DIFFERENTIAL GALOIS THEORY

Abstract. Differential Galois Theory is a branch of abstract algebra that studies fields equipped with a derivation function. In much the same way as ordinary Galois Theory studies field extensions generated by solutions of polynomials over a base field, differential Galois Theory studies differential field extensions generated by solutions to differential equations over a base field. In this paper, we will present some of the basic machinery of differential Galois theory before turning to the question of solving differential equations in terms of integrals. This will lead us to a criterion for whether a function can be integrated in elementary terms, and we will prove the non-integrability of e^{x^2}.

Contents

1. Basic Theory

We begin by defining our basic objects of study. All rings are with identity and all fields have characteristic 0. We will typically use R to denote a ring, and F to denote a field, though additional notation will be used in the cases where multiple rings or fields are being discussed.

Definition 1.1. Let R be a ring. A *derivation on* R is a map $D : R \to R$ satisfying: $D(a + b) = D(a) + D(b)$ and $D(ab) = aD(b) + D(a)b$. A *differential ring* is a ring R equipped with a derivation D_R. A differential ring which is a field is a *differential field*. We will often denote $D(x)$ by x', where x is an arbitrary element. Additionally, we will use the notation $D^i, i \in \mathbb{Z}^+$, to denote applying D i-times. That is, for an arbitrary ring element x, $D^i(x) = D(D(...D(x)...))$, where D is applied i-times. By convention, $D^0(x) = x$.

The usual formulae for derivatives hold in differential rings:

$$D(1) = 0$$
$$D(x^n) = nx^{n-1}D(x)$$
$$D(\tfrac{x}{y}) = \tfrac{yD(x)-xD(y)}{y^2}$$

Date: July 14, 2010.

Definition 1.2. Let R be a differential ring. A *differential ring extension of* R is a differential ring S such that $R \subseteq S$ and $D_S(a) = D_R(a)$ for all $a \in R$. Similarly, a *differential subring of* R is a differential ring T such that $T \subseteq R$ and $D_T(a) = D_R(a)$ for all $a \in T$.

Definition 1.3. Let R be a differential ring. The *set of constants of* R is the kernel of D_R, i.e. $\{a \in R | D_R(a) = 0\}$.

It is clear that the set of constants of R is a subring; if R is a field, then the set of constants is a subfield.

Definition 1.4. A *homomorphism of differential rings* $\varphi : R \to S$ is a ring homomorphism such that $D_S(\varphi(a)) = \varphi(D_R(a))$ for all $a \in R$. In other words, the ring homomorphism must commute with the derivation maps on R and S.

Definition 1.5. Let R be a differential ring, and let $I \subseteq R$ be an ideal. I is a *differential ideal* if $D_R(I) \subseteq I$.

It is not difficult to see that if I is generated by X, i.e. $I = (X)$, and $D_R(X) \subseteq (X)$, then I is a differential ideal. If I is a differential ideal, then the quotient ring R/I can be made into a differential ring with derivation $D_{R/I}(a + I) = D_R(a) + I$. $D_{R/I}$ is well-defined because $D_R(I) \subseteq I$.

Note: From now on, we write the derivation D on R without a subscript, except in the event where ambiguity between derivations on different rings might arise.

We now consider how to extend a derivation on R to its ring of fractions. Let R be a differential ring and let Q be a multiplicatively closed subset of R such that $1 \in Q$ and $0 \notin Q$. Define $D : Q^{-1}R \to Q^{-1}R$ by $D(a/b) = \frac{bD(a)-aD(b)}{b^2}$. To check that D is well-defined, we consider the dual numbers of R:

Definition 1.6. Let R be a ring. The *ring of dual numbers over* R is the ring $R[\epsilon]/(\epsilon^2) = R \oplus R\epsilon$.

Since ϵ is nilpotent, $x = a + b\epsilon$ is a unit in $R[\epsilon]$ if and only if a is a unit in R. Additionally, it is not difficult to see that an additive homomorphism $D : R \to R$ is a derivation on R if and only if $\psi_D = (id_R, D) : R \to R[\epsilon]$ is a ring homomorphism.

Now let R be as above. Then we have a ring homomorphism $\psi_D = (id_R, D) : R \to R[\epsilon]$. Consider the composition ϕ of ψ_D with the homomorphism $R[\epsilon] \to Q^{-1}R[\epsilon]$. The resulting map takes $q \in Q$ to $x = q/1 + (D(q)/1)\epsilon$. Since $q/1$ is a unit of $Q^{-1}R$, x is a unit of $Q^{-1}R[\epsilon]$. This implies ϕ extends to a homomorphism $\gamma : Q^{-1}R \to Q^{-1}R[\epsilon]$, and it is clear that γ takes the form $(id_{Q^{-1}R}, E)$, where E extends D. Then it follows from our above observations that $E(a/q) = \frac{qD(a)-aD(q)}{q^2}$. Hence, $D(a/b)$ is well-defined.

This construction also shows that the fraction field of a differential integral domain is a differential field. We now delve into differential polynomial rings in one variable, a topic central to this paper.

Definition 1.7. Let R be a differential ring. The *ring of differential polynomials over* R *in the variable* Y is the polynomial ring $R\{Y\} = R[\{Y^{(i)}|i = 0, 1, 2, ...\}]$ in the countable set of indeterminates $Y^{(i)}$, with derivation defined to extend that of R and such that $D(Y^{(i)}) = Y^{(i+1)}$.

Although we formally adjoin countably many variables to form the ring of differential polynomials over R, the variables are related through the derivation function in that $D(Y^{(i)}) = Y^{(i+1)}$. Hence, we can think of this ring as being a polynomial ring with a single variable together with its derivatives of all orders.

