

THE KERNEL OF A DERIVATION ON THE FIELD OF RATIONAL FUNCTIONS AND THE ZARISKI CLOSURE OF LOCAL INTEGRAL CURVES

WADE HINDES

1. INTRODUCTION

In this paper we exhibit an algorithm to compute the kernel of a derivation on the rational function field $K(x_1 \dots x_n)$ when K is a field of characteristic zero equipped with the trivial derivation. Also an algorithm to compute the Zariski closure of a local integral curve is included.

2. BACKGROUND

It is first necessary to lay out the ground work crucial for this paper. Only minimal knowledge of elementary field theory, linear algebra, and a mild familiarity with Ideals and Groebner bases are required to comprehend all theorems and examples included within this paper. For the most part this paper is entirely self contained, notions such as Zariski closure, the Wronskian, and Differential Ideals are defined at the outset. With that said, we have our first several definitions.

Definition 1. A **differential field** K , is a field equipped with an additive map $D : K \rightarrow K$ satisfying the Leibniz rule. That is $D(a+b) = D(a) + D(b)$ and $D(ab) = aD(b) + D(a)b$ for all $a, b \in K$.

Definition 2. The kernel of a derivation on a field K , denoted K^D , is called the **field of constants** of K with respect to the derivation D .

It useful to note that if K is a differential field, K^D is a subfield. Certainly, by additivity and the Leibniz rule, K^D is closed under addition, multiplication, and contains zero. Since $D(1) = D(1 \cdot 1) = 1D(1) + D(1)1 = 2D(1)$ we see that $1 \in K^D$. Next suppose $f \in K^D$, then $0 = D(1) = D(ff^{-1}) = fD(f^{-1}) + D(f)f^{-1} = fD(f^{-1})$ so $f^{-1} \in K^D$ and K^D is a subfield. For the purposes of this paper we concern ourselves only with the differential field of rational functions $K(x_1 \dots x_n)$ in n indeterminates. We assume also that K is a field of characteristic zero and that $D(a) = 0$ for all $a \in K$. In order to compute the field of constants of $K(x_1 \dots x_n)$, or using our new notation $K(x_1 \dots x_n)^D$, we must understand what these derivations look like. It is

simple, yet useful for educational purposes, to verify that every derivation D on $K(x_1 \dots x_n)^D$ is of the form $D = \sum_{i=1}^n f_i \partial_i$, with $f_i \in K(x_1 \dots x_n)^D$ and the ∂_i the usual partial derivative in the i th coordinate from ordinary calculus. With this said, the question becomes how would one calculate $K(x_1 \dots x_n)^D$. Upon any reflection it becomes immediately evident that this is in no sense trivial. For instance, what is $K(x_1, x_2, x_3, x_4)^D$ with

$$D = (x_4^7 - x_1 x_2) \partial_1 + (x_3 + x_2 x_4^3) \partial_2 + (x_2 x_3) \partial_3 + (x_1 + x_4^2 x_2) \partial_4$$

Where does one even start? Is it even plausible to find something non-trivial in some time less than the age of the universe? To answer this question affirmatively we need some more powerful tools.

Definition 3. The **wronskian** of the n elements $y_1, y_2 \dots y_n$ is defined as

$$\text{the determinant } W(y_1 \dots y_n) = \begin{vmatrix} y_1 & y_2 & \dots & y_n \\ D(y_1) & D(y_2) & \dots & D(y_n) \\ \vdots & \vdots & \ddots & \vdots \\ D^{n-1}(y_1) & D^{n-1}(y_2) & \dots & D^{n-1}(y_n) \end{vmatrix}$$

This new object leads us to an elementary result which plays a vital role in both of our algorithms.

Proposition 1. *If F is a differential field with field of constants F^D . Then $y_1 \dots y_n \in F$ are linearly dependent over F^D if and only if $W(y_1 \dots y_n) = 0$.*

Proof. Suppose the $y_1 \dots y_n$ are over F^D , ie there exist $c_i \in F^D$ such that $\sum_{i=1}^n c_i y_i = 0$. Upon differentiating this equation $n - 1$ we get n linear homogeneous equations for the c_i 's. Since the c_i 's are not all zero, by the dependence assumption, the determinant of the matrix

$$M_n = \begin{pmatrix} y_1 & y_2 & \dots & y_n \\ D(y_1) & D(y_2) & \dots & D(y_n) \\ \vdots & \vdots & \ddots & \vdots \\ D^{n-1}(y_1) & D^{n-1}(y_2) & \dots & D^{n-1}(y_n) \end{pmatrix}$$

must be zero. Conversely suppose $W(y_1 \dots y_n) = 0$. Then we can find non-trivial solutions $c_1 \dots c_n$ such that $M_n(c_1 \dots c_n) = 0$, hence $\sum_{i=1}^n c_i D^j(y_i) = 0$ for $0 \leq j \leq n - 1$. Without loss of generality we may assume that $c_1 = 1$, and that $W(y_2 \dots y_n) \neq 0$. Differentiating the first $n - 1$ of our equations and then cancelling the appropriate original equations, we arrive at $n - 1$ linear homogeneous equations in $D(c_1) \dots D(c_n)$ with the determinant equal to $W(y_2 \dots y_n)$. Hence $D(c_1) \dots D(c_n) = 0$ for all i . ■

One should note that if $y_1, y_2 \dots y_n \in F$ are elements linearly independent over the field of constants of F , then they are also linearly independent over the field of constants of any differential extension field. In this context (E, D_E) is said to be a differential extension field of (F, D_F) if $E \supseteq F$ and $D_E(a) = D_F(a)$ for all $a \in F$. To see this we just employ the proposition

above. If $y_1, y_2 \dots y_n \in F$ are elements linearly independent over F^D , then $wr(y_1, y_2 \dots y_n) \neq 0$. Next consider $y_1, y_2 \dots y_n$ as elements in E . Again this set is linearly independent over E^D if and only if the wronskian does not vanish. But the wronskian did not change by considering them in the extension field, as the derivation on E restricts to the derivation on F . There is another important thing to notice about the previous result as it pertains to our task of computing $K(x_1 \dots x_n)^D$, the wronskian can be used to find nontrivial constants. Concretely, suppose we have a set $\{a_i\}$ independent over K , and $W(\{a_i\}) = 0$. Then the solutions cannot all be in K , that is some will be nontrivial constants. We will continue this train of thought to an algorithm but first the last auxiliary term must be defined.

