A FIRST LOOK AT DIFFERENTIAL ALGEBRA

JOHN H. HUBBARD AND BENJAMIN LUNDELL

1. Introduction

The object of the paper is to prove that the differential equation

$$u'(t) = t - [u(t)]^2 \tag{1}$$

has no solutions which can be written using elementary functions, or anti-derivatives of elementary functions, or exponentials of such anti-derivatives, or anti-derivative of those, etc. We should note that Equation 1 can be solved using power series, integrals which depend on a parameter, or Bessel functions of order $1/3$. However, as we will see, none of these methods of solution are "algebraic" in nature.

We aim to give a precise definition of "algebraic" by developing the theory of *differential algebra*, which is largely the work of Ritt. Other contributors are Liouville, Picard, Vessoit, Kolchin, Rosenlicht, ... The part of differential Galois theory which we will require is remarkably analogous to the part of Galois theory which leads to a proof of Abel's celebrated result that a general polynomial equation of degree five or higher cannot be solved by radicals. In effort to derive these two areas in parallel, we will also explain why the polynomial equation

$$x^5 - 4x^2 - 2 = 0 \tag{2}$$

has no solutions which can be written as radicals of solutions to lower degree polynomial equations.

The paper is written with a reader in mind who at some point studied Galois theory: either very recently and is therefore not an expert, or long ago has and since forgotten many of the finer points. The examples are chosen to jog the memory: it scarcely possible to give all the details of such proofs in this article. Theorems 1, 2, and 3 require more of an algebraic arsenal than the rest of the paper, and their proofs have been relegated to Section 9, where the approach is less elementary. For further reading, we recommend [2], [3],[4], and [5].

2. Splitting Fields

Our first step will to determine where solutions to Equations 1 and 2 lie. Recall that a *field* is a set in which an addition, subtraction, multiplication, and division are defined, and that they satisfy the rules which one expects from elementary arithmetic. Three standard examples are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$. All fields in the paper will have characteristic 0.

For the case of polynomials, we now have all of the background we need.

Definition. Given a polynomial $f(x) \in \mathbb{Q}[x]$ with rational coefficients, the *splitting field* of f, denoted E_f, is the smallest subfield of $\mathbb{C}$ which contains all of the roots of f.

The reason we can be sure that all solutions to a polynomial f lie in some subfield of $\mathbb{C}$ is the fundamental theorem of algebra, which says that any degree n polynomial with coefficients in $\mathbb{C}$ has n (not necessarily distinct) roots in $\mathbb{C}$.

Example 2.1. Consider the polynomial $f(x) = x^2 - 2$. Then then the field

$$E_f = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}$$

is the splitting field of f. Why?

First, this is a field. One can obviously add, subtract, and multiply numbers of this form and obtain another number of this form. Division is possible since

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2},$$

and $a^2 - 2b^2 = 0$ implies that $a = b = 0$ (since $\sqrt{2}$ is irrational).

Second, it does contain both roots of f: $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Third, it is obviously the smallest field which contains these roots.

Remark. The splitting field need not be thought of as a subfield of $\mathbb{C}$. We need only to fix an algebraic closure of $\mathbb{Q}$ and we could work in there (as the fundamental theorem of algebra on requires the field to be algebraically closed). However, we find it easier to think of subfields of $\mathbb{C}$, but that is just a crutch.

To deal with differential equations rather than polynomial ones, one must consider fields with a bit more structure:

Definition. A *differential field*, here called a $\mathcal{D}$-field, is a field F, together with a derivations $\delta : F \to F$ which satisfies the rules

$$\delta f + g = \delta(f) + \delta(g), \text{ and } \delta(fg) = f\delta(g) + g\delta(f).$$

The first example is $\mathbb{C}(t)$, rational functions in one variable, with usual addition and multiplication, and with the derivation given by the ordinary derivative. The standard rules for differentiating say that indeed the derivative of a rational function is again a rational function. Another example is the field $\mathcal{M}(U)$ of meromorphic functions on an open subset $U \subset \mathbb{C}$, that is, quotients of two analytic functions. For our purposes, the field $\mathbb{C}(t)$ will be the smallest field of interest (analogous to $\mathbb{Q}$ for polynomials), and $\mathcal{M}(U)$ the largest (like $\mathbb{C}$). The reason we can use $\mathcal{M}(U)$ as our "big field" is the existence and uniqueness theorem for differential equations, which says that if U is a simply connected subset of $\mathbb{C}$ and $\alpha_1(t), \ldots, \alpha_k(t)$ are analytic on U, then the differential equation

$$u^{(k)}(t) + \alpha_1(t)u^{(k-1)}(t) + \cdots + \alpha_k(t)u(t) = 0$$

has a unique solution in $\mathcal{M}(U)$ for any t_0 in U and any given initial conditions $u(t_0), u'(t_0), \ldots, u^{(k-1)}(t_0)$. If L is a differential operator, we will write U_L for the largest simply connected open subset of $\mathbb{C}$ on which the differential equation $L = 0$ has solutions.

Definition. If (F, δ) is a differential field, then the *constants* of F are the elements $f \in F$ such that $\delta(f) = 0$.

In this paper, the field of constants will always be $\mathbb{C}$, but this will not always be obvious; the crux of the proof of Theorem 2, given in Section 9, is precisely that the constants of a certain differential field we will manufacture are precisely $\mathbb{C}$.

We now have the background needed to define where the solutions to a differential equation lie.

