A First Look at Differential Algebra

John H. Hubbard and Benjamin E. Lundell

Abstract. This article is an introduction to the common algebraic methods used to study both solutions to polynomial equations and solutions to differential equations: Galois theory and differential Galois theory. We develop both theories simultaneously by studying the solutions to the polynomial equation $x^5 - 4x^2 - 2 = 0$ and the solutions to the differential equation $u' = t - u^2$.

1. INTRODUCTION. The object of this paper is to prove that the differential equation

$$u' = t - u^2 \tag{1}$$

has no solutions which can be written using elementary functions, or antiderivatives of elementary functions, or exponentials of such antiderivatives, or antiderivatives 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 include Liouville, Picard, Vessiot, Kolchin, and 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 an 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 and has since forgotten many of the finer points. The examples are chosen to illuminate the theorems: it is scarcely possible to give all the details of every proof in this article. For further reading, we recommend [**4**], [**5**], [**7**], [**8**], [**9**], or [**10**]. For the basics of Galois theory, differential equations, or algebraic groups, see [**1**], [**2**], or [**3**], respectively.

2. SPLITTING FIELDS. Our first step will be 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 these operations 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 this paper will have characteristic 0.

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

doi:10.4169/amer.math.monthly.118.03.245

Definition 2.1. Given a polynomial f with coefficients in a field $F \subset \mathbb{C}$, the *splitting field* of f over F, denoted E_f, is the smallest subfield of $\mathbb{C}$ which contains F and 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 2.2. Consider the polynomial $f(x) = x^2 - 2$. 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 over $\mathbb{Q}$. 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 any algebraic closure contains the roots any polynomial, by definition). We find it easier to think of subfields of $\mathbb{C}$, but that is just a crutch.

In fact, the results on the Galois theory of polynomials that we collect in this section and the next are true in a much more general setting: if F is *any* characteristic-zero field, we will have the same results for a polynomial f with coefficients in F, provided that we fix an algebraic closure of F to begin with. This level of generality is not appropriate in these introductory sections, but will be necessary in Proposition 4.6.

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

Definition 2.3. A *differential field*, here called a $\mathcal{D}$-field, is a field F, together with a derivation $\delta : F \to F$ which satisfies the rules

$$\delta(u + v) = \delta(u) + \delta(v) \text{ and } \delta(uv) = u\delta(v) + v\delta(u).$$

A *linear differential operator of degree* k on (F, δ) is a map $L \colon F \to F$ given by a formula

$$L(u) = \delta^k(u) + \alpha_{k-1}\delta^{k-1}(u) + \cdots + \alpha_0 u$$

where $\delta^k(u) = \delta(\delta(\ldots(u)\ldots))$ and $\alpha_i \in F$.

The first example of a $\mathcal{D}$-field is $\mathbb{C}(t)$, the set of all rational functions in one variable with complex coefficients, with the usual addition and multiplication, and with the derivation given by the ordinary derivative. The standard rules for differentiating say

that 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 u/v of analytic functions with v not identically zero. 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: if U is a simply connected subset of $\mathbb{C}$ and $\alpha_1, \ldots, \alpha_k$ are analytic on U, then the differential equation

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

has a unique solution in $\mathcal{M}(U)$ for any t_0 in U with any given initial conditions $u(t_0), u'(t_0), \ldots, u^{(k-1)}(t_0)$.

Definition 2.4. If (F, δ) is a differential field, then the *constants* of F are the elements $u \in F$ such that $\delta(u) = 0$.

In this paper, the field of constants will always be $\mathbb{C}$. We now have the background needed to define where the solutions to a differential equation lie.

Definition 2.5. Let $L(u) = \delta^n(u) + \alpha_{n-1}\delta^{n-1}(u) + \cdots + \alpha_0 u$ be a differential operator where the $\alpha_i \in F \subset \mathcal{M}(U)$ are all analytic in some simply connected open set $U \subset \mathbb{C}$. Then the *differential splitting field of L over F in $\mathcal{M}(U)$*, denoted E_L^U, is the smallest $\mathcal{D}$-subfield of $\mathcal{M}(U)$ containing F and all solutions of $L(u) = 0$ on U.

We will suppress U from the notation and write E_L for E_L^U when no confusion can arise.

Example 2.6. One of the simplest differential operators is $L(u) = u' - u$. In this case the only coefficients are the numbers ± 1, which are certainly analytic on all of $\mathbb{C}$, so we may consider the splitting field over $\mathbb{C}(t)$ to be the smallest $\mathcal{D}$-subfield of $\mathcal{M}(\mathbb{C})$ containing the rational functions and the solutions of the differential equation $u' = u$, that is, all functions of the form Ce^t. It should be clear that this subfield, E_L, is precisely the space of functions of the form

$$\frac{p_0(t) + p_1(t)e^t + \cdots + p_m(t)e^{mt}}{q_0(t) + q_1(t)e^t + \cdots + q_n(t)e^{nt}}$$

where the p_i and q_j are polynomials with coefficients in $\mathbb{C}$, with the denominator not identically zero. Indeed, this is a differential field (clearly closed under addition, multiplication, division, and differentiation), and more or less obviously the smallest such field containing 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 3.1. Let $F \subset \mathbb{C}$ be a field and suppose K/F is any field extension. The *Galois group*, denoted $\mathrm{Gal}(K/F)$, is the group of all field automorphisms of K which leave F fixed, where the group law is given by composition of automorphisms. If f is a polynomial with coefficients in F, then we call $\mathrm{Gal}(E_f/F)$ the *Galois group* of f.

