Differential Polynomial Algebra in Characteristic Zero

Notes prepared for the Kolchin Seminar in Differential Algebra
Sally Morrison
September 14, 2002

Abstract

This is an introduction to the language and methods of Differential Algebra for those with little or no previous exposure to the subject. The emphasis is on examples and major ideas rather than on precise techniques and proofs.

Differential polynomial algebra may be regarded as an attempt to use the methods of abstract algebra to obtain information about solutions of systems of differential equations, in much the same way that the theory of polynomial rings yields information about solutions of systems of polynomial equations.

In this talk we review the fundamental definitions and problems of the subject including: the basics of differential rings, ideals, and homomorphisms; the correspondence between solutions of differential equations and differential ideals; decomposition of a solution into its irreducible components—and, in particular, the decomposition of a single differential polynomial into its general and singular components.

1 Differential Algebra as a Generalization of Commutative Algebra

Let R be a commutative ring with 1. We adhere to the following notations and conventions. If $r \in R$, if $S \subseteq R$, and if I is an ideal of R, then (S) is the ideal of R generated by S, $\sqrt{I}$ is the radical ideal generated by I, and $I : r$ is the set of all $x \in R$ such that $xr \in I$. We adopt the convention that a *proper* ideal of R is any ideal of R (including the zero ideal) except for R itself.

Let R be a commutative ring with 1, and let $\Delta = \{\delta_1, \ldots, \delta_m\}$ be a finite set of commuting derivations on R. That is, for every $\delta \in \Delta$ and for every $a, b, \in R$, we have $\delta(a+b) = \delta(a) + \delta(b)$ and $\delta(ab) = a \cdot \delta(b) + \delta(a) \cdot b$. We shall refer to such a pair (R, Δ), as a (commutative) *differential ring*. When no confusion can result, we suppress Δ and refer to this differential ring simply as R. If $m = 1$ (i.e. $\Delta = \{'\}$), R is an *ordinary* differential ring; otherwise it is a *partial* differential ring.

The Δ-ring R is a *differential domain*, (respectively *differential field*) if, considered as a ring, it is an integral domain (respectively field). The quotient field of a differential domain is a differential field with the usual quotient rule for derivatives.

Let Θ be the set of derivative operators generated by Δ; that is, Θ is the free commutative monoid generated by $\delta_1, \ldots, \delta_m$, whence each element θ of Θ is uniquely expressible as $\theta = \delta_1^{e_1} \ldots \delta_m^{e_m}$ for some $(e_1, \ldots, e_m) \in \mathbb{N}^m$. (Here $\mathbb{N}$ denotes the set of all natural numbers, including 0.) The *order* of $\theta = \delta_1^{e_1} \ldots \delta_m^{e_m}$ is the non-negative integer $ord(\theta) = \sum_{j=1}^{m} e_j$. The only element of Θ of order zero is the identity operator.

Clearly any set closed under Δ is also closed under Θ.

Examples of Differential Rings.

1. The rings $\mathbb{Q}[x_1, \ldots, x_m]$, $\mathbb{R}[x_1, \ldots, x_m]$, and $\mathbb{C}[x_1, \ldots, x_m]$ of all polynomial functions (on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$) in the independent variables $x_1, \ldots, x_m$ are partial differential domains under $\Delta = \{\partial/\partial x_1, \ldots, \partial/\partial x_m\}$. The quotient fields are the differential fields $\mathbb{Q}(x_1, \ldots, x_m)$, $\mathbb{R}(x_1, \ldots, x_m)$, and $\mathbb{C}(x_1, \ldots, x_m)$.

2. The ring of all C^∞ functions in one variable x on the real line is an ordinary differential ring—but not a differential domain—under the derivation d/dx.

3. The ring of all entire functions in one complex variable z is an ordinary differential domain under d/dz. Its quotient field is the differential field of all meromorphic functions.

4. The field of all functions in the variables $z_1, \ldots, z_m$ meromorphic in a given region of $\mathbb{C}^m$, with $\Delta = \{\partial/\partial z_1, \ldots \partial/\partial z_m\}$ is a partial differential field.

5. Every commutative ring R may be considered as a differential ring (of *constants*) by putting $\Delta = \{'\}$, where $r' = 0$ for each $r \in R$.

Definitions.

1. An ideal I of R is a *differential ideal* if it is closed under the action of Δ—that is, if $a \in I, \delta \in \Delta \Rightarrow \delta(a) \in I$.

