On *DifferentialAlgebra* and Kolchin's Irreducibility Theorem

François Boulier, David Bourqui, François Lemaire, Adrien Poteaux

June 4, 2023

Context

DifferentialAlgebra is a software project hosted at

`codeberg.org/francois.boulier/DifferentialAlgebra`

It contains the BLAD libraries (C code, embedded in the Maple *DifferentialAlgebra* package) and the BMI interface library

A new *DifferentialAlgebra* package has been developed on top of Python/sympy (demo at the end of the talk)

There is a *gallery* directory to show casual visitors what is the point
New examples welcome!

[Kolchin 1973, Chap. IV, Prop. 10] is proved with elementary arguments. There are other proofs in algebraic geometry based on the resolution of singularities

Kolchin Irreducibility Theorem

Kolchin (1973) Chap. IV Prop. 10 page 200

Let $\mathfrak{p}_0$ be a prime ideal of $\mathscr{F}[y_1, \ldots, y_n]$ of dimension d. Then the perfect differential ideal $\{\mathfrak{p}_0\}$ is a prime differential ideal of $\mathscr{F}\{y_1, \ldots, y_n\}$

The theorem holds for any number m of derivation operators

Kolchin Irreducibility Theorem

Kolchin (1973) Chap. IV Prop. 10 page 200

Let $\mathfrak{p}_0$ be a prime ideal of $\mathscr{F}[y_1, \ldots, y_n]$ of dimension d. Then the perfect differential ideal $\{\mathfrak{p}_0\}$ is a prime differential ideal of $\mathscr{F}\{y_1, \ldots, y_n\}$

The theorem holds for any number m of derivation operators

$\mathscr{F}$ differential field of characteristic zero (the Theorem false in char. $p > 0$)

Kolchin Irreducibility Theorem

Kolchin (1973) Chap. IV Prop. 10 page 200

Let $\mathfrak{p}_0$ be a prime ideal of $\mathscr{F}[y_1, \ldots, y_n]$ of dimension d. Then the perfect differential ideal $\{\mathfrak{p}_0\}$ is a prime differential ideal of $\mathscr{F}\{y_1, \ldots, y_n\}$

$\mathscr{F}\{y_1, \ldots, y_n\}$ differential polynomial ring in n differential indeterminates ($= n$ functions of m independent variables)

$\mathscr{F}[y_1, \ldots, y_n] \subset \mathscr{F}\{y_1, \ldots, y_n\}$ ring of the order zero differential polynomials ($\simeq$ usual non differential polynomials)

$y_1^2 - y_2^3 \in \mathscr{F}[y_1, \ldots, y_n]$

$\dot{y}_1^2 - 4\, y_1 \in \mathscr{F}\{y_1, \ldots, y_n\} \setminus \mathscr{F}[y_1, \ldots, y_n]$

Kolchin Irreducibility Theorem

Kolchin (1973) Chap. IV Prop. 10 page 200

Let $\mathfrak{p}_0$ be a prime ideal of $\mathscr{F}[y_1, \ldots, y_n]$ of dimension d. Then the perfect differential ideal $\{\mathfrak{p}_0\}$ is a prime differential ideal of $\mathscr{F}\{y_1, \ldots, y_n\}$

The Theorem is not as expected as a casual reader would think

Def The perfect differential ideal $\{\mathfrak{p}_0\}$ is the radical of the ideal generated by the elements of $\mathfrak{p}_0$ and their derivatives up to any order

Example The ideal $\mathfrak{p}_0 = (y_2^2 - y_1^3)$ is prime

The differential ideal $\{\mathfrak{p}_0\}$ contains $y_2\,(3\,y_2\,\dot{y}_1 - 2\,\dot{y}_2\,y_1)$

Is it clear that $3\,y_2\,\dot{y}_1 - 2\,\dot{y}_2\,y_1 \in \{y_2^2 - y_1^3\}$?

