DIFFERENTIAL GALOIS THEORY: PROVING ANTIDERIVATIVES AREN'T ELEMENTARY

ARUN DEBRAY AND ROK GREGORIC

AUGUST 9, 2019

TODO: standard blurb

0. Overview

Every year we tell our calculus students that the Gaussian e^{-x^2} has no elementary antiderivative. It's striking and accessible. But the proof is not well known, even though it's absolutely within reach of graduate students. The two of us were interested in learning the proof (and a few other things related to differential algebra); the lecture notes are currently Arun's notes (in progress!) for his talks, leading to a proof of Liouville's theorem, following Hubbard-Lundell (http://pi.math.cornell.edu/~hubbard/diffalg1.pdf), and Arun's live-TEXed notes from Rok's talks. Please let us know if you find any mistakes or typos.

1. Lightning review of Galois theory

Our first goal is to prove that functions such as e^{-x^2} have no elementary antiderivatives; we may more generally consider elementary solutions to differential equations. The proof follows a similar line of reasoning as in Galois theory: study the group of symmetries of a minimal field containing solutions to the equations, and prove that only certain symmetry groups can arise if we want elementary functions. If it's been a while since you've seen Galois theory, you are in good company, so let's begin with a quick review.

Galois theory studies the symmetries of polynomials over fields. It works in great generality, but to simplify the exposition we will assume the base field k has characteristic zero.

Definition 1.1. A *(field) extension* is a map of fields $j\colon k \hookrightarrow L$ (i.e. a ring homomorphism, where L is also a field). Such a map is necessarily injective.

For now, assume for simplicity that this is a *finite* field extension, meaning j makes L into a finite-dimensional k-vector space.

Definition 1.2. A *splitting field* for a collection of polynomials $S \subset k[x]$ is a field extension $k \hookrightarrow L$ such that all $f \in S$ factor completely (i.e. into linear functions), and that L is minimal with respect to this property. A *normal extension* is one isomorphic to the splitting field of some collection of polynomials.

The idea is that a splitting field of f is the minimal field containing all of the roots of f. Abstractly, splitting fields exist and are unique up to unique isomorphism, but you could also just always work inside $\mathbb{C}$.

Example 1.3. If $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, then $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of f: the other two roots of unity are $e^{\pm 2\pi i/3}\sqrt[3]{2}$. Therefore the splitting field of f is $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. ◀

(Finite) normal extensions are examples of *Galois extensions*; in our setting these are synonymous, but not in characteristic p. In this case, the group of symmetries is nice.

Definition 1.4. If $j\colon k \hookrightarrow L$ is a Galois extension, its *Galois group* $\mathrm{Gal}(L/k)$ is the group of automorphisms of L (as a field) which fix k.

The Galois group of the splitting field of $f \in k[x]$ permutes the roots of f, and in fact is a subgroup of $S_{\deg f}$

For example, for $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$, the Galois group is S_3: complex conjugation swaps the two complex roots, giving us a transposition, and we get the 3-cycle from the automorphism

$$a + b\sqrt[3]{2} + ce^{2\pi i/3}\sqrt[3]{2} \longmapsto a + e^{2\pi i/3}\Big(b\sqrt[3]{2} + ce^{2\pi i/3}\sqrt[3]{2}\Big). \tag{1.5}$$

The idea of a Galois group leads quickly to two important theorems.

Given a group G, let $\mathcal{L}(G)$ denote its poset of subgroups, ordered by inclusion Given a field extension $k \hookrightarrow L$, let $\mathrm{Ext}(L/k)$ denote the poset of subextensions of $k \hookrightarrow L$; this is a poset, ordered by inclusion. If $k \hookrightarrow L$ is Galois, then given a subgroup $H \le \mathrm{Gal}(L/k)$, let L^H denote the subfield fixed by the action of H.

Theorem 1.6 (Fundamental theorem of Galois theory)**.** *Let $k \hookrightarrow L$ be a Galois extension. The assignments*

$$\begin{aligned} \mathcal{L}(\mathrm{Gal}(L/k))^{\mathrm{op}} &\longrightarrow \mathrm{Ext}(L/k) \\ H &\longmapsto L^H \end{aligned} \tag{1.7a}$$

and

$$\begin{aligned} \mathrm{Ext}(L/k)^{\mathrm{op}} &\longrightarrow \mathcal{L}(\mathrm{Gal}(L/k)) \\ L' &\longmapsto \mathrm{Aut}(L'/k) \end{aligned} \tag{1.7b}$$

define an order-reversing isomorphism of posets. Moreover, the degrees match: $\dim_{L^H} L = |H|$ and $\dim_k L^H = |\mathrm{Gal}(L/k)|/|H|$. $k \hookrightarrow L^H$ is Galois iff $H \trianglelefteq \mathrm{Gal}(L/k)$; in this case, $\mathrm{Gal}(L^H/k) \cong \mathrm{Gal}(L/k)/H$.

But our immediate focus is a different theorem.

Definition 1.8. Let $\mathbb{Q} \hookrightarrow L$ be a field extension. An $x \in L$ is *solvable by radicals* if:

- $x \in \mathbb{Q}$,
- x is the sum, product, difference, or quotient of two numbers solvable by radicals, or
- x is the n^{th} power or n^{th} root of a number solvable by radicals.

A polynomial $f \in \mathbb{Q}[x]$ is *solvable by radicals* if its roots are, where L is its splitting field.

So the quadratic formula, cubic formula, and quartic formula show all polynomials of degree at most four are solvable by radicals.

Theorem 1.9 (Abel-Ruffini)**.** *$f \in \mathbb{Q}[x]$ is solvable by radicals if and only if the Galois group of its splitting field is solvable. In particular, for $d \ge 1$, there are degree-d polynomials with Galois group S_d; hence, for $d \ge 5$, there exist degree-d polynomials not solvable by radicals.*

Recall that a finite group G has a Jordan-Hölder composition series $1 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$, where the quotients G_i/G_{i-1} are simple groups (i.e. they have no nontrivial normal subgroups). We say G is *solvable* if said quotients are all abelian.

How does the proof of the Abel-Ruffini theorem go? The vague basic idea is: both solvability by radicals and solvability of the Galois group are describing your splitting field as an iterated sequence of particularly nice field extensions. Specifically, adjoining an n^{th} root of some element of your field is an *abelian extension*, i.e. $\mathrm{Aut}(k(\sqrt[n]{a})/k)$ is abelian, and, using Theorem 1.6, if the Galois group of $k \hookrightarrow L$ is solvable, the Jordan-Hölder decomposition describes it as a composition of abelian extensions.

2. Basics of differential algebra

TODO: what I said about the discriminant later is wrong. Also, at various points I assume L is linear.

To discuss differential equations we need derivatives.

Definition 2.1. A *differential field* is a field k together with a *derivation* $\delta\colon k \to k$, i.e. a k-linear map satisfying the *Leibniz rule* $\delta(fg) = f\delta(g) = \delta(f)g$. The *constants* in k are those elements with $\delta(k) = 0$; these form a subfield.