2. Let R and S be Δ-rings, and let $\phi : R \longrightarrow S$ be a (unitary) ring homomorphism. If ϕ commutes with each $\delta \in \Delta$ (and hence with each $\theta \in \Theta$), then ϕ is called a *differential homorphism* (or Δ-homomorphism).

Proposition 1. Let I be a Δ-ideal of a Δ-ring R, and let $\phi : R \longrightarrow R/I$ be the canonical homomorphism. For each $a + I \in R/I$ and $\delta \in \Delta$, define

$$\delta(a + I) = \delta(a) + I.$$

Under this definition R/I is a Δ-ring and ϕ is a Δ-homomorphism. Moreover, the usual one-to-one correspondence between the ideals of R/I and the ideals of R containing I induces a bijection between the Δ-ideals of R/I and the Δ-ideals of R containing I.

Proof. For instance: $a + I = b + I \Rightarrow a - b \in I \Rightarrow \delta(a - b) \in I \Rightarrow \delta(a) - \delta(b) \in I \Rightarrow \delta(a) + I = \delta(b) + I$, so the action of Δ on R/I is well-defined. And $\phi(\delta a) = \delta a + I = \delta(a + I) = \delta(\phi a)$, so ϕ is a Δ-homomorphism. $\square$

As a sort of converse, we have:

Proposition 1′. Let $R \xrightarrow{\phi} S$ be a differential ring homomorphism. Then $ker\,\phi$ is a differential ideal of R and $\phi(R)$ is a differential subring of S.

Now let S be a subset of a differential ring R. The intersection of all differential ideals of R containing S is a differential ideal, which we denote $[S]$; likewise the intersection of all radical differential ideals containing S is a radical differential ideal, which we denote $\{S\}$. These ideals are called, respectively, the *differential ideal generated by S* and *radical differential ideal generated by S*. It is easy to see that the ideal $(\theta s : s \in S, \theta \in \Theta)$ is a differential ideal of R, and hence that it is equal to $[S]$. Our next task is to determine the elements of $\{S\}$.

Recall that, given any proper ideal I of a commutative ring, there are minimal prime ideals containing I, and $\sqrt{I}$ is the intersection of these minimal prime ideals. In the corresponding differential theory, we have the following.

Proposition 2. Let I be a proper radical differential ideal of R. Then every prime ideal of R minimal over I is a differential prime ideal. Consequently, every proper radical differential ideal in a differential ring is an intersection of differential prime ideals.

To prove this, we first establish the following lemma.

Lemma. Let J be a radical differential ideal of a differential ring R, and let $r \in R$. Then $J\!:\!r$ is a radical differential ideal of R.

Proof. Let $x \in J:r$ and let $\delta \in \Delta$. Then $xr \in J$ and, since J is a differential ideal, we have (denoting δ by $'$ for ease of reading), $(xr)' \in J$. Thus

$$(x'r)^2 = (x'r)\,\overbrace{(xr)'}\,-x'r'\,\overbrace{(xr)} \in J,$$

Since J is radical, $x'r \in J$, whence $x' \in J:r$. So $J:r$ is a differential ideal.

Now let $y \in R$ and suppose that $y^n \in J:r$. Then

$$(yr)^n = r^{n-1}(y^n r) \in J.$$

Thus $yr \in J$, whence $y \in J:r$. So $J:r$ is radical. □

Proof of Proposition 2. By Zorn's Lemma there is a radical differential ideal J that is maximal among those radical differential ideals J' such that $I \subseteq J' \subseteq P$. Let $x \in R$ and suppose that $J : x \neq J$. (We shall prove that $x \in J$, and hence conclude that J is prime.) By the Lemma and the maximality of J, there exists $y \in (J:x) \setminus P$. Since $xy \in J \subseteq P$ and P is prime, we have $x \in J:y \subseteq P$. By the lemma and the maximality of J, we have $J:y = J$ whence $x \in J$. Thus J is a prime differential ideal, and $J = P$ by the minimality of P.

Remark. It is important to note that—in contrast to the non-differential case—without further hypotheses Proposition 2 does *not* guarantee that every prime ideal minimal over a proper differential ideal is differential. Nor does it guarantee that the radical of a proper differential ideal is the intersection of prime differential ideals; one obtains only the more cautious statement that for any differential ideal I of R, either $\{I\} = R$ or $\{I\}$ is the intersection of prime differential ideals. The problem here is that $\sqrt{I}$ need not be a differential ideal.