Definition. Given a differential operator L on $\mathbb{C}(t)$, the *differential splitting field* of L, denoted E_L, is the smallest subfield of $\mathcal{M}(U_L)$ containing $\mathbb{C}(t)$ and the solutions of L.

Example 2.2. Consider the simplest differential operator $L(c) = u'(t) - u(t)$. Since in this case the on coefficient is the number 1, it is certainly analytic on all of $\mathbb{C}$, and we may consider the splitting field as the smallest $\mathcal{D}$-subfield of $\mathcal{M}(\mathbb{C})$ containing the rational functions and the solutions of the differential equation $u'(t) = u(t)$., that is, ae^t. It should be clear that this subfield, E_L, is precisely the space of functions of the form

$$\frac{p_1(t)e^t + \cdots + p_m(t)e^{mt}}{q_1(t)e^t + \cdots + q_n(t)e^{nt}}$$

where the $p_i(t)$ and $q_j(t)$ are polynomials with coefficients in $\mathbb{C}$. Indeed, this is a differential field (clearly closed under addition, multiplication, division, and differentiation), and more or less obviously the smallest such field with the constants and e^t. One should think of this splitting field as a close analog of the numbers of the form $a + b\sqrt{2}$

3. Galois Groups

We now investigate the structure of splitting fields. In particular, we try to understand what happens to solutions of a polynomial or differential equation under a field automorphism. We begin with the case of polynomials.

Definition. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial and let E_f be its splitting field. The *Galois group* of f (or E_f), denoted $\mathrm{Gal}(E_f/\mathbb{Q})$, is the group of all field automorphisms of E_f which leave $\mathbb{Q}$ fixed, where the group law is given by composition of automorphisms. Such maps necessarily respect the field operations.

Fix a polynomial f, and let $\sigma \in \mathrm{Gal}(E_f/\mathbb{Q})$. Since σ fixes the rational numbers and respects field operations (both by definition), then we can see $f(\sigma(a)) = \sigma(f(a))$ for any $a \in E_f$. In particular, if a is a root of f, i.e., $f(a) = 0$, we see that

$$0 = f(a) = \sigma(f(a)) = f(\sigma(a)).$$

We conclude that *elements of the Galois group of f permute the roots of f*. Consequently, if we denote the set of roots of f by R_f, then there is a group homomorphism

$$\mathrm{Gal}(E_f/\mathbb{Q}) \to \mathrm{Perm}(R_f)$$

which can easily be seen to be an injection, so $\mathrm{Gal}(E_f/\mathbb{Q})$ is a subgroup of a finite permutation group.

Example 3.1. If f is the polynomial $x^2 - 2$ above, then the group $\mathrm{Gal}(E_f/\mathbb{Q})$ is the group of permutations of $\{\sqrt{2}, \sqrt{2}\}$.

Example 3.2. Let $f(x) = x^5 - 1$. Then the set of roots is the set with the five elements $\omega_k = e^{2k\pi i/5}$, with $k = 0, \ldots, 4$. Clearly the Galois group is not the whole group of permutations; no automorphism can map 1 to anything else. This is a particular case of the following general statement: the Galois group acts transitively on the roots if and only if the polynomial is irreducible.

In out case, $x^5 - 1 = (x^4 + x^3 + x^2 + x + 1)(x - 1)$, and the roots of the two factors cannot get mixed up. How about the other roots? It is not quite obvious[1], but ω_1 can be mapped to any other root ω_k, $k = 1, 2, 3, 4$ by an automorphism $\sigma \in \mathrm{Gal}(E_f/\mathbb{Q})$. Knowing $\sigma(\omega_1)$ completely determines σ, since

$$\omega_k = \omega_1^k, \text{ so } \sigma(\omega_k) = \sigma(\omega_1)^k.$$

Once you see that, it is not hard to see that the Galois group is the multiplicative group of $\mathbb{Z}/5\mathbb{Z}$, which is a cyclic group of order 4. Precisely the same argument shows that the Galois group of the polynomial $x^p - 1$ is the multiplicative group of the field $\mathbb{Z}/p\mathbb{Z}$ for any prime p.

The notion of Galois group which we have just introduced is not general enough for out purposes. We will need to consider a polynomial f with coefficients in a field $K \subset \mathbb{C}$, where K is not necessarily $\mathbb{Q}$, and consider $\mathrm{Gal}(E_f/K)$, the automorphisms of E_f which are the identity on K. Since the coefficients are in K, again $\mathrm{Gal}(E_f/K)$ is a subgroup of $\mathrm{Perm}(R_f)$.

Example 3.3. Consider the polynomial $f(x) = x^3 - 2$. This has three roots, and the Galois group $\mathrm{Gal}(E_f/\mathbb{Q})$ is the full group of permutations of these roots[2]. The splitting field, E_f, contains the ratios of the roots, which are cubic roots of unity. If we set E_g to be the splitting field of $g(x) = x^2 + x + 1$, then $\mathrm{Gal}(E_f/E_g)$ is cyclic of order three. More specifically, set $\omega = e^{2\pi i/3}$. Then $\mathrm{Gal}(E_f/\mathbb{Q})$ is generated by multiplication by ω and complex conjugation, where as $\mathrm{Gal}(E_f/E_g)$ is generated by just multiplication by ω, since complex conjugation is not the identity on E_g.

Definition. We will call and extension L/K of field *normal* when the set of elements of L which are fixed by all the elements of $\mathrm{Gal}(L/K)$ is precisely K; only then is the Galois group really useful[3].

