, \\ x_2^3 - t_1^2, \\ t_1^2\, x_3^2 - x_2^2 - t_1, \\ t_1\, x_2\, x_3^2 - t_1 - x_2, \\ x_2^2\, x_3^2 - t_1\, x_3^2 - x_2 + \boxed{1}\,)\,. \end{array}$$

Remark In the differential case, no algorithm is known to decide inclusion of differential ideals presented by characteristic sets/regular differential chains

Another Definition — Regularity

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Other definition via the localized ring $I_A^{-1}\mathscr{R}$

$$(A) : I_A^\infty = I_A^{-1}(A) \cap \mathscr{R}$$

When localizing, beware to zerodivisors (= non regular) elements

In $\mathbb{Z}/6\mathbb{Z}$ we have

$$2 \times 3 \quad = \quad 0$$

If we introduce $\frac{1}{2}$ then we get a wrong conclusion

$$\frac{1}{2} \times 2 \times 3 \quad = \quad 3 \quad = \quad 0$$

Initials Are Regular modulo $(A) : I_A^\infty$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Prop The initials of the elements of A are regular (= non zerodivisors) modulo $(A) : I_A^\infty$

Initials Are Regular modulo $(A) : I_A^\infty$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

Prop The initials of the elements of A are regular (= non zerodivisors) modulo $(A) : I_A^\infty$

Proof Let h be a power product of initials and f be such that

$$h\,f \quad = \quad 0 \quad \bmod (A) : I_A^\infty$$

i.e. such that

$$h\,f \in (A) : I_A^\infty$$

Initials Are Regular modulo $(A) : I_A^\infty$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d\, f \in (A)\}$

Prop The initials of the elements of A are regular (= non zerodivisors) modulo $(A) : I_A^\infty$

Proof Let h be a power product of initials and f be such that

$$h\,f \quad = \quad 0 \quad \bmod (A) : I_A^\infty$$

i.e. such that

$$h\,f \in (A) : I_A^\infty$$

Then

$$f \in (A) : I_A^\infty$$

i.e.

$$f \quad = \quad 0 \quad \bmod (A) : I_A^\infty$$

Summary $h\,f = 0 \Rightarrow f = 0$ thus h is regular modulo $(A) : I_A^\infty$

Regular Chains — Overview

Regular chains are triangular sets the initials of which satisfy a stronger regularity condition

Regularity testing can be decided by means of resultant computations

An equivalence theorem for regular chains is stated

In the differential case, the separants are the initials of the proper derivatives of the regular chain elements

This leads us to squarefree regular chains

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

The initials of the elements of A are regular modulo $(A) : I_A^\infty$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Triangular set A is not a regular chain

$$A \left\{ \begin{array}{lcl} (x_1 - t_1)\, x_2 - 1 & = & 0 \\ x_1\,(x_1 - t_1) & = & 0 \end{array} \right.$$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Triangular set A is not a regular chain

$$A \left\{ \begin{array}{lcl} (x_1 - t_1)\, x_2 - 1 & = & 0 \\ x_1\,(x_1 - t_1) & = & 0 \end{array} \right.$$

Proof Consider the initial $x_1 - t_1$ of p_2. We have

$$x_1 \quad \neq \quad 0 \quad \mathrm{mod}\ (x_1\,(x_1 - t_1))$$

However $x_1\,(x_1 - t_1) \quad = \quad 0 \ \ \mathrm{mod}\ (x_1\,(x_1 - t_1))$
proving that $x_1 - t_1$ is a zerodivisor modulo $(x_1\,(x_1 - t_1))$

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Triangular set A is **not a regular chain**

$$A \left\{ \begin{array}{lcl} (x_1 - t_1)\, x_2 - 1 & = & 0 \\ x_1\, (x_1 - t_1) & = & 0 \end{array} \right.$$

Indeed, the initial $x_1 - t_1$ and p_1 have a common factor

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Triangular set A is not a regular chain

$$A \begin{cases} (x_1 - t_1)\, x_2 - 1 & = & 0 \\ x_1\, (x_1 - t_1) & = & 0 \end{cases}$$