Example. In $\mathbb{Z}[x]$, let $x' = 1$ and $a' = 0$ for every $a \in \mathbb{Z}$; and extend to a derivation on $\mathbb{Z}[x]$ via the sum and product rules. Let $I = [x^2]$. Then $I = (x^2, 2x, 2) = (2, x^2)$, so $\sqrt{I} = (2, x)$, which is a minimal prime ideal over I, but is not a differential ideal, since $x' = 1$. Thus $1 \in \{I\} = \mathbb{Z}[x]$.

Clearly the difficulty here is that we cannot divide by 2: we have $2x \in I$, but $x \notin I$. This motivates the following definition.

Definition. A *Ritt Algebra* is a differential ring containing the field $\mathbb{Q}$ of rational numbers.

Proposition 3. Let R be a Ritt algebra, and let I be a proper differential ideal of R. Then $\sqrt{I}$ is differential ideal (and hence a *proper* radical differential ideal).

Proof. Let I be a differential ideal of a differential ring R, let $a^n \in I$ and let $\delta \in \Delta$. Then $a^{n-1}(\delta a) = \frac{1}{n}\delta(a^n) \in I$. One easily sees by induction that $a^{n-k}(\delta a)^{2k-1} \in I$ for $1 \leq k \leq n$. Taking $k = n$ gives the desired result. □

Corollary. Let I be a proper differential ideal in a Ritt Algebra R. Then every prime ideal minimal over I is a differential prime ideal, and $\{I\} = \sqrt{I}$.

2 Differential Polynomial Rings and Systems of Differential Equations

We wish to consider systems of algebraic partial differential equations; by "algebraic" we mean that the differential equations are polynomials in the unknown functions and their derivatives, with coefficients in an arbitrary differential field. Thus if x is a complex variable, then $x^2 y''^3 - (\sin\, x) y^2 + e^x = 0$ is an algebraic differential equation whose coefficients are meromorphic functions, but $x^2 y''^3 - x^2(\sin\, y) = 0$ is not an algebraic differential equation.

Definition: Differential Polynomial Ring. Let (k, Δ) be a differential field of characteristic zero, and let $Y = y_1, \ldots, y_n$ be *differential indeterminates* over k; this means that the set of symbols

$$\Theta Y = \{\theta y_i : \theta \in \Theta, 1 \leq i \leq n\}$$

is algebraically independent over k and that Δ acts on ΘY via $\delta(\theta y) = \delta\theta y$. The action of Δ then extends to the polynomial ring $k[\Theta Y]$ according to the usual rules for derivations: $\delta(f+g) = \delta f + \delta g$, and $\delta(fg) = f(\delta g) + (\delta f)g$. Under this action, $k[\Theta Y]$ is a differential domain, which we refer to as the *differential polynomial ring* over k in the n differential indeterminates $y_1, \ldots, y_n$. We denote this differential polynomial ring $k\{y_1, \ldots, y_n\}$. It is a Ritt algebra because k has characteristic zero. The elements of $k\{y_1, \ldots, y_n\}$ are *differential polynomials* over k.

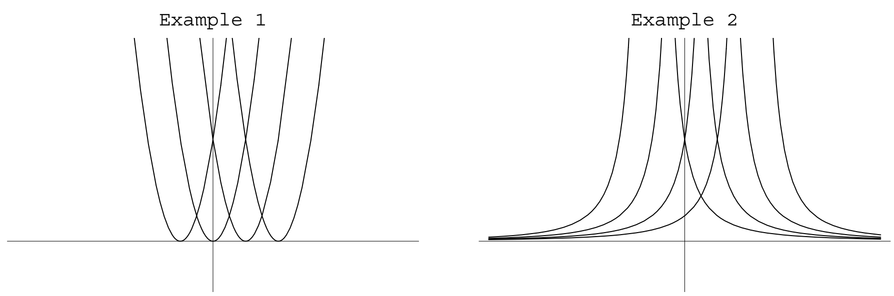
Thus a system of algebraic differential equations is a system

$$\begin{aligned} f_1(y_1, \ldots, y_n) &= 0 \\ &\vdots \\ f_k(y_1, \ldots, y_n) &= 0, \end{aligned}$$

where $f_1, \ldots, f_k$ are elements of a differential polynomial ring $k\{y_1, \ldots, y_n\}$ over a differential field k. Putting $F = \{f_1, \ldots, f_k\}$, we use the abbreviated notation $F = 0$ for the above system of differential equations.