Definition 4. A **total degree ordering on the monomials** is an ordering on the set $M = \{f \in K[x_1 \dots x_n] | f = x_1^{j_1} \dots x_n^{j_n}\}$ such that if $\partial(f) = \sum_{i=1}^N deg_i(f) > \partial(g) = \sum_{i=1}^N deg_i(g)$ then $f > g$ and if $\partial(f) = \partial(g)$ then $f > g$ if and only if $lex(f) > lex(g)$. Here $lex(f)$ denotes the lexicographical ordering on the monomials. For every monomial $m = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$ we associate the vector $(e_1, e_2 \dots, e_n)$. Then $m_1 > m_2$ if and only if $e_{1,i} > e_{2,i}$ where i is the first non zero coordinate in either m_1 or m_2 starting from the left. From this point forward we denote the leading term, or largest monomial, of f as $Lm(f)$.

3. THE KERNEL OF A DERIVATION ON THE RATIONAL FUNCTION FIELD

Now that the groundwork has been laid, we are finally ready to discuss our Algorithm. Suppose $K \neq K(x_1, x_2 \dots x_n)^D$ and we use total degree ordering to list all the monomials in sequential form $M = \{m_1, m_2 \dots\}$. Next we compute $W_2 = W(m_1, m_2)$. If $W_2 = 0$ then we have found non-trivial constant, as the monomials are linearly independent over K . If not, suppose we continue to add monomials to our list to yield $\{m_1, m_2 \dots m_r\}$. Will we eventually reach a point W_r , such that $W_r = 0$ and $W_{r-1} \neq 0$? This result we state in the following proposition.

Proposition 2. *If $K(x_1 \dots x_n)^D \neq K$ then there exists a positive integer r such that $W_r = 0$.*

Proof. Suppose $f = \sum_{i=1}^N a_i m_i / \sum_{j=1}^K b_j m_j = g/h$ with $g, h \in K[x_1 \dots x_n]$ with $f \in K(x_1 \dots x_n)^D$. Then we consider $hf - g = 0$ which yields

$$\sum_{j=1}^K (b_j f) m_j - \sum_{i=1}^N a_i m_i = 0$$

. Then the monomials $\{m_j\} \cup \{m_i\}$ are dependent over $K(f) \subset K(x_1 \dots x_n)^D$. So if $m_r = \max\{Lm(g), Lm(h)\}$ then $W_r = 0$. ■

With this result if $K \neq K(x_1, x_2 \dots x_n)^D$, we can always find some non-trivial constants $c_1, c_2 \dots c_{k-1}$ such that $m_k = \sum_{i=1}^{k-1} c_i m_i$. Suppose now that we keep testing dependence relations among the monomials, excluding

the dependent monomials we have already found. We should also exclude any multiples of the dependent monomials as well, for If m_k is dependent on the independent set $\{m_1, m_2 \dots m_{k-1}\}$ over $L \subseteq K(x_1, x_2 \dots x_n)^D$, then certainly any power of m_k will also be dependent. Now we consider the subfield $K(c_1, c_2 \dots c_k) \subseteq K(x_1, x_2 \dots x_n)^D$. Will there be a set

$$A = \{m_1, m_2, \dots, \widehat{m_k}, m_{k+1} \dots \widehat{m_k^2} \dots m_r\}$$

, with $W_A = 0$ if $K(c_1, c_2 \dots c_k) \neq K(x_1, x_2 \dots x_n)^D$? Can we carry this process forward, continuing to add the constants found in the coefficients in the dependencce relations, to eventually get field generators $f_1, f_2 \dots f_t$ with $K(f_1, f_2 \dots f_t) = K(x_1, x_2 \dots x_n)^D$? The first question about this dependent set A is stated in the following propostion.

Proposition 3. *Let M be the set of monomials in $K[x_1 \dots x_n]$, and $A \subset M$. Suppose $L \subset K(x_1 \dots x_n)^D$ is a subfield such that $\langle A \rangle_{L_{span}} = \langle M \rangle_{L_{span}}$ with A independent over L . If $K(x_1 \dots x_n)^D \supsetneq L$, then A is dependent over $K(x_1 \dots x_n)^D$.*

Proof. Choose $f \in K(x_1 \dots x_n)^D - L$, $f = \sum_{i=1}^N a_i m_i / \sum_{j=1}^K b_j m_j = g/h$ with $g, h \in K[x_1 \dots x_n]$ and $f \in K(x_1 \dots x_n)^D$. By the assumption, f can be written as $f = \sum_{i=1}^N l_i a_i / \sum_{j=1}^K l_j a_j$ with $l_{i,j} \in L$, and $a_{i,j} \in A$. As before we consider the equation

$$\left(\sum_{j=1}^K l_j a_j \right) f - \sum_{i=1}^N l_i a_i = \sum_{j=1}^K (l_j f) a_j - \sum_{i=1}^N l_i a_i = 0$$

. Then the set $\{a_i\} \cup \{a_j\}$ are dependent monomials over $L(g) \subset K(x_1 \dots x_n)^D$. ■

Before we continue on down the road to field generators for the constant subfield, we record a fruitful consequence of our preliminary work.

Example 1. Let $D = f\partial_1 + g\partial_2$ be a derivation on $K(x_1, x_2)$ such that $D(K) = 0$ and $f, g \neq 0$. If $w(f, g) = 0$, then $K(x_1, x_2)^D = K(g/f, g/fx_1 - x_2)$.

