DIFFERENTIAL ALGEBRA

Lecturer: Alexey Ovchinnikov
Thursdays 9:30am-11:40am
Website: http://qcpages.qc.cuny.edu/~aovchinnikov/
e-mail: aovchinnikov@qc.cuny.edu
written by: Maxwell Shapiro

0. Introduction

There are two main topics we will discuss in these lectures:

(I) The core differential algebra:
  (a) Introduction:
  We will begin with an introduction to differential algebraic structures, important terms and notation, and a general background needed for this lecture.
  (b) Differential elimination:
  Given a system of polynomial partial differential equations (PDE's for short), we will determine if
    (i) this system is consistent, or if
    (ii) another polynomial PDE is a consequence of the system.
    (iii) If time permits, we will also discuss algorithms will perform (i) and (ii).

(II) Differential Galois Theory for linear systems of ordinary differential equations (ODE's for short). This subject deals with questions of this sort:
  Given a system

$$\frac{d}{dx}y(x) = A(x)y(x), \tag{$\star$}$$

where $A(x)$ is an $n \times n$ matrix, find all algebraic relations that a solution of ($\star$) can possibly satisfy. Hrushovski developed an algorithm to solve this for any $A(x)$ with entries in $\bar{\mathbb{Q}}(x)$ (here, $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$).

Example 0.1. Consider the ODE

$$\frac{dy(x)}{dx} = \frac{1}{2x}y(x).$$

We know that $y(x) = \sqrt{x}$ is a solution to this equation. As such, we can determine an algebraic relation to this ODE to be

$$y^2(x) - x = 0.$$

In the previous example, we solved the ODE to determine an algebraic relation. Differential Galois Theory uses methods to find relations without having to solve.

1. Foundations of Differential Algebra

1.1. **Definitions and Examples.** We first define the core structures in differential algebra:

Definition 1.1. A commutative ring R with 1 supplied with a finite set $\Delta = \{\partial_1, \ldots, \partial_n\}$ is called a *differential ring* if $\partial_1, \ldots, \partial_n$ are commuting derivations from $R \to R$.

Definition 1.2. For a ring R, a map $\partial : R \to R$ is called a *derivation* if:

(1) For all $a, b \in R$ we have $\partial(a+b) = \partial(a) + \partial(b)$.
(2) For all $a, b \in R$, the Leibniz product rule is satisfied, i.e., $\partial(ab) = \partial(a) \cdot b + a \cdot \partial(b)$.

Definition 1.3. Let $\Delta = \{\partial_1, \ldots, \partial_n\}$ be a set of derivations for a differential ring R. Δ is *commuting* if for all $a \in R$ we have $\partial_i(\partial_j(a)) = \partial_j(\partial_i(a))$ for $1 \leq i, j \leq n$.

Remark. The notation (R, Δ) will sometimes be used for a differential ring R with derivations Δ. If $\Delta = \{\partial\}$ (that is, if Δ consists of only one derivation), then (R, Δ) is called an *ordinary differential ring*. If $\Delta = \{\partial_1, \ldots, \partial_n\}$ (that is, Δ consists of many derivations), then (R, Δ) is called a *partial differential ring*.

Example 1.1. Let R be a commutative ring with 1, $\Delta = \{\partial\}$. R is a differential ring if we define $\partial(r) = 0$ for all $r \in R$. All properties of a differential ring are then trivially satisfied.

Example 1.2. Let $R = \mathbb{Z}$. What are the possible derivations?
To begin, notice that $\partial(n)$ is determined by $\partial(1)$ (or $\partial(-1)$) using additivity. Indeed, for $n \geq 1$,

$$\partial(n) = \partial(\underbrace{1+1+\ldots+1}_{n \text{ times}}) = \underbrace{\partial(1)+\ldots+\partial(1)}_{n \text{ times}} = n\partial(1)$$

(similarly, we have for $n \geq 1$, $\partial(-n) = \partial(\underbrace{(-1)+\ldots+(-1)}_{n \text{ times}}) = n\partial(-1)$).

When $n = 0$, we have $\partial(0) = \partial(0+0) = \partial(0) + \partial(0)$, and we see that $\partial(0) = 0$. For $n = -1$, we have

$$\partial(-1) = \partial(1 \cdot (-1)) = \partial(1) \cdot (-1) + 1 \cdot \partial(-1),$$

Subtracting $\partial(-1)$ we see that $0 = (-1)\partial(1)$, and therefore $\partial(1) = 0$. We can also easily show that $\partial(-1) = 0$. Indeed,

$$0 = \partial(1) = \partial((-1)(-1)) = \partial(-1)(-1) + (-1)\partial(-1) = -2\partial(-1),$$

so $\partial(-1) = 0$. This shows that the only derivation that exists for $\mathbb{Z}$ is the trivial one.

Example 1.3. Let $R = \mathbb{Q}$. Take the element $\frac{1}{b}$ where $b \neq 0 \in \mathbb{Z}$. We have

$$0 = \partial(1) = \partial(b \cdot 1/b) = \partial(b) \cdot 1/b + b \cdot \partial(1/b),$$

and continuing further we get $\partial(\frac{1}{b}) = -\frac{\partial(b)}{b^2}$.

This calculation shows, in fact, how to determine the derivative an element a of any differential ring, provided the inverse of a exists.

More generally, given any $a \neq 0 \in \mathbb{Z}$, we can compute $\partial(\frac{a}{b})$ where b is taking as above. Namely, we get

$$\partial(a/b) = \partial(a \cdot 1/b),$$

and using the Leibniz rule, we get

$$\partial(a \cdot 1/b) = \partial(a) \cdot 1/b + a \cdot \partial(1/b) = \frac{\partial(a)}{b} - \frac{a\partial(b)}{b^2} = \frac{\partial(a)b - a\partial(b)}{b^2}.$$

Combining this result with that fact that both a and b are integers, the following occurs:

$$\partial(a/b) = \frac{\partial(a)b - a\partial(b)}{b^2} = \frac{0 \cdot b - a \cdot 0}{b^2} = 0,$$

and we see that $\mathbb{Q}$ only has trivial derivations.

In examples 1.1-1.3, the derivations are trivial. We will now define a non-trivial derivation:

Example 1.4. Let $R = \mathbb{Q}[x]$, $\partial(x) = 1$. We can determine the following:

$$\begin{aligned}\partial(a_n x^n + \ldots + a_0) &= \partial(a_n x^n) + \ldots + \partial(a_1 x) + \partial(a_0) = \\ &= a_n \partial(x^n) + a_{n-1}\partial(x^{n-1}) \ldots + a_1 = a_n n x^{n-1} + \ldots + a_1.\end{aligned}$$

Exercise 1. Prove that, for every differential ring $R, \Delta = \{\partial_1, \ldots, \partial_n\}$:

(1) For all $x \in R$ and $m \geq 1$, that $\partial_i(x^m) = m x^{m-1}\partial_i(x)$, and
(2) for all $m \geq 1$ and $a, b \in R$,

$$\partial_i^m(ab) = \sum_{p=0}^{m} \binom{m}{p} \partial_i^p(a) \cdot \partial_i^{m-p}(b),$$

where $\partial_i^m(ab) = \underbrace{\partial_i(\partial_i(\ldots(\partial_i}_{m \text{ times}}(ab \underbrace{)\ldots)}_{m \text{ times}}$

Remark. In example 1.4, if we let $\partial(x) = f$ instead of $\partial(x) = 1$ for some $f \in R$, then our result would be analagous to the chain rule one studies in analysis; namely, we get

$$\partial(a_n x^n + \ldots + a_0) = a_n n x^{n-1} \cdot f + \ldots + a_1 \cdot f.$$

This idea leads us to the following notion: If S is an ordinary differential ring, $R = S[x]$, then allowing $\partial(x) = f$ for some $f \in R$ turns R into a differential ring. This notion of arbitrarily defining the derivation only works for the ordinary case. If one wishes to extend to other derivations, a problem may occur.

Example 1.5. This is an example where extension of derivations fails. Consider $R = \mathbb{Q}[x]$, and let $\partial_1(x) = 1, \partial_2(x) = x$. These derivations do not commute, since $\partial_1(\partial_2(x)) = 1$ while $\partial_2(\partial_1(x)) = 0$, and R is therefore no longer a differential ring.

Definition 1.4. $(S, \{\partial_1^S, \ldots, \partial_n^S\}) \subset (R, \{\partial_1^R, \ldots, \partial_n^R\})$ is a *differential ring extension* if $S \subset R$ and for all $i, 1 \leq i \leq m$ we have

$$\partial_i^R|_S = \partial_i^S.$$

Remark. If (R, Δ) is a differential ring and R is a field, then (R, Δ) is called a *differential field.*

Let $(K, \Delta) \subset (L, \Delta)$ be a differential field extension, and let $a \in L$ be algebraic over K, i.e., there exist $b_n, \ldots, b_1, b_0 \in K$ such that $p(a) = b_n a^n + \ldots + b_1 a + b_0 = 0$ where $b_n \neq 0$. For simplicity, consider the case where $\Delta = \{\delta\}$. Consider $\delta(p(a))$, which according to the previous line, yields $\delta(p(a)) = 0$. If we write this out completely, we get:

$$\begin{gathered}\delta(a_n)a^n + a_n n a^{n-1}\delta(a) + \delta(a_{n-1})a^{n-1} + a_{n-1}(n-1)a^{n-2}\delta(a) + \ldots \\ \ldots + \delta(a_1)a + a_1\delta(a) + \delta(a_0).\end{gathered}$$

By grouping accordingly, we get

$$-\delta(a) \cdot \frac{\partial p(a)}{\partial a} = \delta(a_n)a^n + \ldots + \delta(a_1) + \delta(a_0).$$

We see that if $\frac{\partial p(a)}{\partial a} \neq 0$, we can divide by $-\frac{\partial p(a)}{\partial a}$ to get

$$\delta(a) = -\frac{\delta(a_n)a^n + \ldots + \delta(a_0)}{\frac{\partial p(a)}{\partial a}}.$$

Example 1.6. Consider $\mathbb{F}_p$ be a field with p elements, where p is prime. Let $K = \mathbb{F}_p(x^p) \subset L = \mathbb{F}_p(x)$.
Question: Is x algebraic over K? Yes; $p = y^p - x^p$ satisfies $p(x) = 0$. However, $\partial(x^p) = px^{p-1}\partial(x) = 0$, so ∂ is 0 on K, and the extension using the above method fails.

Remark. For a differential ring (R, Δ), we define $R^\Delta := \{r \in R | \partial_i(r) = 0\}$. These r are called constants.

Exercise 2. Prove that R^Δ is a subring of R and, if R is a field, then R^Δ is a subfield of R.

Example 1.7.
(1) If $R = \mathbb{Z}$, then $R^\Delta = \mathbb{Z}$.
(2) If $R = \mathbb{Q}[x]$ and $\partial(x) = 1$, then $R^\Delta = \mathbb{Q}$.

Remark. If K is a field, char$K$=0 and $K^\Delta = K$, then for every algebraic field extension $K \subset L$ (i.e., every $a \in L$ is algebraic over K), then $L^\Delta = L$.

1.2. **Differential Ideals.**

Definition 1.5. Let (R, Δ) be a differential ring. An ideal $I \in R$ is a *differential ideal* (or Δ-*ideal*) if, for all $\partial \in \Delta$ and $a \in I$, we have $\partial(a) \in I$.

From this point further, (R, Δ) will be used to denote a differential ring while R will be used for a commutative ring (we assume commutative rings have unit), and, unless otherwise stated, $\Delta = \{\partial_1, \ldots, \partial_n\}$.

Example 1.8. Consider (R, Δ).
(1) I=(R, Δ) and
(2) I=(0)

are both differential ideals.

Proposition 1.1. *Let $I = (f_1, \ldots, f_m) \subset (R, \Delta)$ be an ideal in (R, Δ) generated by $f_1, \ldots, f_m \in (R, \Delta)$. I is a differential ideal if and only if, for all $j, 1 \leq j \leq m$ and $i, 1 \leq i \leq n$ we have $\partial_i(f_j) \in I$.*

Proof. ($\Rightarrow$) Assume I is a differential ideal. It follows by definition that $\partial_i(f_j) \in I$ for all i, j.
($\Leftarrow$) Assume that $\partial_i(f_j) \in I$ for all i, j. Consider $g \in I$. We represent g as follows:

$$g = a_1 f_1 + \ldots + a_m f_m.$$

We want to show that $\partial_i(g) \in I$. If we differentiate g, we get the following:

$$\partial_i(g) = \partial_i(a_1 f_1 + \ldots + a_m f_m),$$

which, after simplifying, we get

$$\partial_i(g) = \partial_i(a_1) f_1 + a_1 \partial_i(f_1) + \ldots + \partial_i(a_m) f_m + a_m \partial_i(f_m).$$

Since each each $f_j \in I$ and each $\partial_i(f_j) \in I$, each term on the right hand side is in I, and therefore $\partial_i(g) \in I$ □

We continue by noting some notations. If $S \subset (R,\Delta)$, then $[S]$ denotes the smallest differential ideal of (R,Δ) that contains S; it is the intersection of all differential ideals containing S.

In other words, $[S]$ is the ideal of (R,Δ) generated by $\theta(S), \theta \in \Theta$ where

$$\Theta = \{\partial_1^{i_1}\partial_2^{i_2}\cdots\partial_n^{i_n} | i_1,\ldots,i_n \geq 0\}.$$

In particular, we see that $(S) \subset [S]$ by letting all $i_r = 0$.

Example 1.9. Let $(R,\Delta) = \mathbb{Q}[x]$ with $\Delta = \{\partial\}$, and $\partial(x) = 1$. What are the differential ideals in (R,Δ)?

(1) $I_1 = (R)$ and
(2) $I_2 = (0)$,

but are there any other ideals?
To check for others, let $I \subset (R,\Delta)$ be a differential ideal with $(I) \neq 0$. Then, there exists $0 \neq f \in I$ such that $I = (f)$ where f is the of the smallest degree in I. However, $deg(\partial(f)) < deg(f)$, where both $\partial(f)$ and f are contained in I. Therefore, $f \in \mathbb{Q}$ and $I = (R,\Delta)$. Thus, the only two ideals in (R,Δ) are (1) and (2).

1.3. **Radical Differential Ideals.**

Definition 1.6. Let R be a commutative ring. An ideal $I \subset R$ is called *radical* if, for all $f \in R$, if there exists an $n \geq 1$ such that $f^n \in I$, then $f \in I$.

Example 1.10. Let $R = \mathbb{Q}[x]$. Is the ideal $I = (x^2)$ radical? Since $x^2 \in I$ but $x \notin I$, we see that I is not radical.

Exercise 3. Let R be as in Example 1.10. Describe all radical ideals in R.

Given an ideal $I \subset R$, $\sqrt{I}$ denotes the smallest radical ideal containing I.

Remark. If $I \neq R$, then $\sqrt{I} \neq R$. Indeed, if $1 \in \sqrt{I}$, then $1^n \in I$ for some $n \geq 1$, so $1 \in I$.

Definition 1.7. An ideal $I \subset (R,\Delta)$ is called a *radical differential ideal* if:

(1) I is a differential ideal, and
(2) I is a radical ideal.

For a subset $S \subset R$, $\{S\}$ denotes the smallest radical differential ideal containing S. One also says that S generates the radical differential ideal $\{S\}$. It will be clear in which context $\{\}$ will denote a radical differential ideal.

We now turn to the construction of radical differential ideals. Normally, one may intuitively start with S, consider $[S]$, and then take its radical $\sqrt{[S]}$. However, this may not be sufficient.

Example 1.11. Let $(R,\Delta) = \mathbb{Z}_2[x,y]$ where $\partial(x) = y$ and $\partial(y) = 0$. Consider $I = [x^2]$. Notice that $\partial(x^2) = 2xy = 0$, which implies $I = (x^2)$. One can easily show that $\sqrt{I} = (x)$. However, $\sqrt{[x^2]} = \sqrt{(x^2)}$ is not a differential ideal since $\partial(x) = y \notin (x)$.

Exercise 4. Construct an example of an ideal $I \subset (R,\Delta)$ such that $[\sqrt{I}]$ (that is, first taking the radical of I then generating the differential ideal) is not a radical ideal for both $char(p)$ and $char(0)$.

