Differential Galois Theory

Andy R. Magid

Differential Galois theory, like the more familiar Galois theory of polynomial equations on which it is modeled, aims to understand solving differential equations by exploiting the symmetry group of the field generated by a complete set of solutions to a given equation. The subject was invented in the late nineteenth century, and by the middle of the twentieth had been recast in modern rigorous form. But despite being an active subject of contemporary research, and an important tool in applications, and despite the availability of texts and courses on the subject, the basic results of the subject seem not to be widely known. This article is intended to provide a gateway to those results.

The late nineteenth-century work was done by Picard and Vessiot. The modern rigorous form of the subject is due to E. Kolchin. The basic theorems of differential Galois theory seem by now to have entered the public domain, however, and are presented here without reference or attribution. It is safe to assume that they have their origins in Kolchin's work; none should be thought of as work of the present author.

Before starting the discussion of differential Galois theory, we review the fundamental concepts of ordinary, here termed "polynomial", Galois theory. Both Galois theories involve an extension of fields, and each has a Fundamental Theorem. Making use of Galois theory in concrete situations requires being able to compute groups of automorphisms, and this and the inverse problem remain active areas of research. The corresponding problems of differential Galois theory are the ultimate subjects of this article.

Andy R. Magid is George Lynn Cross Professor of Mathematics at the University of Oklahoma, Norman. His e-mail address is amagid@ou.edu.

The author was partially supported by NSA grant MDA904-98-1-0024. This article was written while he was Lady Davis Fellow and Visiting Professor, Institute of Mathematics, Technion, Haifa, Israel.

Polynomial Galois Theory

The Galois theory of fields is a justifiably popular algebraic theory in the mathematics curriculum. At its center is the aptly named Fundamental Theorem: the lattice of intermediate fields of a (finite) Galois extension of fields is in one-to-one order-reversing correspondence with the lattice of subgroups of the (finite) Galois group of the extension. Moreover, the subfields that are themselves Galois extensions of the base field are precisely those corresponding to normal subgroups of the Galois group. One can appreciate and one hopes one's students appreciate the power of the Fundamental Theorem even without knowing what a Galois extension of fields is: for whatever it is, its set of subfields is a complicated-to-conceive, potentially infinite set of hard-to-describe-and-identify objects, while the set of subgroups of a finite group is a far more benign object well within the scope of a beginning algebra student's imagination. And of course the theorem and the theory have those wonderful applications: angles cannot be trisected in general; some regular polygons can be constructed with ruler and compass and some cannot, and one can say which ones; and, most famously, the general fifth-degree polynomial cannot be factored into linear factors just by rational

operations combined with fractional powers. A good beginning algebra course leads students to understand the Fundamental Theorem as quintessential abstract algebra and to enjoy the applications, and an instructor whose students do so is entitled to be satisfied with a teaching assignment successfully accomplished.

The "obvious" appeal of the Fundamental Theorem is of course culturally bound. It assumes that the reader is familiar with both fields and groups. As far as fields go, perhaps this is safe: the field operations—add, subtract, multiply, divide—are truly basic. Groups are another matter, but even so are likely to have been seen by the student before confronting the Fundamental Theorem, and in any event the necessary pieces—namely, definition (set with an associative operation, identity, inverses), subobjects, and quotient objects—are accessible. Generalizations of the Fundamental Theorem, with the same statement but with the objects in correspondence changed, can have the same formal structure but either appear obscure (as with the correspondence between quotients of a scheme over a base and effective equivalence relations) or trivial (as with the correspondence between partitions and equivalence relations on a set). This obscurity or triviality occurs even though the former reduces to the Fundamental Theorem when the scheme is the spectrum of a Galois field extension and the latter is the exact analogue of the former in the category of sets.

Moreover, the focus on exemplary algebra and classical problems obscures part of the tasks that each direction of the bijection of the Fundamental Theorem assumes. To carry on this discussion a bit further, we assume that we have a base field k and that the Galois extension in question is a splitting field $E \supset k$ for the monic separable polynomial $f(x) \in k[x]$: this means that f has leading coefficient 1; is a product of distinct monic linear factors in $E[x]$, say $f = (x - \alpha_1)\dots(x - \alpha_n)$; and that no subfield of E except E itself contains both k and all the α_i. The Galois group G in this case is the group of all automorphisms of the field E that are the identity on the subfield k.

For an elementary example, we consider the direct problem for the polynomial $x^3 - 2$ over the rationals $\mathbb{Q}$. If $\omega = e^{2\pi i/3}$ and $\alpha = 2^{1/3}$, then over the field of complex numbers there is the factorization $(x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$, and so the splitting field E is generated over $\mathbb{Q}$ by α and ω. There are three subfields of E of dimension three over $\mathbb{Q}$—namely, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\omega\alpha)$, and $\mathbb{Q}(\omega^2\alpha)$—and one quadratic subfield, $\mathbb{Q}(\omega)$. There are six automorphisms of E over $\mathbb{Q}$: an automorphism τ of order two that fixes α and carries ω to ω^2; an automorphism σ of order three that carries α to $\omega\alpha$ and fixes ω; and their powers and products, forming a group G isomorphic to the symmetric group S_3. The subfields of dimension three over $\mathbb{Q}$ are the fixed fields of the three subgroups of order two of G: $\{e, \tau\}$, $\{e, \tau\sigma\}$, and $\{e, \tau\sigma^2\}$. The subfield of dimension two is the fixed field of the only subgroup of order three, namely, $\{e, \sigma, \sigma^2\}$.