Kolchin Irreducibility Theorem

Kolchin (1973) Chap. IV Prop. 10 page 200

Let $\mathfrak{p}_0$ be a prime ideal of $\mathscr{F}[y_1, \ldots, y_n]$ of dimension d. Then the perfect differential ideal $\{\mathfrak{p}_0\}$ is a prime differential ideal of $\mathscr{F}\{y_1, \ldots, y_n\}$

The Theorem is not as expected as a casual reader would think

Example Drop the order zero hypothesis and consider $\dot{y}^2 - 4\,y$

The non differential ideal $(\dot{y}^2 - 4\,y)$ is prime

The perfect differential ideal $\{\dot{y}^2 - 4\,y\}$ is not prime:

$$\{\dot{y}^2 - 4\,y\} \quad = \quad \{\dot{y}^2 - 4\,y,\ \ddot{y} - 2\} \cap \{y\}$$

Characteristic Sets

Fact Any prime ideal can be presented by a characteristic set A

Example $$\{\dot{y}^2 - 4\,y,\ \ddot{y} - 2\} \quad = \quad [A] : H_A^\infty$$

where

- A is the singleton $\dot{y}^2 - 4\,y$ and
- H_A is the product of the initials $(= 1)$ and separants $(= 2\,\dot{y})$ of A

Def $[A] : H_A^\infty = \{p \in \mathscr{F}\{y\} \mid \exists\, d \geq 0,\ H_A^d\, p \in [A]\}$

Let us prove $\ddot{y} - 2 \in [A] : H_A^\infty$

Characteristic Sets

Fact Any prime ideal can be presented by a characteristic set A

Example $$\{\dot{y}^2 - 4\,y,\ \ddot{y} - 2\} \quad = \quad [A] : H_A^\infty$$

where

- A is the singleton $\dot{y}^2 - 4\,y$ and
- H_A is the product of the initials $(= 1)$ and separants $(= 2\,\dot{y})$ of A

Def $[A] : H_A^\infty = \{p \in \mathscr{F}\{y\} \mid \exists\, d \geq 0,\ H_A^d\, p \in [A]\}$

Let us prove $\ddot{y} - 2 \in [A] : H_A^\infty$
We have $\dot{y}^2 - 4\,y \in [A] : H_A^\infty$

Fact Any prime ideal can be presented by a characteristic set A

Example $$\{\dot{y}^2 - 4\,y,\ \ddot{y} - 2\} \;=\; [A] : H_A^\infty$$

where

- A is the singleton $\dot{y}^2 - 4\,y$ and
- H_A is the product of the initials $(= 1)$ and separants $(= 2\,\dot{y})$ of A

Def $[A] : H_A^\infty = \{p \in \mathscr{F}\{y\} \mid \exists\, d \geq 0,\ H_A^d\, p \in [A]\}$

Let us prove $\ddot{y} - 2 \in [A] : H_A^\infty$
We have $\dot{y}^2 - 4\,y \in [A] : H_A^\infty$
Thus $2\,\dot{y}\,(\ddot{y} - 2) \in [A] : H_A^\infty$

Characteristic Sets

Fact Any prime ideal can be presented by a characteristic set A

Example $$\{\dot{y}^2 - 4\,y,\ \ddot{y} - 2\} \;=\; [A] : H_A^\infty$$

where

- A is the singleton $\dot{y}^2 - 4\,y$ and
- H_A is the product of the initials $(= 1)$ and separants $(= 2\,\dot{y})$ of A

Def $[A] : H_A^\infty = \{p \in \mathscr{F}\{y\} \mid \exists\, d \geq 0,\ H_A^d\, p \in [A]\}$

Let us prove $\ddot{y} - 2 \in [A] : H_A^\infty$
We have $\dot{y}^2 - 4\,y \in [A] : H_A^\infty$
Thus $2\,\dot{y}\,(\ddot{y} - 2) \in [A] : H_A^\infty$
Thus $\ddot{y} - 2 \in [A] : H_A^\infty$

Summary of the Talk

Let $\mathfrak{p}_0$ be a prime ideal of $\mathscr{F}[y_1, \ldots, y_n]$ of dimension d. Then the perfect differential ideal $\{\mathfrak{p}_0\}$ is a prime differential ideal of $\mathscr{F}\{y_1, \ldots, y_n\}$

The proof relies on elementary arguments but it is subtle and misleading.