Example 3.4. Consider the field L of real numbers of the form

$$a + b2^{1/3} + c4^{1/3}$$

for any rational numbers a, b, c. In this case, $\mathrm{Gal}(L/\mathbb{Q}) = \{1\}$ since any element of the group must send $2^{1/3}$ to a cubic root of 2, and there are no other such roots in L.

The splitting field of a polynomial $f \in K[x]$ is always a normal extension, so we will not consider any others.

---

[1] This is the content of the theorem by Gauss that cyclotomic polynomials are irreducible.

[2] In particular, the real cubic root of 2 cannot be distinguished from the other roots.

[3] When L/K is not normal, the right thing to consider is the set of embeddings $L \subset \mathbb{C}$ which are the identity on K. We will not peruse this here.

Theorem 1. *If K is a field, f is a polynomial with coefficients in K, and E_f is the splitting field of f, then the field extension E_f/K is normal.*

We give a proof in Section 9. It is not perhaps the easiest proof, but it is chosen to motivate the proof of Theorem 2, which needs all the motivation it can get.

4. Differential Galois Groups

Suppose that we have a differential field K which is an extension of a differential field M. Typically, K will be the splitting field of some differential operator L with coefficients in M the field of rational functions.

Definition. The *differential Galois Group*, $\mathrm{DGal}(K/M)$ is the group of field automorphisms $\sigma\colon K \to K$ which restrict to the identity on M, and such that $\sigma(\delta(x)) = \delta(\sigma(x))$ for all $x \in K$.

Example 4.1. Again, let L be the operator given by $u'(t) - u(t)$. The splitting field of L was determined above. Any automorphism of E_L must send one solution of $u'(t) = u(t)$ to another (by the same reasoning as in the polynomial case), so in particular, it must send e^t to Ce^t for some C a non-zero complex number. Moreover, this C completely determines the $\mathcal{D}$-Galois automorphism. Consequently, the $\mathcal{D}$-Galois group is $\mathbb{C}^*$, the multiplicative group of the complex numbers.

Let us suppose that $U \subset \mathbb{C}$ is a simply connected open set, and that $K \subset M(U)$ is a subfield, typically the field of rational functions. Let L be a monic linear differential operator of order ℓ with coefficients in K and analytic on U, so that the space V_L of solutions of $L(f) = 0$ in $M(U)$ has dimension ℓ.

Theorem 2. *Give any element $f \in E_L - K$, there exists $\tau \in \mathrm{DGal}(E_L/K)$ such that $\tau(f) \neq f$.*

This is the analog of Theorem 1 for differential fields. Its proof is given in Section 9.

It is rather hard to think of the $\mathcal{D}$-Galois group, because already the field K is apt to be a big shapeless thing that is hard to grasp. However, just as in the case of polynomials we have a concrete way of thinking. Since the $\mathcal{D}$-Galois group sends solutions of the differential operator to other solutions, we conclude that the $\mathcal{D}$-Galois group of the splitting field of a linear operator L of order ℓ is a subgroup of $\mathrm{GL}_\ell(V_L)$. Thus, if you choose a basis of solutions of $L(u) = 0$, you can think of $\mathrm{DGal}(K/M)$ as a group of invertible complex matrices, $\ell \times \ell$ matrices, in fact.

The proof of the following theorem is again a bit technical, and will be given in Section 9.

Theorem 3. *The differential Galois group $\mathrm{DGal}(E_L/M)$ of a linear differential operator L is an algebraic subgroup of $\mathrm{GL}(V_L)$; that is, it is a subset defined by finitely many algebraic equations.*

Let us see what this says for a few examples. the additive group $\mathbb{C}$ has lots of subgroups, isomorphic to $\mathbb{Z}$, $\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{R}$, etc., but none of them are algebraic. The group $\mathbb{C}^*$ also has lots of subgroups, but only those consisting of the n-th roots of unity for some n are algebraic (obviously defined by the single equation $z^n - 1 = 0$.

The main consequence of Theorem 3 we will want is the following:

Corollary. *Let V be a finite dimensional vector space over $\mathbb{C}$, and $G \subset \mathrm{GL}(V)$ be an algebraic subgroup. Then the connected component $G_0 \subset G$ of G containing the identity is a normal subgroup, which is also algebraic, and the quotient group G/G_0 is finite.*

Indeed, any affine algebraic variety over $\mathbb{C}$ has finitely many connected components, which are each algebraic varieties.

Our next example shows that a $\mathcal{D}$-Galois group can perfectly well be finite.

Example 4.2. Choose a function $\sqrt{1-t^2}$ on the unit disc $U \subset \mathbb{C}$, for instance the one which is positive on $(-1,1)$, and consider the smallest $\mathcal{D}$-subfield $K \subset \mathcal{M}(U)$ which contains $\sqrt{1-t^2}$. This is a set of functions of the form $f(t) + g(t)\sqrt{1-z^2}$ with $f(0) = g(0) = 0$. Then K is a normal $\mathcal{D}$-extension of $\mathbb{C}(t)$, and $\mathrm{DGal}(K/\mathbb{C}(t))$ is the group with two elements, which exchanges $\sqrt{1-t^2}$ with $-\sqrt{1-t^2}$. This field is the splitting field of the linear operator

$$L(u(t)) = u'(t) - \frac{u(t)}{1-t^2};$$

and this illustrates the following fact: even if a linear differential operator is irreducible, in the sense that it is not the composition of two linear differential operators of lower degree, the differential Galois group of the splitting field my well not act transitively on the non-zero solutions, which may have an "individuality" of their own, such as the solution $u(t) = \sqrt{1-t^2}$ of $L(u(t)) = 0$, which satisfies $u(t)^2 + t^2 = 1$.