Indeed, the initial $x_1 - t_1$ and p_1 have a common factor
Indeed, the resultant of the initial and p_1 is zero

$$\mathrm{res}(x_1 - t_1, p_1, x_1) \quad = \quad 0$$

Prop If $\mathscr{R}$ is a domain and $\mathscr{G}$ is its fraction field, $\mathrm{res}(f, p, x) = 0$ if and only if $f, g \in \mathscr{R}[x]$ have a common factor in $\mathscr{G}[x]$

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Is triangular set A a regular chain?

$$A \begin{cases} (x_2 - t_1)\, x_3 - 1 & = & 0 \\ x_2\,(x_2 - t_1) + x_1 & = & 0 \\ x_1 & = & 0 \end{cases}$$

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Is triangular set A a regular chain?

$$A \left\{ \begin{array}{lcl} (x_2 - t_1)\, x_3 - 1 & = & 0 \\ x_2\,(x_2 - t_1) + x_1 & = & 0 \\ x_1 & = & 0 \end{array} \right.$$

No!

The initial $x_2 - t_1$ and p_2 have a common factor modulo (x_1)

The initial $x_2 - t_1$ is a zerodivisor modulo (p_1, p_2)

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Triangular set A is **not a regular chain**

$$A \left\{ \begin{array}{lcl} (x_2 - t_1)\, x_3 - 1 & = & 0 \\ x_2\,(x_2 - t_1) + x_1 & = & 0 \\ x_1 & = & 0 \end{array} \right.$$

We actually have

$$\mathrm{res}(x_2 - t_1, p_2, x_2) \;=\; x_1$$

Idea More generally, the resultant of two polynomials gives a condition for the two polynomials to have a common factor

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Triangular set A is **not a regular chain**

$$A \left\{ \begin{array}{lcl} (x_2 - t_1)\, x_3 - 1 & = & 0 \\ x_2\,(x_2 - t_1) + x_1 & = & 0 \\ x_1 & = & 0 \end{array} \right.$$

We actually have

$$\underbrace{\mathrm{res}(\mathrm{res}(x_2 - t_1, p_2, x_2), p_1, x_1)}_{\mathrm{res}(x_2 - t_1, A)} \quad = \quad 0$$

Regular Chains

Ideal defined by A $(A) : I_A^{\infty} = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Triangular set A is **not a regular chain**

$$A \begin{cases} (x_2 - t_1)\, x_3 - 1 & = & 0 \\ x_2\,(x_2 - t_1) + x_1 & = & 0 \\ x_1 & = & 0 \end{cases}$$

Def (resultant of f with respect to triangular set A)

$$\mathrm{res}(f, A) \quad = \quad \begin{cases} \mathrm{res}(f, p_1, x_1) & (r = 1) \\ \mathrm{res}(\mathrm{res}(f, p_r, x_r), A') & (A' = A \setminus \{p_r\}) \end{cases}$$

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Is triangular set A a regular chain?

$$A \left\{ \begin{array}{lcl} (x_1 - 1)\, x_2 - 1 & = & 0 \\ x_1\,(x_1 - t_1) & = & 0 \end{array} \right.$$

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Is triangular set A a regular chain?

$$A \left\{ \begin{array}{lcl} (x_1 - 1)\, x_2 - 1 & = & 0 \\ x_1\,(x_1 - t_1) & = & 0 \end{array} \right.$$

Let us compute the resultant

$$\mathrm{res}(x_1 - 1, A, x_1) \quad = \quad t_1 - 1$$

Okay. $t_1 - 1$ is regular modulo (0)
Does this prove $x_1 - 1$ is regular modulo (p_1)?

