Illustrating Kolchin's Proof of Kolchin's Irreducibility Theorem

François Boulier*

May 13, 2023

This text comes from a joint work with David Bourqui, François Lemaire, Adrien Poteaux and Julien Sebag on [2, chap. IV, prop. 10, page 200].

1 The Theorem

Theorem 1 *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 $\mathscr{F}\{y_1, \ldots, y_n\}$ having differential dimension polynomial $\omega_{\{\mathfrak{p}_0\}} = d\binom{X+m}{m}$.*

As an example, consider the polynomial $y_1^2 - y_2^3$. It is irreducible in $\mathscr{F}[y_1, y_2]$ and the ideal $(y_1^2 - y_2^3)$. However, we can also view it as an order zero differential polynomial and differentiate it (its first derivative is $2\,y_1\,\dot{y}_1 + 3\,y_2^2\,\dot{y}_2$). The differential ideal $[y_1^2 - y_2^3]$ of $\mathscr{F}\{y_1, y_2\}$ which is the ideal generated by $y_1^2 - y_2^3$ and all its derivatives is not radical. However, according to Kolchin's Theorem, the radical of this differential ideal, which is the perfect differential ideal $\{y_1^2 - y_2^3\}$, is prime. The Theorem would be false in nonzero characteristic. It would be false for general differential ideals (the perfect differential ideal $\{\dot{y}_1^2 - 4\,y_1\}$ is not prime though the polynomial $\dot{y}_1^2 - 4\,y_1$ is irreducible).

Kolchin's proof is short: one page, two paragraphs. The first paragraph is pretty straightforward, in particular for readers used to algorithms for decomposing differential ideals as intersections of differential ideals presented by characteristic sets or regular differential chains. The interesting paragraph is the second one. Though it is pretty theoretical in nature, we show in this document that its subtleties can be illustrated with the *DifferentialAlgebra* package [1] and become (hopefully) much easier to understand.

2 The First Paragraph of Kolchin's Proof

[1]:
```
from sympy import *
from DifferentialAlgebra import *
init_printing ()
```

Let us assume we have a single derivation with respect to some independent variable x (Kolchin's Theorem holds for the partial case also) and introduce a few differential indeterminates which can thus be viewed as functions of x:

[2]:
```
x = var ('x')
y3, y2, y1, rho, alpha, phi, c = function ('y3, y2, y1, rho, alpha, phi, c')
```

[3]:
```
R = DifferentialRing (derivations = [x], blocks = [c, y3, y2, y1, rho, alpha, phi])
```

*Univ. Lille, CNRS, Centrale Lille, Inria, UMR 9189 - CRIStAL - Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille, France.

The differential field $\mathscr{F}$ has characteristic zero but it may contain some non constant element φ. Let us assume $\varphi \in \mathscr{F}$ satisfies some differential relation such as this one:

[4]:
```
phi_defining_equation = Derivative(phi(x),x,x) - 1
phi_defining_equation
```

[4]:
$$\frac{d^2}{dx^2}\phi(x) - 1$$

The first paragraph simply explains that the prime ideal $\mathfrak{p}_0$ admits a characteristic set A, which is made of polynomials of order zero and that this set A is also a characteristic set of the prime differential ideal $\mathfrak{p} = [A] : H_A^\infty$ by [2, chap. IV, sect. 9, Lemma 2]. The claim on the differential dimension polynomial follows immediately from this observation by [2, chap. II, sect. 12, Theorem 6(d)].

In our running example, the characteristic set is made of a single differential polynomial $(y_3 - y_2)^2 - \dot{\varphi}\, y_1^3$, that we denote `A`. The differential polynomial H_A (denoted `H_A`) is the separant $2\,(y_3 - y_2)$ of the differential polynomial `A`:

[5]:
```
A = (y3(x) - y2(x))**2 - Derivative(phi(x),x)*y1(x)**3
A
```

[5]:
$$\left(-\mathrm{y}_2\left(x\right) + \mathrm{y}_3\left(x\right)\right)^2 - {\mathrm{y}_1}^3\left(x\right)\frac{d}{dx}\phi(x)$$

[6]:
```
H_A = R.separant (A)
H_A
```

[6]:
$$-2\,\mathrm{y}_2\left(x\right) + 2\,\mathrm{y}_3\left(x\right)$$

3 The Second Paragraph of Kolchin's Proof

First we quote this paragraph. Then we illustrate some of its parts using *DifferentialAlgebra*. This being done, readers should understand much better its whereabouts and we can rewrite it.