So any field of functions with the usual derivative works. We will think of $\mathbb{C}(t)$ as our "base field," analogous to $\mathbb{Q}$ in Galois theory. Another good example is the field $\mathcal{M}(U)$ of meromorphic functions on some connected open set $U \subset \mathbb{C}$: the existence and uniqueness theorem for ODEs tells us that any system of differential equations has a solution in $\mathcal{M}(U)$ for some U. This will play the role that $\mathbb{C}$ did in Galois theory, sidestepping a lot of existence and uniqueness questions at once. In fact, given a differential operator L acting on $\mathbb{C}(t)$, let $U_L \subset \mathbb{C}$ denote the maximal open subset on which $Lu = 0$ has solutions.

In the rest of this section and the next, k is a differential field containing $\mathbb{C}(t)$ and contained in $\mathcal{M}(U)$ for some U.

Definition 2.2. Let L be a differential operator on k. The *(differential) splitting field* for L, denoted E_L, is the smallest subfield of $\mathcal{M}(U_L)$ containing k and the solutions of L.

Example 2.3. Consider the differential operator $L(u) \coloneqq u - u'$. Of course, the solutions to $Lu = 0$ are the functions $u(t) = Ce^t$. A general element of E_L is of the form

$$\frac{p_1(t)e^t + \cdots + p_m e^{mt}}{q_1(t)e^t + \cdots + q_n(t)e^{nt}}. \tag{2.4}$$

That is, it's "rational functions" in the solutions of L and their derivatives. For intuition, think of this as $\mathbb{C}(t)$ adjoin e^t in the sense of a differential field. ⋖

Recall that the *transcendence degree* of a field extension $k \hookrightarrow L$ is the maximal cardinality of an algebraically independent subset of L.

Lemma 2.5. *The extension $k \hookrightarrow E_L$ has finite transcendence degree.*

Proof. If L is an n^{th}-order differential operator, then $\{u, u', \dots, u^{(n-1)}\}$ contains a transcendence basis for E_L over k. ⊠

We will now construct a canonical subfield of E_L using the Wronskian.

Definition 2.6. Fix a differential operator L, which is *a priori* a higher-order operator, and rewrite it if necessary to a system of first-order operators $W' = A(t)W$, where A and W are matrices which may depend on time. Let $W(t)$ be the particular solution with $W(0) = I$. Then the *Wronskian* of L is $\mathrm{Wr}_L(t) \coloneqq \det(W(t)) \in E_L$.

Proposition 2.7. $\mathrm{Wr}'_L(t) = \mathrm{tr}(A(t))\mathrm{Wr}_L(t)$.

Proof. First assume constant coefficients, i.e. that $A(t) = A \coloneqq A(0)$. The solution to $W' = AW$ is of the form $W(t) = e^{At}$, and $\det(e^{At}) = e^{\mathrm{tr}(At)} = e^{t\,\mathrm{tr}(A)}$.

If $A(t)$ does depend on time, you can "freeze" $A(t)$ at a given time t_0, i.e. run the above argument with constant coefficients $A = A(t_0)$. Thus the theorem is true at time t_0, and of course t_0 is arbitrary. ⊠

One upshot is that the Wronskian can always be expressed in terms of elementary functions (as antiderivatives of rational functions are elementary, and then we exponentiate).

Therefore we may consider the minimal differential subfield of E_L containing $\mathbb{C}(t)$ and Wr_L; call this $K(\mathrm{Wr}_L)$. This will be useful when we think about differential Galois groups (next).

The Wronskian plays the role in differential Galois theory that the discriminant plays in ordinary Galois theory.

3. Differential Galois groups

Now let's define differential Galois groups. The major conclusion of this section are that this is a linear (i.e. affine) algebraic group. As before, k is a differential field containing $\mathbb{C}(t)$ and contained in $\mathcal{M}(U)$ for some $U \subset \mathbb{C}$.

By an automorphism of a differential field we mean a field automorphism which commutes with the derivation.

Definition 3.1. The *(differential) Galois group* of an extension of differential fields $k \hookrightarrow F$ is the group $\mathrm{Gal}(F/k)$ of differential field automorphisms of F which fix k.

Typically F is the splitting field of a differential operator on k. In this case, the elements of the Galois group permute the solutions to $Lu = 0$, so if V_L denotes the vector space of solutions to $Lu = 0$, then $\mathrm{Gal}(E_L/k) \leq \mathrm{GL}(V_L)$.

Example 3.2. Consider $L(u) = u' - u$. An element of $\mathrm{Gal}(E_L/\mathbb{C}(t))$ must send $e^t \mapsto e^{Ct}$ for some $C \in \mathbb{C}^\times$ – and the choice of C determines the automorphism (recall that a general element of E_L has the form (2.4)). Thus $\mathrm{Gal}(E_L/\mathbb{C}(t)) \cong \mathbb{C}^\times$. ⋖

This is a lot bigger than the groups we encountered in Galois theory!

Theorem 3.3. $\mathrm{Gal}(E_L/k)$ *is in fact an algebraic subgroup of* $\mathrm{GL}(V_L)$*; in particular it has finitely many connected components.*

Here by "an algebraic subgroup" we mean that it's cut out by finitely many algebraic equations. The rest of the theorem follows simply because it's an affine variety.

Proof. Let ℓ be the order of L, and choose $\{f_1, \dots, f_\ell\}$ a basis of V_L. This sits inside E_L, and the set $\{f_i^{(j)} \mid 1 \le i, j \le \ell\}$ contains a transcendence basis for E_L over k.

Introduce ℓ^2 formal variables x_{ij}, $1 \le i, j \le \ell$, and consider the ring homomorphism

$$\begin{aligned} K[X] := K[x_{ij} \mid 1 \le i, j \le \ell] &\xrightarrow{\Phi} \mathcal{M}(U_L) \\ x_{ij} &\longmapsto f_i^{(j)}. \end{aligned} \tag{3.4}$$

Hilbert's basis theorem says $K[X]$ is Noetherian, so $\ker(\Phi)$ is finitely generated. Let $P_1, \dots, P_m$ be a generating set. Intuitively, we've started with a bunch of abstract functions and imposed on them the relations that they satisfy as solutions to $Lu = 0$; $\ker(\Phi)$ contains those relations.

Our choice of a basis of V_L identifies $\mathrm{GL}(V_L) \cong \mathrm{GL}_\ell(\mathbb{C})$; explicitly, the $\ell \times \ell$ matrix $A = (a_{ij})$ acts by

$$f_i \longmapsto \sum_j a_{ij} f_j. \tag{3.5}$$

Inside $\mathrm{GL}(V_L)$, $\mathrm{Gal}(E_L/k)$ is precisely the subgroup of elements that send solutions to solutions. Formally, this is the same as specifying

$$P_a\left(\sum_j a_{j1} X_j^0, \dots, \sum_j a_{jk} X_j^{k-1}\right) = 0 \tag{3.6}$$

for $1 \le a \le m$, which is a finite set of polynomials in the variables a_{jk}. ⊠

Proposition 3.7. $\mathrm{Gal}(E_L/k)$ *is finite iff the solutions to* $Lu = 0$ *are algebraic functions over* k.