Fix a polynomial f with coefficients in F, and let $\sigma \in \mathrm{Gal}(E_f/F)$. Since σ fixes F and respects field operations (both by definition), we see that $f(\sigma(a)) = \sigma(f(a))$ 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

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

which can easily be seen to be an injection, so $\mathrm{Gal}(E_f/F)$ is naturally isomorphic to a subgroup of the finite group of permutations of the roots. From now on, we will always identify the Galois group of a polynomial with a subgroup of this permutation group.

In fact, we can say more. Write $f = g \cdot h$, where g is an irreducible, nonconstant polynomial with coefficients in F, and suppose $g(a) = 0$ for $a \in \mathbb{C}$. First, we note that we necessarily have $f(a) = g(a)h(a) = 0$, so that $a \in E_f$. Let $\sigma \in \mathrm{Gal}(E_f/F)$. By the same reasoning as before

$$0 = g(a) = \sigma(g(a)) = g(\sigma(a)),$$

so that not only does $\mathrm{Gal}(E_f/F)$ permute the roots of f, it permutes the roots of the *irreducible factors* of f. Because of this, we can focus solely on the case where f itself is irreducible for the remainder of the paper.

Example 3.2. If $f(x) = x^2 - 2$ as in Example 2.2, then the group $\mathrm{Gal}(E_f/\mathbb{Q})$ is the group of permutations of $\{\sqrt{2}, -\sqrt{2}\}$.

Example 3.3. 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 of a polynomial f (i.e., given any two roots a_1, a_2 of f there exists $\sigma \in \mathrm{Gal}(E_f/\mathbb{Q})$ such that $\sigma(a_1) = a_2$) if and only if f is irreducible.

In our 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. 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.

Definition 3.4. An extension K/F of a field F is called a *Galois extension* if the set of elements of K which are fixed by all the elements of $\mathrm{Gal}(K/F)$ is precisely F; only then is the Galois group really useful.[2]

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

[2] When L/K is not a Galois extension, the right thing to consider is the set of embeddings $K \subset \mathbb{C}$ which are the identity on F. We will not pursue this here.

The following theorem gives us all finite Galois extensions of a field F of characteristic zero.

Theorem 3.5. *If f is an irreducible polynomial with coefficients in a field $F \subset \mathbb{C}$, then the field extension E_f/F is a Galois extension. In fact, every finite Galois extension of F arises as the splitting field of some irreducible polynomial with coefficients in F. Finally, in this setting, $|\mathrm{Gal}(E_f/F)| = [E_f : F]$.*

Proof. See, for instance, Section 14.1 of [**1**]. ∎

In Examples 3.2 and 3.3 we saw examples of Galois extensions. We now look at an extension which is *not* a Galois extension.

Example 3.6. Consider the field F of real numbers of the form

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

for any rational numbers a, b, c. In this case, $\mathrm{Gal}(F/\mathbb{Q}) = \{1\}$ 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 F. Thus, $F/\mathbb{Q}$ is not a Galois extension.

Theorem 3.7 (The Fundamental Theorem of Galois Theory). *Let K/F be a finite Galois extension. If M is a field and $F \subset M \subset K$, then $\mathrm{Gal}(K/M)$ is a subgroup of $\mathrm{Gal}(K/F)$. Furthermore, this defines an inclusion-reversing bijection between the subfields of K containing F and the subgroups of $\mathrm{Gal}(K/F)$. Under this bijection, the normal subgroups correspond to the subfields M such that M/F is also a Galois extension, and, in this case, $\mathrm{Gal}(M/F) \simeq \mathrm{Gal}(K/F)/\mathrm{Gal}(K/M)$.*

Proof. See Section 14.2 of [**1**]. ∎

Example 3.8. 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[3] and so has order six. 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. Therefore, $\mathrm{Gal}(E_f/E_g) \trianglelefteq \mathrm{Gal}(E_f/\mathbb{Q})$ since index-two subgroups are always normal. According to Theorem 3.7, then, $E_g/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(E_g/\mathbb{Q}) \simeq \mathrm{Gal}(E_f/\mathbb{Q})/\mathrm{Gal}(E_f/E_g)$.

More specifically, set $\omega = e^{2\pi i/3}$. Then $\mathrm{Gal}(E_f/\mathbb{Q})$ is generated by complex conjugation and the unique field automorphism σ which maps $2^{1/3} \mapsto \omega \cdot 2^{1/3}$, whereas $\mathrm{Gal}(E_f/E_g)$ is generated by just σ, since complex conjugation is not the identity on E_g. This last statement shows that $\mathrm{Gal}(E_g/\mathbb{Q})$ is isomorphic to the quotient group, which is generated by the coset containing complex conjugation, and so is of order two.

Finally, we consider the order-two subgroup of $\mathrm{Gal}(E_f/\mathbb{Q})$ generated by complex conjugation. The field corresponding to this subgroup under the bijection in Theorem 3.7 is precisely the field considered in Example 3.6. There, we saw that this field was not a Galois extension of $\mathbb{Q}$. This corresponds to the fact that no subgroup of two elements is normal in $\mathrm{Gal}(E_f/\mathbb{Q})$.

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

4. DIFFERENTIAL GALOIS GROUPS. In this section, we will develop an analogous Galois theory for differential field extensions. Throughout this section, we will assume that all differential fields contain $\mathbb{C}(t)$ and lie inside some field $\mathcal{M}(U)$ for $U \subset \mathbb{C}$ a simply connect open set.