Theorem 1.1. *Let (R,Δ) be a differential ring, $\mathbb{Q} \subset R$, and let $I \subset (R,\Delta)$ be a differential ideal. Then, $\sqrt{I}$ is a radical differential ideal.*

Proof. In order to prove this, we first state and prove a lemma:

Lemma 1.1. *Let $I \subset (R,\Delta)$ be a differential ideal and let $\mathbb{Q} \subset R$. Let $a \in R$ such that $a^n \in I$. Then, $(\partial(a))^{2n-1} \in I$.*

Proof of Lemma 1.1. By induction, we will show that, for all k, $1 \le k \le n$, we have

$$(\star) \qquad a^{n-k}\partial(a)^{2k-1} \in I,$$

and the lemma will follow by allowing $k = n$.

If $k = 1$, then

$$a^{n-1}\partial(a) \in I.$$

Indeed,

$$\partial(a^n) = na^{n-1}\partial(a).$$

Since $\mathbb{Q} \subset R$, we divide by n and it follows that $a^{n-1}\partial(a) \in I$.

Now for the inductive step. Assume that $(\star)$ holds. We want to show that

$$(\star\star) \qquad a^{n-(k+1)}(\partial(a))^{2k+1} \in I.$$

Applying ∂ to $(\star)$, we obtain:

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

Multiply the above by $\partial(a)$ to obtain $(\star\star)$, and we are done. □

Back to the theorem, we see that by applying Lemma 1.1, the theorem follows. □

1.4. **Prime Ideals.**

Definition 1.8. An ideal $P \in R$ is call *prime* if, whenever the product $ab \in P$, either $a \in P$ or $b \in P$ for all $a, b \in R$.

Example 1.12. Let $R = \mathbb{Q}[x,y]$, and let $I = (xy)$ be an ideal. I is not prime. Indeed, $xy \in I$ but neither $x \in I$ nor $y \in I$. However, the ideals $P_1 = (x)$ and $P_2 = (y)$ are prime.

Exercise 5. Show that $(xy) = (x) \cap (y)$.

Definition 1.9. Let P be a differential ideal in (R,Δ). P is a *prime differential ideal* if, in addition to being a differential ideal, P is also a prime ideal.

Remark. We make notes of a few items:

(1) If P is prime, then P is radical by definition. Moreover, an intersection of radical ideals is a radical ideal.
(2) P is a prime ideal if and only if R/P is an integral domain. In fact, some texts use this as the definition for prime ideals.
(3) $I \subset R$ is a radical ideal if and only if R/I is reduced, that is, R/I contains no nilpotent elements.
(4) If $I_1, \ldots, I_n$ are differential ideals, then $\bigcap_{i=1}^n I_i$ is a differential ideal.

In commutative algebra, one studies decomposition of ideals. In differential algebra, we have an analagous statement. However, before we state the theorem, we will prove several lemmas. For the following, assume (R,Δ) is a differential ring, and assume $I \subset R$ is a radical differential ideal.

Lemma 1.2. *If $ab \in I$, then $\partial(a)b \in I$ and $a\partial(b) \in I$.*

Proof. Indeed, $ab \in I$ implies that its derivative $\partial(ab) \in I$. However,

$$\partial(ab) = \partial(a)b + a\partial(b) \in I.$$

Multiplying by a, we get

$$\partial(a)ab + a^2\partial(b) \in I,$$

which further implies that $a^2\partial(b) \in I$. Multiply $a^2\partial(b)$ by $\partial(b)$ to obtain

$$(a\partial(b))^2 \in I.$$

Since I is radical, we have $a\partial(b) \in I$. The other inclusion follows immediately. $\square$

Lemma 1.3. *Let $S \subset R$ be any subset. Then*

$$I' = \{x \in (R,\Delta)\,|\,xS \subset I\}$$

is a radical differential ideal.

Proof. First we show that I' is an ideal. Indeed, if $a,b \in I'$ and $s \in S$ then $as + bs \in I$, and therefore $s(a+b) \in I$ which implies $a+b \in I'$. Also, if $a \in I'$, $r \in R$, we have $r(as) \in I$, which implies $(ra)s \in I$, and therefore $ra \in I'$. Hence, I' is an ideal.

I' is a differential ideal. Indeed, for all $a \in I'$ and $s \in S$, we have $as \in I$. By Lemma 1.2, this implies that $\partial(a)s \in I$ which further implies that $\partial(a) \in I'$.

I' is radical. Indeed, let $a^n \in I'$ for $n \geq 1$. This implies $a^n s \in I$. Multiplying by s^{n-1}, we obtain $a^n s^n \in I$. Since I is radical, this inclusion implies that $as \in I$, which shows that $a \in I'$. $\square$

Lemma 1.4. *Let $S \subset R$ be any subset. Then $a\{S\} \subset \{aS\}$.*

Proof. $\{aS\} = I$ in Lemma 1.3. The I' from Lemma 1.3 contains S and therefore contains $\{S\}$. $\square$

Lemma 1.5. *For all subsets $S,T \subset R$, we have $\{S\}\{T\} \subset \{ST\}$.*

Proof. Consider

$$A = \{x \in (R,\Delta)\,|\,x\{T\} \subset \{ST\}\}.$$

(1) $S \subset A$ and
(2) A is a radical differential ideal.

(1) follows from Lemma 1.3, and (2) follows from Lemma 1.4.

$\square$

Lemmas 1.2-1.5 were needed to show the following:

Lemma 1.6. *Let $T \subset R$ be a subset closed under multiplication and let P be a maximal among radical differential ideals that do not intersect T. Then P is prime.*

Proof. By contradiction, suppose P is not prime. Let $a,b \in R$ be such that $ab \in P$ but $a \notin P$ and $b \notin P$. Hence, we get $\{P,a\}$ and $\{P,b\}$ are both proper radical differential ideals containing P. Hence, these two radical differential ideals intersect T, i.e., there exist $t_1,t_2 \in T$ such that $t_1 \in \{P,a\}$ and $t_2 \in \{P,b\}$. Since T is closed under multiplication, $t_1t_2 \in T$, but then $t_1t_2 \in \{Pb, aP, P^2, ab\} \subset \{P\}$. $\rightarrow\leftarrow$, since $\{P\} \cap T = \emptyset$. $\square$

Now we are ready to state our theorem:

Theorem 1.2. *Let $I \subset R$ be a radical differential ideal. Then, there exists $\{P_\alpha \,|\, \alpha \in J\}$, where P_α are prime differential ideals such that*

$$I = \bigcap_{\alpha \in J} P_\alpha.$$

Proof. As in Lemma 1.6, let T be a multiplicatively closed subset of R and let Q be a maximal radical differential ideal in R with $Q \cap T = \varnothing$ (such a Q exists by Zorn's Lemma). By Lemma 1.6, Q is prime.

We will show that, for all $x \in R \backslash I$, there exists a prime differential ideal P_x such that $I \subset P_x$ and $x \notin P_x$. If we can show this, then the theorem follows since we can take

$$I = \bigcap_{x \in R \backslash I} P_x.$$

Let $T = \{x^n | n \geq 1\} \subset R$. T is multiplicatively closed. Let P_x be the ideal from Lemma 1.6, and the theorem follows. □

Corollary 1.1. *Let $\mathbb{Q} \subset R$ and $M \subset R$ be a maximal proper differential ideal. Then, M is prime.*

Example 1.13. Consider the differential ring $(R, \Delta) = \mathbb{Z}_2[x]$ with $\Delta = \{\delta\}$ defined by $\delta(x) = 1$. Take $M = (x^2)$. This ideal is not prime, but it is a maximal differential ideal.

Exercise 6. Prove the above statement. Hint: Any ideal $I \supsetneq M$ is of the from $I = (ax + b)$ where $a, b \in \mathbb{Z}_2$, but I is differential if and only if $a = 0$.

Proof (Corollary 1.1). Consider $\{M\} = \sqrt{[M]} = \sqrt{M}$. If $\sqrt{M} = R$, then $1 \in \sqrt{M} \Rightarrow 1 \in M$, which contradicts M being proper. Therefore, $\sqrt{M}$ is a proper radical differential ideal containing M. Since M is maximal, $\sqrt{M} = M$. Now, since M is radical, Theorem 1.2 states that

$$M = \bigcap_{\alpha \in J} P_\alpha,$$

where each P_α is a prime differential ideal. Therefore, for all $\alpha \in J$, $M = P_\alpha$, and therefore M is prime. □

2. The Ring of Differential Polynomials and its Ideals

2.1. **Ring of Differential Polynomials.** Let (K, Δ) be a differential field with $\Delta = \{\partial_1, \ldots, \partial_m\}$. Using this structure, we want to develop an algebraic structure containing differential equations like:

(1) $u_{xx} = u_t$.
(2) $u_{xx} = u_t^2$.
(3) $u_{xx} + v_{xx} = u_t$.

(Equations of the form $u_{xx} = \sin(u_t)$ will not be considered.) In order to proceed with this, we first give some definitions.

Definition 2.1. The *ring of differential polynomials* with coefficients in K in differential indeterminates $y_1, \ldots, y_n$ is the ring of polynomials

$$K[\theta y_i \,|\, \theta \in \Theta, 1 \leq i \leq n].$$

We denote the above ring as $K\{y_1, \ldots, y_n\}$.

In Definition 2.1, $\Theta = \{\partial_1^{i_1}, \ldots, \partial_m^{i_m} \,|\, i_1, \ldots, i_m \geq 0\}$.

Example 2.1. Let us take (1), (2), and (3) from the beginning of this section and express those equations using Definition 2.1. Take $y_1 = u$, $y_2 = v$, $\partial_1 = \frac{\partial}{\partial x}$, $\partial_2 = \frac{\partial}{\partial t}$. We get

$$u_{xx} = \partial_1^2 y_1,$$

$$v_{xx} = \partial_1^2 y_2,$$

$$u_t = \partial_2 y_1,$$

$$(u_t)^2 = (\partial_2 y_1)^2.$$

Example 2.2. Given our differential field (K,Δ), if $\Delta = \{\delta\}$, we define

$$K\{y\} = K[y, \delta y, \delta^2 y, \ldots, \delta^n y, \ldots], \quad (\star)$$

that is, the field K adjoined with infinitely many indeterminates $\delta^{(i)}y$ for $i \geq 0$. When there is no confusion, we write

$$K[y, y', y'', \ldots, y^{(n)}, \ldots]$$

in place of $(\star)$.

To give a differential structure, we define the following (assume $\Delta = \{\partial_1, \ldots, \partial_m\}$).
For all i, j,

$$\partial_i(\theta y_j) := (\partial_i \theta) y_j,$$

where

$$\partial_i \theta \stackrel{\text{def}}{=} \partial_1^{p_1} \cdots \partial_i^{p_i+1} \cdots \partial_m^{p_m},$$

where $\theta = \partial_1^{p_1} \cdots \partial_i^{p_i} \cdots \partial_m^{p_m}$ and $p_s \geq 0$ for $1 \leq s \leq m$.

Example 2.3. Using the notation from Example 2.1,

$$u_{xxt} = \frac{\partial}{\partial x}(u_{xt}) \longleftrightarrow \partial_1(\partial_1 \partial_2 y_1) = \partial_1^2 \partial_2 y_1.$$

Definition 2.2. A differential ring is called *Ritt-Noetherian* if the set of its radical differential ideals satisfies the ascending chain condition (ACC).

The ACC for radical differential ideals states that, for every chain of radical differential ideals

$$I_0 \subseteq I_1 \subseteq \ldots I_N \subseteq \ldots,$$

there exists some finite $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \ldots$. (we say that such chains *stabilize*).

The Hilbert Basis Theorem in commutative algebra states that, given a field K, $K[x_1, \ldots, x_n]$ is Noetherian. To state this theorem for a differential field (K,Δ), we need more hypotheses.

Theorem 2.1 (Ritt-Raudenbush)**.** *The differential ring $K\{y_1, \ldots, y_n\}$ is Ritt-Noetherian, where (K,Δ) is a differential field and $\mathbb{Q} \subset K$.*

This is not, in fact, the original statement. The original statement is as follows:

Theorem (Ritt-Raudenbush)**.** *If (R,Δ) is a differential ring satisfying ACC on radical differential ideals, then $R\{y\}$ satisfies ACC on radical differential ideals.*

The proof requires more techniques than we presently have, and, therefore, it will be given later.

Exercise 7. Prove that, for every ordinary differential field $(K,\{\delta\})$, where $\mathbb{Q}\subset K$,

$$\left[y^2\right]\subset\left[y^2,(\delta y)^2\right]\subset\ldots\subset\left[y^2,(\delta y)^2,\ldots,(\delta^p y)^2\right]\subset\ldots$$

does not stabilize in $K\{y\}$ (Recall that [ ] is reserved for differential ideals while {} is reserved for radical differential ideals).

Corollary 2.1. *Let $I\subset K\{y_1,\ldots,y_n\}$ be a radical differential ideal. Then there exist $f_1,\ldots,f_p\in K\{y_1,\ldots,y_n\}$ such that $I=\{f_1,\ldots,f_n\}$.*

Proof. Take $0\neq f_1\in I$. Let $f_2\in I\setminus\{f_1\}$, etc. We have a chain

$$\{f_1\}\subset\{f_1,f_2\}\subset\ldots,$$

which, by the ACC, stabilizes after a finite number of steps. □

Exercise 8. Consider $K\{x,y\}$. Prove that $\{xy\}$ does not have a finite generating set as a differential ideal, that is,

$$\{xy\}\neq[f_1,\ldots,f_p].$$

Theorem 2.2. *For every radical differential ideal $I\subset R$, where (R,Δ) is Ritt-Noetherian, there exist a finite number of prime differential ideals $P_1,\ldots,P_q$ such that*

$$I=\bigcap_{i=1}^{q}P_i.$$

Moreover, if the above intersection is irredundant, then this set of prime ideals is unique.

The ideals $P_1,\ldots,P_q$ are called the *minimal differential prime components* of I.

Proof. Suppose the statement of the theorem is not true, i.e., there exist radical differential ideals that are not finite intersections of prime differential ideals. Since (R,Δ) is Ritt-Noetherian, there exists a maximal radical differential ideal Q that is not a finite intersection of prime differential ideals.

By our assumption, Q is not prime (indeed, otherwise Q is a finite intersection of itself). Therefore, there exist $a,b\in R$ such that $ab\in Q$ but $a\notin Q$ and $b\notin Q$. By definition, $1\notin Q$, and, therefore, the radical differential ideals $\{Q,a\}$ and $\{Q,b\}$ both properly contain Q.

Now, $1\notin\{Q,a\}$ (also $1\notin\{Q,b\}$). Indeed, if $1\in\{Q,a\}$, then, in particular, $1\in[Q,a]$. Then

$$1=c+\sum_{\theta}c_\theta\theta(a)\quad(\star),$$

where $c\in Q$, $c_\theta\in R$. Multiply $(\star)$ by b, and, by Lemma 1.2, $b\in Q$, $\rightarrow\leftarrow$. Hence, $1\notin\{Q,a\}$ (and similarly, $1\notin\{Q,b\}$).

Now, since Q is maximal, $\{Q,a\}$ **is** a finite intersection of prime differential ideals. In other words,

$$\{Q,a\}=P_1^a\cap\ldots\cap P_{q_a}^a,$$

where each P_i^a is a prime differential ideal. Similarly,

$$\{Q,b\}=P_1^b\cap\ldots\cap P_{q_b}^b.$$

We will show that $Q=\{Q,a\}\cap\{Q,b\}$.

$Q\subset\{Q,a\}\cap\{Q,b\}$ is clear. To show the reverse, let $c\in\{Q,a\}\cap\{Q,b\}$. Then,

$$c^2\in\{Q,a\}\cdot\{Q,b\}\subset\{Q^2,Qa,Qb,ab\}.$$

By the hypothesis, $ab \in Q$, and, therefore, $c^2 \in Q$. Since Q is radical, $c^2 \in Q$ implies $c \in Q$. Since $\{Q,a\} \cap \{Q,b\} = Q$, we have

$$Q = \left(\bigcap_{k=1}^{q_a} P_k^a \right) \cap \left(\bigcap_{j=1}^{q_b} P_j^b \right),$$

which is a finite intersection.