Elements of $R\{Y\}$ can be understood as differential operators on R, in light of the natural ring homomorphism $R\{Y\} \to End(R)$ sending $Y^{(i)}$ to D^i and $a \in R$ to left multiplication by a. This leads to another important definition:

Definition 1.8. Let R be a differential ring. The *homogenous linear differential operators over* R are the elements $L \in R\{Y\}$ such that the degree in L of each variable $Y^{(i)}$ is at most 1 for $i = 0, 1, 2, ...$

A typical homogenous linear differential operator over R looks like

$$L = Y^{(l)} - \textstyle\sum_{i=0}^{l-1} a_i Y^{(i)},\ a_i \in R$$

Each variable $Y^{(i)}$ has degree 1. By way of comparison, the operator $L = (Y^{(1)})^2 - Y^{(2)}$ is not a homogenous linear differential operator, because the $Y^{(1)}$ term has degree 2.

In the case of our example above, we say L is *monic*, since its leading coefficient is 1. We call l the *order of L*. Later in this paper, we will discuss the problem of finding linearly independent solutions to homogenous linear differential operators. First, we present the definition of a *linear differential ideal.*

Definition 1.9. Let F be a differential field, and let $F\{Y\}_1$ denote the homogenous elements of degree 1 in $F\{Y\}$. A differential ideal $I \subseteq F\{Y\}$ is *linear* if I is generated by $I \cap F\{Y\}_1$. The *dimension* of a linear differential ideal I is the codimension of $I \cap F\{Y\}_1$ in $F\{Y\}_1$

We note that $F\{Y\}_1$ is a D-stable subspace of $F\{Y\}$.

Theorem 1.10. *Let $L \in F\{Y\}$ be a monic homogenous linear differential operator of order l, and let I be the ideal generated by $\{D^i L | i = 0, 1, 2, ...\}$. Then I is a linear differential ideal of dimension l.*

Proof. I is, by construction, a differential ideal. We claim that $F\{Y\}_1/(I \cap F\{Y\}_1)$ has basis $\bar{Y}^{(0)}$, ..., $\bar{Y}^{(l-1)}$, where the overbar denotes the image modulo I.

As mentioned above, D preserves both $F\{Y\}_1$ and $I \cap F\{Y\}_1$, and thus also acts on the quotient $F\{Y\}_1/(I \cap F\{Y\}_1)$. Since $L = Y^{(l)} + M$, where M is an F-linear combination of the $Y^{(i)}$ of order less than l, it follows that $D^n L = Y^{(l+n)} + N$, where N is an F-linear combination of the $Y^{(i)}$ of order less than $l+n$. Since $D^n L$ belongs to I for $n = 0, 1, 2, ...$, it follows that $\bar{Y}^{(0)}$, ..., $\bar{Y}^{(l-1)}$ span $F\{Y\}_1/(I \cap F\{Y\}_1)$.

To see that this set is also linearly independent, assume that there is a nontrivial F-linear combination of $\bar{Y}^{(0)}$, ..., $\bar{Y}^{(l-1)}$ which sums to 0. Then the same combination, without the overbars, belongs to I, giving a relation of the form $\sum_{i=0}^{l-1} c_i Y^{(i)} = \sum_{j=0}^{n} b_j D^j L$, $b_n \neq 0$. By our earlier remarks on $D^n L$ in the preceding paragraph, we know that the coefficient of $Y^{(l+n)}$ on the right-hand side of this equation is b_n, while it is 0 on the left-hand side. Hence, we have a contradiction, so the $\bar{Y}^{(0)}$, ..., $\bar{Y}^{(l-1)}$ are linearly independent, and hence a basis for $F\{Y\}_1/(I \cap F\{Y\}_1)$.

□

In light of this theorem, we make the following definition:

Definition 1.11. Let $L \in F\{Y\}$ be a monic homogenous linear differential operator of order l, and let I be the ideal of $F\{Y\}$ generated by $\{D^iL|i = 0, 1, 2, ...\}$. Then I is called the *linear differential ideal generated by L*. .

We conclude this section with two theorems characterizing the relationship between linear differential ideals and linear differential operators, the latter of which is a converse of Theorem 1.10.

Theorem 1.12. *Let $L = Y^l - \sum_{i=0}^{l-1} a_i Y^{(i)}$ be a linear homogenous differential operator in $F\{Y\}$ of order l. Then $\{Y^{(0)}, ..., Y^{(l-1)}, L, DL, D^2L, ...\}$ is a basis for $F\{Y\}_1$. In particular, if I is the linear differential ideal generated by L, then $F\{Y\}/I$ is isomorphic to the (ordinary) polynomial ring $F[\bar{Y}^{(0)}, ..., \bar{Y}^{(l-1)}]$.*

Proof. The proof of Theorem 1.10 shows that $Y^{(n)} = D^{(n-l)}L$ plus lower ordered terms, provided $n \geq l$, so that $\{Y^{(0)}, ..., Y^{(l-1)}, L, DL, D^2L, ...\}$ spans $F\{Y\}_1$. If some F-linear combination of the set is 0 then we have an equation of the form that appeared in the proof of Theorem 1.10, so the coefficients must be all 0. Hence, $\{Y^{(0)}, ..., Y^{(l-1)}, L, DL, D^2L, ...\}$ is a basis.