Definition 4.1. Let (K, ϵ) be a differential extension of the differential field (F, δ). The *differential Galois Group*, $\mathrm{DGal}(K/F)$, is the group of field automorphisms $\sigma : K \to K$ which restrict to the identity on F and satisfy $\sigma(\epsilon(u)) = \epsilon(\sigma(u))$ for all $u \in K$, and the group law is given by composition of automorphisms. If L is a linear differential operator with coefficients in F, then we call $\mathrm{DGal}(E_L/F)$ the *differential Galois group of* L.

Just as in the case of polynomials, if we fix a linear differential operator L of degree k with coefficients in F, then the elements of $\mathrm{DGal}(E_L/F)$ will map one solution of $L(u) = 0$ to another. The proof is identical to that in the polynomial case. The space V_L of solutions of $L(u) = 0$ in $\mathcal{M}(U)$ has dimension k as a vector space over $\mathbb{C}$ (since we must specify k initial conditions to be guaranteed a *unique* solution). As we just mentioned, elements of the $\mathcal{D}$-Galois group permute the solutions of L and are F-linear (and hence necessarily $\mathbb{C}$-linear). We conclude that the $\mathcal{D}$-Galois group $\mathrm{DGal}(E_L/K)$ is naturally isomorphic to a subgroup of $\mathrm{GL}(V_L)$. Thus, if you choose a basis of solutions of $L(u) = 0$, you can think of $\mathrm{DGal}(E_L/F)$ as a group of invertible complex $k \times k$ matrices. As with polynomials, we will always make this identification.

Example 4.2. Let L be the operator given by $L(u) = u' - u$; in Example 2.6, the splitting field of L was determined. Any automorphism of E_L must send one solution of $u' = u$ to another, so in particular, it must send e^t to Ce^t for some nonzero complex number C. Moreover, C completely determines the $\mathcal{D}$-Galois automorphism. Consequently, the $\mathcal{D}$-Galois group is $\mathbb{C}^* = \mathrm{GL}_1(\mathbb{C})$, the multiplicative group of the complex numbers.

Theorem 4.3. *The differential Galois group* $\mathrm{DGal}(E_L/K)$ *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 polynomial equations.*

Proof. See Section 17 of [**4**]. ∎

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. For instance, $\mathbb{Z}$ is defined by the equation $\sin \pi z = 0$, but $f(z) = \sin(\pi z)$ is not a polynomial (nor is the function $f(z) = z - \bar{z}$, which vanishes exactly on $\mathbb{R}$). The group $\mathbb{C}^*$ also has lots of subgroups, but only those consisting of the nth roots of unity for some n are algebraic (obviously defined by the single equation $z^n - 1 = 0$).

The next theorem is a strong result on algebraic groups, and will be necessary for the proof of Theorem 8.1.

Theorem 4.4. *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.*

Proof. See Chapter II, Section 7.3 of [**3**]. ∎

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

Example 4.5. Let $U \subset \mathbb{C}$ be the open unit disk and consider the linear differential operator

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

whose coefficients are analytic on U. Let w be an analytic branch of $\sqrt{1-t^2}$ on U, for instance the one which is positive on $(-1, 1)$. Then $L(Cw) = 0$ for any $C \in \mathbb{C}$, and the splitting field $E_L \subset \mathcal{M}(U)$ of L over $\mathbb{C}(t)$ is the set of functions of the form $u + v\sqrt{1-t^2}$ with $u, v \in \mathbb{C}(t)$.

Since L is a first-order operator, we see that $\mathrm{DGal}(E_L/\mathbb{C}(t))$ is a subgroup of $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$. Let $\sigma \in \mathrm{DGal}(E_L/\mathbb{C}(t))$, so that $\sigma(w) = Cw$ for some $C \in \mathbb{C}$. Then, $\sigma(w)^2 = C^2w^2 = C^2(1-t^2)$. But also, $\sigma(w)^2 = \sigma(w^2) = \sigma(1-t^2) = 1-t^2$, since σ fixes $1-t^2 \in \mathbb{C}(t)$. Therefore, $C^2 = 1$. Thus, $\mathrm{DGal}(E_L/\mathbb{C}(t))$ is the group of two elements: the identity automorphism and the automorphism which exchanges $\sqrt{1-t^2}$ and $-\sqrt{1-t^2}$.

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 may well not act transitively on the nonzero solutions, which may have an "individuality" of their own.

The situation in this example is completely general.

Proposition 4.6. *Let L be a linear differential operator with coefficients in some $\mathcal{D}$-field $F \subset \mathcal{M}(U)$, where $U \subset \mathbb{C}$ is a simply connected open set. If E_L/F is a Galois extension and* $\mathrm{DGal}(E_L/F)$ *is finite, then all the elements of E_L are algebraic over F.*

Before we prove this proposition, we should explain what we mean by "E_L/F is a Galois extension." By this, we mean that E_L is the splitting field of some irreducible polynomial with coefficients in the $\mathcal{D}$-field F (contained in some algebraic closure of F). In the setting of Example 4.5, we had $E_L = E_f$ where $f(x) = x^2 - (1-t^2) \in \mathbb{C}(t)[x]$. As we mentioned in the remark following Example 2.2, the results on the Galois theory of polynomials we developed in Sections 2 and 3 carry over to this more general setting.