Proof. To see this we employ our pre-algorithm and proposition 2. Note that $w(1, x_1) = 0$ if and only if $f = 0$. Sice it does not, by assumption, we proceed. Note that $w(1, x_1, x_2) = 0$ if and only if $w(f, g) = 0$. Because we have the latter, we may assume there exist $c_1, c_2 \in K(x_1, x_2)^D$ such that $x_2 = c_1 + c_2 x_1$. A routine linear algebra calculation show that $-g/f$ and $g/fx_1 - x_2$ are such constants. So $K(g/f, g/fx_1 - x_2) \subseteq K(x_1, x_2)^D$. To show the other inclusion we use the proposition. We have a subset $A = \{1, x_1, x_1^2 \dots\}$ such that $\langle A \rangle_{L_{span}} = \langle M \rangle_{L_{span}}$ with $L = K(g/f, f/gx_1 - x_2)$ and A independent over L. Thus If A is independent over $K(x_1, x_2)^D$ then $K(x_1, x_2)^D = L$. We prove that A is independent over L by induction on the degree of x_1 . The case where the $deg_1(x_1^i) = 1$ is clear, for if $x_1 = c$ with

$c \in K(x_1, x_2)^D$, then $D(x_1) = 0 = f$. But f was non zero by assumption. Now for the general case where $\deg_1(x_1^i) = n$. Suppose $c_n x_1^n = \sum_{i=1}^{n-1} c_i x_1^i$. Without loss of generality we may assume $c_n = 1$, for if $c_n = 0$ then the set $\{x_1 \dots x_1^{n-1}\}$ is dependent over $K(x_1, x_2)^D$ which contradicts the induction hypothesis. Then by our dependence relation,

$$n x_1^{n-1} D(x_1) = D(x_1^n) = D\left(\sum_{i=1}^{n-1} c_i x_1^i\right) = \sum_{i=1}^{n-1} D(c_i x_1^i) = \sum_{i=1}^{n-1} c_i D(x_1^i) = \sum_{i=1}^{n-1} (c_i)(i)(x_1^{i-1}) D(x_1)$$

. Since we may freely divide by the nonzero $D(x_1)$ and n , our equation yields

$$x_1^{n-1} = \sum_{i=1}^{n-2} k_i x_1^i$$

, with $k_i = c_i(i)/n$ which contradicts the induction hypothesis. So A is independent over $K(x_1, x_2)^D$, hence by proposition 2, $L = K(x_1, x_2)^D$. ■

Conjecture 1. *If $D = f\partial_1 + g\partial_2$ and $W(f, g) = 0$ then either $g/f \in K$ or $g/fx_1 - x_2 \in K$.*

If true, then by the example, either $K(x_1, x_2)^D = K(g/f)$ or $K(x_1, x_2)^D = K(g/fx_1 - x_2)$ in the above setting. It is known that $K(x_1, x_2)^D = K(f)$ for some $f \in K(x_1, x_2)$. For an elegant proof of this fact see Kaplansky's Differential Algebra. It is in general an unsolved problem to determine the number of elements needed to generate K^D for a fixed derivation. Now back to our question of whether it is possible in a finite number of steps to reach field generators for $K(x_1 \dots x_n)^D$ by adjoining the coefficients in the dependence relations among the monomials. In order to do this we realize the gathering of these dependence relations as the computing of a Groebner basis for the kernel of some homomorphism defined below. Since this ideal will be contained in a Noetherian ring, our process must be finite. We record an essential result and define this ideal in the following theorem.

Theorem 2. *Let $\phi : K(x_1 \dots x_n)^D[y_1 \dots y_n] \rightarrow K(x_1 \dots x_n)$ be the ring homomorphism given by $\phi(y_i) = x_i$ and $\phi_{K(x_1 \dots x_n)^D} = Id$. Suppose $I = \ker(\phi)$ has reduced Groebner basis $G = \{g_1 \dots g_k\}$ with $g_i = m_{ki} + \sum_{j=1}^{k_i-1} a_{ij} m_{ij}$, and $a_{ij} \in K(x_1 \dots x_n)^D$. If $W = \{a_{ij}\}$ then $K(x_1 \dots x_n)^D = K(W)$.*

Proof. The first inclusion is clear as $K(W)$ is generated by elements in $K(x_1 \dots x_n)^D$, so $K(W) \subseteq K(x_1 \dots x_n)^D$. On the other hand suppose $f \in K(x_1 \dots x_n)^D$ with

$$f = \sum_{i=1}^N a_i m_i / \sum_{j=1}^K b_j m_j = g/h$$

with $g, h \in K[x_1 \dots x_n]$. Then

$$\phi(h(y_1 \dots y_n)f(x_1 \dots x_n) - g(x_1 \dots x_n)) = 0$$

. As $G = \{g_1 \dots g_k\}$ is a Groebner basis, every $F \in K(x_1 \dots x_n)^D[y_1 \dots y_n]$ has a unique reduction *modulo* (G) , and the projection map $\pi : K(x_1 \dots x_n)^D[y_1 \dots y_n] \rightarrow K(x_1 \dots x_n)^D[y_1 \dots y_n]/I$ by $\pi(F) = \bar{F}$ is a homomorphism of rings. Then we see that

$$0 = \overline{h(y_1 \dots y_n)f(x_1 \dots x_n) - g(y_1 \dots y_n)} = \overline{h(y_1 \dots y_n)f(x_1 \dots x_n) - g(y_1 \dots y_n)} = \overline{\overline{h(y_1 \dots y_n)f(x_1 \dots x_n)} - \overline{g(y_1 \dots y_n)}}$$