When $F\{Y\}$ is regarded as the ordinary polynomial ring $F[Y^{(0)}, Y^{(1)}, ...]$, a change of basis in the homogenous component of degree 1, namely $F\{Y\}_1$, extends to a ring isomorphism so that $F\{Y\}$ is isomorphic to the polynomial ring in the new basis. If we apply this idea to $\{Y^{(0)}, ..., Y^{(l-1)}, L, DL, D^2L, ...\}$, then the ideal I is taken to the ideal generated by the polynomial indeterminates $\{D^iL|i = 0, 1, 2, ...\}$, giving the desired isomorphism. □

We note that this theorem establishes that the differential ideal I generated by a homogenous linear differential operator is prime, and that $F\{Y\}/I$ is a Noetherian ring. Additionally, we see that the derivation D acts on the polynomial ring by:

$$D(\bar{Y}^{(i)}) = \bar{Y}^{(i+1)},\ i < l$$
$$D(\bar{Y}^{(l)}) = \textstyle\sum_{i=0}^{l-1} a_i \bar{Y}^{(i)}$$

Theorem 1.13. *Let $I \subseteq F\{Y\}$ be a linear differential ideal of dimension l. Then there is a monic homogenous linear differential operator L of order l such that I is the linear differential ideal generated by L. Moreover, L is the unique monic homogenous linear differential operator in I of order l, and this is the minimal order for a homogenous linear differential operator in I.*

Proof. Let an overbar denote the image in $F\{Y\}_1/(I \cap F\{Y\})$, and call this quotient V. Choose k maximal such that $\bar{Y}^{(0)}$,...,$\bar{Y}^{(k)}$ are linearly independent. Notice that we must have $k \leq l - 1$. Then there is an element $L \in I$ of the form:

$$L = Y^{(k+1)} - \textstyle\sum_{i=0}^{k} a_i Y^{(i)}$$

Let J be the linear differential ideal generated by L, and let W denote the quotient $F\{Y\}_1/(J \cap F\{Y\})$. Since $J \subseteq I$, W maps surjectively onto V. By assumption, V has dimension l, and by Theorem 1.10, W has dimension $k + 1$. Thus, surjectivity implies that $k + 1 \geq l$; since $k \leq l - 1$, this gives $k + 1 = l$, so $I \cap F\{Y\}_1 = J \cap F\{Y\}_1$. Since I and J are linear, and hence generated by their intersections with $F\{Y\}_1$, it follows that $I = J$.

Now, let M be any homogeneous linear differential operator in I, say $M = Y^{(n)} - \sum_{i=0}^{n-1} b_i Y^{(i)}$. The linear differential ideal generated by M will have dimension

n by Theorem 1.10 and will be contained in I, so as above, the surjectivity on quotients will show that $n \geq l$. This shows that the order of L is minimal. If M is another element of order l, then:

$$L - M = \textstyle\sum_{i=0}^{l-1}(b_i - a_i)Y^{(i)}$$

is in I and, if non-zero, has order less than or equal to l. Hence, $L - M = 0$, and L is unique, as stated. □

2. Solving Differential Equations

We now turn our attention to the question of finding solutions to $L = 0$, where L is a linear homogenous differential operator. Before presenting particular examples, we give a definition and a useful theorem.

Definition 2.1. Let $L = Y^{(l)} - \sum_{i=0}^{l-1} a_i Y^{(i)}$ be a linear homogenous differential operator in $F\{Y\}$. The polynomial ring $R = F[y_0, ..., y_l]$, with derivation extended to $y_0, ..., y_l$ defined by:

$$D_R(y_i) = y_{i+1},\ i < l$$
$$D_R(y_l) = \textstyle\sum_{i=0}^{l-1} a_i y_i$$

is called the *universal solution algebra for L.*

The universal solution algebra for L, which we will abbreviate USA-L, can be understood as an abstract algebraic space in which L has a solution. This construction is formal, though we note that the USA-L is just $F\{Y\}/I$, where I is the differential ideal generated by L. Despite the rather abstract construction of the USA-L, the following theorem, whose elementary proof is omitted, shows that if S is any F-algebra in which $L = 0$ has a solution y, then there is a unique F-algebra homomorphism from the USA-L to S, where $y_0 \mapsto y$.

Theorem 2.2. *Let $L \in F\{Y\}$ be a monic homogenous linear differential operator, and let I be the differential ideal generated by L. Then $F\{Y\}/I$ has the following properties:*

- $L(Y^{(0)} + I) = 0$
- *If S is a differential F-algebra and $y \in F$ satisfies $L(y) = 0$, then there is a unique differential homomorphism $F\{Y\} \to S$, where $Y^{(0)} + I \mapsto y$.*

We will now investigate some examples of adjoining solutions to $L = 0$ for some operator L.

First, consider the equation $Y^{(1)} = 0$ over $\mathbb{C}$, where the derivation is the trivial derivation: $D(z) = 0, \forall z \in \mathbb{C}$. Then the universal solution algebra is $\mathbb{C}[y]$, with the trivial derivation.

Now consider a field F with the trivial derivation and the equation $Y^{(1)} = a$. As simple as this equation seems, our theory is set up to handle only homogenous differential equations, which $Y^{(1)} = a$ is not. However, any solution z to this equation is such that $D^2(z) = D(a) = 0$. Thus, we consider the equation $Y^{(2)} = 0$, which has universal solution algebra $F[y_0, y_1]$, with derivation acting trivially on F, $D(y_0) = y_1$, and $D(y_1) = 0$. Notice also that the ideal I generated by $y_1 - a$ is a differential ideal, since its generator is a constant, and $F[y_0, y_1]/I$ is isomorphic to $F[y]$, where $D(y) = a$.

Next, suppose our base differential field F is arbitrary and consider the equation $Y^{(1)} = a$, where $a \in F$ is not constant. Let $a_1 = a'/a$ and consider the equation $Y^{(2)} - a_1 Y^{(1)} = 0$. The corresponding universal solution algebra is $F[y_0, y_1]$, with derivation extended to y_0 and y_1 by $D(y_0) = y_1$ and $D(y_1) = a_1 y_1$. We consider the ideal P of $F[y_0, y_1]$ generated by $y_1 - a$. Since $D(y_1 - a) = a_1(y_1 - a)$, P is a differential ideal. As above, the quotient $F[y_0, y_1]/P$ is isomorphic to $F[y]$, where $D(y) = a$.