To show the uniqueness, let

$$Q = P_1 \cap \ldots \cap P_r = Q_1 \cap \ldots \cap Q_s.$$

So, for all i, $1 \le i \le s$,

$$Q_i \supset P_1 \cap \ldots \cap P_r.$$

Then, there exists j, $1 \le j \le r$ such that $Q_i \supset P_j$. Indeed, assume the contrary. Let $a_1 \in P_1, a_2 \in P_2, \ldots, a_r \in P_r$ with $a_k \notin Q_i$ for all k. However,

$$a_1 \cdot \ldots \cdot a_r \in P_1 \cdot \ldots \cdot P_r \subset Q_i,$$

contradicting that Q_i is prime. Therefore, $P_j \subset Q_i$. By reversing the roles of P and Q, there exists n, $1 \le n \le s$ such that $P_j \supset Q_n$.

If $n = i$, then $P_j = Q_i$. If $n \ne i$, then $Q_i \supset P_j \supset Q_n$, which contradicts the irredundancy of the decomposition

$$Q_1 \cap \ldots \cap Q_s.$$

□

Exercise. The following is a hint to Exercise 7 above. Let $K\{y\}$ be a ring of differential polynomials of $char(K) = 0$ and $\Delta = \{\delta\}$. We will show, in steps, what needs to be done to solve the problem. We need to show that the inclusions in the following infinite increasing chain are strict:

$$[y^2] \subset [y^2, (y')^2] \subset \ldots \subset [y^2, \ldots, (y^{(n)})^2] \subset \ldots$$

Let $I_n = [y^2, \ldots, (y^{(n)})^2]$ with $n \ge 0$. We will construct a sequence $(V_{2n}, n \ge 0)$ of finite dimensional vector spaces such that, for all $n \ge 0$, $V_{2n} \subset I_n$ but $V_{2n} \not\subseteq I_{n-1}$.

To construct $(V_{2n}, n \ge 0)$, we will first introduce some terminology. For a monomial $m = x^{(i)}y^{(j)}$, we define the *weight* of m to be be $i + j$, denoted $wt(m)$. For example,

$$wt(y \cdot y) = 0,$$
$$wt(y \cdot y') = 1,$$
$$wt(y^{(4)}y^{(5)}) = 9.$$

Let $V_n = span_K(m)$ where $deg(m) = 2$ and $wt(m) = n$. We get the sequence:

$$\begin{aligned}
V_0 =& span_K(y^2) \\
V_1 =& span_K(yy') \\
V_2 =& span_K(yy'', (y')^2) \\
V_3 =& span_K(yy''', y'y'') \\
&\vdots \\
V_{2n} =& span_K(yy^{(2n)}, y'y^{(2n-1)}, \ldots, (y^{(n)})^2) \\
V_{2n+1} =& span_K(yy^{(2n+1)}, y'y^{(2n)}, \ldots, y^{(n)}y^{(n+1)}),
\end{aligned}$$

and from here we see that $dimV_{2n} = n+1 = dimV_{2n+1}$.

(Step 1) Show that $V_{2n+2} = span_K(\delta^2(V_{2n}), (y^{(n+1)})^2)$. Do this by expressing each element

$$\delta^2(y^{(k)}y^{(2n-k)})$$

via the basis of V_{2n+2} and $(y^{(n+1)})^2$, and show that the change of basis matrix is invertible.

(Step 2) Show that, for all n,

$$I_n \cap V_{2n+2} = span_K(\delta^2(V_{2n})) \subsetneq V_{2n+2}.$$

Exercise. We also give a hint to solve Exercise 8 above. Using the setup of Exercise 8, let $I = \{xy\}$ and $J = (x^{(i)}y^{(j)}, i \geq 0, j \geq 0)$ (here, J is just an ideal).

(Step 1) Show that $I = J$. $I \supset J$ follows from Lemma 1.2. To show $I \subset J$, it is sufficient to show that J is a radical differential ideal. J is clearly a differential ideal, since

$$(x^{(i)}y^{(j)})' = x^{(i+1)}y^{(j)} + x^{(i)}y^{(j+1)} \in J.$$

To show that J is radical, we first notice that

$$(f \in K\{x,y\} \,\&\, f \notin J \Leftrightarrow f \text{ has a term with no } y^{(j)} \text{ (or } x^{(i)})).$$

It is then easy to show (using the above observation) that, if $f \notin J$, then, for all $m \geq 1$, $f^m \notin J$.

(Step 2) Suppose that $I = [f_1, \ldots, f_p]$ for some $f_1, \ldots, f_p \in K\{x,y\}$. Then, there exists $q \geq 0$ such that, for all $1 \leq i \leq p$, $f_i \in [x^{(s)}y^{(t)}, 0 \leq s,t \leq q] = J'$. Hence, we would get

$$\{xy\} = J'.$$

We need to show that

$$x^{(q+1)}y^{(q+1)} \notin J', \tag{$\star$}$$

thus getting a contradiction.

In order to show ($\star$), we introduce some new definitions and state a proposition.

Definition 2.3. Let (R,Δ) and (S,Δ) be differential rings. A ring homomorphism $\varphi : R \to S$ is a *differential ring homomorphism* if, for all $\partial \in \Delta$ and $a \in R$, we have $\varphi(\partial(a)) = \partial(\varphi(a))$.

Example 2.4. We introduce some examples of differential ring homomorphisms:

(1) Let $(R,\Delta) = (S,\Delta)$, and condiser id_R, that is, the identity map on R. This is a differential ring homomorphism.

(2) Let $(R,\Delta = K\{y_1,\ldots,y_n\}$ where (K,Δ) is a differential field. Let (L,Δ) be a differential field containing K. Also, let $(a_1,\ldots,a_n) \in L$. The map

$$K\{y_1,\ldots,y_n\} \to L$$

defined by

$$f \mapsto f(a_1,\ldots,a_n),$$

is a differential ring homomorphism (check this!).

Next, we state a proposition whose proof will be left to the reader.

Proposition 2.1. *Let $\varphi : (R,\Delta) \to (S,\Delta)$ be a surjective differential ring homomorphism, and let $I \subset R$ be a differential ideal. Then, $\varphi(I)$ is a differential ideal.*

Now, to show $(\star)$, apply the differential homomorphism from $K\{x,y\} \to K\{y\}$ where $f(x,y) \mapsto f(y,y)$ (e.g., $x^{(i)}y^{(i)} \mapsto y^{(i)}y^{(j)}$). $\square$

With the notion of a differential ring homomorphism now defined, we continue with the following proposition.

Proposition 2.2. *Let (R,Δ), (S,Δ) be differential rings, and $\varphi : R \to S$ be a ring homomorphsim. If φ is a differential ring homomorphism, then $Ker(\varphi)$ is a differential ideal.*

Exercise 9. Prove Proposition 2.2..

Remark. Notice that the converse of Proposition 2.2 is not necessarily true. Consider the following case: Let $R = S = K\{y\}$ be a differential polynomial ring with $\Delta = \{\delta\}$. Let $\varphi : K\{y\} \to K\{y\}$ be defined by

$$\varphi(y) = \delta y$$
$$\varphi(\delta y) = y$$
$$\varphi(\delta^n y) = \delta^n y \ \ (n \geq 2)$$
$$\varphi(a) = a \ \ (a \in K).$$

This is indeed an injective ring homomorphism, and therefore $ker(\varphi) = 0$ is a differential ideal. However,

$$\delta(\varphi(y)) = \delta(\delta y) = \delta^2 y \neq y = \varphi(\delta y).$$

Since δ does not commute with φ, φ is not a differential homomorphism.

Corollary 2.2. *$I \subset R$ is a differential ideal if and only if $(R/I,\Delta)$ is a differential ring (and therefore $I = ker\big(R \to R/I)\big)$.*

Proof. $(\Rightarrow)$ Let $r + I \in R/I$. For each $\partial \in \Delta$, define

$$\partial(r+I) = \partial(r) + I. \quad (\star)$$

To show that $(\star)$ is well defined, we need to show that $(\star)$ is independant of the choice of representative. Let $r + I = s + I$ (so that $r - s \in I$). For all $\partial \in \Delta$, we have $\partial(r+I) = \partial(s+I)$, that is, $\partial(r) + I = \partial(s) + I$. From this equality we have $\partial(r) - \partial(s) = \partial(r-s) \in I$, which is indeed the case, since $r - s \in I$, and I is by assumption a differential ideal.

Exercise. Prove $(\Leftarrow)$.

$\square$

Proposition 2.3. *Let $f_1,\dots,f_p \in K\{y_1,\dots,y_n\}$ be linear (i.e., $deg(f_i) = 1$, $1 \leq i \leq p$). Then either $1 \in [f_1,\dots,f_p] = P$ or $[f_1,\dots,f_p] = P$ is a prime differential ideal.*

Proof. If $1 \in P$, then $ab \in P \Rightarrow a \in P$ for $a,b \in K\{y_1,\dots,y_n\}$.

We will show that, if $a,b \in K\{y_1,\dots,y_n\}$,

$$(\star\star) \qquad ab \in P \Rightarrow a \in P \text{ or } b \in P.$$

Suppose $(\star\star)$ fails. Then

$$ab \in (\underbrace{f_1,\dots,f_p,\Theta_1 f_1,\dots,\Theta_p f_p}_{\text{finitely many}}) = Q \subset K[x_1,\dots x_q],$$

where the $x_1,\ldots,x_q$ are the relabled variables.

Q is an ideal generated by linear polynomials. Apply Gauss-Jordan elimination (Do this!), and let $x_{i1},\ldots,x_{it}$ be the non leading variables. Then

$$K[x_1,\ldots,x_q]/Q \cong K[x_{i1},\ldots,x_{it}],$$

(unless $1\in P$) which is a domain. Therefore, Q is prime and $(\star\star)$ must hold. $\square$

Exercise 10. Let $(K,\{\delta\})$ be and ordinary differential ring with $char(K)=0$.

(1) Show that $[(y')^2+y]$ is not a radical differential ideal by showing that $y'''\in\{(y')^2+y\}$ but $y'''\notin[(y')^2+y]$.

(2) Find the smallest n such that $(y''')^n\in[(y')^2+y]$.

(3) Show that $\{(y')^2+y\}$ is not a prime ideal by showing that

  (a) $\{(y')^2+y\}=\{(y')^2+1,2y''+1\}\cap[y]$.

  (b) $\{(y')^2+1,2y''+1\}$ is prime and is equal to the set of all $f\in K\{y\}$ such that $\exists n:(y')^n f\in\{(y')^2+1\}$ and (a) is irredundant.

2.2. **Characteristic Sets.** We will use characteristic sets to prove the Ritt-Raudenbush Theorem stated in Section 2.1.

Example 2.5. We begin with some motivation:

(1) Given the ring $\mathbb{Z}$, and ideal $(n)\in\mathbb{Z}$, we know that $m\in(n)\Leftrightarrow m=nq+0,\ q\in\mathbb{Z}$.

(2) In $\mathbb{Q}[x]$, if $(f)\in\mathbb{Q}[x]$ is an ideal, by the division algorithm we know that $g\in(f)\Leftrightarrow g=fq+r$ where $r=0$.

(3) However, in the ring $\mathbb{Q}[x_1,\ldots,x_n]$, given an ideal $(f_1,\ldots,f_m)\subset\mathbb{Q}[x_1,\ldots,x_n]$, we use Gröbner bases to test ideal membership.

We recall that in order to use Gröbner bases, one needs to choose some ordering on monomials. We will use an analogous tool for ordering on differential polynomials.

Definition 2.4. let $Y=y_1,\ldots,y_n$ and $\Delta=\partial_1,\ldots,\partial_m$. Recall that $\Theta=\{\theta\,|\,\theta=\partial_1^{i_1},\ldots,\partial_m^{i_m}\}$ (here, $\{\}$ denotes set notation). A *differential ranking* on ΘY is a well-ordering on ΘY (i.e., a total ordering where every non-empty subset has the smallest element) such that:

(1) for all $u,v\in\Theta Y$ and $\theta\in\Theta$,

$$\text{if } u<v, \text{ then } \theta u<\theta v.$$

(2) For all $\theta\neq id$,

$$u<\theta u.$$

Example 2.6. We present a few examples, and introduce orderings from commutative algebra:

(1) Let $Y=y$ and $\Delta=\delta$. The set

$$\Theta Y=y,\delta y,\delta^2 y,\ldots,\delta^p y,\ldots$$

has a unique ranking

$$y<\delta y<\delta^2 y<\ldots<\delta^p y<\ldots$$

(2) Let $Y=y$ and $\Delta=\partial_1,\partial_2$. Note that, for any ordering, we have:

$$y<\partial_1 y<\partial_1\partial_2 y,$$

but we also have

$$y<\partial_2 y<\partial_1\partial_2 y.$$

How do we compare $\partial_1 y$ to $\partial_2 y$?

(3) Let $\prec_{lex}$ be the lexicographic ordering on i_1, i_2 for $i_1, i_2 \geq 0$ $\big($examples include $(0,100) \prec_{lex} (1,2)$ and $(2,1) \prec_{lex} (2,2)\big)$. We can let

$$\partial_1^{i_1}\partial_2^{i_2} y < \partial_1^{j_1}\partial_2^{j_2} y \Leftrightarrow (i_1, i_2) \prec_{lex} (j_1, j_2).$$

(4) We could also use the graded lexicographic ordering (deglex) defined as follows:

$$(i_1, i_2) \prec_{deglex} (j_1, j_2) \Leftrightarrow \text{ either } i_1 + i_2 < j_1 + j_2$$
$$\text{else } i_1 + i_2 = j_1 + j_2 \textit{ and } (i_1, i_2) \prec_{lex} (j_1, j_2).$$

Now that we have rankings on ΘY, we begin to discuss the analog of the division algorithm of Commutative Algebra. Let K be a differential field.

Definition 2.5. Let $f \in K\{y_1, \ldots, y_n\}$. The variable $\partial_1^{i_1} \cdot \ldots \cdot \partial_m^{i_m} y_j$ in f of the greatest rank is called the *leader* of f, denoted u_f.

Example 2.7. Two examples before we continue with the algorithm:

(1) For $\Delta = \{\delta\}$ and $K\{y\}$, consider $f = (y')^2 + y + 1 \in K\{y\}$. We see that $u_f = y'$.

(2) For $\Delta = \{\partial_x, \partial_t\}$ and $K\{u\}$, consider $f = u_{xx} + u_t \in K\{u\}$. What is u_f? To answer, we first need to define a ranking:

(a) Consider the graded lexicographic ordering on $\{(i_1, i_2 \,|\, i_1, i_2 \geq 0\}$. So,

$$\Theta Y = \{\partial_x^{i_1}\partial_t^{i_2} \,|\, i_1, i_2 \geq 0\},$$

and we have

$$u_{xx} = \partial_x^2 u \succ \partial_t u = u_t,$$

as $2 > 1$. Hence, $u_f = u_{xx}$.

(b) Consider the lexicographic order on $\{(i_1, i_2 \,|\, i_1, i_2 \geq 0\}$ so that $\Theta Y = \{\partial_t^{i_1}\partial_x^{i_2} \,|\, i_1, i_2 \geq 0\}$ (i.e., we consider the case $\partial_t > \partial_x$). Then,

$$\partial_x^2 \prec \partial_t,$$

and we have $u_f = u_t$.

Given a polynomial $f \in K\{y_1, \ldots, y_n\}$, once we determine u_f, we write f as a univariate polynomial in u_f as follows:

$$(\star) \quad f = a_p u_f^p + a_{p-1} u_f^{p-1} + \cdots + a_0, \quad a_i \in K\{y_1, \ldots, y_n\}.$$

Example 2.8. Let $K\{y\}$ be an ordinary differential polynomial ring, and let $f = y \cdot y'' + 1 \in K\{y\}$. We have $u_f = y''$ and therefore $a_1 = y$, $a_0 = 1$.

Definition 2.6. In $(\star)$ above, the coefficient a_p is called the *initial* of f, and is denoted by I_f.

Example 2.9. Consider $f = (y')^2 + y \in K\{y\}$ (here, $\Delta = \{\delta\}$). We see that $u_f = y'$, $I_f = 1$. Apply δ to f:

$$\delta((y')^2 + y) = 2y'y'' + y',$$

and call $2y'y'' + y' = g$. We then have $u_g = y''$ and $I_g = 2y'$.