The situation in this example is completely general:

Propostion 4.3. *If E is a normal $\mathcal{D}$-extension of a $\mathcal{D}$-field K and $\mathrm{DGal}(E/K)$ is finite, then all the elements of E are algebraic over K.*

Proof. Choose $f \in E$, and consider the polynomial

$$\prod_{\sigma \in \mathrm{DGal}(E/K)} (x - \sigma(f)).$$

the coefficients of this polynomial are fixed under $\mathrm{DGal}(E/K)$, hence in K by Theorem 2; here is a polynomial with coefficients in K which f satisfies. □

5. The Discriminant and the Wronskian

The resemblance between Galois theory and $\mathcal{D}$-Galois theory is quite striking, but the correspondence between the *discriminant* of a polynomial and the *Wronskian* of a linear differential operator is positively uncanny.

Definition. If f is a polynomial with coefficients in some field K, and E_f is its splitting field, containing roots $x_1, \dots, x_d$, then the *discriminant* of f is

$$\Delta(f) = \pm \prod_{i \neq j} (x_i - x_j),$$

where the sign is $+$ if and only if the number of factors is divisible four.

A priori, this looks like an element of E_f, but it is clearly fixed by $\mathrm{Gal}(E_f/K)$, and is therefore an element of K. In E_f, the discriminant $\Delta(f)$ is the square of $\prod_{i<j}(x_i - x_j)$ (that is what the sign was for), but it is not necessarily a square in K. If it is not a square, there is an intermediate field between K and E_f, namely $K(\sqrt{\Delta(f)})$. It is fairly easy to understand the relation between the various Galois groups.

Propostion 5.1. *We have* $\mathrm{Gal}(E_f/K(\sqrt{\Delta(f)})) = \mathrm{Gal}(E_f/K) \cap \mathrm{Alt}(R_f)$*, where* $\mathrm{Alt}(R_f) \subset \mathrm{Perm}(R_f)$ *is the subgroup of even permutations. In particular, the discriminant is a square in* K *precisely when* $\mathrm{Gal}(E_f/K)$ *consists entirely of even permutations of the roots.*

Proof. An even permutation σ can be written as a product of an even number of transpositions, hence does not change the sign of $\prod_{i<j}(x_i - x_j)$. □

The Wronskian of a differential operator is best understood by making the differential operator into a system of first order equations. Suppose $A(t)$ is an $n \times n$ matrix with entries in some $\mathcal{D}$-field K, and consider the differential equation

$$W' = A(t)W$$

as s differential equation for a matrix function $W(t)$, with $W(t_0) = I_n$.

Definition. The *Wronskian* of the differential equation is the function $\mathrm{Wr}(t) = \det(W(t))$.

The Wronskian looks as if it belongs to the splitting field E_L, but differentiating shows the following:

Propostion 5.2. *The Wronskian* $\mathrm{Wr}_L(t)$ *satisfies the differential equation*

$$\mathrm{Wr}'_L(t) = \mathrm{Tr}(A(t))\,\mathrm{Wr}(t).$$

In particular, the Wronskian can certainly be expressed in terms of anti-derivatives, since it is

$$\mathrm{Wr}_L(t) = \exp\left[\int_{t_0}^{t} \mathrm{Tr}(A(s))ds\right].$$

Again, if the Wronskian is not in the original $\mathcal{D}$-field, this gives an intermediate $\mathcal{D}$-field extension $K \subset K(\mathrm{Wr}_L) \subset E_L$, and it is not too difficult to understand the effect on the $\mathcal{D}$-Galois groups.

Propostion 5.3. *We have*

$$\mathrm{DGal}(E_L/K(\mathrm{Wr}_L)) = \mathrm{DGal}(E_L/K) \cap \mathrm{SL}(V_L),$$

where $\mathrm{SL}(V_L) \subset \mathrm{GL}(V_L)$ *is the subgroup of automorphisms of determinant one. In particular. if the Wronskian is in* K*, then the* $\mathcal{D}$*-Galois group is contained in* $\mathrm{SL}(V_L)$*.*

Proof. Clearly and automorphism τ of V_L will change the Wronskian by multiplication by $\det\tau$. □

6. Radical Extensions and Solvable Galois Groups

Recall the major result in your high school algebra class: the Quadratic Formula. Presuming that you worked mainly in characteristic 0 back then, this simple formula allowed you to find the roots of *any* quadratic polynomial you were given. Not surprisingly, a square root appeared in the solution. This basic setting provides all the intuition needed to continue.

Definition. Suppose that you can find all the roots of a polynomial f with coefficients in a field K by the following procedure:

Extract a root $\zeta_1 = a_1^{1/d_1}$ of some element $a_i \in K$. Consider the splitting field K_1 of $x^{d_1} - a_1$. Then extract a root $\zeta_2 = a_2^{1/d_2}$ of an element $a_2 \in K_1$, and set K_2 to be the splitting field of $x^{d_2} - a_2$. Continue in this way until you have a field K_i which has all the roots of f.

Then, we say that f is *solvable by radicals.*

More complicated (and probably not covered in high school) is the formula for cubics: first, to solve the equation $x^3 + ax^2 + bx + c$, substitute $y = x - \frac{a}{3}$ to find

$$y^3 + py + q, \text{ where } p = b - \frac{a^2}{3} \text{ and } q = \frac{2a^3}{27} - \frac{ab}{3} + c.$$

Then we find

$$y = \left(\frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} \right)^{\frac{1}{3}} - \frac{p}{3\left(\frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} \right)^{\frac{1}{3}}}.$$

Note that this is a typical radical extension: first we adjoin a square root, $\sqrt{q^2 + \frac{4p^3}{27}}$, then a cube root of an element of the field generated by the first extension.