Proof. If the solutions are algebraic, then we can construct E_L from k by adjoining finitely many algebraic elements, so we're in a finite extension, hence must have finite Galois group, let alone differential Galois group. Conversely, suppose $\mathrm{Gal}(E_L/k)$ is finite. Then, $f \in E_L$ satisfies the polynomial

$$\prod_{\sigma \in \mathrm{Gal}(E_L/k)} (x - \sigma(f)) = 0. \tag{3.8}$$

⊠

Finally, we'll need the following lemma later.

Lemma 3.9. $\mathrm{Gal}(E_L/L(\mathrm{Wr}_L)) = \mathrm{Gal}(E_L/K) \cap \mathrm{SL}(V_L)$. *In particular, if* $\mathrm{Wr}_L \in \mathbb{C}(t)$, *then* $\mathrm{Gal}(E_L/\mathbb{C}(t)) \subset \mathrm{SL}(V_L)$.

Proof. If $\tau \in \mathrm{GL}(V_L)$, then τ acts on Wr_L by multiplication by $\det \tau$. ⊠

This is analogous to the following fact from Galois theory: the Galois group of a degree-n irreducible polynomial f is manifestly a subgroup of S_n in that it permutes the roots of f. It lies within $A_n \le S_n$ iff the discriminant of f is the square of a rational number. This fact is often useful in practice for computing Galois groups, and the analogous fact about the Wronskian in differential Galois theory is also true.

4. Liouville's theorem

Definition 4.1. An extension $k \hookrightarrow L$ of differential fields is *Liouvillian* if it factors as a sequence $k = L_0 \hookrightarrow L_1 \hookrightarrow \cdots \hookrightarrow L_n = L$ such that each iterate $L_i \hookrightarrow L_{i+1}$ is one of

(1) a finite extension;[1]
(2) adjoining an antiderivative of some $f \in L_i$, i.e. a splitting field for the operator $D(u) = u' - f$; or
(3) adjoining the exponential of an antiderivative of f, i.e. a splitting field for the operator $D(u) = u' - fu$.

We're thinking of differential extensions of $\mathbb{C}(t)$ as contained inside $\mathcal{M}(U)$ for some U. Sometimes one has to restrict to functions on some $U' \subset U$ because of branch cuts: if f has a pole at some $z \in U$ with nonzero residue, it can only have an antiderivative on simply connected subsets of $U \setminus z$.

Proposition 4.2. *Every elementary function* f *is contained in some Liouvillian extension of* $\mathbb{C}(t)$ *(which may depend on* f*).*

[1] By this I mean a finite extension of ordinary fields that's also a differential field extension. I don't know if this is standard notation in differential algebra.

Proof. What makes this interesting is composition. Let's induct on the "length" of an elementary function f, i.e. the number of symbols needed to define it. The base cases are rational functions and exponentials, which we have by definition. A general f is of one of the following forms.

(1) A sum, product, difference, or quotient of functions which have smaller length, hence contained in a Liouvillian extension by the inductive assumption.
(2) $f = e^g$ where g is elementary of smaller length, which we get from the definition of a Liouvillian extension.
(3) $f = \ln(g)$ where g is elementary of smaller length, which we get by adjoining the antiderivative of g'/g.
(4) $f = \sin(g)$ where g is elementary of smaller length, which we get with Euler's identity $2i\sin(t) = e^{it} - e^{-it}$. ⊠

Here's the analogue of (one part of) the Abel-Ruffini theorem.

Theorem 4.3. *Let k be a differential field containing $\mathbb{C}(t)$ and contained in $\mathcal{M}(U)$ for some $U \subset \mathbb{C}$, and let L be a differential operator on k. If $k \hookrightarrow E_L$ is contained in a Liouvillian extension, then $G := \mathrm{Gal}(E_L/k)$ has a sequence of subgroups*

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G, \tag{4.4}$$

such that each G_j/G_{j+1} is either finite, isomorphic to $\mathbb{C}$, or isomorphic to $\mathbb{C}^\times$.

Our proof leans on the fundamental theorem of differential Galois theory, which you will hear about later this week.

Proof. Using the Liouvillian hypothesis, we have a sequence $k = L_0 \hookrightarrow L_1 \hookrightarrow \cdots \hookrightarrow L_n \supset E_L$ of differential field extensions, where each successive extension is either finite, adjoining an antiderivative, or adjoining the exponential of an antiderivative. These correspond to the three cases finite quotient, $\mathbb{C}$ quotient, $\mathbb{C}^\times$ quotient, respectively.

Without loss of generality we can assume $L_n = E_L$; $\mathrm{Gal}(E_L/k)$ is an algebraic subgroup of $\mathrm{Gal}(L_n/k)$,[2] so when we compute the intersections of the groups in (4.4) with $\mathrm{Gal}(E_L/k)$, we'll end up asking about algebraic subgroups of finite groups, of $\mathbb{C}$, or of $\mathbb{C}^\times$, and these are again finite, $\mathbb{C}$, or $\mathbb{C}^\times$.

Now you can probably see where this is going: $G_j := \mathrm{Gal}(L_j/k)$, and $G_j/G_{j+1} \cong \mathrm{Gal}(L_{j+1}/L_j)$. Normality follows from the fundamental theorem of differential Galois theory.

Now the three cases.

(1) The differential Galois group of a finite extension is finite; this follows from ordinary Galois theory.
(2) Suppose we're adjoining an antiderivative F of f. All other antiderivatives of F are of the form $F = f + C$, and $\mathbb{C}$ acts by addition on the constant.
(3) Suppose we're adjoining the exponential of an antiderivative F of f, generalizing Example 2.3. Then the other solutions to the same differential equation are e^{CF} for all $C \in \mathbb{C}^\times$, so we add these and nothing more (and then take the smallest differential field containing those and L_j). Then the Galois group is $\mathbb{C}^\times$, acting by multiplication on the constant. ⊠

Now let's use this.

Definition 4.5. The *Airy equation* is the second-order differential equation

$$u''(t) - tu(t) = 0. \tag{4.6}$$

Its space of solutions is two-dimensional; the standard basis is $\{\mathrm{Ai}(t), \mathrm{Bi}(t)\}$, where $\mathrm{Ai}(t)$ is the solution with $\mathrm{Ai}(0) = 1/(3^{2/3}\Gamma(2/3))$ and $\mathrm{Ai}'(0) = -1/(3^{1/3}\Gamma(1/3))$ and $\mathrm{Bi}(t)$ is the solution with $\mathrm{Bi}(0) = 1/(3^{1/6}\Gamma(2/3))$ and $\mathrm{Bi}'(0) = 3^{1/6}/\Gamma(2/3)$. $\mathrm{Ai}(x)$ is called the *Airy function (of the first kind)* and $\mathrm{Bi}(x)$ the *Airy function of the second kind.*

[2] We didn't prove this; it's part of the fundamental theorem for differential Galois theory, and proceeds in a similar way to Theorem 3.3.