Let F be an arbitrary differential field. Another basic type of equation looks like $Y^{(1)} - aY^{(0)} = 0$. $a \in F$. The universal solution algebra for this equation is the polynomial ring $F[y]$, where $D(y) = ay$. Extensions of this sort, that is extensions S of R where $R(y) = S$ and $\frac{y'}{y} \in R$ are called *adjoining an exponential.* We now prove a theorem about adjoining exponentials.

Theorem 2.3. *Let $E = F(z)$ be a differential field extension such that $\frac{D(z)}{z} \in F$. Then z is either transcendental over F obtained by adjoining an exponential to F, or for some $n \in \mathbb{Z}^+$, we have $z^n \in F$.*

Proof. Consider the polynomial ring $F[y]$ with derivation $D(y) = ay$, $a = \frac{D(z)}{z}$. This maps to E by the differential homomorphism which maps y to z. The kernel of this homomorphism is a prime differential ideal. Since F is a field, $F[y]$ is a principal ideal domain, so this kernel is either the zero ideal, or is generated by a monic irreducible polynomial p, and since the kernel is differential, we must have $p|D(p)$. Let $p = y^n + p_{n-1}y^{n-1} + ... + p_0$. Then:

$$D(p) = any^n + \textstyle\sum_{i=0}^{n-1}(D(p_k) + akp_k)y^k$$

Since $p|D(p)$, and both have degree n, $D(p) = anp$. Then by comparing terms of equal degree, we know $D(p_k) = (n-k)ap_k$ for $0 \le k \le n-1$. Thus, $D(\frac{z^{n-k}}{p_k}) = 0$, so that $p_k = c_k z^{n-k}$, where c_k is a constant of F. In particular, we have that $z^n = \frac{p_0}{c_0} = d$ is an element of F. When the kernel is zero, z is transcendental over F, and z is obtained by adjoining an exponential to F. □

Before showing our next example, we recall an earlier definition:

Definition 2.4. Let F be a differential field with derivation D. The *subfield of constants of* F, denoted $Const(F)$, is $Const(F) = \{x \in F | D(x) = 0\}$.

As stated before, $Const(F)$ is a differential subfield of F. We now show how adjoining solutions to particular differential equations can result in a field extensions with "new constants," or more formally, differential extensions E of a differential field F with $Const(E) \setminus Const(F) \neq \emptyset$.

Let $\mathbb{C}(z)$ be the field of rational functions in one variable with coefficients in $\mathbb{C}$, and let $\mathbb{C}((z))$ be the corresponding ring of formal power series in $\mathbb{C}$. $\mathbb{C}(z)$ is a differential subring of $\mathbb{C}((z))$, where both have the usual derivation: $D(z) = 1$ and $D(z_0) = 0$, $\forall z_0 \in \mathbb{C}$.

Let f be the usual exponential series. Then $D(f) = f$. Now we consider the differential field $F = \mathbb{C}(f)$ and the equation $Y^{(1)} - Y^{(0)} = 0$. As in our earlier example involving this equation, the universal solution algebra to this equation is $F[y]$, where $D(y) = y$. However, since F already contains a solution to this equation, namely f, this adjunction of y is in some sense superfluous. The existence of these two solutions then gives the following equations on their ratios:

$$D(\tfrac{y}{f}) = \tfrac{fD(y)-yD(f)}{f^2} = \tfrac{fy-yf}{f^2} = 0$$

Hence, adding the superfluous solution generates a new constant: $\frac{y}{f}$. The next section investigates the ideas of adding new constants and superfluous solutions more generally.

3. Linear Independence over the Field of Constants

We begin this section with the definition of the Wronskian determinant, then proceed to discuss its applications to solutions of differential equations.

Definition 3.1. Let $y_1, y_2, ..., y_s$ be elements of the differential field F. Then

$$w = w(y_1, ...y_s) = \begin{vmatrix} y_1^{(0)} & y_2^{(0)} & \dots & y_s^{(0)} \\ y_1^{(1)} & y_2^{(1)} & \dots & y_s^{(1)} \\ \vdots & \vdots & \ddots & \\ y_1^{(s-1)} & y_2^{(s-1)} & \dots & y_s^{(s-1)} \end{vmatrix}$$

where $y_i^{(j)}$ denotes $D^j(y_i)$, is called the *Wronskian determinant of* $y_1, ..., y_s$, or simply the *Wronskian of* $y_1, ..., y_s$.

We now make some comments regarding notation when working with the Wronskian. Let F be a differential field, and let $F^{(n)}$ denote the row n-tuples of elements of F. The elements of $F^{(n)}$ look like $\mathbf{y} = (y_1, ..., y_n)$, and for any i, we define

$$\mathbf{y}^{(i)} = (D^i(y_1), ..., D^i(y_n)).$$

With this notation, $w(\mathbf{y})$=det$(\mathbf{y}^{(0)}, ..., \mathbf{y}^{(n-1)})$.

We now show how the Wronskian relates to linear independence of a set of field elements over the subfield of constants. We begin by proving that a set of solutions of a differential equation which has more elements than the order of the differential equation has a vanishing Wronskian.