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Triangular set A **is a regular chain**

$$A \left\{ \begin{array}{lcl} (x_1 - 1)\, x_2 - 1 & = & 0 \\ x_1\,(x_1 - t_1) & = & 0 \end{array} \right.$$

Let us compute the resultant

$$\mathrm{res}(x_1 - 1, p_1, x_1) \quad = \quad t_1 - 1$$

Okay. $t_1 - 1$ is regular modulo (0)
Does this prove $x_1 - 1$ is regular modulo (p_1)?
Yes, but this is not completely obvious ($\simeq$ technical part in proofs).

Regular Chains

Ideal defined by A $(A) : I_A^\infty = \{f \in \mathscr{R} \mid \exists d \geq 0,\ I_A^d f \in (A)\}$

Def A triangular set $A = \{p_1, \ldots, p_r\}$ is a *regular chain* if each initial i_k is regular modulo the ideal defined by $\{p_1, \ldots, p_{k-1}\}$

Triangular set A **is a regular chain**

$$A \left\{ \begin{array}{lcl} (x_1 - 1)\, x_2 - 1 & = & 0 \\ x_1\,(x_1 - t_1) & = & 0 \end{array} \right.$$

Regular chains can be solved from bottom up

1. Pick a value for t_1
2. Get a value for x_1 using any of the two factors
3. If $p_2 = 0$ becomes inconsistent then change t_1 and restart

Idea When solving from bottom up, at each stage k, every factor of p_k eventually leads to a solution but maybe not for every value of the t variables. In particular $A = 0,\ I_A \neq 0$ always has solutions.

The Equivalence Theorem

Thm The following conditions are equivalent:

1. A is a regular chain
2. $\text{res}(i_k, A) \neq 0$ for $2 \leq k \leq r$
3. $f \in (A) : I_A^\infty$ if and only if $\text{prem}(f, A) = 0$
4. f is a zero divisor modulo $(A) : I_A^\infty$ if and only if $\text{res}(f, A) = 0$

Corollary Nonzero elements of $\mathscr{F}[t_1, \ldots, t_m]$ are regular modulo $(A) : I_A^\infty$

Why?

The Equivalence Theorem

Thm The following conditions are equivalent:

1. A is a regular chain
2. $\mathrm{res}(i_k, A) \neq 0$ for $2 \leq k \leq r$
3. $f \in (A) : I_A^\infty$ if and only if $\mathrm{prem}(f, A) = 0$
4. f is a zero divisor modulo $(A) : I_A^\infty$ if and only if $\mathrm{res}(f, A) = 0$

Corollary Nonzero elements of $\mathscr{F}[t_1, \ldots, t_m]$ are regular modulo $(A) : I_A^\infty$

Why?

By 4 and the fact that they are equal to their own resultant w.r.t. A

Indeed, the Corollary is true for general triangular sets

The Equivalence Theorem

Thm The following conditions are equivalent:

1. A is a regular chain
2. $\mathrm{res}(i_k, A) \neq 0$ for $2 \leq k \leq r$
3. $f \in (A) : I_A^\infty$ if and only if $\mathrm{prem}(f, A) = 0$
4. f is a zero divisor modulo $(A) : I_A^\infty$ if and only if $\mathrm{res}(f, A) = 0$

Corollary Nonzero elements of $\mathscr{F}[t_1, \ldots, t_m]$ are regular modulo $(A) : I_A^\infty$

$$A \left\{ \begin{array}{lcl} (x_1 - 1)\, x_2 - 1 & = & 0 \\ x_1\,(x_1 - t_1) & = & 0 \end{array} \right.$$

Thus a primary decomposition of $(A) : I_A^\infty$ can be computed over $\mathscr{F}(t_1)$

$$A_1 \left\{ \begin{array}{lcl} (x_1 - 1)\, x_2 - 1 & = & 0 \\ x_1 & = & 0 \end{array} \right. \qquad A_2 \left\{ \begin{array}{lcl} (x_1 - 1)\, x_2 - 1 & = & 0 \\ x_1 - t_1 & = & 0 \end{array} \right.$$