. It is essential to note that the coefficients of $\overline{h(y_1 \dots y_n)}$ and $\overline{g(y_1 \dots y_n)}$ are in $K(W)$. We see this by examining the division algorithm. Without loss of generality we reduce h . If $h = \sum_{j=1}^K b_j m_j$, then we write

$$h = \sum_{j=1}^{K-1} b_j m_j - (b_k m_k / m_{k_i}) g_i - (b_k m_k / m_{k_i}) \sum_{j=1}^{k_i-1} a_{ij} m_{ij}$$

for some g_i with $Lt(g_i)/m_k$. If no such i exists then h respectively g have coefficients in $K \subseteq K(W)$. Note that the remainder has coefficients in $K(W)$ as the b_j and a_{ij} . We proceed inductively and see that the remainders of h, g have coefficients in $K(W)$. Then we may rewrite

$$0 = \overline{h(y_1 \dots y_n)f(x_1 \dots x_n) - g(y_1 \dots y_n)}$$

as $0 = (\sum_{i=1}^n w_{1i} m_{1i})f - \sum_{i=1}^n w_{2i} m_{2i}$, with $w_i \in K(W)$. This directly implies $f \in K(W)$, as f is a constant polynomial in $K(x_1 \dots x_n)^D[y_1 \dots y_n]$, our equality forces $w_{1i}f - w_{2i} = 0$ and by selecting a nonzero w_{1i} , we have $f = w_{1i}/w_{2i}$ hence $f \in K(W)$. On the other hand If all $w_{1i} = 0$ then

$$0 = \left(\sum_{i=1}^n w_{1i} m_{1i}\right)f - \sum_{i=1}^n w_{2i} m_{2i}$$

implies all w_{2i} are zero. Thus $h, g \in I$. Then $0 = \phi(h(y_1 \dots y_n)) = h(x_1 \dots x_n)$ which is a contradiction. So we may assume there exists a $w_{1i} \neq 0$. Hence, as above, $f \in K(W)$ and $K(x_1 \dots x_n)^D \subseteq K(W)$. ■

At this point the results are in place to formalize an algorithm to compute the field of constants in $K(x_1, x_2 \dots x_n)$. This is done by collecting the dependence relations among "reduced" sets of monomials. The notion of reduced just means that the largest monomial, with respect to our ordering, is dependent on a set of independent smaller terms. The theorems and propositions stated above will ensure that our algorithm terminates.

3.1. Algorithm 1: The Field of Constants of the Rational Function Field

step(1): $m_1 = 1, S_1 = \emptyset, T_1 = \{1\}, G_1 = \emptyset$

step(2): Choose $\text{inf}\{M - \{1\}\} = m_2$. Here inf just means the smallest monomial within the given set.

(a): If $T_1 \cup \{m_2\}$ is linearly dependent over $K(x_1 \dots x_n)^D$ i.e. $w(T_1 \cup \{m_2\}) = 0$, then there exist $l_1 \neq 0$ such that $m_2 + l_1 = 0$. Set

$$S_2 = S_1 \cup \{m_2\}, T_2 = T_1, G_2 = \{m_2 + l_1 \mid m_2 + l_1 \in K(x_1 \dots x_n)^D [y_1 \dots y_n] \text{ and } \phi(m_2 + l_1) = 0\}$$

.

(b): $T_1 \cup \{m_2\}$ is linearly independent over $K(x_1 \dots x_n)^D$ i.e. $w(T_1 \cup \{m_2\}) \neq 0$, then set

$$T_2 = T_1 \cup \{m_2\}, S_2 = S_1, G_2 = G_1.$$

⋮

step(n): Choose $\text{inf}\{M - A_{n-1}\} = m_k, A_{n-1} = \{m \in M \mid m = s_1^{j_1} \dots s_t^{j_t}, s_i \in S_{n-1}\}$

(a): If $T_{n-1} \cup \{m_k\}$ is linearly dependent over $K(x_1 \dots x_n)^D$ i.e. $w(T_{n-1} \cup \{m_k\}) = 0$, then there exists $l_i \in K(x_1 \dots x_n)^D$ such that $m_k = \sum_{i=1}^{|T_{n-1}|} l_i m_i$, with $m_i \in T_{n-1}$. Then set

$$T_n = T_{n-1}, S_n = S_{n-1} \cup \{m_k\}, G_n = G_{n-1} \cup \{m_k + \sum_{i=1}^{|T_{n-1}|} l_i m_i \mid \phi(m_k + \sum_{i=1}^{|T_{n-1}|} l_i m_i) = 0\}$$

.

(b): $T_{n-1} \cup \{m_k\}$ is linearly independent over $K(x_1 \dots x_n)^D$ i.e. $w(T_{n-1} \cup \{m_k\}) \neq 0$, Then set

$$T_n = T_{n-1} \cup \{m_k\}, S_n = S_{n-1}, G_n = G_{n-1}$$

.

Note that the set G of dependence relations of the form $m_k = \sum_{j=1}^n c_j m_{ij}$, with $\{m_{ij}\}$ independent, generate I . In particular as $K(x_1 \dots x_n)^D [y_1 \dots y_n]$ is Noetherian, there exist a finite subset $G_k = \{g_1 \dots g_k\}$ such that $I = \langle G_k \rangle$. From this point forward we write G_k as G . To see this suppose some $\phi(f) = \phi(m_d + \sum_{i=1}^{d-1} c_i m_i) = 0$ with $c_i \in K(x_1 \dots x_n)^D$, and the m_i are monomials in Y_i . As $\phi(y_i) = x_i$, $\phi(f) = 0$ implies that m_k as a variable in the x_i is dependent on the others. Without loss of generality we may assume that $\{m_1 \dots m_{d-1}\}$ are independent, for if they are not, we merely write them as a linear combination of the lower terms. So we see G generates I . Also since the monomials are independent over the field of constants, then we have that the set is reduced. This argument yields the following result.

Proposition 4. *The set G is a reduced Grobner basis for I . Suppose $f \in \text{Lt}(I)$ then $f = c_1 m_1 + \dots + c_n m_n, c_i \in K(x_1 \dots x_n)^D [y_1 \dots y_n]$ and $m_i = \text{Lt}(h_i)$ with $h_i \in I$. We show that each $m_i \in \text{Lt}(G)$. We have $0 = \phi(h_i) = \phi(m_i + \sum_{j=1}^{i-1} k_j m_j)$.*

Now using the previous two results we can prove that our algorithm will calculate field generators for $K(x_1, x_2 \dots x_n)^D$. Now we set a bound on the number of step it takes to generate the field of constants. It is essential to note that our algorithm is very sensitive to the monomial ordering we chosen at the outset. An interesting topic for future investigation would be to identify which monomial ordering would calculate $K(x_1, x_2 \dots x_n)^D$ in the least number of steps for a fixed derivation.