Note that in Example 2.9, $2y' = \frac{\partial((y')^2 + y}{\partial y'}$ with $deg_{\delta u_f}(\delta f) = 1$.

Exercise 11. Prove that for every $f \in K\{y_1, \ldots, y_n\}$ and a ranking $\succ$ and any $\delta \in \Delta$, $I_{(\delta f)} = \frac{\partial f}{\partial u_f}$.

Definition 2.7. $\frac{\partial f}{\partial u_f}$ is called the *seperant* of f, denoted S_f.

Example 2.10. In Example 2.9, $S_{(y')^2+y} = 2y'$.

For the following, let K be a differential field, $R = K\{y_1, \ldots, y_n\}$ be a differential polynomial ring, and let a ranking on ΘY be fixed (unless otherwise noted).

Definition 2.8. For all $f, g \in R$, we say that f is *partially reduced* with respect to g if none of the terms in of f contains a proper derivative of u_g.

Example 2.11. (1) Let $f = y^2$ and $g = y+1$. Here, $u_g = y$ and we see that f is partially reduced with respect to g.
(2) Let $f = y^2 + y'$ and $g = y+1$. u_g is the same as before, but f is not partially reduced with respect to g, since the term y' in f can be obtained by applying δ to u_g.
(3) Let $f = 2yy'' + y$ and $g = y+1$. Since $2yy''$ in f is divisible by a proper derivative of u_g, we see that f is not partially reduced with respect to g.

Definition 2.9. We say that f is *reduced* with respect to g if
(i) f is partially reduced with respect to g, and
(ii) if $u_f = u_g$, then $deg_{u_f}(f) < deg_{u_g}(g)$.

Example 2.12. Let $f = y$ and $g = y+1$. f is not reduced with respect to g, since (ii) above is not satisfied.

Definition 2.10. A subset $\mathcal{A} \subset R$ is called *autoreduced* if, for all $f, g \in \mathcal{A}$ where $f \neq g$, f is reduced with respect to g.

Example 2.13. Let $\mathcal{A} = 2yy'' + y, y+1$. This is not autoreduced $\big($see Example 2.11(3)$\big)$.

Exercise 12. Prove that every autoreduced set in R is finite.

Let $\mathcal{A}$ and $\mathcal{B}$ be autoreduced. Let $\mathcal{A} = A_1, \ldots, A_p$ and $\mathcal{B} = B_1, \ldots, B_q$ with $A_1 < \ldots < A_p$ and $B_1 < \ldots < B_q$ for some ranking $<$, where we say that $f > g$ if $u_f > u_g$, else if $u_f = u_g$ then $deg_{u_f}(f) > deg_{u_g}(g)$.

We say that $\mathcal{A} < \mathcal{B}$ if:
(1) there exists i, $1 \le i \le p$ such that, for all j, $1 \le j \le i-1$, $\neg(B_j < A_j)$ and $A_i < B_i$. Else,
(2) $q < p$ and $\neg(B_j < A_j)$, $1 \le j \le q$.

Example 2.14. Let $R = K\{y_1, y_2\}$ with $\Delta = \{\delta\}$ with any deglex ranking. Let
$$\mathcal{A} = \{A_1 = (y_2')^2 + 1, A_2 = y_1'' + y_2\} \quad \text{and} \quad \mathcal{B} = \{B_1 = (y_2') + 2\}.$$
Is $\mathcal{A} < \mathcal{B}$? Starting with 1, we compare A_1 to B_1, and we see that $B_1 < A_1$, so we have $\mathcal{B} < \mathcal{A}$.

Now, consider
$$\tilde{\mathcal{B}} = \{\tilde{B}_1 = (y')^2 + 1\},$$
and compare $\mathcal{A}$ with $\tilde{\mathcal{B}}$. Since $\neg(\tilde{B}_1 < A_1)$, we have $\mathcal{A} < \tilde{\mathcal{B}}$.

Exercise 13. Show that every non-empty set of autoreduced sets in R has a minimal element.

Exercise 14. Develop a division algorithm as follows: Fix a ranking, and let $\mathcal{A} = A_1, \ldots, A_p$.
Input:$f \in R$ and $\mathcal{A} \subset R$ an autoreduced set.
Output: $g \in R$ such that

(1) g is reduced with respect to each element of $\mathcal{A}$;
(2) There exists $n \geq 0$ such that
$$I_{A_1}^n \cdot \ldots \cdot I_{A_p}^n \cdot S_{A_1}^n \cdot \ldots \cdot S_{A_p}^n \cdot f - g \in [\mathcal{A}].$$

(Hint: in the regular division algorithm, one sees that if $f = x^2+1$ and $\mathcal{A} = x+1$, then $f = q(x+1)+g$ so that $f - g \in (\mathcal{A})\big)$.

Example 2.15. The setup is the same as that of Example 2.14

(1) Let $f = y_1$ and $\mathcal{A} = A_1 = y_2 \cdot y_1$. Here, $u_{A_1} = y_1$, $I_{A_1} = y_2$, and we have $g = 0$, so $I_A \cdot f - 0 \in [\mathcal{A}]$.
(2) Let $f = y_1' + 1$ and $\mathcal{A} = A_1 = y_2 y_1^2$. Again we have $u_{A_1} = y_1$. Differentiate A_1:
$$A_1' = 2y_2 y_1 y_1' + y_2'(y_1)^2,$$
and we get $S_{A_1} \cdot f - A_1' = 2y_2 y_1 - y_2' y_1^2$. Multiplty through by I_{A_1} to get
$$I_{A_1} \cdot S_{A_1} \cdot f - I_{A_1} \cdot A_1' = 2y_2^2 y_1 - y_2' y_2 (y_1)^2.$$
Finally, we get
$$I_{A_1} \cdot S_{A_1} \cdot f - \underbrace{2y_2^2 y_1}_{g} = y_2' A_1 + I_{A_1} \cdot A_1' \in [\mathcal{A}].$$

Definition 2.11. Let $I \subset R$ be a differential ideal. A minimal, autoreduced subset of I is called a *characteristic set* of I.

We began this section with preliminary information that would help prove the Ritt–Raudenbush Theorem. Before we give the proof, we begin with two lemmas:

Lemma 2.1. *Let $S \subset R$ be a subset and $a \in R$ such that the ideal $\{S, a\}$ has a finite set of generators as a radical differential ideal. Then, there exists $s_1, \ldots, s_p \in S$ such that $\{S, a\} = \{s_1, \ldots, s_p, a\}$.*

Proof. By hypothesis, there exist $b_1, \ldots, b_q \in R$ such that $\{S, a\} = \{b_1, \ldots, b_q\}$. In particular, for all i, $1 \leq i \leq q, b_i \in \{S, a\}$, that is, for all i there exists $n_i \geq 1$ such that $b_i^{n_i} \in [S, a]$. Let $s_1, \ldots, s_p \in S$ be such that, for all i, $b_i^{n_i} \in [s_1, \ldots, s_p, a]$. Therefore, for all i, $b_i \in \{s_1, \ldots, s_p, a\}$, implying
$$\{S, a\} = \{b_1, \ldots, b_q\} \subset \{s_1, \ldots, s_p, a\} \subset \{S, a\}$$
. ∎

Lemma 2.2. *For any ranking, let $I \subset K\{y_1, \ldots, y_n\}$ be a differential ideal, and $\mathcal{C} = c_1, \ldots, c_p$ be a characteristic set of I. Then, if $f \in I$ is reduced with respect to $\mathcal{C}$, then $f = 0$. In particular, for all i, $1 \leq i \leq p$, $S_{c_i} \notin I$ and $I_{c_i} \notin I$.*

Proof. Notice that, for all i, $1 \leq i \leq p$, we have $S_{c_i} < c_i$ and $I_{c_i} < c_i$. Indeed, the latter holds by definition and
$$c_i = I_{c_i} u_{c_i}^{n_i} + \ldots, \quad \text{and} \quad S_{c_i} = n I_{c_i} u_{c_i}^{n_i - 1} + \ldots$$
If there exists an i such that $I_{c_i} \in I$, then notice that, since $\mathcal{C}$ is autoreduced, I_{c_i} and S_{c_i} are reduced with respect to $\mathcal{C}$.

Let now $f \in I$ be reduced with respect to $\mathcal{C}$ and $c_1, \ldots, c_{p_i}$ be the elements in $\mathcal{C}$ such that $c_{p_i} < f$. Then the set $\{c_1, \ldots, c_{p_i}, f\}$ is autoreduced, and
$$\{c_1, \ldots, c_{p_i}, f\} < \mathcal{C},$$
which contradicts the minimality of $\mathcal{C}$. ∎

We are now ready to prove the Ritt-Raudenbush Theorem. We first restate the theorem:

Theorem (See Theorem 2.1 above)**.** *Let (K,Δ) be a differential field with char(K)=0. Then the radical differential ideals in $R = K\{y_1,\ldots,y_n\}$ satisfy the ACC.*

Proof. We will prove an equivalent statement, namely we will prove that for all radical differential ideals $I \subset R$, there exists a finite set $F \subset R$ such that $I = \{F\}$.

Exercise 15. Prove that the set of radical differential ideals in R satisfies the ACC if and only if for all radical differential ideals $I \subset R$, there exists a finite set $F \subset R$ such that $I = \{F\}$ (we say that I is finitely generated as a radical differential ideal).

Back to the proof, suppose that there exists a radical differential ideal $I \subset R$ that is not finitely generated. By Zorn's Lemma, there exists a maximal radical differential ideal J that is not finitely generated. We will first show that J is prime.

Suppose J is not prime, i.e., there exist $a,b \in R$ such that $ab \in J$ but $a \notin J$ and $b \notin J$. Then, the radical differential ideals $\{a,J\}$ and $\{b,J\}$ properly contain J. By maximality of J, we see that both $\{a,J\}$ and $\{b,J\}$ are finitely generated. By Lemma 2.1, there exist $f_1,\ldots,f_q \in J$ and $g_1,\ldots,g_q \in J$ such that:

$$\{a,J\} = \{a,f_1,\ldots,f_q\} \text{ and } \{b,J\} = \{b,g_1,\ldots,g_q\}.$$

We have:

$$\{a,J\}\{b,J\} \subset \{ab, \text{ further products of } a,b,f_i,g_j\} = \mathfrak{a} \subset \{J\}.$$

For all $f \in J$, $f^2 \in \{a,J\}\{b,J\} \Rightarrow f^2 \in \mathfrak{a} \Rightarrow f \in \mathfrak{a}$, and J is therefore finitely generated $\rightarrow\leftarrow$. Thus, J is prime.

Let $\mathcal{C} = c_1,\ldots,c_p$ be a characteristic set of J. Then, for all i, by Lemma 2.2, we have $I_{c_i}, S_{c_i} \notin J$. Therefore, by maximality of J, $\{S_{c_1}I_{c_1}\cdot\ldots\cdot S_{c_p}I_{c_p},J\}$ is finitely generated as a radical differential ideal. By Lemma 2.1, there exist $f_1,\ldots,f_q \in J$ such that

$$\{S_{c_1}I_{c_1}\cdot\ldots\cdot S_{c_p}I_{c_p},J\} = \{S_{c_1}I_{c_1}\cdot\ldots\cdot S_{c_p}I_{c_p},f_1,\ldots,f_q\}.$$

Let $h \in J$. Reduce h with respect to $\mathcal{C}$ and find a $g \in R$ such that:

(1) g is reduced with respect to $\mathcal{C}$, and
(2) $S_{c_1}I_{c_1}\cdot\ldots\cdot S_{c_p}I_{c_p}h - g \in \{\mathcal{C}\} \subset J$.

By Lemma 2.2, one sees that $g = 0$, so $S_{c_1}I_{c_1}\cdot\ldots\cdot S_{c_p}I_{c_p}h \in \{\mathcal{C}\}$, and thus $S_{c_1}I_{c_1}\cdot\ldots\cdot S_{c_p}I_{c_p}J \subset \{\mathcal{C}\}$. We now have:

$$\begin{aligned} J^2 &\subset J\cdot\{S_{c_1}I_{c_1}\cdot\ldots\cdot S_{c_p}I_{c_p},J\} \subset J\cdot\{S_{c_1}I_{c_1}\cdot\ldots\cdot S_{c_p}I_{c_p},f_1,\ldots,f_1\} \\ &\subset \{S_{c_1}I_{c_1}\cdot\ldots\cdot S_{c_p}I_{c_p}J,f_1,\ldots,f_q\} \subset \{c_1,\ldots,c_p,f_1,\ldots,f_q\} \subset J. \end{aligned}$$

We conclude that $\{c_1,\ldots,c_p,f_1,\ldots,f_q\} = J$. ∎

3. Differential Algebraic Extensions.

Recall that, given an extension of fields $L \supset K$, and element $a \in L$ is called *algebraic* over K if there exists a non-zero polynomial $p \in K[x]$ such that $p(a) = 0$. If a is not algebraic, then it is *transcendental*.

Example 3.1. (1) Let $K = \mathbb{Q}$, $L = \mathbb{C}$. $\sqrt{2} \in L$ is algebraic over K, since it is the root of the polynomial $p = x^2 - 2$.
(2) π and e are transcendental over $\mathbb{Q}$.

Recall also that elements $a_1,\ldots,a_n \in L$ are called *algebraically dependent* if there exists a non-zero polynomial $p \in K[x_1,\ldots,x_n]$ such that $p(a_1,\ldots,a_n) = 0$.

Definition 3.1. Let $L \supset K$ be an extension of differential fields. Then an element $a \in L$ is called *differential algebraic* over K if there exists a non-zero $p \in K\{y\}$ such that $p(a) = 0$. In other words, a is differential algebraic if there exists a non-empty finite subset of $\{\theta a \,|\, \theta \in \Theta\}$ that is algebraically dependent over K.

Example 3.2. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(x)$, $\Delta = \{\delta\}$, and $\delta x = 1$. Let $a \in \mathbb{Q}[x]$, i.e., $a = a_n x^n + \ldots + a_0$, where $a_i \in \mathbb{Q}$, $0 \le i \le n$. Then, a is algebraic over K since $\delta^{n+1}(a) = 0$, and we choose such a $p = y^{(n+1)}$.

Exercise 16. In the previous example, if possible, for each $a \in \mathbb{Q}(x)$, find a non-zero $p \in K\{y\}$ such that $p(a) = 0$.

Theorem 3.1. *Let $L \supset K$ be a differential field extension and let $\alpha, \beta \in L$. If α is differential algebraic over K and β is differential algebraic over*

$$K\langle\alpha\rangle := Quot(K\{\alpha\}),$$

then β is differential algebraic over K.

Remark. In Theorem 3.1, $K\langle\alpha\rangle$ is defined to be the quotient field of $K\{\alpha\}$ which is the smallest differential subfield of L containing both K and α.

A proof for Theorem 3.1 will be given later. But there is a corollary:

Corollary 3.1. *Let $L \supset K$ be a differential field extension. Then,*

$$M = \{f \in L \,|\, f \text{ is differential algebraic over } K\}$$

is a differential subfield of L.

Exercise 17. Prove Corollary 3.1.

Definition 3.2. A differential field extension $L \supset K$ is called a *differentially finitely generated* if there exist $a_1,\ldots,a_n \in L$ such that

$$L = K\langle a_1,\ldots,a_n\rangle = Quot(K\{a_1,\ldots,a_n\}),$$

that is, L is the smallest differential subfield of itself containing K and $a_1,\ldots,a_n$.

Definition 3.3. A set $\Delta = \{\partial_1,\ldots,\partial_m\}$ is called *independent* over (K,Δ) if there exist $a_1,\ldots,a_m \in K$ such that

$$\det(\partial_i a_j \,|\, 1 \le i,j \le m) \ne 0,$$

that is, the $m \times m$ matrix with entries $(\partial_i a_j)$ is nonsingular.

Example 3.3. (1) $\Delta = \{\delta\}$ is independent if and only if $K \supsetneq K^\Delta$.
(2) Δ is not independent over $(\mathbb{Q},\Delta)$ (Why?).
(3) Let $K = \mathbb{Q}(x_1,\ldots,x_n)$, $\Delta = \{\partial_1,\ldots,\partial_m\}$ and $\partial_i = \frac{\partial}{\partial x_i}$. Then, Δ is independent over (K,Δ) by taking the $a_i = x_i$.