Squarefree Regular Chains

Def A regular chain $A = \{p_1, \ldots, p_r\}$ is *squarefree* if each separant $s_k = \partial p_k / \partial x_k$ is regular modulo the ideal defined by $\{p_1, \ldots, p_k\}$

Remark A is squarefree if $\operatorname{res}(s_k, A) \neq 0$ for each k (Eqv Thm)

$H_A = i_1 \cdots i_r \, s_1 \cdots s_r$ the product of the initials and separants of A

Thm If A is a squarefree, $(A) : I_A^\infty$ is radical and is equal to $(A) : H_A^\infty$

Def A regular chain $A = \{p_1, \ldots, p_r\}$ is *squarefree* if each separant $s_k = \partial p_k / \partial x_k$ is regular modulo the ideal defined by $\{p_1, \ldots, p_k\}$

Remark A is squarefree if $\mathrm{res}(s_k, A) \neq 0$ for each k (Eqv Thm)

Thm If A is a squarefree, $(A) : I_A^\infty$ is radical and is equal to $(A) : H_A^\infty$

Is the singleton $\{p_1\}$ a regular chain? a squarefree regular chain?

$$
\begin{aligned}
p_1 &= x_1\,(x_1 - t_1)\,(t_1\,x_1 - t_2)^2 \\
s_1 &= (t_1\,x_1 - t_2)\,(\textit{some polynomial})
\end{aligned}
$$

Squarefree Regular Chains

Def A regular chain $A = \{p_1, \ldots, p_r\}$ is *squarefree* if each separant $s_k = \partial p_k / \partial x_k$ is regular modulo the ideal defined by $\{p_1, \ldots, p_k\}$

Remark A is squarefree if $\mathrm{res}(s_k, A) \neq 0$ for each k (Eqv Thm)

Thm If A is a squarefree, $(A) : I_A^\infty$ is radical and is equal to $(A) : H_A^\infty$

The singleton $\{p_1\}$ is a **regular chain** but **not squarefree**

$$\begin{aligned} p_1 &= x_1\,(x_1 - t_1)\,(t_1\,x_1 - t_2)^2 \\ s_1 &= (t_1\,x_1 - t_2)\,(\textit{some polynomial}) \end{aligned}$$

The common factors of p_1 and s_1 are the multiple factors of p_1
The separant s_1 is a zerodivisor modulo (p_1)

Squarefree Regular Chains

Def A regular chain $A = \{p_1, \ldots, p_r\}$ is *squarefree* if each separant $s_k = \partial p_k / \partial x_k$ is regular modulo the ideal defined by $\{p_1, \ldots, p_k\}$

Remark A is squarefree if $\mathrm{res}(s_k, A) \neq 0$ for each k (Eqv Thm)

Thm If A is a squarefree, $(A) : I_A^\infty$ is radical and is equal to $(A) : H_A^\infty$

The singleton $\{p_1\}$ is a **regular chain** but **not squarefree**

$$\begin{aligned} p_1 &= x_1\,(x_1 - t_1)\,(t_1\,x_1 - t_2)^2 \\ s_1 &= (t_1\,x_1 - t_2)\,(\textit{some polynomial}) \end{aligned}$$

Note that the ideal $(p_1) : s_1^\infty$ is radical anyway

$$(p_1) : s_1^\infty = x_1\,(x_1 - t_1)$$

Indeed, if A is any triangular set then $(A) : H_A^\infty$ is radical (Lazard's Lemma)

Regular Differential Chains

Rosenfeld's Lemma restates, in ideal theoretic terms, the properties of the differential systems $A = 0,\ H_A \neq 0$ for which every "non differential zero" can be prolongated to a differential one (Lecture 2)

Combined with Lazard's Lemma, it implies that differential ideals $[A] : H_A^\infty$ are radical

regular differential chains are triangular sets which satisfy the hypotheses of Rosenfeld's Lemma and are squarefree regular chains

An equivalence theorem for regular differential chains is stated

The relationship between regular differential chains and Ritt's characteristic sets is discussed