Theorem 3. *Suppose $K(x_1 \dots x_n)^D = K(f_1 \dots f_k)$ with each $f_i = g_i/h_i$ and $d = \max\{\partial(f_i)\}$. If α is the number of steps such that $K(W_\alpha) = K(x_1 \dots x_n)^D$, then $\alpha \leq \binom{d+n}{n}$.*

Proof. We first show that for each f_i there exists a specific W_{k_i} such that $f_i \in K(W_{k_i})$ and $k_i \leq t$ with $m_t = Lm(f_i)$. Then as our algorithm remembers the dependence relations it saw before, i.e $W_n = \cup W_i \ i \leq n-1$, by choosing $m_e = \max\{Lm(f_i)\}$ we insure $\max\{k_i\} \leq e$ with $K(W_{\max\{k_i\}}) = K(f_1 \dots f_k)$. Then as our preferred ordering is a total degree ordering, we can bound e in terms of d, n . Choose an arbitrary $f_i = \sum_{i=1}^N a_i m_i / \sum_{j=1}^K b_j m_j$, we let $m_{e_i} = \max\{Lm(g_i), Lm(h_i)\}$ and rewrite g, h as sums up to e_i , realizing that the last several terms in either g or h may be zero. Without loss of generality we may assume $Lm(h_i) = m_{e_i}$, for if not then we just use f^{-1} instead of f , as $K(f_1 \dots f_i, \dots f_k) = K(f_1 \dots f_i^{-1}, \dots f_k)$. Then we have the dependence relation $\sum_{j=1}^{e_i} (b_j f_i - a_j) m_j = 0$ and $w_{e_i} = 0$. Then there exists some W_{k_i} , the set of coefficients such that $m_{e_i} = \sum_{t=1}^l c_t m_t \{m_t\}$ independent and $m_t \leq m_{e_i} \forall t$. such that $\{m_1 \dots m_{e_i}\}$ are dependent over $K(W_{k_i})$. Of course $k_i \leq e_i$, and equal if and only if the set $\{m_1 \dots m_{e_i-1}\}$ is independent. Then we compare our algorithm's set of coefficients the W_{k_i} to the coefficients $\{b_j f_i - a_j\}$. Note that the last term $b_{e_i} f_i - a_{e_i} \neq 0$, for this would imply $f \in K$ as $b_{e_i} \neq 0$, which we assume f_i is not in K . Then we can equate our two different dependence relations

$$\left(\sum_{j=1}^{e_i} (b_j f_i - a_j) m_j \right) / - (b_{e_i} f_i - a_{e_i}) = m_{e_i} = \sum_{t=1}^l c_t m_t$$

, with $c_t \in W_{k_i}$ and the $\{m_t\}$ independent. There are two cases: the first being that the set $\{m_1 \dots m_{e_i-1}\}$ are independent over the field of constants, in which case $e_i = l$, and the coefficients on both sides are equal, i.e $(b_j f_i - a_j) / - (b_{e_i} f_i - a_{e_i}) = c_j$. Then we solve for $f = (c_j a_{e_i} - a_j) / (c_j b_{e_i} - b_j)$, for all j with the denominator not zero. Note that there must exist a j such that the denominator is not zero, for this would imply $c_j \in K$ for all j , but this cannot be as the monomials are independent over K . So $f \in K(W_{k_i})$. On the other hand we assume that the $\{m_1 \dots m_{e_i-1}\}$ is dependent over $K(x_1 \dots x_n)^D$. But this poses no problems for we merely reduce the monomials which are a linear combination of the other terms and write them as such. The key is all dependence coefficients will still be in $K(W_{k_i})$, as our algorithm remembers

all dependence relations for lower terms. Then we again have

$$\sum_{t=1}^l l_t((b_t f_i - a_t)m_t) / - (b_{e_i} f_i - a_{e_i}) = \sum_{t=1}^l c_t m_t$$

, with $l_t, c_t \in W_{k_i}$. Then again, because of the independence of the $\{m_t\}$, $f_i = (c_t/l_t a_{e_i} - a_t)/(c_t/l_t b_{e_i} - b_t)$, with not all $l_t = 0$ and not all $(c_t/l_t b_{e_i} - b_t) = 0$. So $f_i \in K(W_{k_i})$. Then choose $m_e = \max\{Lm(f_i)\}$, and its corresponding $W_{\max\{k_i\}}$ with $f_i \in K(W_{\max\{k_i\}}) \forall i$. Then $K(W_{\max\{k_i\}}) = K(f_1 \dots f_k) = K(x_1 \dots x_n)^D$, with $k_i \leq e$. So the number of steps α for which $K(W_\alpha) = K(x_1 \dots x_n)^D$ is bounded by how "far out" the largest term appearing in the f_i 's is. If we use the total degree ordering and let $d = \max\{\Delta(f_i)\}$, then the leading term is no farther out then the total number of monomials with total degree less than or equal to d . Hence $\alpha \leq \binom{d+n}{n}$. ■

Before moving onto the next problem in the paper we should make note on the usefulness of computing the field of constants in $K(x_1, x_2 \dots x_n)$. For linear differential equations on an arbitrary field F ie, equations of the form $L(y) = D^l(y) + \sum_{i=0}^{l-1} c_i D^i(y)$, the solutions form a finite dimensional vector space over the field of constants F^D of dimension at most l . One can ask whether there exist a minimal differential extension E of F such that E has a set of solutions of dimension exactly l over $E^D = F^D$. It turns out, using differential Galois theory, the solvability of the equation L is closely related to the group of differential automorphisms of E , automorphisms that commute with the derivation. However it is quite difficult to understand this if you don't know what the field of constant are. For instance consider $L(y) = D^2(y) + 2(x_1 + x_1 x_2)D(y) + x_2 y$ a linear differential equation over $K(x_1, x_2)$. To find this mysterious extension, as above, one must know $K(x_1, x_2)^D$. A final remark should be made about future topics of discussion. We have proven that our algorithm will eventually calculate the field of constants for $K(x_1 \dots x_n)$. The drawback is that we may never know exactly we our algorithm terminates. We can put a bound that is a function of the field generators, but these are of course the objects we seek. Formally, is there a way to determine if our set $K(W)$ actually encompasses all the constants without continuing to test dependence relations forever. It is not clear whether this problem is even decidable. Now for the second topic of interest.