Proof of Proposition 4.6 Choose $v \in E_L$, and consider the polynomial

$$f := \prod_{\sigma \in \mathrm{DGal}(E_L/F)} (x - \sigma(v)).$$

The coefficients of this polynomial are fixed under $\mathrm{DGal}(E_L/F)$, hence in F by Theorem 4.8 below. Thus, f is a polynomial with coefficients in F which has v as a root, so that v is algebraic over F, as desired. ∎

The previous proposition connects splitting fields of linear differential operators to splitting fields of polynomials. One might ask, then, are Galois $\mathcal{D}$-extensions the right extensions to study in the $\mathcal{D}$-field setting? The answer is no. However, we would still like an analogue of Galois extensions for differential fields.

Definition 4.7. An extension K/F of differential fields is called a *Picard-Vessiot extension* if the set of elements of K which are fixed by all the elements of $\mathrm{DGal}(K/F)$ is precisely F.

Picard-Vessiot extensions play the role in differential Galois theory that Galois extensions play in polynomial Galois theory. In support of this, we offer the following analogues of Theorems 3.5 and 3.7 for differential fields.

Theorem 4.8. *If L is a linear differential operator with coefficients in a differential field $F \subset \mathcal{M}(U)$, then the field extension E_L/F is a Picard-Vessiot extension. Moreover, every Picard-Vessiot extension of F arises as the splitting field of some linear differential operator with coefficients in F.*

Proof. See the section in [**8**] on Picard-Vessiot extensions. ∎

Theorem 4.9 (The Fundamental Theorem of Differential Galois Theory). *Let K/F be a Picard-Vessoit extension. If M is a $\mathcal{D}$-field and $F \subset M \subset K$, then $\mathrm{DGal}(K/M)$ is an algebraic subgroup of $\mathrm{DGal}(K/F)$. Furthermore, this defines an inclusion-reversing bijection between the $\mathcal{D}$-subfields of K containing F and the algebraic subgroups of $\mathrm{DGal}(K/F)$. Under this bijection, the normal subgroups correspond to the $\mathcal{D}$-subfields M such that M/F is also a Picard-Vessoit extension, and, in this case, $\mathrm{DGal}(M/F) \simeq \mathrm{DGal}(K/F)/\mathrm{DGal}(K/M)$.*

Proof. See Sections 15–19 of [**4**]. ∎

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 5.1. If f is an irreducible polynomial with coefficients in some field F, and E_f is its splitting field, containing roots $x_1, \ldots, x_d$, then the *discriminant* of f is[4]

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

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

A priori, this looks like an element of E_f, but it is clearly fixed by $\mathrm{Gal}(E_f/F)$, and is therefore an element of F by Theorem 3.5. 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 F. If it is not a square, there is an intermediate field between F and E_f, namely $F(\sqrt{\Delta(f)})$. It is fairly easy to understand the relation between the various Galois groups.

Proposition 5.2. *We have $\mathrm{Gal}(E_f/F(\sqrt{\Delta(f)})) = \mathrm{Gal}(E_f/F) \cap \mathrm{Alt}(R_f)$, where $\mathrm{Alt}(R_f) \subset \mathrm{Perm}(R_f)$ is the subgroup of even permutations. In particular, the discriminant is a square in F precisely when $\mathrm{Gal}(E_f/F)$ consists entirely of even permutations of the roots of f.*

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

[4]For the sake of comparison with the Wronskian, it might be better to define the discriminant in terms of the resultant of f, but we avoid that here because it is longer and more technical.

Example 5.3. Consider the polynomial $f(x) = x^3 - 2$; one can compute that $\Delta(x^3 - 2) = -108$. In Example 3.8, we saw that $\mathrm{Gal}(E_f/\mathbb{Q}) = S_3$. Proposition 5.2 then shows that $\mathrm{Gal}(E_f/\mathbb{Q}(\sqrt{\Delta(f)})) = A_3$. Of course, we had seen this already in Example 3.8: $-108 = -1 \cdot 2^2 \cdot 3^3$ so that $\mathbb{Q}(\sqrt{\Delta(f)}) = \mathbb{Q}(\sqrt{-3}) = E_g$, where $g(x) = x^2 + x + 1$ is the irreducible polynomial giving the cubic root of unity.

Let U be a simply connected open subset of $\mathbb{C}$ and F a differential subfield of $\mathcal{M}(U)$. The Wronskian of a differential operator L with coefficients in F is best understood by making the differential equation $L(u) = 0$ into a system of first-order equations as follows.

If $L(u) = u^{(n)} + \alpha_{n-1}u^{(n-1)} + \cdots + \alpha_0 u$, then we can represent the equation $L(u) = 0$ as the matrix equation $A_L\mathbf{u} = \mathbf{u}'$, where A_L, $\mathbf{u}$, and $\mathbf{u}'$ are the $n \times n$, $n \times 1$, and $n \times 1$ matrices

$$A_L := \left(\begin{array}{c|c} \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} & I_{n-1} \\ \hline -\alpha_0 \quad -\alpha_1 \quad \ldots \quad -\alpha_{n-1} & \end{array}\right), \quad \mathbf{u} := \begin{pmatrix} u \\ u' \\ \vdots \\ u^{(n-1)} \end{pmatrix}, \text{ and } \mathbf{u}' := \begin{pmatrix} u' \\ u'' \\ \vdots \\ u^{(n)} \end{pmatrix}.$$

If $u_1, \ldots, u_n$ are n linearly independent solutions to $L(u) = 0$, we define a new $n \times n$-matrix W_L whose ith column is $\mathbf{u}_i$ for $i = 1, \ldots, n$. Then W_L satisfies the $n \times n$-matrix differential equation $W' = A_L W$.

