DIFFERENTIAL GALOIS THEORY

SRITEJA VIJAPURAPU & RALPH CAO

Abstract. In this paper, we aim to both prove two important propositions and discuss some of the fundamental components of Differential Galois theory.

1. Introduction

We will prove the following two propositions:

Proposition 1.1. $\int e^{-x^2}\,dx$ is non-elementary.

Proposition 1.2. $Y'' + xY = 0$ has no elementary solutions.

Differential Galois theory, in general, plays a major role in defining the elementary nature of differential equations and integrals. Some theorems and propositions discussed in this paper can be applied to any equation to check for the validity or existence of an elementary solution or antiderivative.

2. A review of ring theory

In order to properly define some of the theorems and terms, a good understanding of ring theory is helpful. For that, we first start with a ring. A ring is an algebraic object similar to fields, however a ring does not necessarily need to have a multiplicative inverse. Because of that, although the set of integers $\mathbb{Z}$ does not form a field, it does form a ring. A more rigorous definition is as follows:

Definition 2.1. A commutative *ring* R is an abelian group equipped with two binary operations: $\times$ and $+$ (multiplication and addition), and satisfies the following conditions:

(1) $a + (b + c) = (a + b) + c$ and $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$
(2) There is an identity element for both binary operations, e_A and e_M, such that $a + e_A = a$ and $a \times e_M = a$ for $a, e_A, e_M \in R$.
(3) All elements $a \in R$ have an additive inverse $a^{-1} \in R$ such that $a + a^{-1} = e_A$
(4) For all $a, b, c \in R$, $a \times (b + c) = a \times b + a \times c$

(5) For all $a, b \in R$, $a + b = b + a$ and $a \times b = b \times a$

One can also redefine fields in the context of rings by creating an element that would serve as the multiplicative inverse. For this reason, any field is also a ring. Throughout field and group theory, we see the notions of subgroups and subfields arising, however in ring theory and especially differential Galois theory, it is not subrings, but rather *ideals* we are interested in. A major reason as to why subrings aren't as interesting is because in some cases, the binary operations don't work well. More specifically, the identity in a subring may not match the identity of the ring itself. An example of this is with the ring $R = \mathbb{R} \times \mathbb{R} = \{(x, y)|x, y \in R\}$. Take a subring L such that $L = \mathbb{R} \times \{0\} = \{(z, 0)|z \in R\}$. The multiplicative identity of R would be $(1, 1)$ while the multiplicative identity in L would be $(1, 0)$. This motivates the following definition.

Definition 2.2. Suppose R is a ring and suppose we have a nonempty proper subset $I \subseteq R$. We consider I to be an *ideal* of R if the following conditions are met:

(1) $a + b \in I$ for all $a, b \in I$
(2) $ar \in I$ for all $a \in I$ and $r \in R$

This allows us to define the following:

Definition 2.3. An ideal I is a *prime ideal* of a ring R if $I \neq R$ and for all $a, b \in R$ such that $ab \in I$, either $a \in I$ or $b \in I$.

Although these definitions sound rather similar, a simple example will clear up the difference. Suppose we have a ring R that is the set of integers $\mathbb{Z}$. Let's take the subset $I = 10\mathbb{Z}$. First, we need to verify that this is indeed an ideal. If we add any number of multiples of 10, we get another multiple of 10, so the first condition is satisfied. If we take any element in R and multiply it by any multiple of 10, we get another multiple of 10. Thus both conditions are satisfied and I is an ideal. However, we can check that it is not a prime ideal because we can take $5 \cdot 2 = 10$, but neither 5 nor 2 are in I. If we take $I = 5\mathbb{Z}$, however, we see that it is not only an ideal, but also a prime ideal because every element in I will have at least one factor that is a multiple of 5. From this, you can also see why it's called a *prime ideal.* The idea of a prime ideal allows us to define the following:

Definition 2.4. The *spectrum* of a ring R is the set of its prime ideals. We also denote this as $\mathrm{Spec}\,(R)$.