Theorem 3.2 (Primitive Element Theorem for Differential Algebra)**.** *Let L and K be differential fields such that $L \supset K$ is a differentially finitely generated differential algebraic differential field extension, and assume that Δ is independent over (K,Δ). Then, there exists $a \in L$ such that $L = K\langle a\rangle$. In other words, if $b_1,\ldots,b_k \in L$ are differential algebraic over K, then there exists $b \in K\langle b_1,\ldots,b_n\rangle$ such that $K\langle b_1,\ldots,b_n\rangle = K\langle b\rangle$.*

Exercise 18. Let $K = \mathbb{Q}$ and $\Delta = \{\delta\}$. Note that Δ is not independent over (K,Δ). Let

$$L = Quot(K\{y_1,y_2\}/[y_1',y_2']).$$

Let c_1,c_2 be the images of y_1 and y_2, respectively, in the above quotient. This gives $L = K(c_1,c_2)$ with $\delta c_1 = 0$ and $\delta c_2 = 0$. Prove that $L \neq K\langle c\rangle$ for any $c \in L$.

Exercise 19. (See Theorem 3.4 below). Prove that Δ is independent over (K,Δ) if and only if, for all $p \neq 0 \in K\{y\}$, there exists $c \in K$ such that $p(c) \neq 0$ (Hint: Use the fact that K is infinite.)

Proof (Differential Primitive Element Theorem). Let $n = 2$. The general case will follow by induction on n. We will show that there exists $c \in K$ such that

$$K\langle b_1,b_2\rangle = K\langle b_1+cb_2\rangle.$$

For this, let t be a differential indeterminate over K. Note that b_1+tb_2 is differential algebraic over $K\langle t\rangle$. Indeed, by Theorem 3.1 (whose proof will be shown later), the previous sentence holds. A corollary to Theorem 3.1:

Corollary 3.2. *For an extension $L \supset K$, the set of differential algebraic elements of L over K is a differential field.*

Proof. Indeed, if $\alpha,\beta \in L$ is differential algebraic over K, then $\alpha+\beta \in K\langle\alpha\rangle\langle\beta\rangle$, and by the theorevm, $\alpha+\beta \in K$. ☐

Continuing with the proof of the Differential Primitive Element Theorem, we know that there exists $p \neq 0 \in K\langle t\rangle\{y\}$ such that $p(b_1+tb_2) = 0$. In general, for $a \in L$, the set

$$I_a = \{f \in K\{y\} \mid f(a) = 0\}$$

is a differential ideal of $K\{y\}$. Let $>$ be a ranking and $I_{b_1+tb_2} \subset K\langle t\rangle\{y\}$. Let $\mathcal{C} = c_1,\ldots c_q$ be a characteristic set of $I_{b_1+tb_2}$. By Lemma 2.2, we have $c_1 \in I_{b_1+tb_2}$ and $S_{c_1} \notin I_{b_1+tb_2}$. Therefore, we have

$$(\star) \qquad c_1(b_1+tb_2) = 0 \text{ and } S_{c_1}(b_1+tb_2) \neq 0.$$

Let $u_{c_1} = \theta y$. By clearing the denominators in $(\star)$, we obtain $g \in K\{y,z\}$ such that

$$(\star\star) \qquad g(b_1+tb_2,t) = 0 \text{ and } \frac{\partial g}{\partial\theta y}(b_1+tb_2,t) \neq 0.$$

We will find $c \in K$ such that $b_2 \in K\langle b_1+cb_2\rangle$. Since $b_2 = \frac{\partial\theta(b_1+tb_2)}{\partial(\theta t)}$, $(\star\star)$ implies

$$\frac{\partial g(b_1+tb_2,t)}{\partial(\theta t)} = \frac{\partial g(b_1+tb_2,t)}{\partial(\theta y)}\cdot b_2 + \frac{\partial g(b_1+tb_2,t)}{\partial(\theta z)} = 0 \quad (\star\star\star).$$

From $(\star)$ and $(\star\star\star)$, we have

$$b_2 = \frac{-\frac{\partial g(b_1+tb_2,t)}{\partial(\theta z)}}{\frac{\partial g(b_1+tb_2,t)}{\partial(\theta y)}}. \tag{1}$$

Let $h = \frac{\partial g}{\partial(\theta y)}(b_1 + tb_2, t) \in K\langle t\rangle\{y\}$. Since $h \neq 0$ and Δ is independant over K, by Exercise 19, there exists c such that $h(c) \neq 0$. By plugging c into (1), we obtain $b_2 \in K\langle b_1 + cb_2\rangle$. □

We will present a proof for Theorem 3.1 later. However, we state a proposition concerning Exercise 19:

Proposition 3.1. *Let (K, Δ) be a differential field with $\Delta = \partial_1, \ldots, \partial_m$ and $x_1, \ldots, x_m \in K$ be such that $\partial_i(x_j) = \delta_{i,j}$, where $\delta_{i,j}$ is the Kroenecker delta defined as*

$$\delta_{i,j} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

(in particular, Δ is independant over K). Then, for every non-zero $p \in K\{y\}$, there exists $c \in K$ such that $p(c) \neq 0$.

Proof. Let $u_p = \partial_1^{i_1} \cdot \ldots \cdot \partial_m^{i_m}(y)$. Search for

$$c = \sum_{j_1+\ldots+j_m \leq i_1+\ldots+i_m} c_{j_1,\ldots j_m} x_1^{i_1} \cdot \ldots \cdot x_m^{i_m},$$

for $c_{j_1,\ldots,j_m} \in K^\Delta$. Plugging in $p(c)$, we claim that

$$p(c)(x_1 = 0, \ldots, x_m = 0)$$

is a nonzero polynomial in $c_{j_1,\ldots,j_m}$. Indeed, since $\mathbb{Q} \subset K^\Delta$, we know that K is infinite, which implies the existence of some $b_{j_1,\ldots,j_m} \in K^\Delta$ such that $j_1 + \ldots + j_m \leq i_1 + \ldots + i_m$ and $p(b_{j_1,\ldots,j_m})(0) \neq 0$. Now let

$$b = \sum_{j_1+\ldots+j_m \leq i_1+\ldots+i_m} b_{j_1,\ldots j_m} x_1^{i_1} \cdot \ldots \cdot x_m^{i_m},$$

and $p(b) \neq 0$. □

This prove hints how to solve Exercise 19; First, prove, using the fact that K^Δ is infitnite, that Δ is independant if and only if, for all $p \neq 0 \in K[\partial_1 y, \ldots, \partial_m]$ there exists $c \in K$ such that $p(c) \neq 0$. Then generalize this case.

3.1. **Differential Nullstellensatz.** We recall the strong and weak polynomial Nullstellensatz:

Theorem (Strong Nullstellensatz)**.** *Let K be an algebraically closed field. Then, for all $F \subset K[y_1, \ldots, y_n]$ and $f \in K[y_1, \ldots, y_n]$, $f \in \sqrt{(F)}$ if and only if, for all $(a_1, \ldots, a_n) \in K^n$, if $F(a_1, \ldots, a_n) = 0$, then $f(a_1, \ldots, a_n) = 0$.*

Theorem (Weak Nullstellensatz)**.** *Let K be an algebraically closed field. Then*

$$\{(a_1, \ldots, a_n) \in K^n \,|\, F(a_1, \ldots, a_n) = 0\} = \varnothing \iff 1 \in (F).$$

Note that for both the strong and weak Nullstellensatz, we require K to be algebraically closed.

Definition 3.4. K is algebraically closed if it is *existentially closed*, meaning, for all $F \subset K[y_1, \ldots, y_n]$, if there exist $L \supset K$ and $(a_1, \ldots, a_n) \in L^n$ such that $F(a_1, \ldots, a_n) = 0$, then there exists $(b_1, \ldots, b_n) \in K^n$ such that $F(b_1, \ldots, b_n) = 0$.

Definition 3.5. (K, Δ) is called *differentially closed* if it is existentially closed, i.e., if, for all $F \subset K\{y_1, \ldots, y_n\}$, if there exist $L \supset K$ and $(a_1, \ldots, a_n) \in L^n$ such that $F(a_1, \ldots, a_n) = 0$, then there exist $(b_1, \ldots, b_n) \in K^n$ such that $F(b_1, \ldots, b_n) = 0$.

Remark. If K is differentially closed, then K is algebraically closed.

Definition 3.6. (L,Δ) is called a *differential closure* of (K,Δ) if $L \supset K$ and, for every differentially closed (M,Δ) with $M \supset K$, there exists a differential homomorphism $\varphi : L \hookrightarrow M$ such that $\varphi|_K = id$.

Theorem 3.3 (Differential Nullstellensatz)**.** *Let K be a differentially closed field. For all $F \subset K\{y_1,\dots,y_n\}$ and $f \in K\{y_1,\dots,y_n\}$, $f \in \{F\}$ if and only if, for all $(a_1,\dots,a_n) \in K^n$, if $F(a_1,\dots,a_n) = 0$, then $f(a_1,\dots,a_n) = 0$.*

Proof. $(\Rightarrow)$ follows from $f^q = \sum_{i=1}^r b_i\theta_i f_i$ for $f_i \in F$.

$(\Leftarrow)$ We will prove this for $f \neq 0$, for when $f = 0$ then $f \in \{F\}$. We will use the Rabinowitsch trick: Consider the radical differential ideal

$$\{F, 1-ft\} \subset K\{y_1,\dots,y_n,t\}.$$

If $F(a_1,\dots,a_n) = 0$, then $(1-ft)(a_1,\dots,a_n) = 1 \neq 0$. Therefore,

$$(\star) \qquad \begin{cases} F &= 0 \\ 1-tf &= 0 \end{cases}$$

has no solutions in K^{n+1}. We will show later that $(\star)$ implies that $1 \in [F, 1-tf]$ (Weak Differential Nullstellensatz), but we will use this fact here. Hence,

$$(\star\star) \qquad 1 = \sum_{i,j} b_{i,j}\theta_{i,j}f_j + \sum_q c_q\theta_q(1-tf)$$

for some $b_{i,j}, c_q \in K\{y_1,\dots,y_n\}$. Since $f \neq 0$, replace t by $\frac{1}{f}$ in $(\star\star)$ to get

$$1 = \sum_{i,j} b_{i,j}(1/f)\theta_{i,j}f_j.$$

Hence, there exists k such that, for all i,j,

$$f^k b_{i,j}(1/f) \in K\{y_1,\dots,y_n\}.$$

Thus $f^k \in [F]$ and therefore $f \in \{F\}$.

□

Proof (Weak Differential Nullstellensatz). Let $I \subset K\{y_1,\dots,y_n\}$ and $1 \notin I$. We will show that there exists $(a_1,\dots,a_n) \in K^n$ such that, for all $f \in I$, $f(a_1,\dots,a_n) = 0$. Let $M \supset I$ be a maximal differential ideal containing I. By Corollary 1.1, M is prime. We will find a zero of M. Let $L = Quot\big(K\{y_1,\dots,y_n\}(M)\big)$, and let $M = \{g_1,\dots,g_s\}$. Let $b_1,\dots,b_n$ be the images of $y_1,\dots,y_n$ in L. Now, for all i, $g_i(b_1,\dots,b_n) = 0$ in L. Since K is differentially closed, there exists $(a_1,\dots,a_n) \in K^n$ with $g_i(a_1,\dots,a_n) = 0$ for all i. □

Before we give a proof for Theorem 3.1, we first remark that, when $|\Delta| \geq 2$, α is differential algebraic over $K \not\Rightarrow trdeg_K(K\langle\alpha\rangle) < \infty$.

Example 3.4. Let $K = \mathbb{Q}(\alpha, \partial_x\alpha, \partial_x^2\alpha, \dots)$ and $\Delta = \{\frac{\partial}{\partial x}, \frac{\partial}{\partial y}\}$ with derivations defined by

$$\partial_x(\partial_x^i\alpha) = \partial_x^{i+1}\alpha \qquad i \geq 0$$

and

$$\partial_y(\alpha) = 0.$$

We see that α is differential algebraic over $\mathbb{Q}$, but $trdeg_{\mathbb{Q}}(K) = \infty$.

Proof (Theorem 3.1). Fix an orderly ranking. Since α is differential algebraic over K, there exists $p \neq 0 \in K\{y\}$ such that

$$p(\alpha) = 0 \text{ and } S_p(\alpha) \neq 0 \tag{2}$$

(see Lemma 2.2). Let $u_p = \theta_1 y$. Our goal will be to estimate the growth of $trdeg_K K(\theta\beta \,|\, ord\theta \leq s)$ as $s \to \infty$. (2) implies that $\delta_1(p(\alpha)) = 0$ where $p = I_p u_p^{n_p} + \ldots$. However,

$$\delta_1(p(\alpha)) = S_p(\alpha)\delta_1(\theta_1(\alpha)) + \text{ expressions with } \theta(\alpha) \text{ where } \theta < \delta_1\theta_1,$$

which further implies that $\delta_1\theta_1(\alpha) \in K(\theta(\alpha) \,|\, \theta < \delta_1\theta_1)$. It can be shown by induction (do this!) that

$$\theta_2\delta_1\theta_1(\alpha) \in K(\theta(\alpha) \,|\, \theta < \theta_2\delta_1\theta_1). \tag{3}$$

Let $r_1 = ord(\delta_1\theta_1)$. Then, (3) implies that, for all $r \geq r_1$,

$$K(\theta(\alpha) \,|\, \theta \in \Theta(r)) = K(\theta(\alpha) \,|\, \Theta(r) \backslash \Theta(r - r_1)\delta_1\theta_1),$$

where $\Theta(r) = \{\theta \,|\, ord(\theta) \leq r\}$.

Similarly, there exists $g \neq 0 \in K\langle\alpha\rangle\{y\}$ such that $g(\beta) = 0$ and $S_g(\beta) \neq 0$, and there exists θ_3 such that

$$\theta_3(\beta) \in K\langle\alpha\rangle(\theta(\beta) \,|\, \theta < \theta_3).$$

Moreover, there exists q such that

$$\theta_3(\beta) \in K(\theta'(\alpha), \theta(\beta) \,|\, ord(\theta') \leq q, \theta < \theta_3).$$

Therefore, for all $\tilde{\theta}$,

$$\tilde{\theta}\theta_3(\beta) \in K(\theta'(\alpha), \theta(\beta) \,|\, ord(\theta') \leq q + ord(\tilde{\theta}) \text{ and } \theta < \theta_3).$$

Furthermore, for all $s \geq ord(\theta_3)$ and $q + s \geq r_1$,

$$\begin{aligned}
L(s) &:= K\big(\theta(\beta) \,|\, \theta \in \Theta(s)\big) \\
&\subset K\big(\theta'(\alpha), \theta(\beta) \,|\, \theta' \in \Theta(q+s) \text{ and } \theta \in \Theta(s) \backslash \Theta(s - ord(\theta_3)) \cdot \theta_3\big) \\
&= K\big(\theta'(\alpha) \,|\, \theta' \in \Theta(q+s) \backslash \Theta(q+s-r_1) \cdot \delta_1\theta_1 \text{ and } \theta \in \Theta(s) \backslash \Theta(s - ord(\theta_3)) \cdot \theta_3\big) \\
&=: M(s).
\end{aligned}$$

To calculate $|\Theta(s)|$, we need to count

$$\{(i_1, \ldots, i_m) \,|\, i_1 + \ldots + i_m \leq s\}.$$

Put s ones as such:

$$\underbrace{\overbrace{11\cdots}^{i_1}\Big|\overbrace{1\cdots}^{i_2}\Big|\cdots\Big|\overbrace{1\cdots}^{i_m}\Big|\cdots 1}_{s},$$

and we see m "thick lines." We know from this that there are

$$\binom{s+m}{m}$$

choices. So,

$$|\Theta(s)| = f(s) = \binom{m+s}{m} = \frac{(s+m)!}{m!s!} = \frac{(s+m)\cdot\ldots\cdot(s+1)}{m!},$$

which is a polynomial in s of degree m. We also have

$$\begin{aligned}
&|\Theta(q+s)\backslash\Theta(q+s-r_1),\Theta(s)\backslash\Theta(s-ord(\theta_3))|\\
&=\binom{q+s+m}{m}-\binom{q+s-r_1+m}{m}+\binom{s+m}{m}-\binom{s-ord(\theta_3)+m}{m}\\
&=g(s),
\end{aligned}$$

and one can show (do this!) that $deg(g)=m-1$. Therefore, there exists s such that the number of generators in $L(s)$ over K is greater than the number of generators in $M(s)$ over K. Thus, $\{\theta(\beta)\,|\,ord(\theta)\leq s\}$ is algebraically dependent over K, as all transcendence bases of a given finitely generated extension have the same number of elements. ☐

Theorem 3.4 (Exercise 19)**.** *$\Delta=\{\partial_1,\dots,\partial_m\}$ is independent over (K,Δ) $\iff$ for all $p\neq 0\in K\{y\}$ there exists $c\in K$ such that $p(c)\neq 0$.*

Before we prove this theorem, we first state and prove a proposition that will help. Note that we are in $charK=0$, so $K\supset\mathbb{Q}$ is infinite.