Definition 5.4. The *Wronskian* of the differential operator L is the function $\mathrm{Wr}_L = \det(W_L)$ of the complex variable t. As the matrix W_L depends on the choice of the basis of solutions to $L(u) = 0$, the Wronskian Wr_L is only defined up to a nonzero complex constant.

Unfortunately, it would seem from the definition that one would have to know a basis for the space of solutions to $L(u) = 0$ to compute the Wronskian. That, in general, could be very difficult to come by. However, the following proposition gives us a method of computing the Wronskian just by considering the matrix A_L.

Proposition 5.5. *The Wronskian* Wr_L *satisfies the differential equation*

$$u' = \mathrm{Tr}(A_L)u.$$

Hence, we can write

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

where t_0 is any point in U and we integrate along any path from t_0 to t in U. In particular, the Wronskian is always contained in a differential extension obtained by adjoining the exponential of an antiderivative.

Proof. To see the first fact, we use the Jacobi identity for invertible $n \times n$ matrices:

$$(\det W)' = \mathrm{Tr}(W' \cdot \mathrm{Adj}\, W),$$

where $\mathrm{Adj}\, W$ is the unique $n \times n$ invertible matrix such that

$$W \cdot \mathrm{Adj}\, W = (\mathrm{Adj}\, W) \cdot W = \det(W) I_n.$$

The first part of the proposition now follows immediately since

$$\begin{aligned}
\mathrm{Wr}_L' &= \mathrm{Tr}(W_L' \cdot \mathrm{Adj}\, W_L) \\
&= \mathrm{Tr}(A_L W_L \,\mathrm{Adj}\, W_L), \quad \text{since } W_L' = A_L W_L, \\
&= \mathrm{Tr}(A_L \cdot \det(W_L) I_n), \quad \text{since } W_L \cdot \mathrm{Adj}\, W_L = \det(W_L) I_n, \\
&= \mathrm{Tr}(A_L \cdot \mathrm{Wr}_L\, I_n) \\
&= \mathrm{Tr}(A_L)\, \mathrm{Wr}_L\,.
\end{aligned}$$

Suppose now that the Wronskian is 0 at $t_0 \in U$. Then there is some linear combination w of $u_1, \ldots, u_n$ such that $w(t_0) = w'(t_0) = \cdots = w^{(n-1)}(t_0) = 0$. However, $L(w) = 0$, so by the uniqueness theorem for solutions to $L(u) = 0$, we must have the w is the constant function 0. This violates the linear independence of the solutions $u_1, \ldots, u_n$, so we may conclude that Wr_L is nonvanishing on U. Thus, we may divide to get

$$\frac{\mathrm{Wr}_L'}{\mathrm{Wr}_L} = \mathrm{Tr}\, A_L$$

as functions on the simply connected set U. Thus, if we pick any $t_0 \in U$, the integral

$$\begin{aligned}
\int_{t_0}^{t} \mathrm{Tr}\, A_L(s)\, ds &= \int_{t_0}^{t} \frac{\mathrm{Wr}_L'(s)}{\mathrm{Wr}_L(s)} ds \\
&= \log \mathrm{Wr}_L(t) - \log \mathrm{Wr}_L(t_0)
\end{aligned}$$

is independent of the path chosen from t_0 to t and the second part of the proposition follows. ∎

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

Proposition 5.6. *After identifying* $\mathrm{DGal}(E_L/F)$ *and* $\mathrm{GL}(V_L)$*, we have*

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

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* F*, then the* $\mathcal{D}$*-Galois group is contained in* $\mathrm{SL}(V_L)$*.*

Proof. Let $\sigma \in \mathrm{DGal}(E_L/F)$. Then, as discussed above, σ permutes the solutions of $L(u) = 0$. As W_L is determined by these solutions, we see that σ acts on W_L by acting on its entries. We will denote this action by $\sigma(W_L)$. Since σ is a field homomorphism, and as $\det W_L$ is a sum of products of elements of F, we can conclude $\sigma(\mathrm{Wr}_L) = \sigma(\det W_L) = \det(\sigma(W_L))$.

By identifying $\mathrm{DGal}(E_L/F)$ and $\mathrm{GL}(V_L)$, we can find a matrix $S \in \mathrm{GL}(V_L)$ such that $\sigma(W_L) = W_L S$.[5] Therefore,

$$\sigma(\mathrm{Wr}_L) = \det(\sigma W_L) = \det(W_L S) = \det(W_L)\det(S) = \det(S)\,\mathrm{Wr}_L\,.$$

In particular, σ fixes Wr_L if and only if $\det S = 1$, as claimed. ∎

[5]This is not obvious, but it can be checked by writing down matrices with respect to the basis $\{u_1, \ldots, u_n\}$. Also, notice that this means that the matrix corresponding to σ acts by right multiplication.

We illustrate these ideas with an example which is crucial to the proof of Theorem 8.1.