3 The Ordinary Differential Polynomial Ring $k\{y\}$

Example 1. In $\mathbb{R}(x)\{y\}$, let $f = y'^2 - 4y$. The solution of the differential equation $f(y) = 0$ consists of the "general solution" $y = (x + c)^2$ together with the singular solution $y = 0$, which is the envelope of the general solution.



Example 2. In $\mathbb{R}(x)\{y\}$, let $f = y'^2 - 4y^3$. The solution of the differential equation $f(y) = 0$ consists of the "general solution" $y = 1/(x + c)^2$ together with the singular solution $y = 0$, which, in a sense to be made precise shortly, is actually part of the general solution.

To handle these differential equations algebraically, we need to collect a bit more information about the differential polynomial ring $(k\{y\},')$. First some notation: Let $f \in k\{y\}$. The highest derivative of y appearing in f, say $y^{(k)}$, is called the $\boxed{\textit{leader}}$ of f, and is denoted $\boxed{u_f}$. The coefficient of the highest power of u_f appearing in f is an element of the polynomial ring $k[y, y', y'', \ldots, y^{(k-1)}]$. This coefficient is called the $\boxed{\textit{initial}}$ of f and denoted $\boxed{i_f}$. The partial derivative of f with respect to u_f is called the $\boxed{\textit{separant}}$ of f and denoted $\boxed{s_f}$.

Example 3. $f = xyy''^2 + y'y'' + xy' + y \in \mathbb{R}(x)\{y\}$. We have $u_f = y''$, $i_f = xy$ and $s_f = 2xyy'' + y'$.

Note that if $j > 0$, then $f^{(j)} = s_f u_f^{(j)} +$ [terms of order lower than $u_f^{(j)}$]; so in particular, $u_{f^{(j)}} = (u_f)^{(j)}$, $i_{f^{(j)}} = s_f$, and $f^{(j)}$ is linear in its leader. In Example 3, for instance, we have

$$f' = \overbrace{(2xyy'' + y')}^{s_f}\, y^{(3)} + (xy' + y + 1){y''}^2 + xy'' + 2y'$$

The theorems of Section 5 (which begins on page 10) when applied to $(\mathbb{R}(x)\{y\},')$, tell us the following about the previous examples: The solution of the single differential equation $f = 0$ (in some differential extension field of $\mathbb{R}(x)$) is the same as the solution of the infinite system $(g = 0 \forall g \in \{f\})$: we refer to this as the *solution set* of $\{f\}$. There are finitely many minimal prime differential ideals containing the radical differential ideal $\{f\}$, and $\{f\}$ is uniquely represented as the irredundant intersection of these prime differential ideals, which are called the *prime components* of f. All except one are *singular components* of f, meaning that they contain the separant s_f; their solution sets are called the *singular components* of the solution. The unique prime component of f that does not contain s_f is called the *general component* of f and denoted $\mathcal{P}(f)$; its solution set is called the *general solution* or the *general component* of the solution. The solution set of $f = 0$ is the union of the solutions of the prime components of f. Thus we can represent our solution algebraically as the *coordinate ring* $\mathbb{R}(x)\{y\}/\{f\}$, and we can represent its irreducible components by the coordinate rings $\mathbb{R}(x)\{y\}/P_1, \ldots, \mathbb{R}(x)\{y\}/P_k$, where $P_1, \ldots P_k$ are the prime components of $\{f\}$.

Example 1, continued. We have $f = {y'}^2 - 4y$ and $s_f = 2y'$. Note that f is irreducible as an element of $\mathbb{R}(x)\{y\}$, so that (f) is a prime (non-differential) ideal of $\mathbb{R}(x)\{y\}$. Let P be a prime differential ideal containing f. Then $f' \in P$, and, since

$$\begin{aligned} f' &= 2y'y'' - 4y' \\ &= 2y'(y'' - 2), \end{aligned}$$

either $y' \in P$ or $y'' - 2 \in P$. That is, either $\{f, y'' - 2\} \subseteq P$ or $\{f, y'\} = [y] \subseteq P$. Since both $[f, y'' - 2]$ and $[y]$ are prime, the general component is $\mathcal{P}(f) = [{y'}^2 - 4y, y'' - 2]$, and the only candidate for a singular component, namely $[y]$, does not contain $\mathcal{P}(f)$; thus $[y]$ is indeed a component of $\{f\}$. So the prime decomposition of $\{f\}$ is

$$\{f\} = \overbrace{[{y'}^2 - 4y, y'' - 2]}^{\mathcal{P}(f)} \cap [y].$$

The generators of $\mathcal{P}$ permit us to find the general solution of ${y'}^2 - 4y = 0$ in $\mathbb{R}(x)$ by integration:

$$[y'' = 2 \wedge {y'}^2 = 4y] \Rightarrow [y' = 2(x+c) \wedge {y'}^2 = 4y]$$
$$\Rightarrow y = (x+c)^2$$