Some misunderstanding can be avoided by illustrating/restating it through examples relying on characteristic sets

Remark Ritt uses characteristic sets both as polynomial system solving tools and theoretical tools (the Basis Theorem follows from: *every set has a characteristic set*)

A Base Field which is a Differential Field

The base field $\mathscr{F}$ is a differential field.

It could be the field of fractions of a residue class ring.

The residue class ring of a differential polynomial ring by a prime differential ideal, presented by a characteristic set

Take $\mathscr{F} = \mathbb{Q}{<}\varphi{>}$ where φ defining equation (a characteristic set) is (say)

$$C \left\{ \ \ddot{\varphi} - 1 \,. \qquad (\mathscr{F}) \right.$$

An Order Zero Ideal Over a Differential Field

Let $\mathfrak{p}_0$ be a prime ideal of $\mathscr{F}[y_1, \ldots, y_n]$ ...

Let us consider a variant of $y_2^2 - y_1^3$

Take $\mathfrak{p}_0 = (A) : H_A^\infty$ where (say)

$$\begin{aligned} A &= (y_3 - y_2)^2 - \dot{\varphi}\, y_1^3\,, \\ H_A &= 2\,(y_3 - y_2)\,. \end{aligned}$$

The whole construct (non trivial base field + $\mathfrak{p}_0$) can be presented by a single characteristic set

$$C \left\{ \begin{array}{ll} (y_3 - y_2)^2 - \dot{\varphi}\, y_1^3\,, & \qquad (\mathfrak{p}_0, A) \\ \ddot{\varphi} - 1\,. & \qquad (\mathscr{F}) \end{array} \right.$$

The Second Paragraph of Kolchin's Proof

At this stage, Kolchin has established that the prime ideal $\mathfrak{p}_0$ has an order zero characteristic set A (so that $\mathfrak{p}_0 = (A) : H_A^\infty$), which defines also a prime differential ideal $\mathfrak{p} = [A] : H_A^\infty$ and ...

It is clear that $\{\mathfrak{p}_0\} \subset \mathfrak{p}$. Let $(\alpha_1, \ldots, \alpha_n)$ be any zero of $\mathfrak{p}_0$. By Chapter 0, Section 16, Corollary 3 to Proposition 11, there exist power series $Q_1, \ldots, Q_n \in \mathscr{U}[[c]]$ such that each element of $\mathfrak{p}_0$ vanishes at $(Q_1, \ldots, Q_n)$, H_A does not, and $Q_j(0) = \alpha_j$ $(1 \leqslant j \leqslant n)$. Now, $\mathscr{U}$ is universal over some differential field of definition $\mathscr{F}_0 \subset \mathscr{F}$ of $\mathfrak{p}$ that is also a field of definition of $\mathfrak{p}_0$. Therefore there exists a point $(\xi_1, \ldots, \xi_n)$ that is a generic differential specialization of $(Q_1, \ldots, Q_n)$ over $\mathscr{F}_0$. It is clear that $(\xi_1, \ldots, \xi_n)$ is a zero of A but not of H_A, hence is a zero of $\mathfrak{p} = [A] : {H_A}^\infty$, and that $(\alpha_1, \ldots, \alpha_n)$ is a differential specialization of $(\xi_1, \ldots, \xi_n)$ over $\mathscr{F}_0$. It follows that $(\alpha_1, \ldots, \alpha_n)$ is a zero of $\mathfrak{p}$. Therefore (by Section 2, Theorem 1) $\mathfrak{p} \subset \{\mathfrak{p}_0\}$, whence $\mathfrak{p} = \{\mathfrak{p}_0\}$.