Another concept that's often used in ring theory is the concept of a polynomial ring, which is similar to the field extension of rational functions, but consists only of polynomials.

Definition 2.5. Let R be some commutative ring. The *polynomial ring* in an indeterminate (variable) X over R is a ring denoted $K[X]$ and consists of polynomial elements of the form $p = p_0 + p_1X + p_2X^2 + ... + p_nX^n$ with all coefficients $p_0, ..., p_n \in K$.

This definition can be generalized to multiple indeterminates, with polynomial ring $R[X_1, X_2, ..., X_n]$ which is the set of all polynomials in $X_1, ..., X_n$ with coefficients in R. For example, an element of $\mathbb{R}[X_1, X_2]$ could be $14X_1 + \frac{\pi}{3}X_1^2X_2 + \sqrt{3}X_2^5$.

3. Differential Ring & Field theory

Now that we have defined most of the algebraic ring and field theory terms we need, we can move onto some of the more interesting theorems and definitions in differential ring and field theory.

Definition 3.1. These are fundamental definitions for this section.

(1) A *differential ring* R is a commutative ring endowed with the derivation D that follows the Leibniz rule $D(ab) = D(a)b + aD(b)$ for $a, b \in R$
(2) A *differential field* K is a field endowed with the derivation D that follows the Leibniz rule $D(ab) = D(a)b+aD(b)$ for $a, b \in K$
(3) An ideal is a *differential ideal* if it is closed under D

An example of a differential field is the field of rational functions over both real and complex numbers. This is the most common field of functions that we can differentiate and these prove to be very useful throughout this paper. In the case of the proposition, we are interested in the elements of K that are of the form of an ordinary differential equation. We can further categorize the equations of interest as the following:

Definition 3.2. A *linear differential equation* is an equation with the successive derivatives of a function of x with respect to y. In other words, it is an operator of the form $a_nD^n + a_{n-1}D^{n-1} + ... + a_1D^1 + a_0$, where $a_i \in K$. n is also known as the *order* of this equation.

Now, we move on to some important properties of differential rings.

Proposition 3.3. Suppose we have a differential ring R such that $K \subset R$.

(1) For all $a, b \in R$, $D(\frac{a}{b}) = \frac{D(a)b-aD(b)}{b^2}$

(2) Let $I \subset R$ be a maximum ideal. I is a prime ideal

Proof. (1) Rewriting this as $D(ab^{-1})$, then applying the Leibniz rule, the proposition follows.

(2) If we assume that R has no proper differential ideals, then we just need to prove that R is an integral domain (meaning the product of any two nonzero elements is nonzero). By way of contradiction, suppose $a, b \in R$ and $ab = 0$. We can say that for all $k \in \mathbb{N}$, $D^k(a)b^{k+1} = 0$. Applying D over this again, we get $D^{k+1}(a)b^{k+1} + (k+1)D^k(a)b^k D(b)$. Multiplying this by b, we arrive at $D^{k+1}(a)b^{k+2} = 0$. Assume we have M as the differential ideal generated by a and its derivatives. This means that all elements of M are zero divisors. In other words, there is a nonzero f such that $ef = 0$, in the context of our equation. M is now a proper differential ideal of R, with a being nonzero and b being nilpotent (there is some n such that $b^n = 0$). It follows that every zero divisor in R is nilpotent. We know that $D(a^n) = na^{n-1}D(a)$. Since $K \subset R$, $na^{n-1} \neq 0$, which means that $D(a)$ must be a zero divisor, so all a is nilpotent. So, this means that M is a proper differential ideal, which is a contradiction. Thus, R is an integral domain and I is a prime ideal.

■

There are other elements of field and ring theory that have differential analogs, such as extensions and homomorphisms

Definition 3.4. A *differential extension* is an extension (of either a ring or a field) that extends the derivative onto new elements while keeping already defined derivatives the same.