Example 5.7. Consider the *Airy* differential operator $L_A(u) = u'' - tu$, and let v be a solution to $L(u) = 0$. Then

$$A_{L_A} = \begin{pmatrix} 0 & 1 \\ t & 0 \end{pmatrix},$$

and, if $L_A(v) = 0$, then

$$\begin{aligned} A_{L_A}\mathbf{v} &= \begin{pmatrix} 0 & 1 \\ t & 0 \end{pmatrix} \begin{pmatrix} v \\ v' \end{pmatrix} \\ &= \begin{pmatrix} v' \\ tv \end{pmatrix} \\ &= \begin{pmatrix} v' \\ v'' \end{pmatrix}, \quad \text{since } L_A(v) = 0, \\ &= \mathbf{v}'. \end{aligned}$$

We can now use Proposition 5.5 to compute the Wronskian Wr_{L_A}. Since $\mathrm{Tr}\, A_{L_A} = 0$, we have that $\mathrm{Wr}_{L_A} = C \exp\left[\int 0\right] = C$, for some nonzero complex number C. Since $C \in \mathbb{C}(t)$, we see that $\mathrm{DGal}(E_{L_A})$ is a subgroup of $\mathrm{SL}_2(\mathbb{C})$ by Proposition 5.6; determining precisely which subgroup is the content of Theorem 8.1.

6. RADICAL EXTENSIONS AND SOLVABLE GALOIS GROUPS. Recall a major result in your high school algebra class: the quadratic formula. Presuming that you worked mainly in characteristic zero 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 6.1. Suppose that you can find all the roots of an irreducible polynomial f with coefficients in a field F by the following procedure:

(i) Choose some element $a_1 \in F$ and consider the splitting field F_1 of $x^{d_1} - a_1$.
(ii) Choose an ~~an~~ element $a_2 \in F_1$, and set F_2 to be the splitting field of $x^{d_2} - a_2$.
(iii) Continue in this way until you have a field F_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 $x^3 + ax^2 + bx + c = 0$, substitute $y = x - \frac{a}{3}$ to convert the problem to

$$y^3 + py + q = 0, \text{ where } p = b - \frac{a^2}{3} \text{ and } q = \frac{2a^3}{27} - \frac{ab}{3} + c.$$

Then we find

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

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

Definition 6.2. A 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 finite 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 next proposition shows that the similarity in naming is no coincidence.

Proposition 6.3. *An irreducible polynomial f with coefficients in F is solvable by radicals if and only if* $\mathrm{Gal}(E_f/F)$ *is a solvable group.*

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 F are those obtained by considering the antiderivative V of an element $v \in F$, and considering the smallest $\mathcal{D}$-field containing F and either V or e^V. We will also consider all finite algebraic extensions of F as elementary.

Definition 7.1. A *Liouvillian* extension K of a $\mathcal{D}$-field F is one such that there is a sequence

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = K$$

such that each field F_{i+1} is either finite algebraic over F_i, or generated by an antiderivative or exponential of an antiderivative of an element of F_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 v has a pole in U with nonzero residue, then there will not be an antiderivative of v defined on all of U, but there will be one on any simply connected subset of U which avoids the poles of v.

Consider the extension F_i/F_{i-1}; there are three possibilities for $\mathrm{DGal}(F_i/F_{i-1})$ depending on how the extension is generated:

(i) If F_i/F_{i-1} is generated by a finite algebraic element, then $\mathrm{DGal}(F_i/F_{i-1})$ is finite.

(ii) If F_i/F_{i-1} is generated by an antiderivative of an element $\alpha \in F_{i-1}$, then we can think of F_i as the splitting field of the linear operator $L(u) = u' - \alpha$. In particular, the solution we use to generate F_i is defined only up to addition of a constant in $\mathbb{C}$. Since $\mathrm{DGal}(F_i/F_{i-1})$ must permute the solutions of $L(u) = 0$, we see that $\mathrm{DGal}(F_i/F_{i-1}) \simeq \mathbb{C}$ (since $\mathbb{C}$ has no algebraic subgroups).

(iii) If F_i/F_{i-1} is generated by the exponential of an antiderivative of an element $\alpha \in F_{i-1}$, then we can think of F_i as the splitting field of the linear operator $L(u) = u' - \alpha u$. In particular, the solution we use to generate F_i is defined only up to multiplication by a constant in $\mathbb{C}^*$, and so $\mathrm{DGal}(F_i/F_{i-1}) \simeq \mathbb{C}^*$ or $\mathrm{DGal}(F_i/F_{i-1})$ is cyclic of order n (corresponding to the algebraic subgroup of the nth roots of unity) and F_i/F_{i-1} is an algebraic extension by Proposition 4.6.

Example 7.2. Let $F \subset \mathcal{M}(U)$, where $U \subset \mathbb{C}$ is some simply connected open set. Parts (ii) and (iii) above show that if L is a first-order linear operator defined over F, then E_L/F is a Liouvillian extension. What can we say about second-order linear operators? The answer requires us to think more about first-order operators.

Suppose $L(u) = u' + \alpha u$ where $\alpha \in F$. Let $\beta \in E_L$ and let v be a solution to the *nonhomogeneous* equation $L(u) = \beta$. Solving for v first requires us to multiply both sides of the equation $v' + \alpha v = \beta$ by the integrating factor $w := \exp\left[\int \alpha\right]$. Note that w is contained in a Liouvillian extension of F.

This multiplication transforms our equation into $(vw)' = w\beta$. Integrating and dividing gives

$$v = \frac{1}{w} \int w\beta;$$

in particular, v is contained in a Liouvillian extension of F since w and β are.