$(\alpha_1, \ldots, \alpha_n)$ is a differential zero

Theorem 1 is a differential Nullstellensatz: if some f vanishes over every zero of a perfect differential ideal $\mathfrak{A}$ then $f \in \mathfrak{A}$

We may restrict $(\alpha_1, \ldots, \alpha_n)$ to a zero with coordinates in a finite differential field extension of $\mathscr{F}$

It is clear that $\{\mathfrak{p}_0\} \subset \mathfrak{p}$. Let $(\alpha_1, \ldots, \alpha_n)$ be any zero of $\mathfrak{p}_0$. By Chapter 0, Section 16, Corollary 3 to Proposition 11, there exist power series $Q_1, \ldots, Q_n \in \mathscr{U}[[c]]$ such that each element of $\mathfrak{p}_0$ vanishes at $(Q_1, \ldots, Q_n)$, H_A does not, and $Q_j(0) = \alpha_j$ $(1 \leqslant j \leqslant n)$. Now, $\mathscr{U}$ is universal over some differential field of definition $\mathscr{F}_0 \subset \mathscr{F}$ of $\mathfrak{p}$ that is also a field of definition of $\mathfrak{p}_0$. Therefore there exists a point $(\xi_1, \ldots, \xi_n)$ that is a generic differential specialization of $(Q_1, \ldots, Q_n)$ over $\mathscr{F}_0$. It is clear that $(\xi_1, \ldots, \xi_n)$ is a zero of A but not of H_A, hence is a zero of $\mathfrak{p} = [A] : H_A{}^\infty$, and that $(\alpha_1, \ldots, \alpha_n)$ is a differential specialization of $(\xi_1, \ldots, \xi_n)$ over $\mathscr{F}_0$. It follows that $(\alpha_1, \ldots, \alpha_n)$ is a zero of $\mathfrak{p}$. Therefore (by Section 2, Theorem 1) $\mathfrak{p} \subset \{\mathfrak{p}_0\}$, whence $\mathfrak{p} = \{\mathfrak{p}_0\}$.

The Zero $(\alpha_1, \ldots, \alpha_n)$

Drop the index, introduce some $\alpha \in \mathscr{G} = \mathscr{F}\langle\alpha\rangle$ through some α-defining equation, stacked over C

$$C \left\{ \begin{array}{ll} \dot\alpha^2 - \varphi\,\alpha\,, & (\mathscr{G}) \\ (y_3 - y_2)^2 - \dot\varphi\, y_1^3\,, & (\mathfrak{p}_0, A) \\ \ddot\varphi - 1\,. & (\mathscr{F}) \end{array} \right.$$

The Zero $(\alpha_1, \ldots, \alpha_n)$

Drop the index, introduce some $\alpha \in \mathscr{G} = \mathscr{F}{<}\alpha{>}$ through some α-defining equation, stacked over C

$$C \left\{ \begin{array}{ll} \dot{\alpha}^2 - \varphi\, \alpha\,, & (\mathscr{G}) \\ (y_3 - y_2)^2 - \dot{\varphi}\, y_1^3\,, & (\mathfrak{p}_0, A) \\ \ddot{\varphi} - 1\,. & (\mathscr{F}) \end{array} \right.$$

Pick a zero of $\mathfrak{p}_0$ hence of A, which annihilates $H_A = 2\,(y_3 - y_2)$ also (the issue in the proof arises for singular zeros)

$$(y_1, y_2, y_3) \;=\; (0, \alpha, \alpha)$$

Expand a Puiseux zero of A, not of H_A (hence of $\mathfrak{p}_0$) centered at $(0, \alpha, \alpha)$

$$(y_1, y_2, y_3) \quad = \quad (Q_1(c), Q_2(c), Q_3(c)) \quad = \quad (c^2,\ \alpha,\ \alpha + \rho\, c^3)$$