Proposition 3.2. *For all finite $\Omega\subset\Theta$ (say, $|\Omega|=q$, i.e., $\Omega=\{\theta_1,\dots,\theta_q\}$), there exist $b_1,\dots,b_q\in K$ such that $det(\theta_i b_j)\neq 0$ $\iff$ for all $0\neq p\in K[\theta y|\theta\in\Omega]$, there exists $c\in K$ such that $p(c)\neq 0$.*

Proof. $(\Leftarrow)$ Consider:

$$det\begin{vmatrix}\theta_1 b_1 & \dots & \theta_1 b_q\\ \vdots & \ddots & \vdots\\ \theta_q b_1 & \dots & \theta_q b_q\end{vmatrix}=m_{11}\theta_1 b_1-m_{21}\theta_2 b_1+\ldots\pm m_{q1}\theta_q b_1, \tag{4}$$

where m_{i1} is the determinant of the $q-1\times q-1$ matrix obtained by deleting the ith row and 1st column. By induction, there exist $b_2,\dots,b_q$ such that $m_{i1}(b_2,\dots,b_q)\neq 0$ for some i. Then, substituting $(b_2,\dots,b_q)$ into (4) yields a non-zero polynomial in b_1.

$(\Rightarrow)$ Let $p\neq 0\in K[\theta_1 y,\dots,\theta_q y]$. By assumption, there exists $b_1,\dots,b_q\in K$ such that $\det(\theta_i b_j)\neq 0$. So, let $B=(\theta_i b_j)$. B is invertible since $\det(B)\neq 0$. Let $C=B^{-1}$. Define $z_1,\dots,z_q$ by

$$\begin{pmatrix}z_1\\ \vdots\\ z_q\end{pmatrix}=C\begin{pmatrix}\theta_1 y\\ \vdots\\ \theta_q y\end{pmatrix}.$$

Then,

$$\begin{pmatrix}\theta_1 y\\ \vdots\\ \theta_q y\end{pmatrix}=B\begin{pmatrix}z_1\\ \vdots\\ z_q\end{pmatrix}.$$

So, $z_1,\dots,z_q$ are algebraically independent over K. Therefore, there exists $P\neq 0\in K[Z_1,\dots,Z_q]$ such that $P(z_1,\dots,z_q)=p(\theta_1 y,\dots,\theta_q y)$. Since $\mathbb{Q}$ is infinite, there exist $c_1,\dots,c_q\in\mathbb{Q}$ such that $P(c_1,\dots,c_q)\neq 0$. Consider

$$c=\sum c_j b_j.$$

Then,

$$\theta_i(c)=\sum\theta_i(b_j)c_j,$$

and therefore

$$\begin{pmatrix} \theta_1(c) \\ \vdots \\ \theta_q(c) \end{pmatrix} = B \begin{pmatrix} c_1 \\ \vdots \\ c_q \end{pmatrix}$$

If we let $z_1 = c_1, \ldots, z_q = c_q$, then $\theta_1(c) \to \theta(y), \ldots, \theta_q(c) \to \theta_q(y)$. So, $p(c) = P(c_1, \ldots, c_q) \neq 0$. $\square$

Proof (Theorem 3.4). ($\Leftarrow$) one can utilize the above proof to show this direction.

($\Rightarrow$) Let $b_1, \ldots, b_m \in K$ be such that $det(\partial_i b_j) \neq 0$. Let $(a_{ij}) = (\partial_i b_j)^{-1}$. We will show that, for all $s \geq 0$, $\Theta(s)$ is independent over K. That is, we will show that

$$det(\partial_1^{i_1} \cdot \ldots \cdot \partial_m^{i_m}(\frac{b_1^{i_1} \cdot \ldots \cdot b_m^{i_m}}{i_1! \cdot \ldots \cdot i_m!}) \,|\, i_1 + \ldots + i_m \leq s) \neq 0.$$

It will be left as an exercise to show this. Hint: introduce $\partial_1', \ldots, \partial_m'$ defined by

$$\begin{pmatrix} \partial_1' \\ \vdots \\ \partial_m' \end{pmatrix} = (a_{ij}) \begin{pmatrix} \partial_1 \\ \vdots \\ \partial_m \end{pmatrix}.$$

Notice that $\partial_i'(b_j) = 1$ if $i = j$ and 0 if $i \neq j$. Then, show that

$$det(\partial_1^{i_1} \cdot \ldots \cdot \partial_m^{i_m}(\frac{b_1^{i_1} \cdot \ldots \cdot b_m^{i_m}}{i_1! \cdot \ldots \cdot i_m!}) = 1.$$

$\square$

4. Algorithms and Open Problems

4.1. **Algorithms.** The following is due to Ritt, Kolchin, Boulier, and Hubert:

Given: $F \subset K\{y_1, \ldots, y_n\}$, $\Delta = \{\partial_1, \ldots, \partial_m\}$ and a ranking $>$.

Output: finite sets $\mathcal{C}_1, \ldots, \mathcal{C}_q$ such that, for all i:

(a) There exists a radical differential ideal I_i such that $\mathcal{C}_i$ is a characterstic set of I_i.

(b) $f \in I_i \iff f$ reduces to 0 with respect to $\mathcal{C}_i$.

(c) $\{F\} = I = I_1 \cap \ldots \cap I_q$.

This procedure is called `RosenfeldGroebner` in MAPLE.

Example 4.1. Consider $K\{x, y\}$. Let $I = (xy)$ and $\mathcal{C} = xy$. Supposed $x < y$. Then, y reduces to 0.

Kolchin showed that, if I is prime and $\mathcal{C}$ is a characteristic set of I, then $f \in I \iff f$ reduces to 0 with respect to $\mathcal{C}$. The Ritt-Kolchin algorithm can find I_i in the previous algorithm such that each I_i is a prime differential ideal (however, this requires factorization over field extensions).

4.2. **Open Problems.**

(1) Give a reasonable complexity estimate of the previous algorithm.

(2) Effective Differential Nullstellensatz is a way to test whether a system of differential polynomials is consistent or, more formally,

$$1 \in \{F\} \iff 1 \in (\theta F \,|\, ord(\theta) \leq h(n, m, O, d)),$$

where $F \subset K\{y_1,\dots,y_n\}$ is a set of differential polynomials, m is the number of derivations, $O = ord(F)$, and $d = deg(F)$. The bounding function h was found by Golubitsky, Kondratieva, Ovchinnikov, and Szanto. However, one needs to improve upon this bound.

(3) Find an (explicit) upper bound for the effective difference Nullstellensatz.

(4) The Ritt Problem: Find an irredundant decomposition for the last part of the algorithm above. There are two equivalent statements that one can prove. First, given a characteristic set of a prime differential ideal P, find F such that $P = \{F\}$. Second, test whether $\{F\}$ is prime. This has been resolved in some cases, for example, when $|F| = 1$.

(5) Jacobi's bound.

(6) Dimension conjecture.

5. Differential Galois Theory

Unless otherwise stated, K will be an ordinary differential field with char$K$=0.

5.1. **Linear Differential Equations.** We begin with three ways to view linear differential equations:

(First View) The first way to view it is via differential modules, which are related to Tannakian Categories.

Definition 5.1. A finite-dimensional K-vector space M is a called a *differential module* if it is supplied with a map $\partial : M \to M$ satisfying:

(a) For all $m,n \in M$, $\partial(m+n) = \partial(m) + \partial(n)$, and

(b) For all $a \in K$ and $m \in M$, $\partial(a \cdot m) = \partial(a)m + a\partial(m)$.

Example 5.1. Let M be any finite-dimensional vector space, and let $\partial : M \to M$ be such that $\partial(m) = 0$ for all $m \in M$. M is a differential module, provided that $\partial(a) = 0$ for all $a \in K$.

Let $\{e_1,\dots,e_n\}$ be a K-basis of M. Then, for all i, there exist $a_{1i},\dots,a_{ni} \in K$ such that

$$\partial(e_i) = \sum_{j=1}^{n} -a_{ji}e_j. \tag{5}$$

We also know that, for any $m \in M$, there exist $a_1,\dots,a_n \in K$ such that $m = \sum_{i=1}^n a_i e_i$. Now, consider the differential equation

$$\partial(y) = 0. \tag{6}$$

$m \in M$ satisfies (6) if and only if $\partial(\sum_{i=1}^n a_i e_i) = 0$. But then we have:

$$\begin{aligned}\partial(\sum_{i=1}^{n} a_i e_i) &= \sum_{i=1}^{n} \partial(a_i)e_i + \sum_{i=1}^{n} a_i \partial(e_i)\\ &= \sum_{i=1}^{n} \partial(a_i)e_i + \sum_{i=1}^{n} a_i \cdot \sum_{i=1}^{n} -a_{ji}e_j\\ &= \sum_{i=1}^{n} \partial(a_i)e_i - \sum_{i,j=1}^{n} a_{ij}a_j e_j,\end{aligned}$$

and by factoring out e_i in that last equality above, we see that the above holds if, for all i, $\partial(a_i) = \sum_j a_{ij} a_j$, which occurs if and only if

$$\begin{pmatrix} \partial(a_1) \\ \vdots \\ \partial(a_n) \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \tag{7}$$

So, to find $m \in M$ such that $\partial(m) = 0$ is equivalent to finding $a_1, \dots, a_n \in K$ satisfying (7). To introduce notation, if

$$\partial \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \partial(a_1) \\ \vdots \\ \partial(a_n) \end{pmatrix},$$

we can rewrite (7) as

$$\partial(Y) = AY. \tag{8}$$

Now, let $\{f_1, \dots, f_n\}$ be another basis of M with

$$(e_1, \dots, e_n) = (f_1, \dots, f_n)B$$

for some change of basis matrix $B \in GL_n(K)$. So, $m = \sum_i b_i f_i$ and

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = B \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

Then, (8) will transform into a new differential equation:

$$\begin{aligned} \partial \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} &= \partial(B \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}) = \partial(B) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + B\partial \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \\ &= \partial(B)B^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} + BA \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \\ &= \partial(B)B^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} + BAB^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ &= (BAB^{-1} + \partial(B)B^{-1}) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \end{aligned}$$

So, (8) becomes:

$$\partial(Y) = (BAB^{-1} + \partial(B)B^{-1})Y. \tag{9}$$

Definition 5.2. The transformation from (8) to (9) is called a *gauge transformation*, and (8) and (9) are said to be *gauge equivalent* (their solutions differ by an invertible matrix).

(Second View) In the first part we were given a differential module and produced a differential equation. Now, given a differential equation $\partial(Y) = AY, A \in M_n(K)$, we will produce a differential module.

Let $M = K^n$ and $\{e_1, \ldots, e_n\}$ be the standard basis (Recall, the vector e_i in the standard basis has a 1 in the ith spot and zeros elsewhere). Define $\partial(e_i)$ as we did in (5) and extend this to a derivation on M by

$$\partial(ae_i) = \partial(a)e_i + a\partial(e_i)$$

for all $a \in K$.

Exercise 20. Show that the construction in the Second View is well defined.

(Third View) The third view discusses our usual notion of scalar differential equations. Let $a_0, \ldots, a_{n-1} \in K$. The equation

$$y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1 y' + y = 0 \tag{10}$$

is a *homogeneous scalar linear differential equation of order n*.

Example 5.2. (a) $y'' - xy = 0$, called the *Airy Equation*.
(b) $y' - y = 0$, of which we know the *exp* function satisfies.

From (10), we wish to construct something similar to (8). To start, let

$$\begin{array}{c} y_1 = y \\ y_2 = y' \\ \vdots \\ y_n = y^{(n-1)} \end{array} \quad \Rightarrow \quad \begin{array}{c} \partial(y_1) = y_2 \\ \partial(y_2) = y_3 \\ \vdots \\ \partial(y_{n-1}) = y_n \\ \partial(y_n) = -a_{n-1}y_n - \ldots - a_0 y_1 \end{array}$$

From this change of variables, we get:

$$\partial \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & 0 & 1 \\ -a_0 & -a_1 & \ldots & -a_{n-2} & -a_{n-1} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}. \tag{11}$$

In (11), the matrix is called the *companion matrix* of (10).

Example 5.3. The companion matrix of the Airy Equation in (5.2) is

$$\begin{pmatrix} 0 & 1 \\ x & 0 \end{pmatrix}.$$

Now, to go from a system to a scalar equation we introduce the cyclic vector method.

Definition 5.3. Given a differential module M, a vector $e \in M$ is called *cyclic* if

$$span(e, \partial(e), \ldots, \partial^p(e)) = M$$

for some p.

Lemma 5.1. *If there exists $a \in k$ such that $\partial(a) \neq 0$, then M has a cyclic vector.*

Suppose now that we are given $\partial(Y) = AY$ such that the corresponding differential module has a cyclic vector e. Then, $\{e, \partial(e), \ldots, \partial^{(n-1)}(e)\}$ is a basis of M.

Exercise 21. Prove the above statement (i.e., why can we remove $\partial^n(e)$ through $\partial^p(e)$ when there may be other ∂^i for $1 \leq i \leq n-1$ that we should have removed to make the set linearly independent).

Using this basis, we obtain a matrix:

$$\begin{array}{c} \partial(e) = 1 \cdot \partial(e) \\ \vdots \\ \partial(\partial^{n-2}(e)) = 1 \cdot \partial^{n-1}(e) \\ \partial(\partial^{n-1}(e)) = a_0 e + \ldots + a_{n-1}\partial^{n-1}(e) \end{array} \quad \overset{\text{yields matrix}}{\Rightarrow} \quad \begin{pmatrix} 0 & 0 & 0 & \ldots & -a_0 \\ -1 & 0 & 0 & \ldots & -a_1 \\ 0 & -1 & 0 & \ldots & -a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & -1 & -a_{n-1} \end{pmatrix}$$

By changing the basis to $f_1 = e_1$, $f_2 = -\partial(e)$, $f_3 = \partial^2(e)$, $f_4 = \partial^3(e)$, etc.

Definition 5.4. $y \in K^n$ is called a *solution* of $\partial(Y) = AY$ if $\partial(y) = Ay$ for some $A \in M_n(K)$.

Lemma 5.2. *Let $v_1, \ldots, v_m$ be solutions of (8). Then $v_1, \ldots, v_m$ are linearly independant over $K \iff v_1, \ldots, v_m$ are linearly independant over $K^\Delta = \{c \in K \,|\, \partial(c) = 0\}$.*

Proof. ($\Rightarrow$) should be clear.