What has come to be known as the *direct problem* of Galois theory then is: given the polynomial f over the base field k, find the group G. In some sense, of course, this is the same as factoring f into linear factors; the point of the fundamental theorem is that the steps to do this, amounting to factoring (splitting) auxillary polynomials or equivalently finding intermediate Galois extensions, means finding normal subgroups of the group G. The smallest steps this task can be divided into amount to constructing a composition series for G (and the fact that equations cannot be solved by radicals in general means that nonabelian simple composition factors may occur). There are theorems that tell, from some criteria on the polynomial f viewed only over k, what types of G might appear. In general, however, despite the fundamental theorem the direct problem is hard.

And, symmetrically, there is the *inverse problem*: given k and given a finite group G, find a separable polynomial $f \in k[x]$ whose splitting field has Galois group G. The difficult part of this problem, by the way, is "given k". It is easy to exhibit the symmetric group S_n as a Galois group of some polynomial, for instance for $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ over the field $k(a_0, \dots, a_n)$, where the a_i are independent transcendentals over k. Since any finite G is isomorphic to a subgroup of some S_n, the splitting field E of this f is a Galois extension of its subfield E^G of G invariants with Galois group G. Somewhat more concretely, it is possible to find Galois extensions of number fields (finite extensions of $\mathbb{Q}$), and even $\mathbb{Q}$ itself, with Galois group S_n, so that the extensions with group G are also extensions of number fields.

Naively, this should be easier than the direct problem, since many polynomials should have the same Galois group, but it has been notoriously difficult even in the case $k = \mathbb{Q}$. An interesting moving target so far has been the smallest finite group not currently known to be the Galois group of an extension of the rationals. That the target is moving reflects the conviction that eventually all finite groups will be shown to be Galois groups over $\mathbb{Q}$. (To be technical for a moment: the group $\hat{G}$ of automorphisms of the separable closure of $\mathbb{Q}$ over $\mathbb{Q}$ is a profinite group, which is unknown in the sense that its finite quotients, the Galois groups over $\mathbb{Q}$, are not known. But much of its structure has been determined: it is an extension of a product of symmetric groups by a free profinite group. One can imagine situations in which knowing that much about a group would be enough to call it "known".)

And finally, it is possible even to know that a group is a Galois group over a given field k and still not know a polynomial whose splitting field

is such a Galois extension: this is the situation with $k = \mathbb{C}(t)$, and solving the corresponding problem seems to lie at the interface of differential and polynomial Galois theory, as we will see below.

Differential Galois Theory

A *derivation* D of a field F is a map $D : F \to F$ satisfying

1. $D(a+b) = D(a) + D(b)$, and
2. $D(ab) = D(a)b + aD(b)$,

for all $a, b \in F$.[1] An example is $F = \mathbb{C}(t)$, the rational functions in one variable over the complex numbers, with $D = \frac{d}{dt}$. A *differential field* is a field F with a specified derivation D_F (usually just denoted D). The *constants* are the members of the kernel of D; these form a subfield of F. A *differential field extension* $E \supset F$ is an inclusion of differential fields F in E such that D_E restricts to D_F on F.

For instance, we could consider the field E generated over $\mathbb{C}$ by t and $f = \log(t)$, with the derivation $D = \frac{d}{dt}$. E is a differential field extension of $\mathbb{C}(t)$, generated over $\mathbb{C}(t)$ by an element f that satisfies $D(f) = \frac{1}{t} \in \mathbb{C}(t)$. As a field extension, $E = \mathbb{C}(t)(f)$ has many subfields: if $g = a_n f^n + \cdots + a_0$ is any polynomial in f over $\mathbb{C}(t)$ of degree at least two, then $\mathbb{C}(t)(g)$ is a subfield of E different from E, but, as we will see shortly, there are no intermediate *differential* subfields.

The Fundamental Theorem of Differential Galois Theory sets up a one-to-one correspondence between differential subfield extensions of a differential field extension and subgroups of the group of automorphisms of the extension. Here the kind of extension that will fit in the correspondence, playing the role of Galois extensions of fields, is a *Picard-Vessiot* extension with algebraically closed constant field, which will be defined below.[2]

The Fundamental Theorem then reads as follows:

Theorem. Let $E \supset F$ be a Picard-Vessiot extension with common algebraically closed field C as the field of constants of both E and F. Let G be the group of differential automorphisms of E over F. Then G has the structure of a linear algebraic group over C, and there is a one-to-one inclusion reversing correspondence between intermediate differential field extensions $E \supset K \supset F$ and closed subgroups H of G, with K corresponding to

$$\{g \in G \mid g(k) = k \quad \text{for all } k \in K\}$$

and H corresponding to

$$\{x \in E \mid h(x) = x \quad \text{for all } h \in H\}.$$

Moreover, H is a normal subgroup of G if and only if the corresponding subextension K is a Picard-Vessiot extension of F, and, if so, then the group of differential automorphisms of K over F is identified with G/H.

A *linear algebraic group* over C is a subgroup of some general linear group $GL_n(C)$ that is the zero locus of a set of polynomials in the matrix entries. Examples are $SL_n(C)$ (the zeros of the determinant minus one), the upper triangular matrices (the zeros of the set of coordinate functions x_{ij} for $i > j$), the additive group C (for example, the zeros in $GL_2(C)$ of $x_{11} - 1$, $x_{22} - 1$, and x_{21}), and the multiplicative group $C - \{0\}$ (the zeros in $GL_1(C)$ of the zero polynomial). A *closed subgroup* of a linear algebraic group is a subgroup that is itself the zero locus of a set of polynomials in the matrix entries. For example, the only closed subgroups of the additive group are itself and the identity.