Remark 4.7. Here are some non-closed-form expressions for the Airy functions, at least on $\mathbb{R}$:

$$\begin{aligned}\operatorname{Ai}(x) &= \frac{1}{\pi}\int_0^\infty \cos\left(\frac{t^3}{3} + xt\right) \mathrm{d}t \\ \operatorname{Bi}(x) &= \frac{1}{\pi}\int_0^\infty \left(\exp\left(-\frac{t^3}{3} + xt\right) + \sin\left(\frac{t^3}{3} + xt\right)\right) \mathrm{d}t.\end{aligned} \tag{4.8}$$

$\blacktriangleleft$

We will prove that these functions (in fact, all nonzero solutions to the Airy equation) are not elementary, first by calculating the differential Galois group of the Airy equation, then showing it doesn't factor as in Theorem 4.3.

Proposition 4.9. *If E_L denotes the splitting field of the Airy equation,* $\operatorname{Gal}(E_L/\mathbb{C}(t)) \cong \mathrm{SL}_2(\mathbb{C})$.

Proof. Since L is second-order (or: there's a two-dimensional space of solutions), $G \coloneqq \operatorname{Gal}(E_L/\mathbb{C}(t)) \le \mathrm{GL}_2(\mathbb{C})$. Let's compute the Wronskian. Proposition 2.7 implies that (this is true in general)

$$\operatorname{Wr}_L(t) = \exp \int_{t_0}^{t} \operatorname{tr} A(s)\,\mathrm{d}s. \tag{4.10}$$

In our setting, let $v = u'$, so that the Airy equation is equal to the system

$$\begin{aligned} u' &= v \\ v' &= tu, \end{aligned} \tag{4.11}$$

so

$$A(t) = \begin{pmatrix} 0 & 1 \\ t & 0 \end{pmatrix}, \tag{4.12}$$

which is traceless. By (4.10), $\operatorname{Wr}_L = 1$, so $G \le \mathrm{SL}_2(\mathbb{C})$.

Let G_0 be the connected component of the identity of G, so that $G/G_0 = \pi_0 G$ is finite, and assume that $G_0 \ne \mathrm{SL}_2(\mathbb{C})$. There are not many proper connected algebraic subgroups of $\mathrm{SL}_2(\mathbb{C})$; in fact, up to conjugation, our options are:

- the trivial subgroup $\{1\}$;
- the (standard) maximal torus
  $$T \coloneqq \left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} : a \in \mathbb{C}^\times \right\}, \tag{4.13}$$
  which is a $\mathbb{C}^\times$;
- the (standard) nilpotent subgroup[3]
  $$N \coloneqq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{C} \right\}, \tag{4.14}$$
  which is a $\mathbb{C}$; and
- the (standard) Borel subgroup
  $$B \coloneqq \left\{ \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} : a \in \mathbb{C}^\times, b \in \mathbb{C} \right\}. \tag{4.15}$$

So G_0 is one of these. These act on V_L through the defining representation of $\mathrm{SL}_2(\mathbb{C})$; in these representations, all four of these groups have a common eigenvector. That is, for $G_0 \in \{\{1\}, T, N, B\}$, there is some $u \in V_L$ such that $Au = \lambda(A)u$ for all $A \in G_0$ and some $\lambda(A) \in \mathbb{C}$ (which can depend on A).

In particular, $v \coloneqq u'/u$ is fixed by G_0, and therefore the differential Galois extension generated by $\mathbb{C}(t)$ and v is a subfield $M \subset E_L$; the fundamental theorem of differential Galois theory tells us that $\operatorname{Gal}(M/\mathbb{C}(t))$ is a quotient of G by a group containing G_0. Thus $\operatorname{Gal}(M/\mathbb{C}(t))$ is finite, so by Proposition 3.7 v is algebraic.

However, we can prove by hand that v isn't algebraic. Applying the quotient rule to $v = u'/u$,

$$v'(t) = t - v(t)^2, \tag{4.16}$$

which is called the *Riccati equation*. Any solution to this equation has infinitely many poles: fix a point $t_0 < -1/\pi/2$ and consider the specific solution with $v(t_0) = 0$. Then $v(t) > \tan(t + t_0)$ for $t \in (t_0, t_0 + \pi/2)$

[3] I think, at least.

and $v(t) < \tan(t + t_0)$ for $t \in (t_0 - \pi/2, 0)$; continuing in this way, we get at least as many poles as $\tan(t)$. Thus, v isn't algebraic, so $G_0 = \mathrm{SL}_2(\mathbb{C})$, and therefore $G = \mathrm{SL}_2(\mathbb{C})$. ⊠

Proposition 4.17. *There is no chain of subgroups of* $\mathrm{SL}_2(\mathbb{C})$ *satisfying Theorem 4.3.*

Proof. It suffices to prove that $\mathrm{SL}_2(\mathbb{C})$ has no proper connected normal subgroup with finite or abelian quotient, and $\mathrm{SL}_2(\mathbb{C})$ is simple, so we're done. ⊠

Corollary 4.18. *The Airy functions are not elementary.*

Remark 4.19. This approach does not work for showing that antiderivatives of elementary functions aren't elementary, as adjoining an antiderivative is an example of a Liouvillian extension. We will (probably) be able to discuss the case $f(x)e^{g(x)}$, f and g rational, using a related but different method (TODO: fill this bit in), by reducing it to an algebraic question: $f(x)e^{g(x)}$ has an elementary antiderivative iff there is a rational function h with $f = h' + hg$. This kills, for example, $g(x) = \pm x^2$.

For other functions, such as $(\sin x)/x$ or x^x, the same broad ideas apply but the details are different. ◀

5. Integration in elementary terms

Now let's focus specifically on integration. Now we need something different than a Liouvillian extension.

Definition 5.1. Call an extension of differential fields $k \hookrightarrow L$ *elementary* if it factors as

$$k = L_0 \hookrightarrow L_1 \hookrightarrow \cdots \hookrightarrow L_n = L \tag{5.2}$$

such that each intermediate extension $L_i \hookrightarrow L_{i+1}$ is either

- finite,
- *adjoining a logarithm* of f (i.e. taking the splitting field of $D(u) = u' - f'/f$), or
- *adjoining an exponential* of f (i.e. taking the splitting field of $D(u) = f'u$).

Compare Definition 4.1, and note that the proof of Proposition 4.2 really yields the following, stronger result.

Proposition 5.3. *A function* $f \in \mathcal{M}(U)$ *is contained in an elementary extension of* $\mathbb{C}(t)$ *if and only if it's elementary (in the usual sense).*

As usual, k is a differential field containing $\mathbb{C}(t)$ and contained within some differential field $\mathcal{M}(U)$ of meromorphic functions.

Theorem 5.4 (Liouville). *Let* $\alpha \in k$. *Then* α *has a primitive in an elementary extension*[4] *of* k *if and only if there are constants* $c_1, \ldots, c_m \in \mathbb{C}$ *and functions* $\beta_1, \ldots, \beta_m, \gamma \in k$ *such that*

$$\alpha = \sum_{i=1}^{m} c_j \frac{\beta_j'}{\beta_j} + \gamma'. \tag{5.5}$$

Before we provide a proof (sketch), let's use this. First, we can simplify it in the case of exponentials.

Corollary 5.6 (Liouville). *Let* $g \in k$ *be such that* e^g *is transcendental over* k, *and let* $f \in k$. *Then* $fe^g \in k(e^g)$ *has a primitive in an elementary extension iff there is some* $h \in k$ *such that* $f = h' + hg'$.