Definition. A finite group G is said to be *solvable* if there is a chain of subgroups,

$$\{1\} = G_n \subset G_{n-1} \subset \cdots \subset G_0 \subset G_{-1} = G,$$

such that each G_j is a normal subgroup of G_{j-1} and the quotient groups G_{j-1}/G_j are all abelian.

Standard examples of solvable groups are the symmetric groups S_3 and S_4, the latter via the chain

$$\{1\} \subset V \subset A_4 \subset S_4,$$

where V is the Klein four group and A_4 is the alternating group. The groups S_n and A_n are not solvable, however, for $n \geq 5$.

The similarity in naming is no coincidence: a polynomial is solvable by radicals if and only if $\mathrm{Gal}(E_f/K)$ is a solvable group. This will be crucial shortly.

7. Liouvillian Extensions and Solvable Differential Galois Groups

Of course, we can consider radical extensions of a differential field, but they are not the right analog of radical extensions in the context of differential fields. There, the "simple" extensions of a $\mathcal{D}$-field K are those obtained by considering an element $f \in K$, such that and anti-derivative F of f is not in K, and considering the smallest $\mathcal{D}$-field containing K and either F or e^F. We will also consider all finite algebraic extensions as elementary.

Definition. A *Liouvillian* extension M of a $\mathcal{D}$-field K is one such that there is a sequence

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n = M$$

such that each field K_{i+1} is either finite algebraic over K_i, or generated by an anti-derivative or exponential of an anti-derivative of an element of K_i.

Notice that if you are thinking of all these fields as subfields of $\mathcal{M}(U)$ for an appropriate U, then it may be necessary to restrict to some $U_1 \subset U$: if f has a pole in U with non-zero residue, then there will not be an anti-derivative F defined on all of U, but there will be one on any simply connected subset of U which avoids the poles of f.

Propostion 7.1. *All elementary functions are contained in a Liouvillian extension of* $\mathbb{C}(t)$

Proof. The difficulty is that the definition of a $\mathcal{D}$-field never mentioned compositions, like

$$e^{\sin t} \text{ or } \log\left(\sqrt{1-t^2}+1\right).$$

But such compositions are contained in the Liouvillian extensions. Indeed, any composition will be of the form e^f, $\log f$, or $\sin f$. Trigonometric functions are dealt with using Euler's formula

$$\cos t = \frac{e^{it}+e^{-it}}{2} \text{ and } \sin t = \frac{e^{it}-e^{-it}}{2i}.$$

The exponentials were explicitly included in the definition of Liouvillian extensions, and the logarithm is the anti-derivative of df/f. □

The following proposition says that Liouvillian extensions are the analogs of radical extensions.

Propostion 7.2. *Let G be the $\mathcal{D}$-Galois group of a linear differential operator L with coefficients in a $\mathcal{D}$-field K, and suppose that the $\mathcal{D}$-splitting field of L is contained in a Liouvillian extension. Let G_0 be the connected component of the identity in G. There there exists a sequence of subgroups*

$$\{1\} = G_n \subset G_{n-1} \subset \cdots \subset G_0 \subset G_{-1} = G$$

such that each G_{j+1} is normal in G_j, and such that G_j/G_{j+1} is isomorphic to $\mathbb{C}$ or $\mathbb{C}^*$, or is finite.

Proof. The splitting field field E_L is contained in a field M, where there is a finite sequence of extensions

$$K \subset M_1 \subset M_2 \subset \cdots \subset M_k = M$$

with each intermediate extension either generated by an anti-derivative, and exponential of an anti-derivative, or an extension with finite $\mathcal{D}$-Galois group.

Simply restrict these groups to E_L; the restrictions will give algebraic subgroups of C or C^*, or be finite. This is precisely what we need. □

8. Solutions of Equations (1) and (2)

We now restate our goals in the new language we have developed over the previous sections:

(i) The polynomial $f(x) = x^5 - 4x - 2$ is not solvable by radicals, and
(ii) No solution of the differential equation $u'(t) = t - [u(t)]^2$ is contained in a Liouvillian extension.

We begin by showing (i). Recall that a polynomial is solvable by radicals only if the Galois group of its splitting field is a solvable group; that is, it suffices to show that $\mathrm{Gal}(E_f/\mathbb{Q})$ is not solvable.

Since f has degree five, there are five roots defined over $\mathbb{C}$. The Galois group $\mathrm{Gal}(E_f/\mathbb{Q})$ permutes these roots and is thus a subgroup of S_5. If $\alpha \in \mathbb{C}$ is such that $f(\alpha) = 0$, then the field $\mathbb{Q}(\alpha)$ is an extension of $\mathbb{Q}$ of degree five. Since $\mathbb{Q}(\alpha) \subset E_f$, we must have the degree of $E_f/\mathbb{Q}$ is divisible by five. Consequently, $\mathrm{Gal}(E_f/\mathbb{Q})$ contains a 5-cycle.

Note that $f(-2) < 0 < f(-1)$ and $f(0) < 0 < f(2)$, so that f has real roots a, b, c satisfying

$$-2 < a < -1 < b < 0 < c < 2.$$

By considering derivatives of f, one sees that these are the only real roots. Thus, there are two complex conjugate roots of f.