In our example $E = \mathbb{C}(t)(f) \supset \mathbb{C}(t)$ with $f = \log(t)$, any differential automorphism σ of E over $\mathbb{C}(t)$ has to send $Y = f$, which satisfies the equation $Y' = \frac{1}{t}$, to another solution $\sigma(f)$, and then $(\sigma(f) - f)' = 0$. So $\sigma(f) - f$ is a constant, say $s \in \mathbb{C}$, and then $\sigma(f) = f + s$. The map $\sigma \mapsto \sigma(f) - f$ is a group homomorphism from the group G of differential automorphisms of E over $\mathbb{C}(t)$ to the additive group $\mathbb{C}$. Since the value of an automorphism on f determines the automorphism everywhere, the map is injective, in fact, an isomorphism. Since $\mathbb{C}$ has no proper algebraic subgroups, the Fundamental Theorem implies that $E \supset \mathbb{C}(t)$ has no proper subextensions.

This Fundamental Theorem is formally the same as the Fundamental Theorem of the Galois theory of fields and presumably has the same appeal. On the field side, the passage from "field" to "differential field" is, presumably, not a matter of great conceptual difficulty: to the idea of field has been attached the familiar notion of derivative.

Naming the field extensions to which the Fundamental Theorem applies after Picard and Vessiot is an appropriate and historically accurate reflection of their work. The group of the theorem, the group of differential field automorphisms, has come to be known as the *differential Galois group*. Although this is just contemporary shorthand reflecting the analogy with the Galois theory of fields, it is also appropriate and historical, Lie having pointed out the analogy in 1895.

The situation on the group side is a bit more complicated. As noted above, a linear algebraic group over C can be regarded a subgroup of some $GL_n(C)$ determined by the vanishing of some polynomials in the matrix coordinate functions. There is also an intrinsic definition, but it will not concern us. The basic papers of Picard and of Vessiot on differential Galois theory date to the 1880s

[1] *We will use the same formulas for the definition of a derivation of a commutative ring.*

[2] *It has not been stated explicitly yet that this is a characteristic zero theory, but it will be. There are differential Galois theories in positive characteristic, the most powerful being recent work of B. Matzat and M. van der Put, and of Y. André.*

and 1890s; according to T. Springer in his book *Linear Algebraic Groups*, Picard introduced the term "algebraic group" at that time. Still according to Springer, in the late 1940s Kolchin again took up the subject, also for the purpose of differential Galois theory applications, and Kolchin's work led to fundamental work of A. Borel in the mid-1950s setting out the theory of linear algebraic groups over arbitrary fields.[3]

One could also look at (not necessarily linear) general algebraic groups, where now "algebraic group" means group in the category of algebraic varieties. An example of a nonlinear algebraic group is an elliptic curve, or one-dimensional abelian variety. It is a theorem of M. Rosenlicht from the mid-1950s (which he attributes to C. Chevalley) that a general connected algebraic group is an extension of an abelian variety by a linear algebraic group. (It is interesting also that Rosenlicht subsequently did much work in differential algebra.) Kolchin expanded the context of the Fundamental Theorem to allow arbitrary groups as differential Galois groups, expanding the class of differential field extensions to what he called "strongly normal" (which I suppose we will eventually call Kolchin extensions). Kolchin further planned to expand the group context to differential algebraic groups (these are groups in the categories of differential algebraic varieties), and such Galois theories have been developed in work of Kolchin, P. Cassidy, J. Kovacic, A. Buium, A. Pillay, and others.

Picard-Vessiot Extensions

From now on, we fix the differential base field F with derivation D. We require F to have characteristic zero. For elements a in F or in differential extensions of F, we will write a' (and $a^{(n)}$) for $D(a)$ (and $D^n(a)$). A *constant* of F is an element $c \in F$ with $c' = 0$. The set C of constants of F is a subfield.

Let $L = L(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1Y' + a_0Y^{(0)}$, where $a_i \in F$, be a monic, homogeneous, linear differential operator over F. If $E \supset F$ is a differential field extension, we can apply L to elements y in E:

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y' + a_0y.$$

In particular, we can talk about the solutions $V = \{y \in E \mid L(y) = 0\}$ in E to the (order n linear homogeneous ordinary) differential equation $L = 0$. Because L is homogeneous linear, V is closed under addition and under scalar multiplication by scalars from the field C_E of constants of E.

Our field F and our operator L are completely arbitrary. In particular, $L = 0$ may already have solutions in F. Nonetheless, we always have the following construction for a given L:

Let $R = F[y_0, \ldots, y_{n-1}]$ be the polynomial ring over F in n indeterminates. Define a derivation D_R of R so that on coefficients of polynomials it is D_F, it obeys the usual rules for derivations, and on the variables, is defined by $D_R(y_i) = y_{i+1}$ for $i < n-1$ and $D_R(y_{n-1}) = -a_{n-1}y_{n-1} - \cdots - a_1y_1 - a_0y_0$. R is an integral domain and D_R extends (using the quotient rule) to a derivation D_E of its quotient field $E = F(y_0, \ldots, y_{n-1})$, so that $E \supset F$ is a differential field extension. By construction y_0 is a new solution, in E but not in F, for the differential equation $L = 0$. And this happens whether or not there are any solutions of $L = 0$ in F already!