A common differential extension used in this paper is the polynomial ring, denoted by $R\{Y\} = R[Y, Y', Y'', ...]$, consisting of all polynomials in variables $Y, Y', ...$ with coefficients in R. $R\{Y\}$ is known as the ring of polynomials in differential indeterminate Y. This definition can similarly be extended to multiple indeterminates by $R\{Y_1, Y_2, ..., Y_n\}$.

A differential field extension, denoted by $K\langle Y\rangle$, can be similarly defined as the field of differential rational functions in Y.

In other words, $R\{Y\}$ can be considered the differential analog of polynomial ring $R[x]$, while $K\langle Y\rangle$ can be considered the differential analog of the field of rational functions $K(x)$.

Homomorphisms and automorphisms are also important to bring over from regular field theory, and become especially important in the context of Galois theory.

Definition 3.5. Let R and S be differential rings with derivations D_R and D_S respectively. A *homomorphism of differential rings* $\phi : R \to S$ is a homomorphism from R to S that respects the derivation, such that $\phi(D_R(a)) = D_S(\phi(a))$ for any $a \in R$.

The definition is the same for a homomorphism of differential fields.

We note that a lot of the properties we deal with in differential ring theory is simply the differentiation rules taught in basic calculus. We can apply the differential operator D to a variety of cases to manipulate a differential equation or prove something, and it's important to note that a lot of these concepts are directly analagous to the concepts in algebraic ring theory.

4. Solution Sets and Picard-Vessiot Theory

Differential Galois theory has many parallels in algebraic Galois theory; we are just dealing with differential equations and their respective solutions this time. Just like in algebraic Galois theory, where the roots of a polynomial define a splitting field, the solutions to the differential equation define a Picard-Vessiot extension. However, the solutions to a differential equation are slightly different than roots of a polynomial:

Definition 4.1. Suppose we have a differential equation $\mathcal{L}(Y) = 0$. If $\mathcal{L}$ has order n with coefficients in the field K, then the differential extension E/K is a *Picard-Vessiot extension* if:

(1) E is generated by some $\{y_1, \dots, y_n\}$ with $y_i \in E$ that form a fundamental solution set to $\mathcal{L}(Y) = 0$ such that $E = K\langle y_1, \dots, y_n\rangle$
(2) $C_E = C_K$

We can see an example of a Picard-Vessiot extension with the differential equation $\mathcal{L}(Y) = Y' + Y = 0$. The solution set to this is $\{e^{-x}\}$, thus the Picard-Vessiot extension is $K\langle e^{-x}\rangle/K$. With higher order differential equations, it's possible to apply change of variables, and find a system of differential equations with a solution set. Now, the similarities between a Picard-Vessiot extension and a splitting field from algebraic Galois theory should be clear.

Another important aspect of differential equations is the notion of a fundamental solution set, which deals with linear independence and solubility.

Definition 4.2. Let $\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1Y^{(1)} + a_0Y$ be a monic homogeneous linear differential equation over differential field K, with $a_i \in K$. A *fundamental solution set* of $\mathcal{L}$ is a set of solutions

$\{y_1, \ldots, y_n\}$ such that $\mathcal{L}(y_i) = 0$ for $i = 1, \ldots, n$. Additionally, this set must be linearly independent over the field of constants C_K.

Often times, checking for linear independence through more rudimentary methods may be difficult or time-consuming. Because of this, we have a tool known as the Wronskian which is used in the study of differential equations to easily verify whether any set of elements in a differential field is linearly independent, and it requires a bit of linear algebra.