4. THE ZARISKI CLOSURE OF LOCAL INTEGRAL CURVES

For the second algorithm to compute the Zariski Closure of Local integral curves, we will use our first algorithm and the results that go along with it as a model, although it is necessary to be a little more sophisticated. That is to say a few more auxiliary terms must be defined and more intricate results proven.

Definition 5. A **differential Ideal** I , contained in a differential Ring R , is an ideal such that $D(I) = \{b = D(a) | a \in I\} \subseteq I$. A maximal differential Ideal is therefore a differential ideal with no proper nonzero differential ideals. If I is a differential Ideal then the quotient R/I is also a differential Ring with derivation $D(a + I) = D(a) + I$, where D is the derivation on R . A result contained in Kaplansky's differential algebra is recorded below. It is useful for understanding the algebraic object we hope to compute later on.

Proposition 5. *Let R be differential ring containing the field of rational numbers then the radical of a differential ideal is a differential ideal*

Proof. We show that if I is a differential ideal and $a^n \in I$, then $D(a)^{2n-1} \in I$. Note that this will prove the proposition. We have that $D(a^n) = na^{n-1}D(a) \in I$. Since I admits multiplication by n^{-1} , we have that $a^{n-1}D(a) \in I$. This is the case $k = 1$ of the statement $a^{n-k}D(a)^{2k-1} \in I$. We proceed by induction. We differentiate:

$$(n - k)a^{n-k-1}D(a)^{2k-1} + (2k - 1)a^{n-k}D(a)^{2k-2} \in I$$

After multiplying by $D(a)$ we see that the second term lies in I . We can cancel the factor $n-k$ in the first term and we find $a^{n-k-1}D(a)^{2k-1} \in I$, which is the case $k + 1$ of the statement we are proving inductively, then we arrive at $k = n$, which gives $D(a)^{2n-1} \in I$. ■

Definition 6. If $D = \sum_{i=1}^N P_i \partial_i$ with $P_i \in K[y_1, y_2 \dots y_n]$ is a derivation on $K(y_1, y_2, \dots y_n)$. Then $y(t) : K^N \rightarrow K^N$ with $y(t_1, t_2 \dots t_n) = (y_1(t_1), y_2(t_2) \dots y_n(t_n))$, $y_i(t_i) = \sum_{j=1}^{\infty} D^j(x_1, x_2 \dots x_n) t^j / j!$ for a fixed vector $(x_1, x_2 \dots x_n) \in K^n$ and $t_i \in (x_i - \epsilon, x_i + \epsilon)$ for some $\epsilon < 0$ is called a **local integral curve about** $(x_1, x_2 \dots x_n)$.

We should remark on why these particular functions are called local integral curves. It is simply because if $D = \sum_{i=1}^N P_i \partial_i$ then $y(t) = (y_1(t), y_2(t) \dots y_n(t))$ with $y(0) = x$ satisfies the system of differential equations $D(y_i) = P_i(y_1, y_2 \dots y_n)$. It is beyond the scope of this paper, infact it is a classical analysis result, to verify that for each vector $(x_1, x_2 \dots x_n)$, such a function y exists i.e the infinite series converge on some possibly small interval. Infact, by using some compactness argument, one can show that it does not depend on ϵ . This leads us to the definitions and the algebraic object we wish to calculate.

Definition 7. The **Zariski closure of a local integral curve y** , as in the previous definition, is the set $I_x = \{f \in K[y_1, y_2 \dots y_n] | f(y(t)) = 0 \text{ for some } \epsilon\}$.

This brings us to a useful result of the former notion.

Proposition 6. *If y is a local integral curve for the point $(x_1, x_2 \dots x_n)$, Then the Zariski closure of y , denoted I_x , is a maximal differential ideal contained in $m_x = \{f \in K[y_1, y_2 \dots y_n] | f(x_1, x_2 \dots x_n) = 0\}$.*

Proof. This follows immediately from the fact that $f \in I_x$ if and only if $(D^j f)(x) = 0$ for all positive integers j , as an application of the chain rule. This seems like an easier notion of membership in I_x to work with. It is thus valid to make this notion our definition.

Definition 8. The Zariski Closure of a local integral curve about the point $x \in K^n$ is the set $I_x = \{f \in K[x_1, x_2, \dots, x_n] \mid (D^i f)(x) = 0 \text{ for all } i\}$. ■

With this definition we record some useful properties of I_x .

Proposition 7. I_x is a prime ideal for all points $x \in K^n$.

Proof. Suppos $p, q \in K[x_1, \dots, x_n]$ are such that $pq \in I_x$ for some $x \in K^n$. Equivalently, $D^i(pq)(x) = 0$ for all positive integers i . We wish to show either $p \in I_x$ or $q \in I_x$. Suppose there exists an integer k such that $D^k(q)(x) \neq 0$. Then our goal becomes to show $p \in I_x$. If no such k exists, then $q \in I_x$. Without loss of generality we may assume that k is minimal, that is $D^j(q)(x) = 0$ for all $j < k$. We show by induction that $D^i(p)(x) = 0$ for all $i \geq 0$. By assumption

$$0 = D^k(pq)(x) = \left[\sum_{i=0}^k C_{ki}(D^i p) D^{k-i}(q) \right](x) = \left[\sum_{i=1}^k C_{ki}(D^i p) D^{k-i}(q) \right](x) + (pD^k)(x)$$

where C_{ki} are the coefficients $\binom{k}{i}$. Note however that the sum

$$\left[\sum_{i=1}^k C_{ki}(D^i p) D^{k-i}(q) \right](x) = 0$$

as each term has a coefficient $(D^j q)(x)$ with $j < k$ which is zero by assumption. Then our equation above yields