Before going further, let us observe what happens with the analogous situation in ordinary polynomial Galois theory: start with a field k and a polynomial $f \in k[x]$ of degree at least two. Corresponding to R would be the ring $A = k[x]/(f)$ that we get by formally adding a solution of $f = 0$ to k. But if $f = 0$ already has a root in k, A will not be a field. So we go outside the accepted domain of discourse (field extensions) if we try to formally solve what is already solved.

Thus it is not surprising that some restriction on the domain of discourse is required in the differential case also. Here is what to do: the operator L is of order n. This means that the dimension of the space of solutions of $L = 0$ in F over the constants C is at most n (this is established by the same Wronskian[4] argument used in the theory of linear ordinary differential equations). So we could say that $L = 0$ has a *full set of solutions* if it has n solutions linearly independent over the field of constants C. Then if L has a full set of solutions in F and we add another by the above construction that is even algebraically independent (over F) of those in F, then we must also have added a new constant. Thus we can rule out the problem of adding a new solution to an equation that is already formally solved by requiring that the extensions under consideration have no new constants.

This is the first condition, and perhaps the least intuitive, in the definition of a Picard-Vessiot extension. For the rest, just as a Galois field extension is the splitting field of a polynomial, which is an extension generated over the base by all the roots of a separable polynomial, a Picard-Vessiot extension is generated as a differential field by a

[3] *C. Chevalley had also taken up the theory of algebraic groups in the second volume of his* Théorie de Groupes de Lie, *published in 1951. In the introduction to his 1956 paper, Borel points out that Chevalley relied on Lie methods, which is basically a characteristic zero theory. Borel, following Kolchin's methodology, wanted to work within the groups themselves, with the support of algebraic geometry when necessary. In a May 1999 conversation in Hong Kong, Borel said that "Lie methods" referred to use of the formal exponential.*

[4] *The Wronskian of elements $a_0, \ldots, a_{n-1}$ is the determinant of the $n \times n$ matrix whose i, j entry is $a_j^{(i)}$, $0 \le i, j \le n-1$.*

full set of solutions of a differential equation. Precisely,

Definition. Let L be a differential operator over the differential field F. A differential field extension $E \supset F$ is a *Picard-Vessiot extension of F for L* if:

1. The constants of E are those of F.
2. E contains a full set V of solutions of $L = 0$.
3. E is the smallest differential subfield of E containing both V and F ("E is generated over F as a differential field by solutions of $L = 0$").

We can make the above definition without further hypotheses on the field C of constants of F. However, to establish the existence of Picard-Vessiot extensions, we will subsequently require that the field of constants be *algebraically closed*.

If L is of order n, then n^{th} and higher derivatives of elements of V are F linear combinations of elements of V, so that E is finitely generated over F as a field. $E \supset F$ is a *Picard-Vessiot* extension if it is a Picard-Vessiot extension for some L over F. (Later we will note that there is an intrinsic definition of Picard-Vessiot extension not referring to any operator L.)

In our example $E = \mathbb{C}(t)(f) \supset \mathbb{C}(t)$ with $f = \log(t)$, the field E is a Picard-Vessiot extension of $\mathbb{C}(t)$. That there are no new constants in E is obvious. But while E is generated over $\mathbb{C}(t)$ by a solution (f) of the equation $Y' - \frac{1}{t} = 0$ of order one, the equation, although monic and linear, is not homogeneous. The general procedure in such a case is to replace an equation of the form $Y' - b = 0$ by the equation $Y'' - \frac{b'}{b}Y' = 0$. A solution y of the original equation is a solution of the new one, and 1 is also a solution. In our case, the resulting equation is $Y'' + \frac{1}{t}Y' = 0$, of order two. It has the two solutions (linearly independent over constants) f and 1 in E, which generate E over $\mathbb{C}(t)$. So E is a Picard-Vessiot extension of $\mathbb{C}(t)$.

Here are the basic facts about Picard-Vessiot extensions:

Theorem. Let L be a monic homogenous linear differential operator over the differential field F with algebraically closed field of constants C. Then:

1. A Picard-Vessiot extension E for L over F exists, and any two are differentially isomorphic over F.
2. Any two differential monomorphisms from E to a no-new-constants extension K of F that restrict to the identity on F have the same image in K (this is a normality-type condition).
3. If $a \in E - F$, then there exists a differential automorphism σ of E fixing F such that $\sigma(a) \neq a$.

Another way of phrasing the third conclusion would be to say that if G denotes the group of differential automorphisms of E over F, then $F = E^G$, where the latter denotes the elements of E left fixed by all elements of G.

Since G fixes F it carries solutions of $L = 0$ into solutions; that is, if $V = L^{-1}(0)$, then $G(V) \subseteq V$. In fact, G acts as C linear transformations on V, so that we have a homomorphism $G \to GL(V)$. Since V generates E over F as a differential field, this is actually an injection.

Part (2) of the theorem is termed a normality condition in analogy with the corresponding condition for polynomial Galois theory. Sometimes normality for polynomial Galois theory is defined by calling an algebraic extension $E \supset F$ of fields normal if every irreducible polynomial over F with a root in E splits in E. We show that this implies the condition analogous to (2) of the theorem. Suppose σ_1 and σ_2 are monomorphisms of E over F into an extension K of F and α is an element of E with irreducible polynomial f. By assumption f splits in both $\sigma_1(E)$ and $\sigma_2(E)$, so all its roots in K lie in both fields. For $i = 1, 2$, $\sigma_i(\alpha)$ is a root of f in K and hence lies in both fields. Applying this for all $\alpha \in E$ shows that $\sigma_1(E) = \sigma_2(E)$.