Definition 4.3. Let R be a differential ring and $y_1, \ldots, y_n \in R$. The *Wronskian* of these elements is the determinant of an $n \times n$ matrix comprising of the elements and their $n-1$ derivations.

$$W(y_1, y_2, ..., y_n) = \det\left(\begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix}\right)$$

Theorem 4.4. *Let K be a differential field, and let C be its field of constants. Any elements $y_1, \ldots, y_n \in K$, are linearly dependent over C if and only if $W(y_1, \ldots, y_n) = 0$.*

Proof. Let A be the matrix corresponding to $W(y_1, \ldots, y_n)$. It can be proven using linear algebra that there is some non-trivial column vector v consisting of n elements in C that is a solution to the equation $Av = 0$ if and only if A is not invertible. It can further be shown that A is not invertible if and only if its determinant is zero.

Assume $y_1, \ldots, y_n$ are linearly dependent such that there exist some $c_1, \ldots, c_n \in C_K$ such that $c_1 y_1 + \cdots + c_n y_n = 0$. Furthermore, if we take any kth derivative of the equation, we get $c_1 y_1^{(k)} + \cdots + c_n y_n^{(k)} = 0$. The column vector consisting of $c_1, \ldots, c_n$ is then a solution to $Av = 0$, and the determinant $W(y_1, \ldots, y_n) = 0$.

Conversely, the determinant being 0 guarantees a column vector solution, which gives a non-trivial linear combination of $y_1, \ldots, y_n$ that equals 0, proving linear dependence. ■

We can apply this theorem to a fundamental solution set, and for some solution set $\{y_1, \ldots, y_n\}$, if $W(y_1, \ldots, y_n) \neq 0$, it follows that $\{y_1, \ldots, y_n\}$ is not linearly independent. The matrix corresponding to the Wronskian for some fundamental solution set is known as a *fundamental solution matrix*.

Furthermore, since we can find a solution set that is linearly independent, we can create the *solution space* of $\mathcal{L}$, which is the n-dimensional vector space over C_K with a fundamental solution set as its basis. All elements of this solution space will be a solution of $\mathcal{L}(Y) = 0$.

For example, a fundamental solution set of $\mathcal{L}(Y) = Y'' - Y' = 0$ is $\{1, e^x\}$. Its Wronskian $W(1, e^x) = \det(\left[\begin{smallmatrix} 1 & e^x \\ 0 & e^x \end{smallmatrix}\right]) = e^x \neq 0$, meaning that the solution set is linearly independent. Therefore, the solution space of this linear differential equation consists of elements in the form $c_1 + c_2 e^x$ for $c_1, c_2 \in C_K$.

5. Special extensions and Liouville's Theorem

There are a few special types of Picard-Vessiot extensions that we are interested in, comparable to radical extensions in algebraic Galois theory.

Definition 5.1. Let E/K be a differential field extension. An element $y \in E$ is *Liouvillian* over K if

(1) y is algebraic over K
(2) y is the antiderivative of some element in K, i.e. $y' \in K$
(3) y is the exponential of the antiderivative of some element in K, i.e. $\frac{y'}{y} \in K$

Definition 5.2. An extension E/K is a *Liouvillian extension* if there exists a tower of field extensions

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = E$$

such that for all $i = 1, \ldots, n$ there is some $y \in F_i$ that is Liouvillian over F_{i-1} and $F_i = F_{i-1}(y)$.

Definition 5.3. Let E/K be a differential field extension. An element $y \in E$ is called *elementary* over K if

(1) y is algebraic over K
(2) y is the logarithm of some element in K
(3) y is the exponential of some element

Definition 5.4. An extension E/K is an *elementary extension* if there exists a tower of field extensions

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = E$$

such that for all $i = 1, \ldots, n$ there is some $y \in F_i$ that is elementary over F_{i-1} and $F_i = F_{i-1}(y)$.

We note that the definitions for elementary and Liouvillian elements are very similar, except that elementary elements do not allow the use of the antiderivative. This definition additionally includes all of the usual calculus functions such as logarithms, exponentials, and trigonometric functions (using Euler's identity), so it is a fitting definition. It also allows us to state and prove the following theorem, which will not be used until the Galois theory section but is important to note.