The corresponding coordinate rings are

$$\mathbb{R}(x)\{y\}/\mathcal{P}(f) \approx \mathbb{R}(x)[u_0, u_1], \text{ and}$$
$$\mathbb{R}(x)\{y\}/[y] \approx \mathbb{R}(x),$$

where u_0 is transcendental over $\mathbb{R}(x)$ and $u_1^2 = 4u_0$, and where $u_0' = u_1$, and $u_1' = 2$. The canonical differential homomorphism is given by

$$\mathbb{R}(x)\{y\} \xrightarrow{\phi} \mathbb{R}(x)[u_0, u_1]$$
$$y \to u_0$$
$$y' \to u_1$$
$$y'' \to 2$$
$$y^{(k)} \to 0 \text{ if } k > 2$$

<u>Example 2, continued</u>. Again, $f = {y'}^2 - 4y^3$ is irreducible as an element of $\mathbb{R}(x)\{y\}$. Differentiating and factoring as before, we once again find just two candidates for prime components of $\{f\}$, namely $\mathcal{P}(f) = [{y'}^2 - 4y^3, y'' - 6y^2]$ and $\{{y'}^2 - 4y^3, 2y'\} = [y]$. But this time we have $\mathcal{P}(f) \subset [y]$, so $[y]$ is not a component of f; the singular solution $y = 0$ is a solution of the general component $\mathcal{P}(f)$.

We note that $\mathbb{R}(x)\{y\}/\mathcal{P}(f) \approx \mathbb{R}(x)[u_0, u_1]$, where u_0 is an indeterminate over k and $u_1^2 = 4u_0^3$. We have ${u_0}' = u_1$, and ${u_1}' = 6u_0^2$.

In each of these examples, note that $\mathcal{P}(f) = \{f\} : s_f = [f] : s_f^\infty$, where by $[f] : s_f^\infty$ we mean $\cup_{n=0}^\infty([f] : s_f^n)$. Also, the transcendence degree of each coordinate ring is equal to the number of "arbitrary constants". Both these observations hold for any single irreducible differential polynomial $f \in k\{y\}$.

Our method here was very *ad hoc*, and we were so lucky as to be able to actually determine *generating sets* for the components of f. In general we cannot do this; we can only find (at least in theory) the prime components of f in the form $[p] : s^\infty$, where p is an irreducible element of $k\{y\}$.

Before leaving these two examples, it is worth noting that by using the Low Power Theorem (see Section 5) we could have predicted in advance that $[y]$ is a component in Example 1 but not in Example 2. To see this, we first state a very special case of the Low Power Theorem, in which the word "degree" means the total degree in y and its derivatives $y', y'', \ldots$.

> Let f be an irreducible element of $k\{y\}$ and suppose that $f \in [y]$. Then $[y]$ is a component of f if and only if, considered as a polynomial in y and its derivatives, f has a term in y alone that is of lower degree than every other term of f.

Now the term of lowest degree in Example 1 is $-4y$, which tells us that $[y]$ is a component of $f = {y'}^2 - 4y$. In Example 2, the term of lowest degree is ${y'}^2$, so $[y]$ is not a component of $f = {y'}^2 - 4y^3$. In Example 3, we again have $\{f\} \subseteq [y]$, and

$$f = \overbrace{y + xy'}^{\text{deg } 1} + \overbrace{y'y'}^{\text{deg } 2} + \overbrace{xy{y'}^2}^{\text{deg } 3}.$$

Since there are two terms of lowest degree, by the Low Power Theorem, $[y]$ is not a component of f.