($\Leftarrow$) Let $v_1, \ldots, v_m$ be linearly dependent over K. We will show that they are linearly dependent over K^Δ. By induction, we may assume that $\{v_2, \ldots, v_m\}$ are linearly independent (otherwise, they would be linearly dependent over K^Δ by inductive assumption, implying that $\{v_1, \ldots, v_m\}$ are linearly dependent over K^Δ). Then, there exist unique $a_2, \ldots, a_m \in K$ such that

$$v_1 = \sum_{i=2}^m a_i v_i.$$

We then have the following:

$$\begin{aligned} 0 = \partial(0) = \partial(v_1 - \sum_{i=2}^m a_i v_i) \\ = \partial(v_1) - \sum_{i=2}^m \partial(a_i)v_i - \sum_{i=2}^m a_i\partial(v_i) \\ = Av_1 - \sum_{i=2}^m \partial(a_i)v_i - \sum_{i=2}^m a_i A v_i \\ = Av_1 - \sum_{i=2}^m \partial(a_i)v_i - A\sum_{i=2}^m a_i v_i \\ = Av_1 - \sum_{i=2}^m \partial(a_i v_i) - Av_1 \\ = -\sum_{i=2}^m \partial(a_i)v_i, \end{aligned}$$

and by the inductive hypothesis, $v_2, \ldots, v_m$ are linearly independent, implying that $\partial(a_i) = 0$ for $1 \leq i \leq m$, implying that $a_2, \ldots, a_m \in K^\Delta$. Therefore, a nontrivial linear combination $1v_1 - a_2v_2 - \ldots - a_mv_m = 0$, and $v_1, \ldots, v_m$ are linearly dependent. □

Definition 5.5. Given $\partial(Y) = AY$, the solution space is

$$V = \{v \in K^n \,|\, \partial(v) = Av\}.$$

Corollary 5.1. *V is a vector space over K^Δ with $dim_{K^\Delta} V \leq n$.*

The proof of this will be left as an exercise. Also, in *Galois Theory of Linear Differential Equations* written by Singer and Van der Put, do all exercises in section 1.14. An *inhomogeneous differential equation* is one of the form:

$$y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1y' + a_0y = b.$$

To make this homogeneous one can divide by b and differentiate the above.

5.2. **Picard-Vessiot Theory.** Unless otherwise noted, K^Δ is algebraically closed.

Definition 5.6. A differential ring R is called a *Picard-Vessiot (PV) ring* of $\partial(Y) = AY$ over K if:

(1) R is a simple differential ring, i.e., there are no nonzero proper differential ideals.
(2) There exists $Z \in GL_n(R)$ such that $\partial(Z) = AZ$.
(3) R is generated over K as a $K-algebra$ by the entries of Z.

Definition 5.7. *Quot*(R) is called a *Picard-Vessiot extension* of K for $\partial(Y) = AY$.

Definition 5.8. The *Differential Galois Group* of $\partial(Y) = AY$ with a chosen PV extension L is

$$G = \{\sigma : L \to L\}$$

such that:

(1) σ is an automorphism,
(2) $\sigma(a) = a$ for all $a \in K$,
(3) $\sigma(\partial(b)) = \partial(\sigma(b))$ for all $b \in L$.

5.3. **Existence of PV Rings.** Let K be an ordinary differential field of characteristic 0, and let $C = K^\partial$ be an algebraically closed field.

Proposition 5.1. *Let R be a simple differential ring that is a finitely generated $K-$algebra. Then R is an integral domain and, for $L = Quot(R)$, we have $L^\partial = C$.*

Proof. First, we will show that, if $a \neq 0 \in R$ is not nilpotent, then a is not a zero divisor. Let $I = \{b \in R \,|\, \text{there exists } n \text{ with } a^n b = 0\}$. I is a differential ideal. Indeed, for $b_1, b_2 \in I$,

$$a^{n_1}b_1 = 0 \text{ and } a^{n_2}b_2 = 0 \Rightarrow a^{n_1}b_1 + a^{n_2}b_2 = 0,$$

which further implies that

$$a^{\max(n_1,n_2)}(b_1 + b_2) = 0,$$

so $b_1 + b_2 \in I$. $rb \in I$ as well for all $r \in R$ since, if $a^n b = 0$, then $a^n rb = 0$. Furthermore,

$$0' = (a^n b)' = na^{n-1}a'b + a^n b',$$

and multiplying by a we get $a^{n+1}b' = 0$. Hence, I is a differential ideal. By assumption, R is simple, so $I = R$ or $I = (0)$. If $I = R$, then, more specifically, each $a \in R$ is nilpotent if we choose $b = 1$.

This contradicts our assumption, and therefore $I = (0)$ and a is not a zero divisor.

Now, we will show that there are no nilpotent elements in R. Let $J = \{a \in R \,|\, a \text{ is nilpotent}\}$. J is a differential ideal (Show this!). Again, R is simple, and since $1 \notin J$, we have $J = (0)$.

We will now show that $L^\partial = C$. Let $a \in L$ such that $a' = 0$. First we show that $a \in R$. Let $\mathfrak{a} = \{b \in R \,|\, ba \in R\}$, which is a differential ideal. Indeed, for $b_1, b_2 \in \mathfrak{a}$, we have

$$b_1 a + b_2 a = (b_1 + b_2)a \in R$$

and $rb_1 a \in R$ for all $r \in R$, showing that $b_1 + b_2$ and rb_1 are contained in $\mathfrak{a}$. Moreover,

$$(b_1 a)' = b_1' a + b_1 a' = b_1' a + 0 = b_1' a \in R,$$

which implies that $b_1' \in \mathfrak{a}$. Again, R is a simple ring, and $\mathfrak{a} \neq (0)$, so $1 \in \mathfrak{a} \Rightarrow a \in R$. Now suppose $a \in L^\partial$ but $a \notin C$. For every $c \in C$, consider the ideal $(a - c) \in R$. This is a differential ideal, and since $a \neq c$, $(a - c) \neq (0)$. Since R is simple, we have, therefore, $1 \in (a - c)$. In particular, $a - c$ is invertible in R. We now state a lemma of which proof will be given later:

Lemma 5.3. *Let an integral domain R be a finitely generated $k-$algebra for any general field k. Let $x \in R$ be such that $S = \{c \in k \,|\, x - c \text{ is invertible}\}$ is infinite. Then x is algebraic over k.*

Using Lemma (5.3), we have that a is algebraic over K. Let $p \in K[x]$ be the minimal polynomial of a over K, i.e., $p = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. So,

$$a^n + a_{n-1}a^{n-1} + \ldots + a_0 = 0 \Rightarrow a_{n-1}' a^{n-1} + \ldots + a_0' = 0,$$

further implying that all $a_i' = 0$ or $deg(p') < deg(p)$. Since p is minimal, we have that $a_i' = 0$ and a is algebraic over C. Since, by assumption, C is algebraically closed, we have $a \in C$. □

Proof (Of Lemma (5.3)). Let x be transcendental over k. Let $R = k[x_1, \ldots, x_n]$, $x_i \in R$, and $x_1 = x$ with $x_1, \ldots, x_p$ a transcendence basis of $F = k(x_1, \ldots, x_n)$ over k. By the [algebraic] primitive element theorem, there exists $y \in F$ such that $F = k(x_1, \ldots x_p, y)$ with y algebraic over $k(x_1, \ldots, x_p)$. Let $P \in k(x_1, \ldots, x_p)[X]$ be the minimal polynomial of y over $k(x_1, \ldots, x_p)$. Then, there exists $G \in k[x_1, \ldots, x_p]$ such that G is divisible by all the denominators of P and $x_{p+1}, \ldots, x_n \in k[x_1, \ldots, x_p, y, G^{-1}]$. In particular,

$$R \subset k[x_1, \ldots, x_p, y, G^{-1}].$$

Since S is infinite, there exist $c_1 \ldots, c_p \in S$ such that $G(c_1, \ldots, c_p) \neq 0$.Then, there exists a $k-$algebra homomorphism

$$k[x - 1, \ldots, x_p, y, G^{-1}] \to F^{alg},$$

the algebraic closure of F, such that $x_i \mapsto c_i$, fixing R pointwise. However, $x_1 - c_1$ is invertible in R, contradicition. □

5.4. **Construction and Uniqueness of a PV Extension.** Given $A \in M_n(K)$ and $Y' = AY$, consider $R_1 = K[x_{11}, \ldots, x_{nn}, \frac{1}{det(x_{ij})}]$.

Example 5.4. For $n = 1$, we get $R = K[x_{11}, \frac{1}{x_{11}}]$. For $n = 2$, we get

$$R = K[x_{11}, x_{12}, x_{21}, x_{22}, 1/(x_{11}x_{22} - x_{12}x_{21})].$$

Define ∂ on R_1 by $\partial((x_{ij})) = A(x_{ij})$. Let I be a maximal differential ideal of R_1 and let $R = R_1/I$, which is a simple differential ring, and let $Z \in GL_n(R) = \pi((x_{ij}))$ where π is the projection $\pi : R_1 \to R_1/I$. Thus, R is a PV ring of $Y' = AY$ over K. Therefore, PV extensions always exist for $Y' = AY$ with the given conditions.

To show uniqueness, Let R be a differential $K-$algebra and $Z_1, Z_2 \in GL_n(R)$ be such that $Z_1' = AZ_1$ and $Z_2' = AZ_2$. A simple calculation shows:

$$(Z_2^{-1}Z_1)' = Z_2^{-1}AZ_1 + (Z_2^{-1})'Z_1 = Z_2^{-1}AZ_1 - Z_2^{-1}Z_2'Z_2^{-1}Z_1 = Z_2^{-1}AZ_1 - Z_2^{-1}AZ_1 = 0,$$

which implies that $Z_2^{-1}Z_1 = c$ for some constant c, so $Z_1 = Z_2c$.

Proposition 5.2. *Let R_1 and R_2 be PV rings of $Y' = AY$ over K. Then, R_1 and R_2 are isomorphic as differential $K-$algebras (K^∂ is assumed to be algebraically closed).*

Proof. Let $R_3 = (R_1 \otimes_K R_2)\big/I$, where I is a maximal differential ideal of $R_1 \otimes_K R_2$, and $(r_1 \otimes r_2)' = r_1' \otimes r_2 + r_1 \otimes r_2'$ (check that this is well defined). The maps

$$\varphi_1 : R_1 \to R_3,\, r_1 \mapsto r_1 \otimes 1$$

and

$$\varphi_2 : R_2 \to R_3,\, r_2 \mapsto 1 \otimes r_2$$

are differential K-algebra homomorphisms (check this!). Since $Ker\varphi_i$ is a differential ideal of R_i, $Ker\varphi_i = (0)$, and $R_i \cong \varphi_i(R_i)$ as differential $K-$algebras for $i = 1,2$. We will now show that $\varphi_1(R_1) = \varphi_2(R_2)$.

Let $Z_1 \in GL_n(R_1)$ and $Z_2 \in GL_n(R_2)$ be fundamental solution matrices of $Y' = AY$. Since φ_i is a differential homomorphism, we have:

$$(\varphi_i(Z_i))' = A\varphi_i(Z_i).$$

Moreover, $\varphi_i(Z_i) \in GL_n(R_3)$. Therefore, there exists $B \in GL_n(R_3^\partial)$ such that $\varphi_1(Z_1) = \varphi_2(Z_2)$. Since K^∂ is algebraically closed, $R_3^\partial = K^\partial$. Therefore, $B \in GL_n(K^\partial)$. Since φ_i is a $K-$algebra homomorphism, $\varphi_1(Z_1) = \varphi_2(Z_2B)$. Since $\varphi_1(R_1)$ is generated by $\varphi_1(Z_1)$ over K, we have $\varphi_1(R_1) \subset \varphi_2(R_2)$. Similarly, $\varphi_2(R_2) \subset \varphi_1(R_1)$. Thus, $\varphi_1(R_1) = \varphi_2(R_2)$. $\square$

Example 5.5. Let $n = 1$, K be a ordinary differential field of characteristic 0, $a \in K$, and $y' = ay$. We have two cases:

(1) If $b \in K$ and there exists $n \in \{1,2,\ldots\}$ such that $b' = nab$, then $b = 0$.

Let $R = K[x, \frac{1}{x}]$ where $x' := ax$. We will show that R is a simple differential ring. Let $I \subset R$ be a maximal differential ideal. Then, there exists $p \in K[x]$ such that $I = (p)$,

$$p = x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0,$$

where $a_i \in K, 0 \le i \le m-1$. $p' \in I$ where

$$p' = max^m + \big((m-1)aa_{m-1} + a_{m-1}'\big)x^{m-1} + \ldots + (a_1' + a_1)x + a_0'.$$

Since $\deg(ma \cdot p - p') < \deg(p)$,

$$ma \cdot p - p' = 0.$$

Therefore,

$$ma \cdot a_0 = a_0' \Rightarrow a_0 = 0.$$

However, I is a maximal differential ideal, implying I is a prime ideal, but p is reducible, contradiction.

(2) There exists $b \neq 0 \in K$ such that there exists $n \geq 1$ such that $b' = nab$. Let n be minimal such that $b' = nab$. let $f = x^n - b$ and $I = (f) \subset R_1 = K[x, \frac{1}{x}]$ where, again, $x' := ax$. We have:

$$f' = nax^n - b' = nax^n - nab = na(x^n - b) \in I,$$

implying that I is a differential ideal. Further, I is maximal. Indeed, let $J \supsetneq I$ where $J \subset R$ is a differential ideal. Let $J = (g)$. This means that:

$$g = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$$

for $m < n$. Since J is a differential ideal, $g' \in J$ where

$$g' = max^m + \ldots + a_0' \Rightarrow ma \cdot g - g = 0 \Rightarrow ma \cdot a_0 = a_0'.$$

However, $m < n$, contradiction. Therefore,

$$Quot(R_1/I) = K[x]/(x^n - b).$$

5.5. **Galois Group and its Properties.** Let R be a PV ring of $Y' = AY$ over K with K^∂ algebraically closed. Let $L = Quot(R)$, and let $\sigma \in$Galois Group. Let $Z \in GL_n(R)$ be a fundamental solution matrix. In particular, $Z = AZ$. Apply σ to Z:

$$(\sigma(Z))' = \sigma(Z') = \sigma(AZ) = \sigma(A)\sigma(Z) = A\sigma(Z).$$

Moreover, since Z is invertible, $\sigma(Z)$ is invertible, and we have that $\sigma(Z)$ is a fundamental solution matrix of $Y' = AY$. Hence, there exists $B_\sigma \in GL_n(K^\partial)$ such that $\sigma(Z) = Z \cdot B_\sigma$. We therefore have a map:

$$\rho : G \to GL_n(K^\partial),\ \rho : \sigma \mapsto B_\sigma.$$

Exercise 22. Prove ρ is an injective group homomorphism, and therefore $\rho(G) \cong G$.

Theorem 5.1 (The Fundamental Theorem of Differential Galois Theory)**.** *Let K be a differential field such that $K^\partial = C$ is algebraically closed. Let $A \in M_n(K)$ and L be a Picard-Vessiot extension for $Y' = AY$ over K. Let G be the differential Galois group of L over K. The fixed field of G, denoted by L^G, is defined by*

$$L^G = \{a \in L \,|\, \sigma(a) = a \forall \sigma \in G\}.$$

Then, $L^G = K$.

Proof. Let $\frac{a}{b} \in L/K$, that is, $a \neq c \cdot b$ for all $c \in K$ and $b \neq c \cdot a$ for all $c \in K$. Therefore, the set $\{a, b\}$ is linearly independent over K. In particular, $a, b \neq 0$.

Consider $d = a \otimes b - b \otimes a \in R \otimes_K R$, where R is a PV ring (recall, $L = Quot(R)$). Since R is an integral domain, R has no nilpotent elements.

Claim. *$R \otimes_K R$ has no nilpotent elements.*

Indeed, let $\alpha \in R \otimes_K R$ such that $\alpha \neq 0$ and $\alpha^2 = 0$ (it is enough to show the claim for this case). Let S be the K subalgebra of R generated by the components of α. Then, we may assume that R was finitely genreated over K. Since R is a vector space over K, we may choose a basis $\{e_i\}_{i=1}^{\infty}$ of R over K. Then, there exist $\{a_i\}_{i=1}^{\infty} \subset R$ with finitely many nonzero elements such that

$$\alpha = \sum_{i=1}^{\infty} a_i \otimes e_i$$

that is a finite sum. Since $\alpha \neq 0$, there exists some j such that $a_j \neq 0$. Since a_j is not nilpotent, there exists a maximal ideal $\mathfrak{m} \subset R$ with $a_j \notin \mathfrak{m}$ (show this!). Therefore, the image of α under the map

$$R \otimes_k R \longrightarrow R/\mathfrak{m} \otimes_K R$$

is nonzero and nilpotent. Since $\mathfrak{m}$ is maximal, $F = R/\mathfrak{m}$ is a field. By the Nullstellensatz, F is an algebraic field extension over K. Since R is finitely generated over K, this is a finite extension of K.

Repeating the same arguement, we may assume that we started at the beginning with R being a finite field extension of K, that is, $F = K[x]/(p)$ where p is an irreducible polynomial. Therefore,

$$F \otimes_K F \cong F \otimes_K K[x]/(p) \cong F[x]/(p)F[x]$$

which has no nilpotent elements (show this!), thus ending the claim.