Theorem 5.5. *If an element y is elementary, it will be also contained in some Liouvillian extension of* $\mathbb{C}(x)$*.*

Proof. We can show that any element that is elementary over some differential field K is also Liouvillian over K, so we can use the same tower of field extensions of the elementary element y as a Liouvillian extension. There are 3 cases:

(1) y is algebraic over K is the same for both definitions.
(2) If some elementary element w is the logarithm of some element $a \in K$, it is the antiderivative of the element a'/a, which is guaranteed to appear in K.
(3) If some elementary element w is the exponential of some element $a \in K$, it is the exponential of the antiderivative of a', which is guaranteed to appear in K.

■

The formal definitions of a Liouvillian element and a Picard-Vessiot extension and field greatly help with solubility. Liouville also came up with an important theorem that will help us complete the proof of our proposition. First, we informally define the elementary extension field of a field F as the extension containing all elementary solutions to a particular differential equation.

Theorem 5.6. *(Liouville) Suppose F is a field of characteristic* 0 *and we have $\alpha \in F$. If we have $Y' = \alpha$ for some Y in the elementary extension field of F, then there exists constants $c_1, ..., c_n \in F$ and elements $y_1, ..., y_n, v \in F$ such that*

$$\alpha = \sum_{i=1}^{n} (c_i \cdot \frac{y_i'}{y_i}) + v'$$

The proof of this theorem is rather long ($6 - 7$ pages), so we leave that to the reader to look into. The theorem basically states that if an elementary solution exists, it can be written in this form. More specifically:

Proposition 5.7. If α can be written in the form of Theorem 21, then α has an antiderivative that lies in the elementary field extension of F.

Proof. $F(\ln(y_1), ..., \ln(y_n))$ is an elementary field extension. Rewriting this in the form of Theorem 12, we see that this is equivalent to

$$y = \sum_{i=1}^{n} (c_i \cdot \ln(y_i)) + v'$$

We note that $D(\ln(y_i)) = \frac{y_i'}{y_i}$, thus y is an elementary antiderivative of a. ∎

Liouville's theorem and the above proposition give rise to a corollary that will be useful to prove the nonexistence of an elementary solution to any given integral (that is non-elementary, of course). Our initial proposition is proving that e^{-x^2} has no elementary solution. So, we are interested in functions in the form fe^g with $f, g \in \mathbb{C}(x)$.

Corollary 5.8. If $f, g \in \mathbb{C}(x)$ and f is nonzero and g is non-constant, then $y = f(x)e^{g(x)}$ has an elementary antiderivative iff there exists a rational function $R \in \mathbb{C}(x)$ such that $R'(x) + g'(x) \cdot R(x) = f(x)$.

Proof. Suppose a rational function R exists that satisfies this equation. Then it follows that:

$$\begin{aligned}(R(x) \cdot e^{g(x)})' &= R'(x) \cdot e^{g(x)} + g'(x) \cdot R(x) \cdot e^{g(x)} \\ &= (R'(x) + g'(x) \cdot R(x))e^{g(x)} \\ &= f(x) \cdot e^{g(x)}\end{aligned}$$

This means that $f(x) \cdot e^{g(x)}$ does indeed have an elementary antiderivative, namely, $(R(x) \cdot e^{g(x)})$. ∎

This is an extremely powerful tool when proving insolubility, and it's exactly what we need to prove proposition 1.1. So, we move to that.

6. Proof of the first proposition

In order to prove the nonexistence of an elementary solution for the function e^{-x^2}, by the corollary, it suffices to show that it cannot be written in the form $R'(x) + g'(x) \cdot R(x)$, with the function being in the form $f(x)e^{g(x)}$.