Proof sketch. Let's get the reverse direction out of the way: $(he^g)' = fe^g$.

Going forward, use Theorem 5.4 to write

$$fe^g = \sum_{i=1}^{m} c_j \frac{\beta_j'}{\beta_j} + \gamma', \tag{5.7}$$

where β_j, γ are elements of $k(e^g)$ and $c_j \in \mathbb{C}$. We may assume without loss of generality that each β_j is either in k or is a nonconstant monic irreducible polynomial in e^g.[5] Now γ is a rational function in e^g. Then, e^g is the only possible monic irreducible factor in the denominator of a partial fraction expression for γ: TODO.

Moreover, e^g is the only monic irreducible in $k[e^g] \setminus k$ that can occur as a β_j: TODO.

[4] We also want to specify that the field of constants remains the same.

[5] This is one of the reasons this says "proof sketch" and not "proof": there's a small argument to make here. But you can think of this as a kind of normalization.

Therefore $\beta'/\beta \in k$, not just $k(e^g)$, and we can write

$$\gamma = \sum_{j=-t}^{t} \alpha_j (e^g)^j \tag{5.8}$$

for some $\alpha_j \in k$. Hence (5.7) simplifies to

$$fe^g = c + \sum_{j=-t}^{t} \alpha_j'(e^g)^j + g' \sum_{j=-t}^{t} j\alpha_j(e^g)^j = \sum_{j=-t}^{t} (\alpha_j' + jg'\alpha_j)(e^g)^j. \tag{5.9}$$

Now compare the coefficients of the powers of e^g (here is where we need that it's transcendental over k), we have

$$f = \alpha_1' + \alpha_1 g'. \tag{5.10}$$

⊠

Great, now let's apply this to the Gaussian.

Corollary 5.11. *The functions $f(x) = e^{\pm x^2}$ have no elementary antiderivative.*

Proof. This is true iff there is an $a \in \mathbb{C}(x)$ with $1 = a' \pm 2ax$. We can directly compute that this differential equation has no rational solutions: let $a = p/q$, and without loss of generality assume p and q are relatively prime. Since

$$1 = \frac{qp' - q'p}{q^2} \pm \frac{2tp}{q}, \tag{5.12}$$

then $q \mp 2tp - p' = q'p/q$, i.e. $q \mid q'p$. Since $\mathbb{C}[t]$ is a Euclidean domain, we can choose $r, s \in \mathbb{C}[t]$ with $rq + sp = 1$, i.e. $rqq' + spq' = q'$. Since $q \mid q'p$, we see that $q \mid q'$, which forces q to be constant. And certainly $1 = a' \pm 2ax$ doesn't have a polynomial solution: the degrees don't match. ⊠

Remark 5.13. For other functions you might care about, such as $\sin(t)/t$, the approach is to produce a variant of Corollary 5.6, which is apparently neither trivial nor too hard. $\triangleleft$

Probably we won't have time to get to this, but here's how the general theorem is proven.

Proof sketch of Theorem 5.4. We can induct on the *length* of the elementary extension, i.e. the number of fields in (**??**); therefore the proof reduces to proving that if α can be expressed as in (5.5) with $\gamma, \beta_j \in k(\ell)$ (this notation used to denote the splitting field of some element ℓ), then it can also be expressed in this form (possibly with different m, c_j) with $\gamma, \beta_j \in k$.

There are three cases: ℓ can be algebraic, an exponential, or a logarithm. First, let's assume it's algebraic, which means $k[\ell] = k(\ell)$, and $\mathrm{Gal}(k(\ell)/k)$ is finite. Let $\mathrm{id} = \sigma_1, \dots, \sigma_m$ be the elements of $\mathrm{Gal}(k(\ell)/k)$ and $\ell_i := \sigma_i(\ell)$. If $q \in k[\ell]$ then $\sigma_i(q(\ell)) = q(\ell_i)$ and $\sigma_i(q'(\ell) = q'(\ell_i)$.

In particular, $\beta_j = \beta_j(\ell)$ and $\gamma = \gamma(\ell)$ are polynomials in ℓ. TODO: the notation is confusing: these derivatives are in $k[\ell]$, with respect to ℓ! Since σ_i fixes α,

$$\alpha = \sum_j \frac{\beta_j'(\ell_i)}{\beta_j(\ell_i)} + \gamma'(\ell_i). \tag{5.14}$$

Now average over $\mathrm{Gal}(k(\ell)/k)$:

$$\alpha = \sum_j \frac{c_j}{m} \left(\sum_i \frac{\beta_j'(\ell_i)}{\beta_j(\ell_i)} \right) + \frac{1}{s} \sum_{i=1}^{s} \gamma'(\ell_i) \tag{5.15a}$$

$$= \sum_j \frac{c_j}{s} \frac{\prod_i \beta_j'(\ell_i)}{\prod_i \beta_j(\ell_i)} + \frac{\mathrm{d}}{\mathrm{d}t} \left(\frac{1}{s} \sum \gamma(\ell_i) \right), \tag{5.15b}$$

which has the desired format.

TODO: for the remaining cases, prove the lemma (prop 4.3) because that's the bulk of it?

For the second case, assume ℓ is a logarithm, i.e. $\ell' = f'/f$, and assume ℓ is transcendental. Without loss of generality, we can normalize the expression (5.5) such that each $\beta_j \in k[\ell]$, and those which are in $k[\ell] \setminus k$ are monic and irreducible; we can also assume they're all distinct. Hence $\beta_j \nmid \beta_j'$, which actually forces $\beta_j \in k$! The idea is to prove that if $p \in k[\ell]$ is monic and irreducible, and $p \nmid p'$, then p cannot be any β_j. The idea is to study the partial fraction decomposition of the first term of (5.5) (i.e. with the β_j): it must contain only one term with a denominator including p, and the denominator is exactly p. Since α doesn't have p in the denominator, this has to be canceled by something in γ'...

Ok, so once $\beta_j \in k$, we only have to deal with γ. We have $\gamma' \in k$, ...

For the final case, assume ℓ is a transcendental exponent, and that (5.5) is normalized in the same sense... ☒

6. Differential Galois theory in a more general setting

This begins the part of the course that Rok taught. We'll begin by discussing what differential Galois theory is about, so let's first talk about what ordinary Galois theory is about. Tomorrow we'll cover the fundamental theorem of Galois theory, and discuss how differential Galois theory breaks down, and needs to be fixed, in characteristic p; this is related to interesting things about different notions of $\mathcal{D}$-modules.

Galois theory is about fields, or as Galois originally said it, about polynomials. Differential Galois theory is about differential fields, and/or about linear ordinary differential equations. Much of what we've discussed and will discuss today is due to Picard-Vessiot, in the last two decades of the 19th century, not coincidentally around the same time Emil Artin reformulated Galois theory in its modern form, about field extensions rather than just polynomials. Kolchin also did important work in the 1950s relating this to linear *partial* differential equations and integrable systems. More recently there's been work relating differential algebra to $\mathcal{D}$-modules.