Continuing the proof, we have $d = 0$ or d is not nilpotent. However, $d \neq 0$ since, if V and W are vector spaces over K and $v_1, \ldots, v_n \in V$ are linearly independent over K, and $w_1, \ldots, w_n \in W$, then, if,

$$v_1 \otimes w_1 + \ldots + v_n \otimes w_n = 0 \in V \otimes_K W,$$

then $w_1 = \ldots = w_n = 0$. Thus, $d \neq 0$ and therefore d is not nilpotent. Now, consider the differential ring $R \otimes R[1/d]$ and let M be a maximal differential ideal. Let

$$S = (R \otimes_K R[1/d])/M.$$

As before (see Proposition 5.2), consider the differential K-algebra homomorphisms:

$$\varphi_1 : R \longrightarrow S, \quad r \mapsto \bar{r} \otimes 1$$
$$\varphi_2 : R \longrightarrow S, \quad r \mapsto 1 \otimes \bar{r}.$$

Since R is a simple differential ring, both φ_i are injective. Since S is a simple differential ring and a finitely generated K-algebra, and since K^∂ is algebraically closed, $S^\partial = C = K^\partial$. As in Proposition 5.2, $\varphi_1(R) = \varphi_2(R)$. Therefore $\varphi_2^{-1} \circ \varphi_1$ is a differential automorphism of R. Therefore, there exists $\sigma \in G$ such that $\varphi_1 = \varphi_2 \circ \sigma$. We will show that

$$\sigma(\frac{a}{b}) \neq \frac{a}{b}.$$

For this, notice that the image $\bar{d}$ of d in S is not 0. On the other hand, since

$$d = a \otimes b - b \otimes a = (a \otimes 1)(1 \otimes b) - (b \otimes 1)(1 \otimes a),$$

we have

$$\bar{d} = \varphi_1(a)\varphi_2(b) - \varphi_1(b)\varphi_2(a) \neq 0.$$

Since $\varphi_1 = \varphi_2 \circ \sigma$, this implies that

$$\begin{aligned}\bar{d} &= \varphi_2(\sigma(a)) \cdot \varphi_2(b) - \varphi_2(\sigma(b)) - \varphi_2(a) \\ &= \varphi_2(\sigma(a) \cdot b) - \varphi_2(\sigma(b) \cdot a) \\ &= \varphi_2(\sigma(a)b - \sigma(b)a) \\ &\Rightarrow \sigma(a)b - \sigma(b)a \neq 0.\end{aligned}$$

Dividing the last equations, we get $\frac{\sigma(a)}{\sigma(b)} \neq \frac{a}{b}$, thus completing the proof. □

6. Linear Algebraic Groups

Definition 6.1. An *affine algebraic group G* is:

(1) A group, with binary operation $m : G \times G \to G$, an identity e, and inverse $i : G \to G$, and
(2) an affine variety such that m and i are morphisms of affine varieties.

Example 6.1. $\mathbb{C}$ is an algebraic group with respect to $+$, where $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ sending $(a,b) \mapsto a+b$ for all $a,b \in \mathbb{C}$. More generally, given an algebraically closed field C (we will try to remain in the case of $charC = 0$), we define

$$\mathbb{G}_a(C) := (C, +, 0),$$

the additive group of C.

Definition 6.2. An *algebraic subgroup* of an affine algebraic group is a subgroup and a subvariety.

Example 6.2. Continuing Example 6.1, we want to find the subgroups of $\mathbb{G}_a(C)$ (recall that the coordinate ring of $\mathbb{G}_a(C)$ is $C[x]$).

(1) We have $\{0\}$, given by the polynomial $x = 0$, and
(2) $\mathbb{Z}$.

Only the first of these two subgroups is an algebraic subgroup, and, as a matter of fact, $\{0\}$ is the only proper algebraic subgroup of $\mathbb{G}_a(C)$, as every non-zero subgroup of $(C, +, 0)$ is infinite, and every proper subvariety of C is finite.

Example 6.3. Let C be algebraically closed ($charC = 0$). Define

$$\mathbb{G}_m(C) = (C^*, \cdot, 1) = \{(x,y) \in C^2 | xy = 1\}$$

This is a group. Indeed, with operation defined by $(x_1,y_1)(x_2,y_2) = (x_1x_2, y_1y_2)$, $\mathbb{G}_m(C)$ is a group with identity $(1,1)$ and inverse $(x,y)^{-1} = (y,x)$.

Example 6.4. Consider the group $GL_n(C)$, which the set of invertible $n \times n$ matrices. We can indentify this with an algebraic subgroup of $(n+1) \times (n+1)$ matrices via

$$\{\begin{pmatrix} A & 0 \\ 0 & a \end{pmatrix} | \, det(A)a = 1\}$$

Definition 6.3. An algebraic subgroup of $GL_n(C)$ is called a *linear algebraic group*.

Examples of linear algebraic groups are $GL_n(C)$ and $SL_n(C)$.

Theorem 6.1. *For every affine algebraic group G, there exists an imbedding ρ into GL_n with $\rho(G)$ being an algebraic subgroup.*

Let G be an algebraic group such that $G = G_1 \cup \ldots \cup G_m$, a disjoint union, where each G_i is an irreducible variety. The connected component (or irreducible component) of G containing e is called the *identity* component of G, denoted G^0. Moreover, G^0 is a normal subgroup of G, and G/G^0 is finite.

Hopf algebras appear by taking the duals to the group multiplication ($G \times G \to G$), inverse ($G \to G$), and the inclusion of the identity element into the group ($\{e\} \hookrightarrow G$):

Definition 6.4. A *Hopf Algebra* over C is a commutative, associative algebra with 1, and C-algebra homomorphisms:

(a) $\Delta : A \to A \otimes_C A$, called comultiplication,
(b) $S : A \to A$, called coinverse, and
(c) $E : A \to C$, called counit,

such that

$$(\Delta \otimes id) \circ \Delta = (id \otimes \Delta) \circ \Delta, \quad m \circ (S \otimes id) \circ \Delta = m \circ (id \otimes S) \circ \Delta = E, \quad (E \otimes id) \circ \Delta = (id \otimes E) \circ \Delta = id,$$

where $m : A \otimes_C A \to A$ is the multiplication homomorphism.

Example 6.5. Let $G = \mathbb{G}_m$. Its coordinate ring is $A = C[x,y]/(xy-1) = C[x, 1/x]$. For comultiplication, define

$$\Delta : C[x, 1/x] = A \to A \otimes_C A = C[x, 1/x] \otimes_C C[x, 1/x]$$

where

$$\Delta(d) = \sum e_i \otimes d_i, \quad d \in A,$$

such that $\Delta = m^*$. Now, we have a map $m : \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ given by $(a,b) \mapsto ab$ for all $a, b \in C^*$. Now, we construct Δ for all $d \in A$ by

$$\Delta(d)(a,b) = m^*(d)(a,b) = d(m(a,b)) = d(ab),$$

that is,

$$d(ab) = \sum e_i(a) \cdot f_i(b)$$

for all $a, b \in C^*$. For $d = x$, we get $x(ab) = ab$, so $\Delta(x) = x \otimes x$. For $d = \frac{1}{x}$,

$$\frac{1}{x}(a,b) = \frac{1}{ab} \Rightarrow \Delta(\frac{1}{x}) = \frac{1}{x} \otimes \frac{1}{x}.$$

For the coinverse, take $S : A \to A$ defined by $S(d)(a) = d(\frac{1}{a})$. To check this, notice that $S(x)(a) = x(\frac{1}{a}) = \frac{1}{a}$, and we see that

$$S(x) = \frac{1}{x}.$$

For the counit, define $E : A \to C$ by

$$E(d) = d(1).$$

Example 6.6. Let $G = \mathbb{G}_a$. Its coordinate ring is given by $A = C[x]$. For comultiplication, define $d(m(a,b)) = d(a,b)$, where $d(m(a,b)) = \sum e_i(a) \cdot f_i(b)$. We get

$$\Delta(x) = x \otimes 1 + 1 \otimes x.$$

For coinverse, $S(d)(a) = d(-a)$. To check, for $d = x$,

$$S(x)(a) = x(-a) = -a \Rightarrow S(x) = -x.$$

For counit, define

$$E(d) = d(0).$$

Exercise 23. Find Δ, S, E for $G = GL_n$. Hint: they will look like formulae for matrix multiplication and inverse, but with $\otimes$ inserted somewhere.

Theorem 6.2 (Cartier)**.** *Let A be a Hopf Algebra, $charC = 0$. Then A is reduced.*

Theorem 6.3. *Let K have $charK = 0$, $K^{\partial} = C$ be algebraically closed. Let $Y' = AY$, where $A \in M_n(K)$, and $L \supset K$ is a PV extension of K for $Y' = AY$. Then the differential Galois group is a linear algebraic group.*

Proof. Consider $K[X_{ij}, 1/\det]$, $X'_{ij} = AX_{ij}$. Let M be a maximal differential ideal, and let

$$R = K[X_{ij}, 1/\det]/M.$$

Define $C[Y_{ij}, 1/\det] = B$ with the zero derivation. Let

$$R' := K[X_{ij}, 1/\det] \otimes_C B.$$

Let $M = (f_1, \dots, f_m)$. R is a C-vector space with basis $\{e_\alpha\}$. Let $g : R' \to R'$ be the B-algebra homomorphism induced by

$$g(X_{ij}) = (X_{ij})(Y_{ij}).$$

For all f_i, there exists $c_{\alpha i} \in B$ such that

$$\overline{g(f_i)} = \sum e_\alpha \otimes c_{\alpha i} \mod M \otimes_C B.$$

We claim that $I = (c_{\alpha i}) \subset B$ is the defining ideal. Recall that the Galois group consists of differential automorphisms of $R \to R$ preserving K pointwise. oreover, G is identified with $n \times n$ matrices via

$$\sigma \mapsto c_\sigma \in GL_n(C)$$

with $\sigma \in G$ such that the homomorphism induced by

$$(X_{ij}) \mapsto (X_{ij})c_\sigma$$

maps M into itself.

Now let $A = B/I$. Let $H = Hom(A, C)$, and let c_σ be suh that $(X_{ij}) \mapsto (X_{ij})c_\sigma$ maps M into itself, implying that $\sigma(f_i) = 0 \bmod M$ for all $i \Rightarrow c_{\alpha i}(c_\sigma) = 0 \Rightarrow f(c_\sigma) = 0$ for all $f \in I$; and vice versa. By the above, H is a group. Therefore, A is a Hopf Algebra implies that it is reduced by Theorem 6.3. ☐

Example 6.7. Consider $y' = ay$ over K. We know from Example 5.5 that either $R = K[x]$ given by $x' = ax$, or $R = K[x]/(x^n - b)$ for $b \in K$. In the first case, $M = (0) \Rightarrow b_{ij} = 0 \Rightarrow B = C[y, \frac{1}{y}] \Rightarrow G = \mathbb{G}_m(C)$. In the second case,

$$M = (x^n - b) = f_1 \Rightarrow \sigma(f_1) = (xy)^n - b = x^n y^n - b \mod M \equiv by^n - b = b(y^n - 1).$$

Since $b \neq 1$, let $e_1 = 1, e_2 = b, \dots \Rightarrow b_{11} = 0, b_{21} = y^n - 1, \dots, b_{i1} = 0 \Rightarrow G$ has coordinate ring $C[y]/(y^n - 1)$.

Theorem 6.4. *Let L be a PV extension of K and $G \subset GL_n(K^{\partial})$ be the differential Galois group of L over K. Then $dim_C(G) = tr.deg_K(L)$.*

6.1. **Galois Correspondence.** Let $charK = 0$, $K^\partial = C$ is algebraically closed. Let $A \in M_n(K)$, and let $L \supset K$ be a PV extension and let G be the Galois group. Let $\mathcal{G} = \{$algebraic subgroups of $G\}$, $\mathcal{F} = \{$all intermediate subfields of L containing $K\}$. The correspondence

(1)
$$\mathcal{G} \longleftrightarrow \mathcal{F}$$
given by
$$H \longmapsto L^H,$$
where $L^H = \{a \in L | g(a) = a, g \in H\}$ and
$$F \longmapsto Gal(L/F) \subset G,$$
is a bijection.

(2) H is normal $\iff$ L^H is invariant as a set under G. In this case, L^H/K is a PV extension, and G/H is the Galois group of L^H over K.

(3) L^{G^0} is a finite extension of K, so by (2), G/G^0 is the Galois group.

Exercise 24. Prove that, if, in the preceding theorem, L^H/K is a PV extension then L^H is G invariant as a set.

7. Liouvillian extensions

Definition 7.1. A differential field extension L/K is called *Liouvillian* if there exists $K = L_0 \subset L_1 \subset \ldots \subset L_n = L$, where $L_i = L_{i-1}(t_i)$ such that either:

(1) t_i is algebraic over L_{i-1},
(2) $t_i' \in L_{i-1}$ (that is, "$t_i = \int a, a \in L_{i-1}$") , or
(3) $t_i'/t_i \in L_{i-1}$ (i.e., $t_i' = at_i, a \in L_{i-1}$; "$t_i = e^{\int a}$").

Theorem 7.1. *Let L/K be a PV extension of $Y' = AY$ with Galois group G. Then L is Liouvillian $\iff$ G^0 is solvable.*

7.1. **Kovacic's Algorithm.** As an example, consider $y'' + r_1y' + r_2y = 0$. Substituting $y = ze^{\frac{1}{2}\int r_1}$, we get a new equation:
$$z'' = rz,$$
where $r = \frac{1}{4}r_1^2 + \frac{1}{2}r_1' - r_2$. The algorithm starts with an equation of the form $z'' = rz$ and computes from there.

Exercise 25. The Galois group of $z'' = rz$ is a subgroup of SL_2.

7.1.1. *Airy Equation.* $r = x, K = \mathbb{C}(x)$. The Airy equation is
$$y'' = xy. \tag{12}$$
We will show that the Galois group of (12) is SL_2.

Theorem 7.2. *If $G \subset GL_n$ is a linear algebraic group with G^0 solvable. Then either G is finite, or G^0 is diagonalizable and $[G : G^0] = 2$, or G can be put simultaneously to an upper-triangular form.*

Theorem 7.3. *Consider a general $y'' = ry, r \in K$. Let its PV extension be Liouvillian and not finite. Then the* Riccati *equation $u' = u^2 - r$ has a solution in a quadratic extension of K or in K.*

Proof. Since L is not finite, so by 7.2, there exists a quadratic extension $F \supset K$ such that $Gal(L/F)$ can be put into an upper triangular form. This means that there exists $y \in L$ such that for all $g \in Gal(L/F)$, $g(y) = yC_g$. Then, let $u = \frac{y'}{y}$, and we have $g(u) = \frac{g(y')}{g(y)} = \frac{y'}{y} \in F$. Then, $-\frac{y'}{y}$ satisfies $u' = u^2 - r$. Indeed,

$$\left(-\frac{y'}{y}\right)' = -\frac{yy'' - y^2}{y^2} = -\frac{2y^2 - (y')^2}{y^2} = -r + \frac{(y')^2}{y^2},$$

and

$$-\left(\frac{y'}{y}\right)^2 = \frac{(y')^2}{y^2} + r.$$

□

An observation can be made here. If $G \subsetneq SL_2$ is an algebraic subgroup, this implies first that G^0 is solvable. It also implies that, for the Airy equation, if $G \neq SL_2$, it is Liouvillian. Now why is it not finite? From differential equations, $y'' = xy$ implies that y is defined over $\mathbb{C}$. If the PV extension L for $y'' = xy$ were finite, y would be algebraic over $\mathbb{C}(x)$. From complex analysis we know that this implies that y is a polynomial, but $y'' = xy$ has no polynomial solutions other than 0. This implies that $u' = u^2 - x$ has a solution in a quadtratic extension of $\mathbb{C}(x)$.

Lemma 7.1. *If $u' = u^2 - r$ and $u^2 + a_1 u + a_2 = 0$ implies $a_1'' + 3a_1 a_1' + a_1^3 - 4a_1 r - 2r' = 0$.*

To finish with the Airy equation, one plugs $r = x$ and arrives at a contradiction via a partial fraction decompisition of a_1. The rest of the details are in Kaplansky. Read Kovacic's algorithm from his 1986 paper.