Proof. By way of contradiction, suppose we can rewrite e^{-x^2} in the form $R'(x) - 2x \cdot R(x) = 1$, for some rational function $R(x)$. However, this can never be the case because $\deg(2x \cdot R(x)) \geq 1 > \deg(R'(x))$, assuming $R(x) \neq 0$. Thus, e^{-x^2} has no elementary antiderivative, completing the proof of this proposition. ∎

7. Differential Galois Theory

For this section, we will be utilizing some advanced theorems and propositions from linear algebra and group theory in order to delve deeper into the topic of differential Galois theory.

We start by defining the differential Galois group, whose structure is almost identical to its algebraic counterpart.

Definition 7.1. Let E/K be the Picard-Vessiot extension of linear differential equation $\mathcal{L}(Y) = 0$. The *differential Galois group*, denoted $\mathrm{Gal}(E/K)$, is the group of differential automorphisms of E which fix K.

Since differential homomorphisms respect derivation, we are able to draw even more parallels to algebraic Galois groups.

Proposition 7.2. Let E/K be the Picard-Vessiot extension of linear differential equation $\mathcal{L}(Y) = 0$, and let $\sigma \in \mathrm{Gal}(E/K)$ be some automorphism of E/K. For any $y \in E$ that is a solution to $\mathcal{L}$, $\sigma(y)$ must be a solution to $\mathcal{L}$ as well.

Proof. Suppose $\mathcal{L}(Y) = a_n Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y^{(1)} + a_0 Y$ for $a_i \in K$ (which are fixed by σ).

$$\begin{aligned} 0 &= \sigma(\mathcal{L}(y)) \\ &= \sigma(a_n y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y^{(1)} + a_0 y) \\ &= a_n\sigma(y^{(n)}) + a_{n-1}\sigma(y^{(n-1)}) + \cdots + a_1\sigma(y^{(1)}) + a_0\sigma(y) \\ &= a_n\sigma(y)^{(n)} + a_{n-1}\sigma(y)^{(n-1)} + \cdots + a_1\sigma(y)^{(1)} + a_0\sigma(y) \end{aligned}$$

This implies that $\sigma(y)$ is also a solution of $\mathcal{L}$. ■

Similar to algebraic Galois theory, automorphisms of a Picard-Vessiot extension must map a solution to another solution. Furthermore, automorphisms are completely defined by their action on generators of the field extension. But, the difference is that there is no longer a finite solution set, as the solutions of a differential equation form an n-dimensional vector space, which somewhat complicates the automorphism.

Subsequently, while the Galois group of a minimal polynomial is isomorphic to a subgroup of a symmetric group, differential Galois groups of linear differential equations are isomorphic to the subgroup of a specific kind of group in linear algebra.

Definition 7.3. The *general linear group* over a ring R of degree n is the group of $n \times n$ matrices that are invertible (non-zero determinant) and have entries in R. The binary operator of this group is standard matrix multiplication. The general linear group is generally denoted $\mathrm{GL}_n(R)$.

We can show that any differential automorphism of a Picard-Vessiot extension can be represented as some $n \times n$ matrix with entries in C_K.
Let M be the fundamental solution matrix of $\mathcal{L}(Y) = 0$, and let E/K be its Picard-Vessiot extension. We know for any automorphism $\sigma \in \mathrm{Gal}(E/K)$, $\sigma(y_i) = c_{i1}y_1 + c_{i2}y_2 + \cdots + c_{in}y_n$ for all $i = 1, 2, \ldots, n$, and we know that $\sigma(y_i^{(k)}) = \sigma(y_i)^{(k)}$ which will keep the constants the same, so we can represent this automorphism in matrix form:

$$\sigma(M) = M \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{bmatrix}$$

Furthermore, the columns must be linearly independent and have a nonzero determinant, thus automorphisms are elements of the general linear group. This allows us to state the following theorem.