$$0 = (pD^k)(x) = p(x)(D^k q)(x)$$

hence $p(x) = 0$ as $(D^k q)(x) \neq 0$. Now for the inductive step. Assume for a positive integer m , we have $(D^i p)(x) = 0$ for all $i \leq m-1$. From the assumption that $pq \in I_x$ we have

$$0 = (D^{k+m} pq)(x) = \left[\sum_{i=0}^{k+m} C_{k+m,i}(D^i p) D^{k+m-i}(q) \right](x) = \left[\sum_{i=0}^{m-1} C_{k+m,i}(D^i p) D^{k+m-i}(q) \right](x) + C_{k+m,m}(D^m p)(D^k q)(x) + \left[\sum_{i=m}^{k+m} C_{k+m,i}(D^i p) D^{k+m-i}(q) \right](x)$$

Note that the sum

$$\left[\sum_{i=0}^{m-1} C_{k+m,i}(D^i p) D^{k+m-i}(q) \right](x) = 0$$

as every term contains a coefficient $(D^i p)(x)$ for $i < m$ which are all zero by the induction hypothesis. Similarly

$$\left[\sum_{i=m}^{k+m} C_{k+m,i} (D^i p) D^{k+m-i}(q) \right](x) = 0$$

as each term in the sum contains a coefficient $(D^j q)(x)$ with $j \leq k$. Then our equation above yields

$$0 = C_{k+m,m} (D^m p) (D^k q)(x) = C_{k+m,m} (D^m p)(x) (D^k q)(x)$$

hence $(D^m p)(x) = 0$ as $(D^k q)(x) \neq 0$. So $(D^i p)(x) = 0$ for all $i \geq 0$. ■

Proposition 8. *The differential ideal I_x a radical differential ideal.*

Proof. We show that $\text{rad}(I_x) = I_x$. Certainly by definition $I_x \subseteq \text{rad}(I_x)$. On the other hand suppose $f \in \text{rad}(I_x)$. Then $f^n \in I_x$ for some n . Then $f^n(x) = 0$, as $K[y_1, y_2 \dots y_n]$ is a domain, $f(x) = 0$. So $\text{rad}(I_x) \subseteq I_x$. But by proposition 5, $\text{rad}(I_x)$ is a differential ideal. Then as I_x is the maximal differential ideal contained in m_x , $\text{rad}(I_x) \subseteq I_x$. So we have equality. ■

To compute generators for I_x , an approach mirroring that of the field of constants algorithm is adopted.

Proposition 9. *If $I_x \neq 0$, then there exists a positive integer r such that $W_r(x) = 0$.*

Proof. Suppose $f = \sum_{i=1}^n c_i m_i \in I_x$ with $f \neq 0$. Then $(D^j f)(x) = \sum_{i=1}^n c_i (D^j m_i)(x) = 0$ for all $0 \leq j \leq n-1$. Then the vector $(c_1, c_2 \dots c_n)$ is a solution to $M_n(x) : K^n \rightarrow K^n$, i.e

$$\begin{pmatrix} m_1(x) & m_2(x) & \dots & m_n(x) \\ D(m_1)(x) & D(m_2)(x) & \dots & D(m_n)(x) \\ \vdots & \vdots & \ddots & \vdots \\ (D^{n-1}m_1)(x) & (D^{n-1}m_2) & \dots & (D^{n-1}m_n)(x) \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

furthermore $(c_1, c_2 \dots c_n)$ is a nontrivial solution as f was assumed to be nonzero. Then $W_n(x) = 0$. ■

This of course bares a remarkable similarity to the results on the kernel of a derivation. Suppose we try as before to list the monomials out, using are total degree ordering, and reach a point r such that $W_r(x) = 0$. Then there exist nontrivial solutions $(c_1, c_2 \dots c_r)$ such that $\sum_{i=1}^r c_i (D^j m_i)(x) = 0$ for all $0 \leq j \leq r-1$. Then set $f = \sum_{i=1}^r c_i m_i$. Is $f \in I_x$? Not quite, it is only a candidate. By construction $(D^j f)(x) = 0$ for all $0 \leq j \leq r-1$. However we can not be entirely certain that $D^r f(x) = 0$, or thereafter. However if it is the case that $D^i f(x) = 0$ for all natural numbers i , then $f \in I_x$ as I_x is a maximal differential ideal contained in m_x . How does one verify this? Let $\langle f \rangle_D$ denote the smallest differential ideal containing

f , that is $\langle f \rangle_D = \langle f, Df \dots D^r f \dots \rangle$. However since we are in the Noetherian setting, there exist a k such that $\langle f \rangle_D = \langle f, Df \dots D^k f \rangle$. Then it is enough to show that $D^i f(x) = 0$ for all $0 \leq i \leq k$ to show $f \in I_x$. This becomes the ideal membership problem, which is to say if $I_k = \langle f, Df \dots D^k f \rangle$, then we are searching for a k such that $I_k = I_{k+1}$. For this would imply that $D^{k+1} f \in I_k$. Hence $D^{k+1} f = \sum_{i=0}^k g_i D^i f$ for some $g_i \in K[y_1, y_2 \dots y_n]$. Then applying D to both sides we see that

$$\begin{aligned} D^{k+2} f &= \sum_{i=0}^k D(g_i D^i f) = \sum_{i=0}^k g_i D^{i+1} f + D^i f D(g_i) = \\ &= \sum_{i=0}^k D^i f D(g_i) + \sum_{i=0}^k g_i D^{i+1} f = \sum_{i=0}^k D^i f D(g_i) + \sum_{i=0}^{k-1} g_i D^{i+1} f + g_k D^{k+1} f = \\ &= \sum_{i=0}^k D^i f D(g_i) + \sum_{i=0}^{k-1} g_i D^{i+1} f + \sum_{i=0}^k g_k g_i D^i f = \sum_{i=0}^k [D(g_i) + g_k g_i] D^i f + \sum_{i=0}^{k-1} g_i D^{i+1} f \in I_k \end{aligned}$$

and we continue inductively to show that $I_k = \langle f \rangle_D$. Next we just need to check that the first k powers of the derivative applied to f vanish at x . If so, we have found something nontrivial in the zariski closure. If not we return to our algorithm and check $W_{r+1}(x)$. The clear question becomes, if $I_x \neq 0$, can we find generators for I_x by the above method. As we have already seen, we must be a little more careful as the problem seems slightly more subtle than before. With this in mind, a few more results and observations are needed.