Theorem 3.2. *Let F be a differential field, and let $y_1, ..., y_{n+1}$ be elements of F which satisfy the equation $Y^{(n)} - \sum_{i=0}^{n-1} a_i Y^{(i)}$, $a_i \in F$. Then $w(y_1, ..., y_{n+1}) = 0$.*

Proof. Let $\mathbf{y}$=$(y_1, ..., y_{n+1})$. Then $w(\mathbf{y})$=det$(\mathbf{y}^{(0)}, ..., \mathbf{y}^{(n-1)})$, using the notation above. In this determinant, the last row is a linear combination of the preceding ones, so the determinant is 0. □

We now give necessary and sufficient conditions for the Wronskian to vanish.

Theorem 3.3. *Let F be a differential field, and let $C = Const(F)$. Then $y_1, ..., y_n \in F$ are linearly dependent over C if and only if $w(y_1, ..., y_n) = 0$.*

Proof. First suppose that the y_i are linearly dependent over C. Then there are elements $c_i \in C$, $1 \leq i \leq n$, such that $\sum_{i=1}^n c_i y_i = 0$. Then applying D^k, we have $\sum_{i=0}^n c_i D^k(y_i) = 0$ for all k. In particular, $c_1, ..., c_n$ is a non-trivial solution of the system of linear equations

$$\textstyle\sum_{i=1}^n y_i^{(k)} x_i = 0 \text{ for } 0 \leq k \leq n-1$$

The determinant of the matrix with coefficients of the above system is the Wronskian $w(y_1, .., y_n)$, and since the system has a non-trivial solution, this determinant is 0.

Conversely, if $w(y_1, ..., y_n) = 0$, then by the same reasoning, the system:

$$\textstyle\sum_{i=1}^n y_i^{(k)} x_i = 0 \text{ for } 0 \leq k \leq n-1$$

has a non-trivial solution $b_1, ..., b_n$, where $b_i \in F$. In particular, if $k = 0$, then we have $\sum_{i=0}^n b_i y_i = 0$. We can rearrange indices so that $b_1 \neq 0$, and then dividing through by b_1, we can assume $b_1 = 1$. Now for each k, $0 \leq k \leq n-1$, we have that

$$\textstyle\sum_{i=0}^n y_i^{(k)} b_i = 0$$

Applying D to this equation for $0 \leq k \leq n-2$, we also have that

$$\textstyle\sum_{i=0}^n y_i^{(k+1)} b_i + \sum_{i=0}^n y_i^{(k)} D(b_i) = 0$$

In this equation, the first sum is 0 by the preceding equation. In the second sum, the first term is 0 since $D(b_1) = D(1) = 0$, so that $D(b_2), ..., D(b_n)$ is a solution for the system of linear equations

$$\textstyle\sum_{i=2}^n y^{(k)} x_i = 0 \text{ for } 0 \leq k \leq n-2$$

The determinant of the matrix of coefficients of this system of linear equations is the Wronskian $w(y_2, ..., y_n)$. If $w(y_2, ..., y_n) \neq 0$, then the solution $D(b_2), ..., D(b_n)$ is trivial so that $D(b_i) = 0$ and each b_i for $2 \leq i \leq n$ is a constant. Since $\sum_{i=1}^n b_i y_i = 0$, we have the y_i linearly dependent over C. If $w(y_2, ..., y_n) = 0$, then we proceed by induction to find a linear dependence over $y_2, ..., y_n$ using the same argument just employed, thus establishing the theorem. □

We can now give a short theorem on the structure of the solution set for a linear differential equation:

Theorem 3.4. *Let L be a monic linear homogenous differential operator of order l over the differential field F. Let E be a differential extension field of F, and let S be the set of solutions to $L = 0$ in E. Then S is a vector space over the field of constants $Const(F) = C$ of dimension at most l.*

Proof. The map $y \mapsto L(y)$ on E is a C-linear transformation, so its kernel, namely S, is a C-vector space. By Theorem 3.2, any $l + 1$ elements of S have vanishing Wronskian, so by Theorem 3.3, they are linearly dependent over C. It follows that S has dimension at most l over C. □

Hence, we have an upper bound on the size of the solution set of a differential equation. We introduce some terminology to denote the idea of a maximal solution set.

Definition 3.5. Let L be a monic linear differential operator of order l over the differential field F. We say that $L = 0$ has a *full solution set in the differential field extension E of F* if the set of solutions in E has dimension l over the field of constants of E. That is, if there are elements $y_1, ..., y_l \in E$ such that $L(y_i) = 0$ and the Wronskian $w(y_1, ..., y_n) \neq 0$.

By placing an upper limit on the size of the solution set, Theorems 3.2 and 3.3 also imply that a full solution set uniquely determines the equation:

Theorem 3.6. *Let L_1 and L_2 be monic homogeneous linear differential operators of order l over the field F, and suppose there are elements $y_1, ..., y_l \in F$ linearly independent over $C = Const(F)$ such that $L_1(y_i) = L_2(y_i) = 0$ for each i, that is, $y_1, ..., y_n$ is a full solution set for L_1 and L_2. Then $L_1 = L_2$. In fact, $L_1 = L_2 = \frac{w(Y, y_1, ..., y_l)}{w(y_1, ..., y_l)}$.*

Proof. Suppose $L_1 = \sum_{i=0}^{l} a_i Y^{(i)}$ and $L_2 = \sum_{i=0}^{l} b_i Y^{(i)}$, where $a_l = b_l = 1$. Let j be the maximum index where $a_j \neq b_j$. Consider $L = (a_j - b_j)^{-1}(L_1 - L_2)$. Now L is a monic homogeneous linear differential operator of order $< l$, but the space of solutions for $L = 0$ contains $y_1, ..., y_l$, so it has dimension over the field of constants $\geq l$. This contradicts Theorem 3.4, so no such j exists. Hence, $a_i = b_i$ for each i, so $L_1 = L_2$.