Let k be a differential field, and call its derivation ∂. Let C be the field of constants, i.e. $\ker(\partial)$. It will be helpful to assume C is algebraically closed, and we do so. Let $\mathcal{D}$ denote the noncommutative k-algebra of differential operators generated by ∂, i.e. the subalgebra $\mathrm{End}_{\mathcal{V}ect_k}(k)$ consisting of polynomials in ∂ with coefficients in k. You can describe this explicitly as a noncommative k-algebra generated by ∂ modulo a relation.

Definition 6.1. A *$\mathcal{D}$-module* is a left module over $\mathcal{D}$, i.e. a k-vector space together with a k-linear map $\partial\colon M \to M$ such that if $f \in k$ and $s \in M$,

$$\partial(f \cdot s) = \partial(f) \cdot s + f \cdot \partial s. \tag{6.2}$$

We will always assume $\mathcal{D}$-modules are finite-dimensional over k.

Via Serre-Swan, you can think of M as some sort of vector bundle, and then the data and conditions ∂ are the same as specifying a connection.

Remark 6.3. Sometimes in algebraic geometry, people call more general objects $\mathcal{D}$-modules. ◀

Let $e_1, \dots, e_n$ be a k-basis for M. Then ∂ is equivalent to the coefficients $a_{ij} \in k$ in

$$\partial e_i = -\sum_{j=1}^{n} a_{ij} e_i. \tag{6.4}$$

This is a system of linear first-order ODEs over k,[6] and this is a useful perspective to have on $\mathcal{D}$-module. Indeed, if $y' = Ly$ is a (possibly higher-order) differential operator over k, with $L \in \mathcal{D}$, then we can define a $\mathcal{D}$-module $M \coloneqq \mathcal{D}/\mathcal{D} \cdot L$.

Remark 6.5. A possibly helpful analogy: $\mathcal{D}$ is like the ring of functions $\mathcal{O}_X$ on an affine variety X; if $f \in \mathcal{O}_X$, the zero set of f is the affine algebraic set corresponding to the ring $\mathcal{O}_X/\mathcal{O}_X \cdot f$. ◀

Definition 6.6. Given a $\mathcal{D}$-module M (or equivalently, a system of linear ODEs), the *Picard-Vessiot ring* of M is a differential (commutative) ring R such that

1. R is *simple* as a differential ring, i.e. its only differential ideals are 0 and R.[7]
2. If V denotes the kernel of the map $\partial\colon R \otimes_k M \to R \otimes_k M$, which we think of as "the space of solutions to the ODE defined by M," then $\dim_C V = \dim_k M$.
3. Fixing any k-basis $\{e_i\}$ of M and $v \in V \subset R \otimes_k M$, we can write $v = \sum_i v_i \otimes e_i$ for some $v_i \in R$. Then we ask for $\{v_i \mid 1 \le i \le n, v \in V\}$ to generate R as a k-algebra.[8]

[6] And, in the usual way, you can convert higher-order differential operators into systems of first-order linear differential operators and incorporate them into this perspective too.

[7] A *differential ideal* of a differential ring R is an ideal I of R such that $\partial I \subset I$.

[8] This condition corresponds to the fact from ODE that every linear system of ODEs has a *fundamental solution* $F \in \mathrm{GL}_n(k)$, which is a solution, and such that any solution y satisfies $y = Fy_0$ for some $y_0 \in C^n$.

This is not always a differential field, but it's as good as we can do in general: intuitively, because it's simple, it's very close to a field. This generalizes the notion of a splitting field of an ODE, in that we can recover that as the field of fractions of the Picard-Vessiot ring. Also, the way we've talked about this suggests some sort of existence and uniqueness up to suitable isomorphism; this is true, and not hard, but not immediate.

One can show that R has no zero divisors.

Definition 6.7. The *Picard-Vessiot field of M* is the field of fractions of R.

This recovers the splitting field that was discussed earlier.

Let's construct R. Begin with the ring $R_0 := k[x_{ij}, \det^{-1}]$, where $1 \le i, j \le n$ and $\det := \det(x_{ij})$. We can extend the differentiual ∂ from k by specifying

$$\partial(x_{ij}) = \sum_j a_{i\ell} x_{\ell j}, \tag{6.8}$$

where the $\mathcal{D}$-module M corresponds to the matrix-valued ODE $x' = Ax$. One can show that R is a differential local ring, meaning it has a unique maximal differential ideal $\mathfrak{m}$, and we define $R := R_0/\mathfrak{m}$.

Remark 6.9. You don't actually need to know that R_0 is local to check that R satisfies Definition 6.6 – any choice of maximal ideal $\mathfrak{m} \subset R$ will work. ◀

Definition 6.10. The *Galois group* of M, denoted $\mathrm{Gal}(R/k)$, is the group of differential k-algebra automorphisms of R.

If you used the Picard-Vessiot field instead of the Picard-Vessiot ring, what you get is canonically isomorphic to the group we defined.

The Galois group acts on the space of solutions: it acts on R, hence acts on $R \otimes_k M$, and its action intertwines ∂, so it therefore acts on $\ker(\partial) = V$. Thus we have an embedding $\mathrm{Gal}(R/k) \hookrightarrow \mathrm{GL}(V)$, and $\mathrm{GL}(V)$ is isomorphic to $\mathrm{GL}_n(C)$ (of course, choosing an isomorphism amounts to choosing a basis of solutions).

Remark 6.11. This is closely analogous to the case of a Galois extension of (non-differential) fields: if $k \hookrightarrow K$ is a Galois extension, so K is the splitting field of a polynomial f with zeros $x_1, \dots, x_n$, then $\mathrm{Gal}(K/k)$ permutes the zeros, hence comes with an embedding $G \hookrightarrow S_n$, where S_n is the symmetric group on n elements.

Another feature of the analogy is that $|\mathrm{Gal}(K/k)| = [K : k]$, which corresponds to the fact that for a Picard-Vessiot extension of differential fields, $\dim_C \mathrm{Gal}(L/k)$ is equal to the transcendence degree of L over k (in general, L is rarely algebraic). ◀

Remark 6.12. You can recover ordinary Galois theory from differential Galois theory as follows: if $k \hookrightarrow K$ is a finite Galois extension, where k is a differential field, then its derivation extends uniquely to K. You can prove this using the primitive element theorem: we can write $K = k(a)$ for some $a \in K$ with characteristic polynomial $f \in k[x]$, so $f(a) = 0$ and $f'(a) \neq 0$, and then define

$$\partial\left(\sum_i \lambda_i a^i\right) = \sum_i \partial(\lambda_i) a^i + \sum_i i\lambda_i a^{i-1} \partial a. \tag{6.13}$$

TODO: what is ∂a? ◀

Next, we'd like to describe $\mathrm{Gal}(L/k)$ as an algebraic subgroup of $\mathrm{GL}(V)$, i.e. that it's Zariski closed. Choose a basis of V; then, the Galois group admits an explicit description as the set of matrices $M \in \mathrm{GL}_n(C)$ whose associated automorphism $\sigma_m \in \mathrm{Aut}(R_0)$ (which is an automorphism of differential rings), explicitly

$$\sigma_M(x_{ij}) = (x_{ij})M, \tag{6.14}$$

carries $\mathfrak{m}$ into itself.