Proposition 10. *If $A_n = \{(c_1, c_2 \dots c_n) \in \ker M_n(x) \subseteq K^n \mid f = \sum_{i=1}^n c_i m_i \in I_x\}$ then $A_n \subseteq \ker M_n(x)$ is a subspace.*

Proof. Suppose $(c_1, c_2 \dots c_n), (k_1, k_2 \dots k_n) \in A_n$. Consider $g = \sum_{i=1}^n (c_i - \lambda k_i) m_i$ with $\lambda \in K$. Then

$$(D^t g)(x) = \sum_{i=1}^n D^t(c_i m_i)(x) + \lambda \sum_{i=1}^n D^t(k_i m_i)(x)$$

for all $t \geq 0$. But both terms are zero by assumption that $(c_1, c_2 \dots c_n), (k_1, k_2 \dots k_n) \in A_n$. So $(D^t g)(x) = 0$ for all $t \geq 0$ and $g \in I_x$. \blacksquare

Now we define the algorithm for computing ideal generators for I_x . After which we shall discuss the several drawbacks of the method and possible methods for resolving these difficulties.

4.1. Algorithm 2: The Zariski Closure of Local Integral Curves

Step(1) Choose m_1 :

(a): If $m_1(x) = 0$ then set

$$T_1 = \{m_1\}$$

(b): If $m_1(x) \neq 0$ then set

$$T_1 = \emptyset$$

Step(2) Choose m_2 :

(a): If $W_2(x) = 0$ then there exist c_1, c_2 such that $D^i m_1(x) + D^i m_2(x)$ for $0 \leq i \leq 1$. Let $f = c_1 m_1 + c_2 m_2$. Compute a k such that $\langle f \rangle_D = \langle f, Df \dots D^k f \rangle = I_k$. If $D^j f(x) = 0$ for all $0 \leq j \leq k$, then set

$$T_2 = T_1 \cup \{f\}$$

. Otherwise set $T_2 = T_1$.

(b): If $W_2(x) \neq 0$ then set

$$T_2 = T_1$$

⋮

step(n): Choose m_n :

(a): If $W_n(x) = 0$ then compute a basis $\beta_n = \{\alpha_1, \alpha_2 \dots \alpha_k\}$ for $A_n \subseteq \ker(M_n(x))$, as in the previous proposition. Then set $f_i = \sum_{j=1}^n \alpha_{ij} m_j$ with $\alpha_i = (\alpha_{i1}, \alpha_{i2} \dots \alpha_{in})$. Next compute

$$\langle f_i \rangle_D = \langle f, Df \dots D^{c_i} f \rangle$$

and set $A_n = \{f_i \mid (D^j f_i)(x) = 0 \text{ for all } 0 \leq j \leq c_i\}$. Set $T_n = T_{n-1} \cup A_n$.

(b): If $W_n(x) \neq 0$ then set $T_n = T_{n-1}$.

Now we record a theorem regarding the number of steps it will take for our algorithm to compute ideal generators for I_x .

Theorem 4. If $I_x = \langle g_1, g_2 \dots g_k \rangle$ and $d = \max\{\partial(f_i)\}$ and $\alpha = \binom{d+n}{n}$, then $I_x = \langle T_\alpha \rangle$. In particular the number of steps it takes for our algorithm to compute generators for I_x is bounded by $\binom{d+n}{n}$.

Proof. This is a rather straightforward result. As we kept track of every polynomial, modulo to scaling by elements in the ground field, in I_x with leading term less than or equal to m_n , by continuing our algorithm out to $m_n = Lm(f_i)$ we will have captured all the generators. The calculation that computes a bound for our chosen monomial ordering, the total degree ordering, is the same as in theorem 3. ■

We now parse and lay out possible venues for improvement. For one it is perfectly possible to compute $\langle f \rangle_D = \langle f, Df, \dots D^k f \rangle$ using the ideal membership problem and employing Groebner basis. However it is known that this method is doubly exponential, and since our algorithm uses this at every stage at least once, we are left with a very impractical approach. However in special situations this may not be so unrealistic. For instance

if our derivation is locally finite, or what is also commonly called locally nilpotent which means for every $f \in K[x_1, x_2 \dots x_n]$ there exists some k such that $D^k f = 0$, then we need only calculate up until the vanishing point. However, this is in no way general, as many interesting derivations are not locally finite. A different approach may also be fruitful in certain situations. Suppose $D^k f = 0$ for all $k \leq n$, as in the case where $w_n(x) = 0$, and $D^{n+1} f \in \text{rad}(\langle f, Df \dots D^n f \rangle)$. Then $D^{n+1} f = 0$. In general the radical ideal membership is much less impractical and is simply exponential. In closing, I wish to extend to professor Derksen my utmost gratitude. His patient demeanor and elegant insight endowed me with the opportunity of success in mathematical research.

REFERENCES

- [1] David Cox, John Little, Donald O'Shea (1997) *Ideals, Varieties, and Algorithms*, Springer-Verlag, New York.
- [2] H.G.J Derksen (1993) *The Kernel of a Derivation*, Journal of Pure and Applied Algebra (84) 13-16, North-Holland.
- [3] David Dummit and Richard Foote (2004) *Abstract Algebra*, John Wiley and Sons Inc.
- [4] Irving Kaplansky (1976) *Introduction to Differential Algebra*, Herrman. Paris, France
- [5] Andy R. Magrid (1994) *Lectures on Differential Galois Theory*, American Mathematical Society.