Now, let $L_3 = \frac{w(Y, y_1, ..., y_l)}{w(y_1, ..., y_l)}$. L_3 is a monic, homogeneous linear differential operator over F of order l, such that $L_3(y_i) = 0$. Hence, we have just proven that $L_3 = L_1 = L_2$. □

Theorem 3.4 also tells us that given a linear differential equation $L = 0$ of order l, the most we can hope for is to add l linearly independent solutions over the field of constants. We now show how to do just that, namely how to adjoin a full solution set in a general way.

Definition 3.7. Let $L = Y^{(l)} - \sum_{i=0}^{l-1} a_i Y^{(i)}$ be a monic linear homogeneous differential operator in $F\{Y\}$. Let $S = F[y_{ij} | 0 \leq i \leq l-1, 1 \leq j \leq l][w^{-1}]$ be the localization of the polynomial ring $R = F[y_{ij}]$ in l^2 variables at $w = \det(y_{ij})$. Define a derivation D_R on R by:

$$D_R(y_{ij}) = y_{i+1,j},\ i < l-1$$
$$D_R(y_{l-1,j}) = \sum_{i=0}^{l-1} a_i y_i$$

and extend to S. S is the *full universal solution algebra for (the differential equation)* $L = 0$, abbreviated FUSA-L.

This construction mirrors our earlier construction for adjoining a single solution, except here, we invert w. This is to formally ensure that the solutions we adjoin are linearly independent over the subfield of constants.

Having established how to construct, for a given linear differential equation L over a differential field F, a differential extension of F where L has a full solution set, we turn to the question of finding a minimal such extension field. We saw earlier an example where adjoining an extra solution resulted in creating a new constant. In the next section, we will show that, for a given L, it is possible to construct a unique differential extension E of F where L has a full solution set, and E has no constants not in F. Such extensions are called *Picard-Vessiot extensions.*

4. Picard-Vessiot Extensions

We begin this section with the precise definition of Picard-Vessiot Extensions, before proving their existence and uniqueness.

Definition 4.1. Let L be a monic homogeneous linear differential operator of order l over the differential field F. A differential extension field $E \supseteq F$ is called a *Picard-Vessiot extension of F for L* if:

- E is generated over F by the set V of solutions of $L = 0$ in E ($E = F\langle V\rangle$)
- E contains a full solution set of $L = 0$, that is, there are $y_1, ..., y_l \in V$ with $w(y_1, ..., y_l) \neq 0$
- Every constant of E lies in F

We will shortly establish the existence of Picard-Vessiot extensions in the case when the field of constants C is algebraically closed. We first prove some properties of Picard-Vessiot extensions, beginning with their minimality with respect to having a full solution set to $L = 0$.

Theorem 4.2. *Let $E \supseteq F$ be a Picard-Vessiot extension of F for the operator L. If $E \supseteq K \supseteq F$ is an intermediate extension such that K contains a full set of solutions of $L = 0$, then $E = K$.*

Proof. By the third criterion of Definition 4.1, every constant of E lies in F. Hence, every constant of E lies in K. Assume that E properly contains K. Let V_E be the solution set for $L = 0$ in E. Then $E = F\langle V_E\rangle$, so $K \subset F\langle V_E\rangle$. It follows that V_K, the solutions to $L = 0$ in K, is a proper subset of V_E, and that $K = F\langle V_K\rangle$. But since V_K spans V_E over $Const(E)$, $Const(E)$ must properly contain $Const(K)$. This contradicts every constant of E lying in K, so $E = K$. □

Picard-Vessiot Extensions also satisfy a normality condition, stated as follows:

Theorem 4.3. *Let $E_1, E_2 \supseteq F$ be Picard-Vessiot extensions of order l for the operator L over F, and let $E \supseteq F$ be an extension with no new constants. Assume that $\sigma_i : E_i \to E$ is an F-differential embedding, i=1,2. Then $\sigma_1(E_1) = \sigma_2(E_2)$.*

Proof. Let $V_i = L^{-1}(0)$ in E_i, and let $V = L^{-1}(0)$ in E. Then V_i is a vector space of dimension l over the field of constants C of F, and V is a vector space over C of dimension at most l. This follows from the fact that the field of constants of E_i and E coincide with C. Since we also have $\sigma_i(V_i) \subseteq V$, all three vector spaces coincide: $\sigma_1(V_1) = V = \sigma_2(V_2)$. Since $E_i = F\langle V_i\rangle$, this means $\sigma(E_1) = \sigma(E_2)$. □

We now turn our attention to proving the existence and uniqueness, up to differential isomorphism, of Picard-Vessiot extensions. First, we prove a few lemmas. These lemmas require a result from commutative algebra, which we now state without proof. The interested reader can see a proof on page 10 of Magid's text.

Theorem 4.4. *Let R be a finitely generated F-algebra, and let d be an element of R. Then either d is algebraic over F or there exists $c \in F$ such that $d - c$ is a non-unit of R.*

We now state and prove our lemmas.

Lemma 4.5. *Let R be a differential integral domain, finitely generated over the differential field F. Let E denote the quotient field of R, and let C denote the field of constants of F. Suppose E contains a constant, d, not in F. If d is not algebraic over C, then R contains a proper differential ideal.*

Proof. Let $I = \{h \in R | hd \in R\}$. Then I is an ideal of R; it is non-zero because d is a fraction of elements of R. It is a differential ideal because d is constant, so $D(hd) = D(h)d$ is in R if hd is. If $I \neq R$, then it is our desired proper ideal. If not, then d is an element of R, and we consider the ideals $(d-c)R$ for $c \in C$. These are all differential ideals. If one of them is properly contained in R, then it is the desired ideal. If all are improper, the d is algebraic over F, by Theorem 4.4. Let $p(x) = x^n + p_{n-1}x^{n-1} + ... + p_0 \in F[x]$ be the minimal polynomial of d over F. Then $0 = D(p(d)) = D(p_{n-1})d^{n-1} + ... + D(p_0)$, so that d is also a root of $q(x) = D(p_{n-1})x^{n-1} + ... + D(p_0)$, which has degree less than that of $p(x)$. By minimality of $p(x)$, we have $q(x) \equiv 0$ and hence $D(p_i) = 0$ for each i. Hence, $p(x) \in C[x]$, so that d is algebraic over C.