> 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 exists 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 $Q_j(0) = \alpha_j$ $(1 \leq j \leq n)$. 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 tuples $(\alpha_1, \ldots, \alpha_n)$ are zeros of the order zero ideal $\mathfrak{p}_0$ but they must run over a sufficiently large set of zeros to permit the application of the differential Theorem of Zeros [2, chap. IV, sect. 2, Theorem 1]. Kolchin takes the coordinates α_i in a universal differential field extension $\mathscr{U}$ of $\mathscr{F}$. Thanks to the Theorem which states that every perfect differential ideal is the intersection of the prime differential ideals which contain it, it is possible to avoid this heavy theoretical construct and consider some zero $(\alpha_1, \ldots, \alpha_n)$, defined by some prime differential ideal containing $\{\mathfrak{p}_0\}$.

In the next computations, the zero is denoted `Alpha`. Its coordinates are taken in some differential field extension $\mathscr{G} = \mathscr{F}\langle\alpha\rangle$ of $\mathscr{F}$ where α (denoted `alpha`) satisfies some differential equation such as this one:

[7]:
```
alpha_defining_equation = Derivative(alpha(x),x)**2 - phi(x)*alpha(x)
alpha_defining_equation
```

[7]:
$$-\alpha(x)\phi(x) + \left(\frac{d}{dx}\alpha(x)\right)^2$$

This is not mentioned in Kolchn's proof but the issue arises when the zero $(\alpha_1, \ldots, \alpha_n)$ annihilates H_A. Let us thus consider such a zero:

[8]:
```
Alpha = { y1(x):0, y2(x):alpha(x), y3(x):alpha(x) }
Alpha
```

[8]:
$$\{\mathrm{y}_1(x) : 0,\ \mathrm{y}_2(x) : \alpha(x),\ \mathrm{y}_3(x) : \alpha(x)\}$$

[9]:
```
R.evaluate (A, Alpha)
```

[9]:
$$0$$

[10]:
```
R.evaluate (H_A, Alpha)
```

[10]:
$$0$$

By an analogue of Puiseux Lemma [2, chap. 0, sect. 16, corollary 3 to prop. 11], Kolchin then builds a tuple $(Q_1, \ldots, Q_n)$ of formal power series in $\mathscr{U}[[c]]$ centered at $(\alpha_1, \ldots, \alpha_n)$, which annihilate $\mathfrak{p}_0$ (hence A), but do not annihilate H_A. The coefficients of these formal power series actually belong to a finite algebraic extension $\mathscr{L}$ of $\mathscr{G}$. Here we only need to introduce the square root ϱ of $\dot{\varphi}$:

[11]:
```
rho_defining_equation = rho(x)**2 - Derivative(phi(x),x)
rho_defining_equation
```

[11]:
$$\rho^2(x) - \frac{d}{dx}\phi(x)$$

The example was chosen so that the formal power series Q_i are polynomials but this would not be true in general. The tuple $(Q_1, Q_2, Q_3) = (c^2, \alpha, \alpha + \varrho\, c^3)$ is denoted `Beta`:

[12]:
```
Beta = { y1(x):c(x)**2, y2(x):alpha(x), y3(x):alpha(x) + rho(x)*c(x)**3 }
Beta
```

[12]:
$$\left\{\mathrm{y}_1(x) : c^2(x),\ \mathrm{y}_2(x) : \alpha(x),\ \mathrm{y}_3(x) : \alpha(x) + c^3(x)\rho(x)\right\}$$

Let us check that (Q_1, Q_2, Q_3) annihilates A but not H_A (the ϱ defining equation is needed in the simplification process):