A Picard-Vessiot extension $E \supset F$ has the property that an element α of E satisfying a linear homogeneous differential equation over F is a solution of a (possibly different) equation with a full set of solutions in E. This is close to the similar normality condition in polynomial Galois theory mentioned above.

Now we can characterize Picard-Vessiot extensions:

Theorem. Let $E \supset F$ be a differential field extension with no new constants and algebraically closed common field of constants C. Suppose that there are a finite-dimensional C subspace V of E generating E over F differentially and a group G of differential automorphisms of E over F such that

1. $G(V) \subseteq V$, and
2. $E^G = F$.

Then E is a Picard-Vessiot extension of F for the operator

$$L(Y) = \frac{w(Y, v_1, \ldots, v_n)}{w(v_1, \ldots, v_n)},$$

where Y is a differential indeterminate; $v_1, \ldots, v_n$ is a C basis of V; and w denotes the Wronskian determinant.

For example, we can let $F = \mathbb{C}(t)$ and $E = F(f)$ with $f = \log(t)$. We have already seen that $E^G = F$, where G is the additive group of $\mathbb{C}$ acting by $f \mapsto f + c$ for $c \in \mathbb{C}$. Let V be the $\mathbb{C}$ span of 1 and f. V has 1 and f as a basis. We compute $w(Y, 1, f) = \frac{1}{t}Y'' + \frac{1}{t^2}Y'$ and $w(1, f) = \frac{1}{t}$, so that $L(Y) = Y'' + \frac{1}{t}Y'$.

This theorem points out, as the reader may have already suspected, that a Picard-Vessiot extension may be Picard-Vessiot for many operators L, just as a Galois extension may be a splitting field

for many different polynomials. Indeed, in the notation of the theorem, if we have another subspace W finite dimensional over C, generating E differentially over F, and with $G(W) \subseteq W$, then we also have E a Picard-Vessiot extension for $w(Y, w_1, \ldots, w_n)/w(w_1, \ldots, w_n)$ if the w_i are a basis of W. And we could apply the same construction to the subspace $V + W$. And while it seems possible that there is a canonical subspace, say, a maximal one, this turns out not to be the case, as we will see below.

The theorem also may be used to associate a canonical differential equation to elements satisfying differential equations; this is something like associating the irreducible polynomial to an element satisfying an algebraic equation. Suppose f is a solution of the differential equation $L = 0$ over F. We can assume that f is in the Picard-Vessiot extension E_1 of F for L, with field of constants C. Let G be the group of differential automorphisms of E over F. The element f lies in the finite-dimensional C space $L^{-1}(0)$. Let V be the G and C submodule of $L^{-1}(0)$ generated by V, and let E be the differential subfield of E_1 generated by V over F. Then E, V, and G satisfy the hypotheses of the theorem, and the operator $L(Y)$ of the theorem gives a differential equation canonically associated with f that has f as a solution.

The Differential Galois Group

Definition. The group of differential automorphisms of a differential field extension $E \supset F$ that restrict to the identity on F is denoted $G(E/F)$. If $E \supset F$ is a Picard-Vessiot extension, then $G(E/F)$ is called the *differential Galois group* of E over F.

In our example $E = \mathbb{C}(t)(f) \supset \mathbb{C}(t)$ with $f = \log(t)$, all the automorphisms are given by mapping f to f plus a constant, so $G(E/\mathbb{C}(t))$ is (isomorphic to) $\mathbb{C}$.

In the previous section we have described Picard-Vessiot extensions, which are the field subjects of the Fundamental Theorem. The theorem then asserts first that the differential Galois group is a linear algebraic group and then that there is a Galois correspondence between closed subgroups and intermediate differential fields. Recall that in the theorem we required that the common field of constants C of the extension be algebraically closed. Now we will look at how the differential Galois group is an algebraic group over C.

Fix a Picard-Vessiot extension $E \supset F$, say, for the operator L; let $V = L^{-1}(0) \subset E$; and let $G = G(E/F)$. We have already observed that $G \to GL(V)$ by restriction is an injection. Then it is a fact that the image of G is actually an algebraic subgroup of $GL(V)$ (we will have more to say about proving this later):

Theorem. Let $E \supset F$ be a Picard-Vessiot extension of F for L. Then the image of $G(E/F) \to GL(L^{-1}(0))$ is an algebraic subgroup.

Now as previously noted, the extension $E \supset F$ can be Picard-Vessiot for many operators. Thus we should like to know that the algebraic group structure on G from the monomorphism $G \to GL(V)$ is independent of the choice of the operator L. And this is indeed the case: suppose V and W are the subspaces of E that are the sets of solutions for two operators for which E is the Picard-Vessiot extension of L. We can find an operator for which E is Picard-Vessiot and the solution space is $V + W$ because the latter is a finite-dimensional C subspace of E stable under G and differentially generating E over F. Hence $G \to GL(V + W)$ has an algebraic group as image, compatible with the algebraic group structures from both $G \to GL(V)$ and $G \to GL(W)$. Thus:

Corollary. The algebraic group structure on $G(E/F)$ depends only on the fact that $E \supset F$ is Picard-Vessiot and not on any particular operator for which it is the Picard-Vessiot extension.