Rosenfeld's Lemma and a Consequence of Lazard's Lemma

$\mathscr{F}\{y_1, \ldots, y_n\}$

$A = \{p_1, \ldots, p_r\}$ triangular

$\mathscr{R}_1$ the ring of the differential polynomials partially reduced w.r.t. A

Assume the elements of A pairwise partially reduced and A coherent. Then

Prop (Rosenfeld's Lemma)

$$[A] : H_A^\infty \cap \mathscr{R}_1 \quad = \quad (A) : H_A^\infty$$

Prop The differential ideal $[A] : H_A^\infty$ is radical

Regular Differential Chains

$\mathscr{F}\{y_1, \ldots, y_n\}$

Def A *regular differential chain* is a squarefree regular chain which is coherent and made of pairwise partially reduced polynomials

Thm If A is coherent and made of pairwise partially reduced polynomials then the following conditions are equivalent

1. A is a regular differential chain,
2. for each k we have $\operatorname{res}(i_k, A) \neq 0$ and $\operatorname{res}(s_\ell, A) \neq 0$,
3. $f \in [A] : H_A^\infty$ if and only if $\operatorname{fullrem}(f, A) = 0$ (Ritt's full remainder),
4. f is a zerodivisor modulo $[A] : H_A^\infty$ if and only if $\operatorname{res}(\operatorname{partialrem}(f, A), A) = 0$ (resultant of Ritt's partial remainder).

Specification of the Differential Elimination Algorithm

Given an input system Σ and a ranking, it is possible to compute an equivalent set of finitely many regular differential chains

$$A_1, \ldots, A_\varrho$$

Recall from Lecture 2 If this decomposition is empty ($\varrho = 0$) then $1 \in \{\Sigma\}$ (the perfect differential ideal) and Σ has no solution at all

If this decomposition is nonempty ($\varrho > 0$) then every non differential zero of

$$A_i = 0\,, \qquad H_{A_i} \neq 0$$

can be prolongated into a differential zero of Σ

Hence there exist initial values for which Σ has formal power series solutions

Specification of the Differential Elimination Algorithm

Given an input system Σ and a ranking, it is possible to compute an equivalent set of finitely many regular differential chains

$$A_1, \ldots, A_\varrho$$

In ideal theoretic terms we have

$$\{\Sigma\} \quad = \quad [A_1] : H_{A_1}^{\infty} \cap \cdots \cap [A_\varrho] : H_{A_\varrho}^{\infty}$$

This decomposition permits to decide membership to $\{\Sigma\}$

It is not minimal: no algoritm is known to decide inclusion between the ϱ components

For this reason, it does not permit to decide regularity modulo $\{\Sigma\}$

Relationship With Characteristic Sets

Ritt defines the characteristic sets of a set of differential polynomials Σ as minimal elements among some subsets of Σ for some ordering on sets

Ritt proves that *every* set has characteristic sets and deduces important theorems such as the Basis Theorem

If Σ is a prime differential ideal then any characteristic set A of Σ is a regular differential chain and $\Sigma = [A] : H_A^\infty$. Conversely, up to some minor degree condition, every regular differential chain A such that $[A] : H_A^\infty$ is prime is a characteristic set of $[A] : H_A^\infty$. Ritt used characteristic sets for differential polynomial system solving via a decomposition in prime ideals

If Σ is not prime, its characteristic sets are not regular differential chains (in general) and cannot be used for differential polynomial system solving

In summary, for differential polynomial system solving, regular differential chains are the right generalization of characteristic sets. They can be used without testing the primality of the ideal they define

History

The founding text is Ritt's *Differential Algebra*, which introduces characteristic sets, even in the non differential case

The first mention of *regular chains* seems to go back to Kalkbrener in 1991

The regular chains theory has then a long and complicated history (incomplete proofs, partial results, interlaced study of the differential and non differential case)

The proof of the equivalence theorem in *An Introduction to Differential Algebra* (the lecture notes) is new and the simplest one I know