We now have all we need to consider a second-order linear operator $L(u) = u'' + \alpha_1 u' + \alpha_0 u$ with $\alpha_0, \alpha_1 \in F$. Suppose v satisfies $L(v) = 0$ and let $K \subset E_L$ be the smallest $\mathcal{D}$-subfield which contains v and F. It need not be the case the K/F is a Liouvillian extension. However, we can show that E_L/K is a Liouvillian extension.

Let w be another, linearly independent, solution to $L(w) = 0$; then, up to a scalar multiple, we have

$$\mathrm{Wr}_L = \det \begin{pmatrix} v & w \\ v' & w' \end{pmatrix} = vw' - wv'.$$

This shows that w satisfies the first-order nonhomogeneous differential equation

$$w' - \frac{v'}{v} w = \frac{Wr_L}{v},$$

where W_L/v is contained in a Liouvillian extension of K. From what we saw above, this shows that E_L/K is a Liouvillian extension. It is worth noting that if K/F is a Liouvillian extension, then E_L/F will be a Liouvillian extension as well.

Proposition 7.3. *Any elementary function is contained in some Liouvillian extension of* $\mathbb{C}(t)$.

Proof. The difficulty is that the definition of a $\mathcal{D}$-field never mentioned compositions, like $e^{\sin t}$ or $\log\left(\sqrt{1-t^2}+1\right)$. But such compositions are contained in Liouvillian extensions. Indeed, any composition will be of the form e^u, $\log u$, or $\sin u$. Trigonometric functions are dealt with using Euler's formulas

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

The exponentials were explicitly included in the definition of Liouvillian extensions, and the logarithm is the antiderivative of u'/u. ∎

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

Proposition 7.4. *Let L be a linear differential operator with coefficients in a $\mathcal{D}$-field F, and let $G = \mathrm{DGal}(E_L/F)$. The $\mathcal{D}$-splitting field E_L is (contained in) a Liouvillian extension if and only if G_0, the connected component of the identity in G, is solvable.*

Proof. See Sections 25, 26, and 27 of [**4**]. ∎

8. SOLUTIONS OF EQUATIONS (??) AND (??). 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.

(ii) No solution of the differential equation $u' = t - u^2$ 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 (naturally isomorphic to) a subgroup of S_5. If $a \in \mathbb{C}$ is such that $f(a) = 0$, then, since f is irreducible, the field $\mathbb{Q}(a)$ is an extension of $\mathbb{Q}$ of degree five. Since $\mathbb{Q}(a) \subset E_f$, the degree of $E_f/\mathbb{Q}$ must be divisible by five. By Theorem 3.5, the order of $\mathrm{Gal}(E_f/\mathbb{Q})$ is divisible by five as well. By Cauchy's theorem, there is therefore an element of order five (or 5-cycle) in $\mathrm{Gal}(E_f/\mathbb{Q})$.

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. Up to this point, we have considered only *linear* differential operators and their solutions. In light of this, our results so far would seem to have little bearing on the solutions to the *nonlinear* equation $u' = t - u^2$. However, there is still hope: recall the *Airy* differential operator

$$L_A(u) = u'' - tu$$

from Example 5.7. It is certainly linear, and, since the function t has no poles, the splitting field E_{L_A} is a subfield of the meromorphic functions on $\mathbb{C}$, $\mathcal{M}(\mathbb{C})$.

Let $v \in E_{L_A}$ be any function such that $L_A(v) = 0$, and let $w = v'/v$ be the logarithmic derivative of v (this is necessarily in the field E_{L_A}). Then differentiation shows that

$$\begin{aligned} w' &= \frac{v \cdot v'' - [v']^2}{v^2} \\ &= \frac{t \cdot v^2 - [v']^2}{v^2}, \quad \text{since } v'' - tv = 0 \text{ by assumption,} \\ &= t - w^2; \end{aligned}$$

that is, w is a solution to $u' = t - u^2$! Moreover, we can reverse this process to see that if w is *any* function such that $w' = t - w^2$, then $v = \exp\left[\int w\right]$ satisfies $L_A(v) = 0$. Thus, we have a way of relating solutions of $u' = t - u^2$ to solutions of the linear differential equation $L_A(u) = 0$.

$v'' = (e^{\int w} \cdot w)' = e^{\int w} \cdot w^2 + e^{\int w} \cdot w'$
$= v w^2 + v \cdot w'$
$= (w^2 + w')/v = rv$

Theorem 8.1. *We have that* $G = \mathrm{DGal}(E_{L_A}/\mathbb{C}(t)) = \mathrm{SL}_2(\mathbb{C})$.

Proof. In Example 5.7, we found that $G \subset \mathrm{SL}_2(\mathbb{C})$. To prove equality, let G_0 be the connected component of the identity. Then G/G_0 is finite by Theorem 4.4.

Since $\mathrm{SL}_2(\mathbb{C})$ is 3-dimensional, there are very few proper connected subgroups. In particular, they are all conjugate to one of the following four:

(i) $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$,

(ii) $\left\{ \begin{bmatrix} a & 0 \\ 0 & 1/a \end{bmatrix} : a \in \mathbb{C}^* \right\}$,

(iiii) $\left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{C} \right\}$, or

(iv) $\left\{ \begin{bmatrix} a & b \\ 0 & 1/a \end{bmatrix} : a \in \mathbb{C}^*, b \in \mathbb{C} \right\}$.