4 Partial Differential Polynomial Rings in Several Variables

The main problem in making the transition from ordinary differential polynomial rings to partial differential polynomial rings is one of organization and notation. (Ellis Kolchin used to remind us on occasion that if we were able to prove a theorem only in the ordinary case, we hadn't yet figured out what was really going on. As far as I know, he was always right about that.) We introduced much of the notation in Section 2, but, given a partial differential polynomial f in several variables, we need to say what we mean by its *leader*. (Recall that we defined the leader of an ordinary differential polynomial f simply to be the highest derivative $y^{(k)}$ appearing in f.)

We now return to an arbitrary Δ-polynomial ring $k\{y_1, \ldots, y_n\} = k[\Theta Y]$ under a set $\Delta = \{\delta_1, \ldots, \delta_m\}$ of derivations. We first well-order the elements of ΘY in a way that is compatible with the derivations: that is, so that for $y, z \in Y$ and α, $\beta \in \Delta$, we have

$$y < \delta y, \text{ and } \qquad \alpha y < \beta z \Rightarrow \delta\alpha y < \delta\beta z.$$

Next, for $u, v \in \Theta Y$ and for positive integers p and q, define $u^p < v^q$ if $u < v$ or if $u = v$ and $p < q$. Then, for $f \in k\{y_1, \ldots, y_n\} \setminus k$, define the $\boxed{\textit{leader}}$ of f

to be the highest element of ΘY appearing in f; as before, denote this element u_f. For $f \in k\{y_1, \ldots, y_n\} \setminus k$, define the $\boxed{\textit{rank}}$ of f to be $u_f^{d_f}$, where d_f is the highest power of u_f appearing in f. Finally, extend $<$ to a *pre-order* on $k\{y_1, \ldots, y_n\} \setminus k$ by putting $f < g$ if and only if $rank(f) < rank(g)$.

Examples of differential rankings include an "orderly" ranking induced by ordering $\mathbb{N}^{m+1}$ lexicographically and making the identification

$$\delta_1^{e_1} \ldots \delta_m^{e_m} \leftrightarrow \left(\sum_{k=1}^{m} e_k, e_m, \ldots, e_2, j \right),$$

and an "elimination" ranking induced by the identification

$$\delta_1^{e_1} \ldots \delta_m^{e_m} \leftrightarrow \left(j, \sum_{k=1}^{m} e_k, e_m, \ldots, e_2, \right).$$

Now that we have said what we mean by the leader of a partial differential polynomial in several indeterminates, we can define the *initial* and *separant* exactly as we did before: if $rank(f) = u_f^{d_f}$, then the coefficient of $u_f^{d_f}$ in f—considered as a polynomial in $(k[\theta y \in \Theta Y : \theta y < u_f])[u_f]$—is the $\boxed{\textit{initial}}$ of f, and $\partial f / \partial u_f$ is the $\boxed{\textit{separant}}$ of f.

5 The Basic Theorems of Differential Polynomial Algebra

Let $R = (k\{y_1, \ldots, y_n\}, \Delta)$ be a differential polynomial ring, and let $F = \{f_1, \ldots, f_r\}$ be a finite subset of R.

Theorem 1. ("The Basis Theorem") R satisfies the the ascending chain condition on radical differential ideals. Equivalently: Let I be a radical differential ideal in R. Then there are finitely many differential polynomials $g_1, \ldots, g_s$ in R such that $I = \{g_1, \ldots, g_s\}$.

Theorem 2. ("Prime Decomposition") Every proper radical differential ideal of R is uniquely expressible as a *finite* irredundant intersection of differential prime ideals.

Theorem 3. (The "Differential Nullenstatz" or "Theorem of Zeros") The radical differential ideal $\{F\}$ is precisely the set of all differential polynomials in R that vanish at every zero of F. In particular, $\{F\} = R$ if and only if F has no zeros.

Here, “zero of F” may be interpreted to mean “solution of the system of differential equations $F = 0$.” This immediately raises the foundational question “solution where?" There are two major theorems in differential algebra that legitimize the concept of “zeros of a system.” They assert the existence of a *universal differential field* and a *constrainedly closed differential field* over k. These correspond roughly to the notions of “universal field” and “algebraically closed field” in algebraic geometry. In short, they provide a legitmate algebraic entity in which the zeros of differential polynomial ideals live.

Putting Theorems 1–3 together, we see that we can always express the solution (in some universal extension) of a potentially infinite system of algebraic differential equations as the set of zeros of a finite number of algebraic differential equations (Theorems 1 and 3), and (Theorem 2) we can express the set of zeros as a finite union of “irreducible components”, that is, as a finite union of zeros of prime differential ideals.