This step requires a (differential) algebraic extension $\mathscr{L} = \mathscr{G}{<}\rho{>}$

$$C \begin{cases} \rho^2 - \dot{\varphi}\,, & (\mathscr{L}) \\ \dot{\alpha}^2 - \varphi\,\alpha\,, & (\mathscr{G}) \\ (y_3 - y_2)^2 - \dot{\varphi}\, y_1^3\,, & (\mathfrak{p}_0, A) \\ \ddot{\varphi} - 1\,. & (\mathscr{F}) \end{cases}$$

It is clear that $\{\mathfrak{p}_0\} \subset \mathfrak{p}$. Let $(\alpha_1, \ldots, \alpha_n)$ be any zero of $\mathfrak{p}_0$. By Chapter 0, Section 16, Corollary 3 to Proposition 11, there exist power series $Q_1, \ldots, Q_n \in \mathscr{U}[[c]]$ such that each element of $\mathfrak{p}_0$ vanishes at $(Q_1, \ldots, Q_n)$, H_A does not, and $Q_j(0) = \alpha_j$ $(1 \leqslant j \leqslant n)$. Now, $\mathscr{U}$ is universal over some differential field of definition $\mathscr{F}_0 \subset \mathscr{F}$ of $\mathfrak{p}$ that is also a field of definition of $\mathfrak{p}_0$. Therefore there exists a point $(\xi_1, \ldots, \xi_n)$ that is a generic differential specialization of $(Q_1, \ldots, Q_n)$ over $\mathscr{F}_0$. It is clear that $(\xi_1, \ldots, \xi_n)$ is a zero of A but not of H_A, hence is a zero of $\mathfrak{p} = [A] : H_A^{\infty}$, and that $(\alpha_1, \ldots, \alpha_n)$ is a differential specialization of $(\xi_1, \ldots, \xi_n)$ over $\mathscr{F}_0$. It follows that $(\alpha_1, \ldots, \alpha_n)$ is a zero of $\mathfrak{p}$. Therefore (by Section 2, Theorem 1) $\mathfrak{p} \subset \{\mathfrak{p}_0\}$, whence $\mathfrak{p} = \{\mathfrak{p}_0\}$.

The Two Last Steps

If one evaluates a differential polynomial $f \in \mathscr{F}\{y_1, \ldots, y_n\}$ at

$$(y_1, y_2, y_3) \;=\; (Q_1(c), Q_2(c), Q_3(c)) \;=\; (c^2,\ \alpha,\ \alpha + \rho\, c^3)$$

one gets a differential power series in $\mathscr{L}\{\{c\}\}$

This one is easy to illustrate using a software

If $f \in \mathfrak{p} = [A] : H_A^\infty$ then it evaluates to zero (all its coefficients are reduced to zero by C)

$$C \begin{cases} \rho^2 - \dot\varphi\,, & (\mathscr{L}) \\ \dot\alpha^2 - \varphi\,\alpha\,, & (\mathscr{G}) \\ (y_3 - y_2)^2 - \dot\varphi\, y_1^3\,, & (\mathfrak{p}_0, A) \\ \ddot\varphi - 1\,. & (\mathscr{F}) \end{cases}$$

The Two Last Steps

If one evaluates a differential polynomial $f \in \mathscr{F}\{y_1, \ldots, y_n\}$ at

$$(y_1, y_2, y_3) \;=\; (Q_1(c), Q_2(c), Q_3(c)) \;=\; (c^2,\ \alpha,\ \alpha + \rho\, c^3)$$

one gets a differential power series in $\mathscr{L}\{\{c\}\}$

This one is not

"A diagram commutes" (if c is a differential indeterminate or an arbitrary contant)

The two following operations yield the same result:

1. Evaluate f at $(Q_1(c), Q_2(c), Q_3(c))$ then c at zero
2. Evaluate c at zero then f at $(Q_1(0), Q_2(0), Q_3(0)) = (0, \alpha, \alpha)$