[13]:
```
R.evaluate (A, Beta)
```

[13]:
$$c^6(x)\rho^2(x) - c^6(x)\frac{d}{dx}\phi(x)$$

[14]:
```
rem (R.evaluate (A, Beta), rho_defining_equation, rho(x))
```

[14]:
$$0$$

[15]:
```
R.evaluate (H_A, Beta)
```

[15]:
$$2c^3(x)\rho(x)$$

At this stage, it should be clear that $(Q_1, \ldots, Q_n)$ is a zero of the ideal $\mathfrak{p}_0$ which does not annihilate H_A but, to permit the application of the differential Theorem of zeros, it is necessary that $(Q_1, \ldots, Q_n)$ is a

differential zero of the prime differential ideal $\{\mathfrak{p}_0\}$. In order to get convinced that this is actually the case, let us pick some differential polynomial f of arbitrary order, from this differential ideal:

[16]:
```
f = Derivative(A,x,x) + y1(x)*Derivative(A,x)
f
```

[16]:
$$\mathrm{y}_1\,(x)\frac{d}{dx}\left(\left(-\mathrm{y}_2\,(x)+\mathrm{y}_3\,(x)\right)^2-{\mathrm{y}_1}^3\,(x)\frac{d}{dx}\phi(x)\right)+\frac{d^2}{dx^2}\left(\left(-\mathrm{y}_2\,(x)+\mathrm{y}_3\,(x)\right)^2-{\mathrm{y}_1}^3\,(x)\frac{d}{dx}\phi(x)\right)$$

Let us evaluate it at $(Q_1,\ldots,Q_n)$. The result is a formal power series (it is a differential polynomial over this particular example) in c and its derivatives with coefficients in $\mathscr{L}$ i.e. an element of the differential power series algebra denoted $\mathscr{L}\{\{c\}\}$ in [2, chap. I, sect. 12]. The variables `koeffs` and `terms` contain the coefficients k_i and the terms t_i of the formal power series `series`, which is then equal to the sum of the $k_i\,t_i$:

[17]:
```
series = R.evaluate (f.doit(), Beta).doit ()
```

[18]:
```
koeffs, terms = R.coeffs(series, c(x))
terms
```

[18]:
$$\left[c^5(x)\frac{d^2}{dx^2}c(x),\ c^4(x)\left(\frac{d}{dx}c(x)\right)^2,\ c^7(x)\frac{d}{dx}c(x),\ c^5(x)\frac{d}{dx}c(x),\ c^8(x),\ c^6(x)\right]$$

[19]:
```
koeffs
```

[19]:
$$\left[6\rho^2(x)-6\frac{d}{dx}\phi(x),\ 30\rho^2(x)-30\frac{d}{dx}\phi(x),\ 6\rho^2(x)-6\frac{d}{dx}\phi(x),\ 24\rho(x)\frac{d}{dx}\rho(x)-12\frac{d^2}{dx^2}\phi(x),\right.$$
$$\left.2\rho(x)\frac{d}{dx}\rho(x)-\frac{d^2}{dx^2}\phi(x),\ 2\rho(x)\frac{d^2}{dx^2}\rho(x)-\frac{d^3}{dx^3}\phi(x)+2\left(\frac{d}{dx}\rho(x)\right)^2\right]$$

All the coefficients must be zero. To complete the simplification process, we need to simplify the coefficients with the differential ideal generated by the defining equations we have introduced. Here is a characteristic set `C` for this ideal. Observe that the ϱ defining equation is part of the characteristic set and that the derivatives of this equation are needed in the simplification process. In more algebraic terms, the field extension $\mathscr{L}$ is endowed with a differential field structure which extends that of $\mathscr{G}$. The characteristic set `C` provides an algorithmic description of $\mathscr{L}$ as a differential field extension of the field of the rational numbers:

[20]:
```
C = RegularDifferentialChain ([rho_defining_equation,
        alpha_defining_equation, phi_defining_equation], R)
C.equations(solved=True)
```

[20]:
$$\left[\frac{d^2}{dx^2}\phi(x)=1,\ \left(\frac{d}{dx}\alpha(x)\right)^2=\alpha(x)\phi(x),\ \rho^2(x)=\frac{d}{dx}\phi(x)\right]$$

And here is the verification:

[21]:
```
C.normal_form (koeffs)
```

[21]:
$[0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0]$

Last, Kolchin claims that $(\alpha_1,\ldots,\alpha_n)$ is a differential specialization of $(Q_1,\ldots,Q_n)$. How does this translate? Over our example, we have $f(Q_1,\ldots,Q_n)=0$ thus $f(Q_1,\ldots,Q_n)$, evaluated at $c=0$ is zero also. However, we eventually need $f(Q_1(0),\ldots,Q_n(0))$ i.e. that the composition of the evaluation at $(Q_1,\ldots,Q_n)$ and the evaluation at $c=0$ is a differential homomorphism.