□

Corollary 4.6. *Let R be a differential integral domain, finitely generated over the differential field F. Let E denote the quotient field of R, and let C denote the field of constants of F. Assume that R contains no proper differential ideals and that the field of constants of C is algebraically closed. Then the field of constants of E coincides with C.*

Lemma 4.7. *Let R be a differential ring, and let I be a maximal differential ideal of R such that the quotient R/I is of characteristic zero. Then I is prime.*

Proof. We pass to the quotient R/I, so we can assume that R has no proper differential ideals. We then need to show that R is an integral domain. So suppose that a and b are non-zero elements of R and that $ab = 0$. We first claim that if $ab = 0$, then $D^k(a)b^{k+1} = 0$ for $k > 0$. We proceed by induction on k. Note first that $0 = D(ab) = D(a)b + aD(b)$, so multiplication by b gives the claim for $k = 1$. Now assume the claim holds for $k = 1, ..., n-1$. Since $D^n(ab) = 0$, we have $D^n(ab)b^n = 0$. Notice that the formula:

$$D^n(ab) = \textstyle\sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k}(b)$$

can be used to expand this equation. Then the inductive hypothesis gives us, after simplification, that $0 = D^n(a)bb^n = D^n(a)b^{n+1}$, which establishes our claim by induction.

Let J denote the differential ideal generated by a, that is, $J = \sum_{i=0}^{\infty} RD^i(a)$. Suppose that no power of b is zero. Then our claim above implies the element $\sum_{i=0}^{n} r_i D^i(a)$ of J is multiplied to 0 by b^{n+1}, and hence that every element of J is a zero divisor. In particular, it is impossible that $1 \in J$, and since $0 \neq a \in J$, we have that J is a proper differential ideal. This contradicts I maximal, since we are in R/I. Hence, some power of b is necessarily 0. Since b was an arbitrary zero divisor, it follows that every every zero divisor of R is nilpotent, in particular that $a^n = 0$ for some $n \in \mathbb{Z}^+$, and we can choose n minimal. Then $0 = D(a^n) = na^{n-1}D(a)$ and na^{n-1} is non-zero, since we are in characteristic zero, so $D(a)$ is a zero divisor. Repeating this process shows that every $D^n(a)$ is a zero divisor, hence nilpotent, and the ideal they generate, namely J is a differential ideal consisting entirely of nilpotent elements. In particular, it again cannot contain 1, and hence is a proper ideal, contracting our hypothesis. It follows that there are no non-zero a and b such that $ab = 0$, and thus R/I is an integral domain, so I is prime. □

We now prove the existence of Picard-Vessiot extensions:

Theorem 4.8. *Let F be a differential field with algebraically closed field of constants C. Let L be a monic homogeneous linear differential operator over F, let S be its full solution algebra over F, and let P be a maximal differential ideal of S. Then P is prime and the fraction field E of the integral domain S/P is a Picard-Vessiot extension of F for L.*

Proof. S is differentially generated over F by solutions of $L = 0$ and the inverse Wronskian, hence so is S/P. By Lemma 4.7, P is prime, and, since P is a maximal differential ideal, S/P has no proper differential ideals. By Corollary 4.6, the field of constants of E coincides with C. Moreover, E is differentially generated over F by solutions to $L = 0$, and the inverse Wronskian from S is also a unit in S/P and hence in particular is non-zero in E, so $L = 0$ has a full set of solutions in E. It follows that E is a Picard-Vessiot extension of F for L, since it meets all three criteria of Definition 4.1 □

Since S could have more than one maximal ideal, the reader might wonder how canonical the construction just shown is. We answer this question by proving that Picard-Vessiot extensions are unique up to isomorphism.

Theorem 4.9. *Let E_1, E_2 be Picard-Vessiot extensions of F for the operator L of order l. Assume that F has an algebraically closed field of constants. Then there is an F-differential isomorphism $E_1 \to E_2$.*

Proof. We can assume that E_1, say, is the Picard-Vessiot extension constructed in Theorem 4.8. We use the notation of that theorem and its proof.

We consider the ring $R = S/P \otimes_F E_2$. R is differentially generated as an algebra over E_2 by the generators of S/P. Since S/P is, by construction, generated over F by linearly independent solutions $v_1, ..., v_n$ of L, R is finitely generated over E_2. Let Q be a maximal proper differential ideal of R and consider its inverse image I in S/P, i.e. $I = \{a \in S/P | a \otimes_F 1 \in Q\}$. Now I is a differential ideal of S/P, which by construction has no proper differential ideals, so either $I = S/P$ or I is the zero ideal.