Note that for each of these groups, $(1\ 0)^t$ is a common eigenvector. Thus, if G_0 were a proper subgroup of $\mathrm{SL}_2(\mathbb{C})$, then all elements of G_0 would have a common eigenvector $v \in E_{L_A}$ which satisfies $L_A(v) = 0$.

Since differentiation commutes with the action of G on E_{L_A}, we then see that $w = v'/v$ is left fixed by G_0. Thus, the Picard-Vessiot extension generated by w is a $\mathcal{D}$-subfield, M say, of E_{L_A} and $G_0 \subset \mathrm{DGal}(E_L/M)$ (because G_0 fixes w). In particular, we can apply the Fundamental Theorem of Differential Galois Theory (Theorem 4.9) so that $\mathrm{DGal}(M/\mathbb{C}(t)) \simeq G/\mathrm{DGal}(E_L/M)$ is a quotient of G by a group containing G_0; hence, $\mathrm{DGal}(M/\mathbb{C}(t))$ is finite, so that w is an algebraic function by Proposition 4.6 (and so has finitely many poles).

However, as we saw above, $w' = t - w^2$ since w is the logarithmic derivative of the solution v of $L_A(u) = 0$. For any number $t_0 < -1 - \pi/2$, the solution w with $w(t_0) = 0$ 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, w has at least as many poles as $\tan(t)$, which has infinitely many poles. Hence w is not algebraic and our guess that $G_0 \neq \mathrm{SL}_2(\mathbb{C})$ is false. ∎

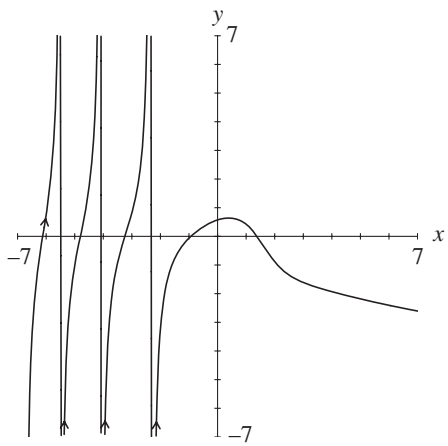

Figure 1. Solutions to $w'(t) = t - w^2$.

Corollary 8.2. *No nonzero solution of the Airy equation belongs to a Liouvillian extension of* $\mathbb{C}(t)$.

Proof. By Proposition 7.4, if one nonzero solution (and hence all solutions by Example 7.2) of the Airy equation belonged to a Liouvillian extension, then $G_0 = \mathrm{SL}_2(\mathbb{C})$ would be solvable. Since solvability is preserved by quotients (this is an exercise using the definition and the isomorphism theorems for groups), we would also have that $\mathrm{PSL}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})/\{\pm \mathrm{Id}\}$ would be solvable. By Theorem 8.4 of [**6**], $\mathrm{PSL}_2(\mathbb{C})$ is simple. Thus, $\mathrm{PSL}_2(\mathbb{C})$ is solvable only if it is abelian. One can easily check that this is not the case. ∎

We have (finally!) reached our second goal:

Corollary 8.3. *The differential equation* $u' = t - u^2$ *has no solutions which belong to a Liouvillian extension of* $\mathbb{C}(t)$.

Proof. Suppose v is such a solution. Then $\exp\left[\int v(t)\,dt\right]$ is contained in a Liouvillian extension of $\mathbb{C}(t)$ and satisfies the Airy equation. This contradicts the previous corollary. ∎

REFERENCES

1. D. Dummit and R. Foote, *Abstract Algebra*, 3rd ed., John Wiley, Hoboken, NJ, 2004.
2. J. Hubbard and B. West, *Differential Equations: A Dynamical Systems Approach*, Texts in Applied Mathematics, vol. 5, Springer-Verlag, New York, 1995; corrected reprint of the 1991 edition.
3. J. Humphreys, *Linear Algebraic Groups*, Graduate Texts in Mathematics, vol. 21, Springer-Verlag, New York, 1975.
4. E. Kolchin, Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations, *Ann. of Math. (2)* **49** (1948) 1–42. doi:10.2307/1969111
5. ———, *Differential Algebra and Algebraic Groups*, Pure and Applied Mathematics, vol. 54, Academic Press, New York, 1973.
6. S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
7. A. Magid, *Lectures on Differential Galois Theory*, University Lecture Series, vol. 7, American Mathematical Society, Providence, RI, 1994.
8. ———, Differential Galois theory, *Notices Amer. Math. Soc.* **46** (1999) 1041–1049.

9. J. Ritt, *Differential Algebra*, American Mathematical Society Colloquium Publications, vol. XXXIII, American Mathematical Society, New York, 1950.
10. M. van der Put and M. Singer, *Galois Theory of Linear Differential Equations*, Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), vol. 328, Springer-Verlag, Berlin, 2003.

JOHN H. HUBBARD received his undergraduate degree from Harvard University and his doctorate from the Université de Paris-Sud. He is currently a professor at Cornell University and the Université de Provence. His research interests lie in differential equations and complex dynamics.
Department of Mathematics, Cornell University, Ithaca, NY 14850
jhh8@cornell.edu

BENJAMIN E. LUNDELL received his undergraduate degree from the University of Illinois at Urbana-Champaign and a Certificate of Advanced Study in Mathematics from Cambridge University. He is currently a doctoral candidate at Cornell University studying number theory and arithmetic geometry.
Department of Mathematics, Cornell University, Ithaca, NY, 14850
blundell@math.cornell.edu