Now consider the action of complex conjugation on the field E_f. It is certainly an automorphism, and it fixes $\mathbb{Q} \subset \mathbb{R}$. It is therefore an element of $\mathrm{Gal}(E_f/\mathbb{Q}) \subset S_5$. We just concluded that three of the roots of f are real, and thus fixed by complex conjugation, and that the two remaining roots are swapped. We can therefore conclude that $\mathrm{Gal}(E_f/\mathbb{Q})$ contains a 2-cycle as well.

That is all we need, however. It is a fact from elementary group theory that a 2-cycle and a 5-cycle generate all of S_5. We conclude that $\mathrm{Gal}(E_f/\mathbb{Q}) = S_5$, and f is not solvable by radicals.

We now proceed to our second goal. To do so, we introduce the *Airy* differential operator

$$L_A = (u(t)) = u''(t) - tu(t).$$

Since the function t has no poles, the splitting field E_{L_A} is subfield of the meromorphic functions on $\mathbb{C}$, $\mathcal{M}(\mathbb{C})$.

Theorem 4. *We have that* $G = \mathrm{DGal}(E_{L_A}/\mathbb{C}(t)) = \mathrm{SL}_2(\mathbb{C})$.

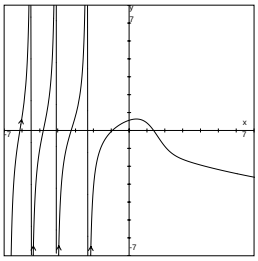

FIGURE 1. Solutions to $v(t) = t - [v(t)]^2$

Proof. Since the Wronskian of L_A is 1, Proposition 5.3 shows that $G \subset SL_2(\mathbb{C})$. To prove equality, let G_0 be the connected component of the identity. Then G/G_0 is finite.

Since $SL_2(\mathbb{C})$ is 3-dimensional, there are very few proper connected subgroups. In particular, they are all conjugate to one of the following four:

$$\{1\},\ \begin{bmatrix} a & 0 \\ 0 & 1/a \end{bmatrix},\ a \in \mathbb{C}^*;\ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix},\ b \in \mathbb{C};\ \text{or}\ \begin{bmatrix} a & b \\ 0 & 1/a \end{bmatrix},\ a \in \mathbb{C}^*, b \in \mathbb{C}.$$

Suppose now that G_0 was a proper subgroup of $SL_2(\mathbb{C})$. Then all elements of G_0 would have a common eigenvector $u(t) \in E_{L_A}$, since each of the four groups just listed does. Since differentiation commutes with the action of G on E_{L_A}, we then see that $v(t) = u'(t)/u(t)$ is left fixed by G_0. Thus, the $\mathcal{D}$-Galois extension generated by $v(t)$ is a subfield, M say, of E_{L_A} and $\mathrm{DGal}(M/\mathbb{C}(t))$ is a quotient of G by a group containing G_0; in particular $\mathrm{DGal}(M/\mathbb{C}(t))$ is finite, so that $v(t)$ is an algebraic function by Proposition 4.3.

Differentiating shows that $v(t)$ satisfies the Ricatti equation associated to the Airy equation:

$$\begin{aligned} v'(t) &= \frac{u \cdot u''(t) - [u'(t)]^2}{[u(t)]^2} \\ &= \frac{t \cdot [u(t)]^2 - [u'(t)]^2}{[u(t)]^2} \\ &= t - [v(t)]^2, \end{aligned}$$

and any solution of this equation has infinitely many poles. Indeed, the key point is that for any number $t_0 < -1 - \pi/2$, the solution $v(t)$ with $v(t_0) = 0$ has domain of definition (a, b) with $t_0 - \pi/2 < a < b < t_0 + \pi/2$, since the solution is above $\tan(t + t_0)$ for $t > t_0$ and beneath $\tan(t + t_0)$ for $t < t_0$ (see Figure 1). Thus, $v(t)$ has at least as many poles as $\tan(t)$, which has infinitely many poles. Hence $v(t)$ is not algebraic and our guess that $G_0 \neq SL_2(\mathbb{C})$ is false. □

Corollary 8.1. *No non-zero solution of the Airy equation belongs to a Liouvillian extension of* $\mathbb{C}(t)$.

Proof. By Proposition 7.2, if one (and hence all) solutions of the Airy equation belonged to a Liouvillian extension, then $G_0 = SL_2(\mathbb{C})$ would have a connected normal subgroup with commutative or finite quotient. Such subgroups of $SL_2(\mathbb{C})$ do not exist. □

We have (finally!) reached our second goal:

Corollary 8.2. *The differential equation $u'(t) = t - [u(t)]^2$ has no solutions which belong to a Liouvillian extension of $\mathbb{C}(t)$.*

Proof. Suppose $v(t)$ is such a solution. Then $e^{\int v(t)dt}$ is contained in a Liouvillian extension of $\mathbb{C}(t)$ and satisfies the Airy equation. This contradicts the previous corollary. □

9. Three Technical Proofs

In this section, we give the proofs of Theorems 1, 2, and 3, which use some more sophisticated tools from algebra.

Theorem 1. *If K is a field, f is a polynomial with coefficients in K, and E_f is the splitting field of f, then the field extension E_f/K is normal.*

Proof. We need to show that given any $\alpha \in E_f - K$, there exists $\tau \in \mathrm{Gal}(E_f/\mathbb{Q})$ with $\tau(\alpha) \neq \alpha$.