Theorem 4. (“Decomposition of a single differential polynomial into its components") Let f be an irreducible differential polynomial in $k\{y_1, \ldots, y_n\}$. Then:

1. Among the components of $\{f\}$ is one, denoted $\mathcal{P}_k(f)$, that does not contain any separant (under any ranking) of f. Each of the other components contains every separant of f.

2. If s is any separant of f, then $\mathcal{P}_k(f) = [f] : s^\infty = \{f\} : s$.

Theorem 5. (“The Component Theorem”.) Let $f \in k\{y_1, \ldots, y_n\} \setminus k$ be irreducible, and let P be a prime component of f. Then there is an irreducible differential polynomial $g \in k\{y_1, \ldots, y_n\}$ such that $P = \mathcal{P}_k(g)$.

Corollary. Let P be a singular prime component of f. Then $P = \mathcal{P}_k(g)$, where g is irreducible, f involves a proper derivative of u_g (relative to any ranking), and $ord(g) < ord(f)$.

<u>Definition</u>. By a *differential monomial* in the indeterminates $Z = z_1, \ldots, z_r$, we mean a power product in the elements of ΘZ.

If M is a differential monomial in Z and $f_1, \ldots, f_r \in k\{y_1, \ldots, y_n\}$, the notation $M(f_1, \ldots, f_r)$ of course refers to the differential polynomial obtained by substitution: for example, if $M = z^3(\delta^2 z)$, then $M(f) = f^3(\delta^2 f)$.

Theorem 6. (Existence of a "Preparation Equation" with respect to a single differential polynomial p.) Let f and p be elements of $k\{y_1, \ldots, y_n\} \setminus k$. Then there exists a "preparation equation"

$$hf = \sum_{j=1}^{s} q_j M_j(p),$$

where $h, q_1, \ldots, q_s \in k\{y_1, \ldots, y_n\} \setminus \mathcal{P}_k(p)$, and $M_1, \ldots, M_s$ are distinct differential monomials in z.

Remark. The statement above is not the most general statement of this result. (See Kolchin's book, pp 183–185.)

Theorem 7. ("The Low Power Theorem") Let f and p be elements of $k\{y_1, \ldots, y_n\}$, and let

$$hf = \sum_{j=1}^{s} q_j M_j(p)$$

be a preparation equation for f with respect to p. Then $\mathcal{P}_k(p)$ is a component of $\{f\}$ if and only if one of the M_j's is of form z^d, and the (total) degree of every other M_j is strictly greater than d.

Remark. Kolchin considerably generalized and strengthened this result. (See Theorem 7 on page 188 of his book.)

Remark. If F is a finite subset of $k\{y_1, \ldots, y_n\}$, we can, at least in theory, compute a finite set of prime differential ideals among which are included all of the prime components of $\{F\}$. However, we do not how to find generating sets for these prime ideals; rather we find them in the form $[G] : h^\infty$, where $G \subset k\{y_1, \ldots, y_n\}$. Unfortunately, we do not know how to determine whether or not two prime ideals given in this form satisfy a containment relation; therefore, we can't extract the prime components of $\{F\}$ from the finite set of prime ideals containing F mentioned above. In the case of the decomposition of a single differential polynomial f, we can use the Low Power Theorem to make this determination. However, even in this case—and even for an ordinary differential polynomial f in one differential indeterminate—we cannot determine whether a given component is contained in a given prime differential ideal, even when we have generators for that ideal.

6 An Open Question: "The Ritt Problem"

Let f be irreducible in $k\{y_1, \ldots, y_n\}$, and suppose that $f \in [y_1, \ldots, y_n]$. Determine whether $\mathcal{P}_k(f) \subseteq [y_1, \ldots, y_n]$.

Remark. A solution to this problem would also provide a solution to the more general problem: Determine whether a solution of $f = 0$ belongs to the general solution.

7 Bibliography

This talk was for the most part extracted from the three books listed below. Section 1 more or less follows Kaplansky, Sections 2 and 3 are more in the spirit of Ritt's book, although the material appears in all three books, and Sections 4 and 5 mostly come from Kolchin's book.

1. Irving Kaplansky, *An Introduction to Differential Algebra*, Hermann, Paris (1957).

2. Ellis R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, (1973)

3. Joseph Fels Ritt, *Differential Algebra*, AMS (1950). Republished by Dover (1966).