Theorem 7.4. *The differential Galois group of a linear differential equation $\mathcal{L}$ of degree n is a closed subgroup of $GL_n(C_K)$.*

Example: Consider the linear differential equation $\mathcal{L}(Y) = Y'' - Y' = 0$ over field $F = \mathbb{C}(x)$. Its fundamental solution set is $\{1, e^x\}$. Any automorphism $\sigma \in \mathrm{Gal}(F(e^x)/F)$ must map $\sigma(e^x) = c_1 + c_2e^x$ for some $c_1, c_2 \in C_F = \mathbb{C}$. From here, we can take the derivative of $\sigma(e^x)$ to get more information about c_1 and c_2: $D(\sigma(e^x)) = \sigma(D(e^x)) \implies D(c_1 + c_2e^x) = \sigma(e^x) \implies c_2e^x = c_1 + c_2e^x \implies c_1 = 0$. The Galois group can be written as

$$\mathrm{Gal}(E/K) \cong \left\{ \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} \middle| c \in \mathbb{C}^\times \right\}$$

since c must be non-zero.
The Galois correspondence also has a differential analogue as follows:

Theorem 7.5. *Let E/K be a Picard-Vessiot extension, and let $G = \mathrm{Gal}(E/K)$. There is an inclusion-reversing bijection between intermediate differential fields F and subgroups H of the Galois group, given by $H \mapsto E^H$ and $F \mapsto \mathrm{Gal}(E/F)$.*

8. Proof of Proposition 1.2

In order to prove this proposition, we use an approach involving *Airy Equations*.

Definition 8.1. An *Airy Equation* is a differential equation of the form $Y'' - xY = 0$.

The equation of interest for us is in this form, so we aim to prove that the Airy Equation does not have an elementary solution set, concluding the proof of this proposition. The proofs of the next theorem and proposition are rather long, so we leave them for the reader to look into. (The proof for Theorem 8.2 involves the differential Galois correspondence analogue, which can be seen from Theorem 7.5). Also note that theorem 8.2 is the differential analogue of the Abel-Ruffini Theorem.

Theorem 8.2. *Suppose we have a differential field K such that $\mathcal{M}(U)/K/\mathbb{C}(x)$ with $U \subset \mathbb{C}$. ($\mathcal{M}$ is the field of meromorphic functions). Let L be a differential operator on K. If we have $K \hookrightarrow F$, where F represents the splitting field, and it is contained in a Liouvillian extension, then there exists a sequence of subgroups such that $1 = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$ for some group $G := \mathrm{Gal}(E_L/K)$, where E_L represents the splitting field and each G_i/G_{i+1} is finite, isomorphic to $\mathbb{C}$, or isomorphic to $\mathbb{C}^\times$.*

Proposition 8.3. Suppose the splitting field of an Airy Equation is represented by E_L. Then we have $\mathrm{Gal}(E_L/\mathbb{C}(x)) \cong \mathrm{SL}_2(\mathbb{C})$.

Proposition 8.4. No chain of subgroups of $SL_2(\mathbb{C})$ exists such that Theorem 8.2 is satisfied.

Proof. Since $SL_2(\mathbb{C})$ is simple, it contains no proper subgroups with a finite or abelian quotient, thus the chain of subgroups satisfying the properties of 8.2 can never be attained. ■

This leads to the following corollary, which will be enough to prove our initial proposition.

Corollary 8.5. The Airy functions do not have an elementary solution set.

References

[1] William Cook. Some differential galois theory, 2016.
[2] Teresa Crespo and Zbigniew Hajto. *Algebraic groups and differential Galois theory*, volume 122. American Mathematical Soc., 2011.
[3] Arun Debray and Rok Greogoric. Differential galois theory: Proving antiderivatives aren't elementary, 2019.
[4] Viraaj Jayaram. Proving the non-existence of elementary anti-derivatives for certain elementary functions.
[5] Moshe Kamensky. Differential galois theory. *University of East Anglia, England*, pages 1–7.
[6] Simon Rubinstein-Salzedo. *Abstract Algebra*.
[7] Bruce Simon. An introduction to differential galois theory, 2015.