Tannakian Category Method

There is another more sophisticated and more powerful way, due to P. Deligne, to see $G = G(E/F)$ as an algebraic group which uses the fact that an algebraic group H over a field k can be recovered from its category $\mathrm{Rep}_k(H)$ of finite-dimensional rational k-modules, considered as a category with tensor product. The group H is recovered as the group of "tensor automorphisms", a term we do not define.

Even more is true: *any* abelian category C of k vector spaces with a tensor product, generated as a tensored category by a finite set of objects, is the category of finite-dimensional representations of an algebraic group, which as above has to be its group of tensor automorphisms.[5]

In the present context one considers finite-dimensional F vector spaces M equipped with an additive endomorphism D_M satisfying $D_M(fm) = D_F(f)m + fD_M(m)$ for $f \in F$ and $m \in M$; these are called *connections*. Corresponding to the operator $L = Y^{(n)} + a_{n-1}Y^{(n-1)} + \ldots a_0Y^{(0)}$, there is a connection $M = M_L$ with F basis $e_0, \ldots, e_{n-1}$ such that $D_M(e_0) = -a_0e_{n-1}$ and $D_M(e_i) = -e_{i-1} + a_ie_{n-1}$ for $i > 0$.

This particular connection may be easier to understand if we write $\sum f_ie_i$ as the row $(f_0, \ldots, f_{n-1})$, which D_M then sends to $(f_0', \ldots, f_{n-1}') - (f_1, \ldots, f_{n-1}, \sum a_if_i)$. So the kernel of D is tuples with $f_i = f_0^{(i)}$ for $0 \le i \le n-1$ and $f_0^{(n)} + a_{n-1}f_0^{(n-1)} + \cdots + a_0f_0 = 0$, that is, tuples corresponding to solutions of $L = 0$.

[5] *This is A. Grothendieck's theory of Tannakian categories, named after the Tannaka Duality Theorem, which recovers a compact Lie group from its finite-dimensional analytic representations.*

For example, if $L = Y^{(2)} + \frac{1}{t}Y^{(1)}$, the operator associated to the Picard-Vessiot extension $E = \mathbb{C}(t)(f) \supset \mathbb{C}(t)$ with $f = \log(t)$, then M_L has basis e_0, e_1 with $D_L(e_0) = 0$ and $D_L(e_1) = -e_0 + \frac{1}{t}e_1$.

For another example, even simpler, we consider the operator $L = Y^{(1)} - Y^{(0)}$, which is the operator associated to the Picard-Vessiot extension $E = \mathbb{C}(t)(g) \supset \mathbb{C}(t)$ with $g = \exp(t)$. Now M_L has basis e_0 and $D_L(e_0) = -e_0$. We will call this the *exponential connection*.

The connections over F form a tensored category: if M_1 and M_2 are connections with endomorphisms D_1 and D_2, a morphism $M_1 \to M_2$ is an F linear map T such that $D_2T = TD_1$. $M_1 \oplus_K M_2$ with operator $D_1 \oplus D_2$ is a connection, and $M_1 \otimes M_2$ with operator $D_1 \otimes 1 + 1 \otimes D_2$ is a connection. Also, the F linear dual M^* of a connection M is a connection.

For the exponential connection M we let $M(n)$ denote its n-fold tensor power; it has a basis, which we denote e_0^n, with $D(e_0^n) = -ne_0^n$. Then

$$M(n_1) \oplus M(n_2) \oplus \cdots \oplus M(n_m)$$

has basis $\{e_0^{n_1}, \ldots, e_0^{n_m}\}$ with D given on each basis vector as above, and the dual $M(n)^*$ has a basis that we denote e_0^{-n}, since $D(e_0^{-n}) = ne_0^{-n}$. Thus we will also extend notation and write $M(n)^* = M(-n)$.

Now we go back to the general operator L and its associated connection M_L and consider the tensored category $C_F(L)$ generated by M_L and its dual. Let $G_F(L)$ denote its group of tensor automorphisms. This is an algebraic group over F. In the case of the exponential connection, all the tensor automorphisms are just the scalars, so the group is just $GL_1(F)$.

Now we let E be the Picard-Vessiot extension of F for L. We extend scalars to E,[6] and we consider the tensored category $C_E(L)$. For every connection M in this category, we can consider the kernel space $V_M = \{m \in M | D_M(m) = 0\}$, which is a vector space over the field of constants C. And if $T : M_1 \to M_2$ is a morphism of connections, T carries kernel space to kernel space. So there is a category $\mathcal{K}$ of kernel spaces of connections; since $C_E(L)$ is a tensored category, so is $\mathcal{K}$. Note that for $M = M_L$, V_M is identified above with the solutions of $L = 0$, so that $\mathcal{K}$ is generated by V_M.

Finally, the group G of tensor automorphisms of $\mathcal{K}$ turns out to be the differential Galois group $G(E/F)$ for the Picard-Vessiot extension E of F for the operator L.

In the case of the exponential connection, the kernel space for $M(n) \otimes_F E$, which we denote $V(n)$, will be those elements ae_0^n satisfying

$$D(ae_0^n) = (a' - na)e_0^n = 0.$$

E here is $\mathbb{C}(t)(g) \supset \mathbb{C}(t)$ with $g = \exp(t)$, so that $V(n) = \mathbb{C}g^n$. Automorphisms of the $V(n)$'s are given by the multiplications by constants, and these are all tensor automorphisms. So in this case the group G is $GL_1(\mathbb{C})$, which is the differential Galois group of $\mathbb{C}(t)(g)$ over $\mathbb{C}(t)$ with $g = \exp(t)$: any differential automorphism σ has $\sigma(g)' = \sigma(g)$. Thus $(\frac{\sigma(g)}{g})' = 0$, so that $\frac{\sigma(g)}{g} = c \in \mathbb{C}$ and $\sigma(g) = cg$. The association $\sigma \mapsto c$ is an isomorphism of $G(\mathbb{C}(t)(g)/\mathbb{C}(t))$ with $GL_1(\mathbb{C})$.