The condition $\sigma_m(\mathfrak{m}) \subset \mathfrak{m}$ doesn't look polynomial – but wait, there's more! Using the Hilbert basis theorem, we can find a finite set $g_1, \dots, g_r$ of generators of $\mathfrak{m}$, and let $\{e_i\}$ be a basis of R. Then,

$$\sigma_M(g_j) \bmod \mathfrak{m} = \sum_i C(M, i, j) e_i, \tag{6.15}$$

where C is a polynomial in $M_{\alpha\beta}$ and $\det(M)^{-1}$. This is a lot of polynomial equations, but it's a finite number, so that's fine. *Post facto*, you can reduce this to a smaller set of equations, but for our purposes we're done.

Remark 6.16. There's a slightly fancier algebro-geometric way to understand this: let $Z := \operatorname{Spec} R \subset \mathrm{GL}_n(k)$. Then $\mathrm{GL}_n(C)$ acts on Z through its action on $\mathrm{GL}_n(k)$. One can show that it acts transitively, and the stabilizer of Z is precisely $\mathrm{Gal}(L/k)$.

In fact, Z is an étale torsor for $\mathrm{GL}_n(C)$ over k, which is the algebro-geometric incarnation of a principal bundle. "Étale" here means it's locally trivial in the étale topology, rather than the Zariski topology, over $\operatorname{Spec} k$, which resolves something that might confuse the differential geometers here: that this is something like a principal bundle, but it has stabilizer! Things can be a little subtler in algebraic geometry.

To make the connection to Galois theory more explicit, étale extensions of $\operatorname{Spec} k$ are of the form $\operatorname{Spec} L$, where $k \hookrightarrow L$ is a Galois extension of fields. So the assertion that Z is an étale torsor means precisely that there is a Galois extension $k \hookrightarrow L$ and an isomorphism

$$Z_L \cong \mathrm{GL}_n(C)_L \cdot \mathrm{pt}, \tag{6.17}$$

where $(-)_L$ denotes base change from k to L. As the notation suggests, we can take L to be the Picard-Vessiot field of our $\mathcal{D}$-module. ◀

Deligne provided a really slick way to define $\mathrm{Gal}(L/k)$ using the Tannakian formalism: if $\mathcal{C}$ is a "nice enough" category (k-linear rigid symmetric monoidal together with an exact k-linear faithful functor $\omega\colon \mathcal{C} \to \mathcal{V}ect_k$), where there are plenty of examples, then there is an algebraic group G such that $\mathcal{C} \cong \mathcal{R}ep_G$ (here we mean finite-dimensional representations), and this sends ω to the forgetful functor from a representation to its underlying vector space.

So we can define $\mathrm{Gal}(L/k)$ through its category of representations. Given a $\mathcal{D}$-module M, let $\langle M\rangle$ denote the full subcategory of $\mathcal{M}od_{\mathcal{D}}^{fd}$ generated by M and $M^\vee$ under subquotients, direct sums, and tensor products.

We need to define ω (which, by the way, is called the *fiber functor*), which sends N to its "solution space," more explicitly the kernel of

$$\partial\colon R \otimes_k N \longrightarrow R \otimes_k N, \tag{6.18}$$

where R is the Picard-Vessiot ring of M.

Theorem 6.19 (Deligne). *There's an isomorphism from $\langle M\rangle$ to the category of representations of* $\mathrm{Gal}(L/k)$*, where L is the Picard-Vessiot field of M.*

So $\mathcal{D}$-modules are precisely the things which admit Galois representations.

There's also a correspondence between $\mathcal{M}od_{\mathcal{D}}$ and the absolute differential Galois group, which is associated to the differential ring that's the colimit of all of the ones associated to finite-dimensional $\mathcal{D}$-modules. This is one of the cases where it's crucial that we work with rings and not just fields.

7. The fundamental theorem of differential Galois theory

Fix a $\mathcal{D}$-module X over our ground field k, with the same notation and assumptions as in the previous lecture. In particular, $G := \mathrm{Gal}(L/k)$ is an algebraic subgroup of $\mathrm{GL}(V) \cong \mathrm{GL}_n(C)$, which acts on Z. Let $k \hookrightarrow \widetilde{k}$ be a finite Galois extension such that $Z_{\widetilde{k}} \cong G_{\widetilde{k}}$, which exists because Z is an étale torsor for G. There is an isomorphism

$$G \times_C Z \xrightarrow{\cong} Z \times_k Z \tag{7.1}$$

sending $(g, z) \mapsto (gz, z)$.

Theorem 7.2 (Galois correspondence). *Let $k \hookrightarrow L$ be a Picard-Vessiot extension of differential fields and G denote its Galois group. Let $\mathcal{S}$ denote the set of (Zariski-)closed subgroups of G and $\mathcal{L}$ denote the set of differential subfields of L containing k, both posets ordered under inclusion. The functions $\alpha\colon \mathcal{S} \to \mathcal{L}$ sending $H \mapsto L^H$ and $\beta\colon \mathcal{M} \to \mathcal{S}$ sending $M \mapsto$* $\mathrm{Gal}(L/M)$ *are inverse order-reversing bijections.*

More is true, e.g. a relationship between normal subgroups and normal extensions.

Proof. Let M be a differential subfield of L containing k, and let $y' = Ay$ denote the ODE corresponding to L (originally associated to X as per last lecture). Then, the Picard-Vessiot field of $y' = Ay$ over M is again L; hence $M \hookrightarrow L$ is also a Picard-Vessiot extension, and $\mathrm{Gal}(L/M)$ is a closed subgroup of both $\mathrm{GL}_n(C)$ and of G.

If $M \in \mathcal{L}$, then $\alpha\beta(M) = L^{\mathrm{Gal}(L/M)}$; we want to show this is M. As $M \hookrightarrow L$ is a Picard-Vessiot extension, it suffices to show that for an arbitrary Picard-Vessiot extension $k \hookrightarrow L$, $L^{\mathrm{Gal}(L/k)} = k$; let's do it. By definition, $k \subseteq L^{\mathrm{Gal}(L/k)}$, so all we have to do is, given $a \in L \setminus k$, find an element of $\mathrm{Gal}(L/k)$ which doesn't fix it.