Consider the K-algebra $A = E \otimes_K E$; the hypothesis that $\alpha \notin K$ says precisely that the element $a = \alpha \otimes 1 - 1 \otimes \alpha \in A$ is non-zero. The element a is not nilpotent (since we are in characteristic zero, A has no nilpotents at all) and thus there is a maximal ideal $\mathfrak{a} \subset A$ which does not contain a. Let k be the residue field $A/\mathfrak{a}$ and $\bar{a}$ be the non-zero image of a in k. Note that since $K^* \subset A^*$, we have that $\mathfrak{a} \cap K = \{0\}$. We can therefore view K as a subfield of k.

There are two homomorphisms $i_1, i_2 \colon E \to k$; the one induced by $b \mapsto b \otimes 1$ and the one induced by $b \mapsto 1 \otimes b$. Under both of these maps, the roots of f are taken to roots of f, and in particular, i_1 and i_2 agree on these roots. Let k' be the subfield of k generated by K and the roots of f. Then $i_1, i_2 \colon E \to k'$ are field isomorphisms, and $\tau = i_2^{-1} \circ i_1 \colon E \to E$ is an element of $\mathrm{Gal}(E_f/K)$ with $\tau(\alpha) = \alpha - \bar{a} \neq a$. □

The proof of Theorem 2 follows the same outline, but we need a bit more of differential algebra first. In fact, we need even some non-differential algebra.

Lemma 9.1. *Let K be a field of characteristic zero, so that $\mathbb{Q} \subset K$ and A a finitely generated K-algebra. Any element $a \in A$ such that $a - c$ is invertible for infinitely many rational numbers c is algebraic over K.*

Proof. Since A is a finitely generated K-algebra, we can apply Noether's Normalization Lemma to find algebraically independent elements $x_1, \ldots, x_m \in A$ such that A is integral over $B = K[x_1, \ldots, x_m]$. Let C be the K-algebra generated by B and $(a-c)^{-1}$ for all c for which the inverse exists. Then A is integral over C.

We now apply Proposition 7.8 in [1] to conclude that C is a finitely generated K-algebra. Thus, there exist finitely many rational numbers $c_1, \ldots, c_n$ such that $(a - c_1)^{-1}, \ldots (a - c_n)^{-1}$ satisfy an algebraic dependence over K. Clearing denominators in this dependence gives a polynomial with coefficients in K which a satisfies. That is, a is algebraic over K. □

Now for the differential algebra we will need. Besides differential fields, we will need differential rings (A, δ) which are commutative rings with units, having a derivation $\delta\colon A \to A$. We will of course need differential ideals, which are ideals closed under the derivation. We leave it to the reader to check that the quotient of a differential ring by a differential ideal is again a differential ring.

Example 9.2. Let A be an arbitrary (non-differential) $\mathbb{C}$-algebra. Then the algebra $A[[T]]$ of formal power series with coefficients in A, and derivation ∂_T, the ordinary derivative with respect to T, is a differential $\mathbb{C}$-algebra.

All differential algebras are more or less of this form. More precisely, let (A, δ) be an arbitrary differential $\mathbb{C}$-algebra, and consider the "Taylor Series" map

$$A \to A[[T]],\ a \mapsto a + \delta(a)T + \frac{1}{2!}\delta^2(a)T^2 + \dots,$$

which is a homomorphism $(A, \delta) \to (A[[T]], \partial_T)$ of *differential* $\mathbb{C}$-algebras.

The next proposition is a nice application of this construction. In (non-differential) algebra, if A is a ring and $a \in A$ is an element which is not nilpotent, then there is a maximal ideal which does not contain a. In the same situation, if (A, δ) is a differential algebra, there is still, by an easy application of Zorn's Lemma, a maximal differential ideal which does not contain a, but it isn't clear what properties such an ideal might have.

Propostion 9.3. *Let (A, δ) be a difference $\mathbb{C}$-algebra, and $a \in A$ be an element which is not nilpotent. Then there exists a prime differential ideal $\mathfrak{p} \subset A$ which does not contain a. In particular, there exists a maximal differential ideal not contain a which is prime.*

Proof. Choose a maximal (non-differential) ideal $\mathfrak{q} \subset A$ which does not contain a. Consider the composition

$$\varphi\colon A \xrightarrow{T} A[[T]] \xrightarrow{\pi} (A/\mathfrak{q})[[T]].$$

First, φ is a homomorphism of differential rings, so its kernel is a differential ideal. The image of φ is an integral domain, so $\operatorname{Ker}\varphi$ is a prime ideal, and $\varphi(a) \neq 0$. □

Our next statement concerns constants. For the differential fields we have been considering, all subfields of $\mathcal{M}(U)$ for an appropriate U, the constants are obviously $\mathbb{C}$. But when we start considering algebras like $E \otimes_K E$, nothing is obvious anymore, and we must spell things out.

Let K be a differential field with field of constants $\mathbb{C}$, and A be a differential K-algebra, which is finitely generated as a K-algebra. Let $\mathfrak{p}$ be a maximal prime differential ideal, not the unit ideal. We can consider the differential algebra $B = A/\mathfrak{p}$, and its field of fractions $\bar{B}$.

Propostion 9.4. *The field of constants of $\bar{B}$ is $\mathbb{C}$.*

Proof. Let b be a constant of $\bar{B}$, and consider the set $I = \{h \in B | bh \in B\}$. The set I is obviously an ideal, and it is a differential ideal because b is constant. It is non-zero since b is the ratio of elements of B (with the denominator possibly being 1). Therefore, there exists a differential ideal $\mathfrak{a} \subset A$ such that $\mathfrak{p} \subsetneq \mathfrak{a}$. By the maximality of $\mathfrak{p}$, we have that $\mathfrak{a} = A$ is the unit ideal, and hence $b \in B$.