The advantage of the Tannakian category approach is that the category of $G(E/F)$ modules, which is (isomorphic to) the category $\mathcal{K}$, is at the front of the discussion, so that properties of the group expressed in terms of its modules (for example, that all modules are semisimple) can take center stage in the direct problem of differential Galois theory.

Torseurs

The algebraic group $G_F(L)$ over F that appeared above is closely related to the differential Galois group $G(E/F)$, which is an algebraic group over C. To see this precisely requires that we use the algebraic closure $\overline{F}$ of F: then $\overline{F} \times_F G_F(L)$ ($G_F(L)$ with scalars extended from F to $\overline{F}$) is isomorpic over $\overline{F}$ to $\overline{F} \times_C G(E/F)$. This isomorphism comes about naturally from the Tannakian category approach above.

One can alternatively look at related objects directly in terms of the Picard-Vessiot extension E of F for L: let $T = T(E/F)$ be the set of elements of E satisfying monic homogeneous linear differential equations over F. T is clearly a $G(E/F)$ stable ring, and in fact if H is any algebraic subgroup of $G(E/F)$ with $E^H = F$, then one can show that T has no H stable ideals. It also turns out that T is finitely generated as an F algebra. Consequently, $\overline{F} \otimes_F T$ turns out to be isomorphic to $\overline{F} \otimes_C C[H]$, where $C[H]$ is the coordinate ring of the algebraic group H. Since a similar isomorphism follows using $G(E/F)$ itself, we conclude that $H = G(E/F)$, and this is the key step in the proof of the Fundamental Theorem (subgroups corresponding to the same intermediate field are equal).

Thus T is the affine coordinate ring over F of an affine variety that is a torseur ("twisted form") of $G_F(L)$, which becomes isomorphic to the latter over $\overline{F}$. It is possible to construct the torseur directly in the context of Tannakian categories, and thus establish the proof of the Fundamental Theorem in that context as well.

An Example

To illustrate the Fundamental Theorem, we will do a more elaborate example. As with the examples in the pedagogy of polynomial Galois theory, we will freely draw on general mathematical information to make calculations.

The base field F will be the field $\mathbb{C}(t)$ of rational complex functions in one variable, and the

[6] *By tensoring with E over the field F.*

extension field $E = F(u_1, u_2, u_3)$ will be generated by algebraically independent elements such that $u_1' = \frac{1}{t}$, $u_2' = \frac{1}{t+1}$, and $u_3' = \frac{1}{t}u_2$. This makes E a differential field extension of F.

It is further true that the constants of E are those of F, namely $\mathbb{C}$. This fact requires proof. One could try to embed E in the field $\mathbb{C}\{\{t\}\}$ of convergent power series by sending u_1 to $\log(t)$, u_2 to $\log(t+1)$, and u_3 to $\int \frac{1}{t}\log(t+1)$. This will work provided one can show the three functions are algebraically independent over F. Alternatively, one can use the fact that the quotient field of a differential unique factorization domain over F (like the polynomial ring $F[u_1, u_2, u_3]$) has no new constants provided there are no elements of f of the UFD satisfying $D(f) = af$ for a in the UFD.

Now define automorphisms σ and τ of E by $\sigma(u_1) = u_1 + 1$, $\sigma(u_i) = u_i$ for $i = 2$ and 3, and $\tau(u_2) = u_2 + 1$, $\tau(u_3) = u_3 + u_1$, $\tau(u_1) = u_1$. We can check that these are differential automorphisms. Notice that they both preserve the subring $F[u_1, u_2, u_3]$ of polynomials.

The only elements f of E fixed by both σ and τ are the elements of F. To give some flavor of how computations like this go, the following paragraph contains a proof.

Write $f = \frac{p}{q}$, where p and q are relatively prime elements of $F[u_1, u_2, u_3]$. Then $f^\sigma = f$ implies that $qp^\sigma = pq^\sigma$, so that p is a factor p^σ; looking at p as a polynomial in u_1 over $F[u_2, u_3]$ then shows that p cannot involve u_1. Similarly p is a factor of p^τ, and looking at p as a polynomial in u_3 shows that u_3 cannot occur either (since then u_1 would). Thus p is a polynomial in u_2 alone and fixed under $u_2 \mapsto u_2 + 1$. Hence p belongs to F, and so does q for similar reasons.

It follows that the full group of differential automorphisms G of E over F has fixed field F.

Let $V = C + \sum Cu_i$. We prove that any differential automorphism $g \in G$ preserves V. Readers willing to accept this may want to skip the rest of this paragraph. All differential automorphisms preserve $C \subset V$. For $u = u_1$ or $u = u_2$, we have $u' \in F$. Thus $g(u)' = g(u') = u'$, so that $(g(u) - u)' = 0$ and $g(u) - u$ is a constant, hence in C. In other words, $g(u) \in C + Cu \subset V$. For $u = u_3$, $g(u)' = g(u') = g(\frac{1}{t}u_2) = \frac{1}{t}g(u_2) = \frac{1}{t}(u_2 + c)$ (where $c \in C$). Since $(cu_1)' = c\frac{1}{t}$, $(g(u_3) - u_2 - cu_1)' = 0$. Therefore $g(u_2) = cu_1 + u_2 + d$ (where $d \in C$) and $g(u_3) \in V$ also.