If $I = S/P$, then $1 \otimes_F 1 \in Q$, which is impossible, so $I = (0)$. It follows that S/P injects into R/Q under the map sending $a \mapsto (a \otimes_F 1) + Q$. The map $E_2 \to R/Q$ under $b \mapsto (1 \otimes_F b) + Q$ is also injective. Now by Lemma 4.7, Q is prime, so R/Q is an integral domain. Let E denote the fraction field of R/Q. The differential integral domain R/Q has no proper differential ideals, is finitely generated as an algebra over the differential field E_2, and the field of constants of E_2, which is the same as the field of constants of F, is algebraically closed. By Lemma 4.5, the constants of E the coincide with those of E_2 and hence with those of F. The embedding of S/P to R/Q extends to an embedding σ_1 of E_1 into E, and the embedding of E_2 to S/Q extends to an embedding σ_2 of E_2 to E. Both embeddings are the identity on F. Now we have two embeddings of Picard-Vessiot extensions for L over F into E, a no new constants extension of F. By Theorem 4.3, they have the same image, so the map $\sigma_2^{-1} \circ \sigma_1$ is the desired F-isomorphism from E_1 into E_2. □

We end our theoretical discussion on this note, moving to applications to non-integrability in the next section.

5. Liouville's Theorem

The main goal of this section will be proving that e^{x^2} is not integrable in elementary terms; our main theorem in proving this will be Liouville's Theorem. Before any discussion of the problem can begin, however, we must define what we mean by "elementary terms." To this effect, we state several definitions:

Definition 5.1. Let F be a differential field, K a differential field extension. We call $t \in K$ a *primitive over* F if $D(t) \in F$. We say $t \in K$, $t \neq 0$, is a *hyperexponential over* F if $\frac{D(t)}{t} \in F$.

Definition 5.2. Let F be a differential field, K a differential field extension. We say $t \in K$ is *Liouvillian over* F if t is either algebraic, or a primitive, or a hyperexponential over F. Similarly, we call K a *Liovillian extension of* F if there are $t_1, ..., t_n \in K$ such that $K = F(t_1, ..., t_n)$ and t_i is Liouvillian over $F(t_1, ..., t_{i-1})$ for $1 \leq i \leq n$.

We now introduce the particular Liouvillian extensions that define our integration problem.

Definition 5.3. Let F and K be as above. We say $t \in K$ is a *logarithm* over F if $D(t) = \frac{D(b)}{b}$ for some $b \in F$, $b \neq 0$. We say $t \in K$, $t \neq 0$ is an *exponential* over F if $\frac{D(t)}{t} = D(b)$ for some $b \in F$.

Definition 5.4. Let F be a differential field, K a differential field extension. We say $t \in K$ is *elementary over* F if it is either algebraic, or a logarithm, or an exponential over F. We say $t \in K$ is an *elementary monomial over* F if t is transcendental and elementary over F, and $Const(F(t)) = Const(K)$. Similarly, K is an *elementary extension of* F if there are $t_1, ..., t_n$ in K such that $K = F(t_1, ..., t_n)$ and t_i is elementary over $F(t_1, ..., t_{i-1})$ for $1 \leq i \leq n$. We say that $f \in F$ has an *elementary integral over* F if there exists an elementary extension E of F and $g \in E$ such that $D(g) = f$.

Definition 5.5. An *elementary function* is any element of any elementary extension of the differential field $\mathbb{C}(x)$ with the usual derivation $\frac{d}{dx}$.

All of the usual functions from calculus, such as $log(x)$, e^x, and the trigonometric functions are elementary over $\mathbb{C}(x)$, so this definition is appropriate.

We now state our main theorem for this section, which gives necessary and sufficient conditions for integrability in elementary terms:

Theorem 5.6. *(Liouville's Theorem) Let K be a differential field and $f \in K$. If there exists an elementary extension of E of K with $Const(E) = Const(K)$, and $g \in E$ such that $D(g) = f$, then there are $v \in K, u_1, ..., u_m \in K$, $u_i \neq 0$, and $c_1, ..., c_m \in Const(K)$ such that:*

$$f = D(v) + \textstyle\sum_{i=1}^{m} c_i \frac{D(u_i)}{u_i}$$

Corollary 5.7. *Let E be a differential field, and let K be a no new constant differential field extension of E generated by adjoining an exponential, that is, $K = E(e^g)$ for some $g \in K$. Suppose that e^g is transcendental over E. For any $f \in E$, $fe^g \in K$ has a primitive within some elementary no new constant differential field extension of K, i.e. fe^g is elementary integrable, if and only if there is some element $a \in E$ such that $f = a' + ag'$.*

We omit the proofs of these results for space considerations. The curious reader should consult Bronstein's text for more details.

We can now prove that e^{x^2} is not integrable in elementary terms: by Corollary 5.5, e^{x^2} has an elementary primitive if and only if there is a function $a \in \mathbb{C}(x)$ such that $1 = a' + 2ax$. We claim there is no such function. To see this, assume $a = \frac{p}{q} \in \mathbb{C}(x)$ satisfies this equation, where $gcd(p, q) = 1$. Then:

$$1 = \frac{qp' - q'p}{q^2} + 2\frac{px}{q}$$

so

$$q - 2px - p' = \frac{q'p}{q}$$

This implies that $q|q'p$. But $gcd(p, q) = 1$, so $q \not| p$. This means $q|q'$, so q is constant. Then without loss of generality, $a = \frac{p}{q} = p$. Comparing the degrees in x on the two sides of $1 = a' + 2ax$ now results in a contradiction, since the left hand side has degree 0 in x, but the right hand side has degree ≥ 1. Hence, no such a exists, so e^{x^2} is not elementary integrable.

Acknowledgements. It is my pleasure to thank my mentors Ian Shipman and Aaron Marcus for their help in learning Differential Galois Theory. I would also like to thank Peter May and the REU staff for an enjoyable and engaging summer.

References

[1] Manuel Bronstein. Symbolic Integration I: Transcendental Functions. Springer-Verlag, 2005.

[2] Andy R. Magid. Lectures on Differential Galois Theory. American Mathematical Society, 1994.