Similarly, the ideals $B(b-c)$ with $c \in \mathbb{C}$ are all differential ideals which are non-zero, so they are all the unit ideal, so $b - c$ is invertible in B.

By Lemma 9.1, this shows that b is algebraic over K; let

$$m(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0$$

be its minimal polynomial with coefficients in K. Differentiating $m(b) = 0$ yields

$$\delta(a_{k-1})b^{k-1} + \cdots + \delta(a_0) = 0$$

since b is constant. But this is an equation of degree less than k which is satisfied by b, hence the coefficients are all zero. Thus the coefficients are all constants of K; that is, the coefficients are all in $\mathbb{C}$. Since $\mathbb{C}$ is algebraically closed and b satisfies a polynomial over $\mathbb{C}$, we conclude that $b \in \mathbb{C}$. □

Theorem 2. *Let K be a differential field and L a linear differential operator defined over K of degree ℓ. Given any element $f \in E_L - K$, there exists $\tau \in \mathrm{DGal}(E_L/K)$ such that $\tau(f) \neq f$.*

Proof. Let V be the complex vector space of solutions of $L = 0$ in E_L. Consider the differential algebra $A = E_L \otimes_K E_L$. First observe that it has no nilpotents because we are in characteristic zero. The hypothesis that $f \notin K$ says precisely that the element $a = f \otimes 1 - 1 \otimes f \in A$ is non-zero. Find a maximal differential ideal $\mathfrak{p} \subset A$ which does not contain a. This time, the ideal is maximal only among differential ideals, and there is no reason to expect it to be maximal in A. By Proposition 9.3, however, we may take $\mathfrak{p}$ to be prime so that $B = A/\mathfrak{p}$ is an integral domain. Denote by $\bar{B}$ its field of fractions and $\bar{a}$ the (necessarily non-zero) image of a.

Again, there are two homomorphisms $i_1, i_2 \colon E_L \to \bar{B}$; the one induced by $g \mapsto g \otimes 1$ and the one induced by $g \mapsto 1 \otimes g$, which are clearly extensions of differential fields. By Proposition 9.4, the field of constants of $\bar{A}$ is $\mathbb{C}$, and hence the space of solutions to $L = 0$ in $\bar{B}$ is a complex vector space W of dimension at most ℓ.

But both $i_1(V)$ and $i_2(V)$ are complex vector spaces of solutions of $L = 0$ in $\bar{B}$, hence $i_1(V) = i_2(V) = W$. Consider the subfield $F \subseteq \bar{B}$ generated by K and W. Clearly both i_1 and i_2 are isomorphisms $E \to F$, and $\tau = i_2^{-1} \circ i_1$ is an element of $\mathrm{DGal}(E_L/K)$ with $f - \tau(f) = f - \bar{a} \neq 0$. □

We close with the proof of Theorem 3.

Theorem 3. *The differential Galois group $\mathrm{DGal}(E_L/K)$ of a linear differential operator L defined over a differential field $K \supseteq \mathbb{C}(t)$ is an algebraic subgroup of $\mathrm{GL}(V_L)$; that is, it is a subset defined by finitely many algebraic equations.*

Proof. Chose a basis $f_1, \ldots, f_k$ for E_L over K and k^2 variables X_i^j, with $1 \leq i \leq k$ and $0 \leq j \leq k-1$. Denote by $K[X]$ the K-algebra of polynomials in the variables X_i^j. Let $U \subset \mathbb{C}$ be such that $E_L \subset \mathcal{M}(U)$. Consider the mapping $\Phi \colon K[X] \to \mathcal{M}(U)$ obtained by substituting $f_i^{(j)}$ for X_i^j. By Hilbert's Basis Theorem, the kernel, $\operatorname{Ker}\Phi \subset K[X]$ is finitely generated, say by $P_1, \ldots P_M$.

Identify $\mathrm{GL}(V_L)$ with the group of invertible $k \times k$ matrices in the standard way, and identify the matrix $A = (a_{i,j})$ with automorphism which sends f_i to $\displaystyle\sum_{j=1}^{k} a_{j,i} f_j$.

Then the elements of $\mathrm{DGal}(E_L/K)$ satisfy the set of equations

$$Q_m(A) = P_m\left(\sum_j a_{j,1}X_j^0, \sum_j a_{j,2}X_j^1, \ldots, \sum_j a_{j,k}X_j^{k-1}\right),$$

for $1 \leq m \leq M$. This is a collection of M polynomials equations in the variables $a_{i,j}$, and so $\mathrm{DGal}(E_L/K)$ is algebraic. □

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] D. Dummit and R. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[3] J.H. Hubbard and B. West. *Differential equations: a dynamical systems approach*, volume 5 of *Texts in Applied Mathematics*. Springer-Verlag, New York, 1995. Ordinary differential equations, Corrected reprint of the 1991 edition.

[4] I. Kaplansky. *An introduction to differential algebra*. Hermann, Paris, second edition, 1976. Actualités Scientifiques et Industrielles, No. 1251, Publications de l'Institut de Mathématique de l'Université de Nancago, No. V.

[5] A.R. Magid. *Lectures on differential Galois theory*, volume 7 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1994.

Dept. of Math., Malott Hall, Cornell University, Ithaca, NY 14853.

E-mail address: jhh8@cornell.edu

Dept. of Math., Malott Hall, Cornell University, Ithaca, NY 14853.

E-mail address: blundell@math.cornell.edu