In order to obtain this, we can define c as a differential indeterminate (this is what we have done) but we could also have defined c as an arbitrary constant i.e. have computed modulo the differential relation $\dot{c} = 0$. More generally, we could have computed modulo any differential relation $g(c) = 0$ such that $g(c) = 0 \not\Rightarrow c \neq 0$.

We are now ready to rewrite the second paragraph of Kolchin's proof.

> It is clear that $\{\mathfrak{p}_0\} \subset \mathfrak{p}$. It is thus sufficient to prove the converse inclusion. Let $f \in \mathfrak{p}$ be a differential polynomial of arbitrary order i.e. a differential polynomial such that $h\,f \in [A]$ where h stands for some power product of the initials and separants of A. Let $\mathfrak{P}$ be a prime differential ideal containing $\{\mathfrak{p}_0\}$ and $\alpha = (\alpha_1, \ldots, \alpha_n)$ be the zero of $\{\mathfrak{p}_0\}$ defined by $\mathfrak{P}$ in the differential field obtained by taking the fraction field $\mathscr{G}$ of $\mathscr{F}\{y_1, \ldots, y_n\}/\mathfrak{P}$. The tuple α is a generic zero of $\mathfrak{P}$ (i.e. it annihilates f if and only if $f \in \mathfrak{P}$) and $\{\mathfrak{p}_0\}$ is the intersection of the prime differential ideals which contain it. Thus it is sufficient to prove that α annihilates f to conclude the proof of the Theorem. Since $h\,f \in [A] \subset \{\mathfrak{p}_0\}$ we have $(h\,f)(\alpha) = 0$. If $h(\alpha) \neq 0$ then $f(\alpha) = 0$. Assume $h(\alpha) = 0$. Then $\dim \mathfrak{p}_0 \geq 1$. By [2, chap. 0, sect. 16, Corollary 2 to Prop. 11], there exists a prime ideal $\mathfrak{p}_1$ such that $\mathfrak{p}_1$ vanishes at α, $\dim \mathfrak{p}_1 = 1$, $\mathfrak{p}_0 \subset \mathfrak{p}_1$ and $h \notin \mathfrak{p}_1$. Then, by Puiseux Lemma applied on $\mathfrak{p}_1$ and α, there exists a tuple of power series $Q_1, \ldots, Q_n \in \mathscr{L}[[c]]$ where $\mathscr{L}$ is a finite algebraic field extension of $\mathscr{G}$ such that A vanishes at $\beta = (Q_1, \ldots, Q_n)$, h does not and $Q_j(0) = \alpha_j$ $(1 \leq j \leq n)$. The field $\mathscr{L}$ can be endowed with a differential field structure extending that of $\mathscr{G}$ (that would not be true in arbitrary characteristic). View c as a new differential indeterminate or an arbitrary constant. Then β is a zero of the differential ideal $[A]$ hence it annihilates f. Thus $f(\beta)$, which is an element of $\mathscr{L}\{\{c\}\}$ (or of $\mathscr{L}[[c]]$ if c is an arbitrary constant) is the zero series. Thus $f(\beta)(0)$ (i.e. $f(\beta)$ evaluated at $c = 0$) is zero also. Our assumptions on c imply that $f(\beta)(0)$ is also equal to $f(Q_1(0), \ldots, Q_n(0))$. Thus $f(\alpha) = 0$ and the proof is complete.

References

[1] François Boulier and al. DifferentialAlgebra. https://codeberg.org/francois.boulier/DifferentialAlgebra.

[2] Ellis Robert Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1973.