We can write $a = b/c$ for $b, c \in R$ (where R is the Picard-Vessiot ring associated to this Picard-Vessiot extension; hence L is the field of fractions of R) and let

$$d \coloneqq b \otimes c - c \otimes b \in R \otimes_k R. \tag{7.3}$$

Then $R_1 \coloneqq (R \otimes_k R)[d^{-1}]$ has a differential k-algebra structure in which

$$\partial(x \otimes y) \coloneqq \partial x \otimes y + x \otimes \partial y. \tag{7.4}$$

Let $\mathfrak{m}_1 \subset R_1$ be a maximal differential ideal and $N \coloneqq R_1/\mathfrak{m}_1$; N_1 is a simple differential ring (and generally is not a field). Let $\overline{d} \coloneqq d \bmod \mathfrak{m}_1 \in N$. Consider the two maps $\phi_1, \phi_2 \colon R \rightrightarrows N$ sending $x \mapsto x \otimes 1 \bmod \mathfrak{m}_1$, resp. $x \mapsto 1 \otimes x \bmod \mathfrak{m}_1$; then

$$\overline{d} = \phi_1(b)\phi_2(c) - \phi_1(c)\phi_2(b). \tag{7.5}$$

Since d is invertible, so is $\overline{d}$, and in particular $\overline{d} \neq 0$, i.e. $\phi_1(b)\phi_2(c) \neq \phi_1(c)\phi_2(b)$.[9]

Since N is simple, $\operatorname{Im}\phi_1$ and $\operatorname{Im}\phi_2$ are each simple differential rings and are generated by solutions to some ODEs. In particular, they agree and are isomorphic to R, so there is some $\sigma \in \mathrm{Aut}_k^{\mathit{diff}}(R) = G$ with $\phi_1\sigma = \phi_2$.

Now, since $\phi_1(b)\phi_2(c) \neq \phi_1(c)\phi_2(b)$, then $\phi_2(\sigma(b)c) \neq \phi_2(\sigma(c)b)$, i.e.

$$\phi_2(\sigma(a)) = \phi_2\left(\frac{\sigma(b)}{\sigma(c)}\right) \neq \phi_2\left(\frac{b}{c}\right) = \phi_2(a), \tag{7.6}$$

and we conclude.

In the other direction, let $H \in \mathcal{S}$; then $\beta\alpha(H) = \mathrm{Gal}(L/L^H)$. Again, since $L^H \hookrightarrow L$ is Picard-Vessiot, we can forget about the base field and prove this for an arbitrary Picard-Vessiot extension $k \hookrightarrow L$. We want to show that if $H \leq G \coloneqq \mathrm{Gal}(L/k)$ is a closed subgroup with $L^H = k$, then $H = G$. This is where the "torsor-ness" of Z kicks in: assume $L^H = k$; the G-equivariant isomorphism $Z_{\widetilde{k}} \cong G_{\widetilde{k}}$ implies $R \otimes_k \widetilde{k} \cong \mathcal{O}(G) \otimes_C \widetilde{k}$. Passing to fraction fields, we get

$$L \otimes_k \widetilde{k} \cong \mathcal{K}(G) \otimes_C \widetilde{k}, \tag{7.7}$$

where $\mathcal{K}(G)$ is the field of rational functions on G. Hence $L^H \otimes_k \widetilde{k} \cong \mathcal{K}(G)^H \otimes_C \widetilde{k}$; by our assumption, the left-hand side is $\widetilde{k}$. Since $\mathcal{K}(G)^H \cong (G/H)$, we've just shown that $\mathcal{K}(G/H) \cong C$, so $G/H = \operatorname{Spec} C$, which is a point, and we conclude $G = H$. $\boxtimes$

This concludes the main material of the course; now a few sprinkles on the cake.

Kolchin theory is to PDEs as Picard-Vessiot theory is to ODEs. The analogue of a differential field is a field k with n commuting derivations $\partial_1, \ldots, \partial_n$, e.g. rational functions on $\mathbb{A}^n_C = C(t_1, \ldots, t_n)$, with $\partial_i \coloneqq \frac{\partial}{\partial t_i}$. You can also do this formally, i.e. apply the same thing to $C((t_1, \ldots, t_n))$, which is the field of rational functions on $\widehat{\mathbb{A}}^n_C$, or you could look at germs of meromorphic functions at $0 \in \mathbb{C}^n$, or so on.

Now let $\mathcal{D}$ denote the ring of differential operators which are polynomial in the ∂_i. A $\mathcal{D}$-module is now equivalent data to a k-vector space together with n derivations $\partial_1, \ldots, \partial_n$ which all satisfy the Leibniz rule. Commutativity imposes another condition, though, which we have to suss out. So let $e_1, \ldots, e_n$ be a basis for M, and define the *Christoffel symbols* Γ^k_{ij} to satisfy

$$\partial_i e_j = \Gamma^k_{ij} e_k, \tag{7.8}$$

where we sum over repeated upper and lower indices as in differential geometry. If $s \in M$, we can write it as $s = f^j e_j$. Let $\partial_i(s) \coloneqq \partial_i(f^j)e_j$, i.e. the result of applying ∂_i (acting on k) componentwise. Let $\partial_i s$ denote the $\mathcal{D}$-module action of ∂_i on s. Then

$$\partial_i s = \underbrace{(\partial f^j) e_j}_{\partial_i(s)} + \Gamma^k_{ij} f^j e_k, \tag{7.9}$$

[9] There was some piece of intuition here, which was erased before I could write it down. Sorry about that!

or $\partial_i s = \partial_i(s) + A_i(s)$, where $A_k \coloneqq \Gamma_{ij}^k$. You can think of this as the collection of PDEs we're trying to solve (TODO: I think). Anyways, we need to impose the condition

$$\partial_i \partial_j s = \partial_j \partial_i s, \tag{7.10}$$

and when you expand this out, it becomes the condition

$$\partial_i(A_j) - \partial_j(A_i) + [A_i, A_j] = 0. \tag{7.11}$$

This is exactly the curvature defined by the connection (or Christoffel symbols), so we're looking only at flat connections. From the PDE perspective, this means we restrict to looking at integrable systems, which includes most of the things we care about in mechanics, which is fine.

Anyways, then Kolchin theory carries on in a very similar way, defining the analogue of Galois extensions and Galois groups, and a Galois correspondence.

Another thing you could ask about is positive characteristic p. The fact that ∂ must be k^p-linear makes life very interesting: $\partial(f^p) = pf^{p-1}\partial f = 0$, and therefore all p^{th} powers are constants! Since $[k : k^p] = p$, the field of constants is very close to being everything.

So differentials look like $\Omega_k^1 = k^p \, \mathrm{d}z$, and if $z \in k \setminus k^p$, we get a basis of k over k^p given by $\{1, z, \dots, z^{p-1}\}$, and therefore $\partial \coloneqq \frac{\partial}{\partial z}$ satisfies a pretty strong uniqueness property!

In particular, $\partial^p = 0$. But things get a bit weirder when we pass to $\mathcal{D}$-modules: ∂^p isn't necessary zero, but it *is* k-linear (i.e. linear over functions). This is weird, especially from the perspective of differential geometry. ∂^p is called the *p-curvature* of M; those $\mathcal{D}$-modules with vanishing p-curvature are exactly those with $\partial = 0$ (which I guess you can think of as k-modules).

Cartier proves there's an equivalence of categories $\mathcal{M}od_{\mathcal{D}} \simeq \mathcal{M}od_{k^p[t]}$, where t acts by the p-curvature.

There is a different notion of differential operators, called *crystalline differential operators*, which correspond to the notion of *iterated differential equations*. The idea is that $\frac{\partial^n}{\partial t^n}$ is different from $\frac{\partial}{\partial (t^n)}$. You might think the difference is a factor of $1/n!$, but that's your characteristic 0 brain speaking: $n!$ might be zero. Anyways, if you use this notion of differential operators, Picard-Vessiot extensions and differential Galois theory goes through in much the same way as in characteristic zero.