Since E is generated as a differential field over F by V, and we have $G(V) \subseteq V$ and $E^G = F$, we know that E is a Picard-Vessiot extension of F.

It follows that the algebraic subgroup generated by σ and τ in $G = G(E/F)$, since it has fixed field F, must, by the Fundamental Theorem, be all of G.

Let $\gamma \in G$ be defined by $\gamma(u_i) = u_i$ for $i = 1, 2$ and $\gamma(u_3) = u_3 + 1$. Then $\sigma\tau = \gamma\tau\sigma$ and γ is the commutator (σ, τ). Moreover, γ commutes with both σ and τ. Thus the group generated by σ and τ is two-generator two-step unipotent, actually the integral Heisenberg group. Its Zariski closure, namely G, is the two-generator two-step unipotent group. Every element δ of G generates a one-dimensional unipotent subgroup that we will denote $\delta^{\mathbb{C}}$.

Some of the differential subfields of E over F are $F(u_2, u_3)$, which correspond to the group $\sigma^{\mathbb{C}}$; $F(u_1, u_1u_2 - u_3)$, corresponding to $\tau^{\mathbb{C}}$; $F(u_1, u_2)$, corresponding to $\gamma^{\mathbb{C}}$; $F(u_1)$, corresponding to $\tau^{\mathbb{C}} \times \gamma^{\mathbb{C}}$; and $F(u_2)$, corresponding to $\sigma^{\mathbb{C}} \times \gamma^{\mathbb{C}}$. The remaining proper differential subfields are all of the form $F(au_1 + bu_2)$; we omit the easy demonstration of this statement and the determination of the corresponding groups.

Direct and Inverse Problems of Differential Galois Theory

The direct problem, we recall, is "given the (differential) equation, find the (differential) Galois group". There is an extensive literature of computations, and applications of computations, of differential Galois groups for various classes of equations. The survey article [S] provides a first-rate introduction and guide to this literature.

The inverse problem, on the other hand, we further recall, is "given the (algebraic) group (over the field of constants of the base field F), find an equation (whose Picard-Vessiot extension E has the given group as differential Galois group)". For the case $F = \mathbb{C}(t)$, C. Tretkoff and M. Tretkoff showed in 1979 that every linear algebraic group G over $\mathbb{C}$ was a differential Galois group by showing that this could be reduced to showing that a finitely generated Zariski dense subgroup of G was a monodromy group of a differential equation with rational function coefficients and only regular singular points; this latter is Hilbert Problem 21, which has an (analytic) solution. More recently, C. Mitschi and M. Singer, building on earlier work of Kovacic, gave an algebraic proof in 1996 that every connected linear algebraic group G over an algebraically closed characteristic zero field C was a differential Galois group for every differential field F with constants C and of finite nonzero transcendence degree over C. (The bibliography of [S] gives references for the statements in this paragraph.)

J.-P. Ramis's work in this area also gave a solution to the inverse problem; van der Put's lecture "Recent Work on Differential Galois Theory" in the 1997–98 Seminaire Bourbaki provides a nice exposition.

Derivations of fields extend uniquely to separable algebraic extensions, and consequently any finite algebraic extension E of a differential field F can be made into a differential extension (and in only one way). If E is an (ordinary) Galois extension of F, then the characterization of Picard-Vessiot extensions shows that E is also Picard-

Vessiot (take for V the C span of the conjugates of a primitive element). Thus realizing finite groups, or more generally not-necessarily-connected linear algebraic groups, as differential Galois groups is essentially the inverse problem for ordinary Galois theory. It is known that every finite group is a Galois group over $\mathbb{C}(t)$ for topological reasons (or for analytic reasons, as in the solution of Hilbert Problem 21), but until this has an algebraic proof we will not have an algebraic proof that every linear algebraic group is a differential Galois group over $\mathbb{C}(t)$.[7]

References

There are two excellent recent expository articles about differential Galois theory to which interested readers can turn for guidance into the literature: Singer [S] is the more comprehensive, while D. Bertrand [Be] gives, among other things, a concise account of differential Galois theory inspired by the Tannakian category approach. Both have good bibliographies as well. The algebraic development of differential Galois theory is due to Kolchin, and his book [Ko] is a complete account of both his strongly normal theory and the simpler Picard-Vessiot theory discussed here. Borel's Kolchin Lecture [Bo] provides a good expository account of Kolchin's work on the Picard-Vessiot theory. I. Kaplansky's classic text [Ka] is still a brief and accessible introduction, dating, in its first edition, almost back to the emergence in the 1950s of the modern theory of linear algebraic groups over arbitrary fields. And of course the author likes his own approach, [M], which assumes some familiarity with linear algebraic groups.

[Be] BERTRAND, D., Review of "Lectures on Differential Galois Theory" by A. Magid, *Bull. Amer. Math. Soc.* **33** (1996), 289–294.

[Bo] BOREL, A., Algebraic groups and Galois theory in the work of Ellis R. Kolchin, *Selected Works of Ellis Kolchin with Commentary* (H. Bass, et al., eds.), American Mathematical Society, Providence, RI, 1999, pp. 505–526.

[Ka] KAPLANSKY, I., *An Introduction to Differential Algebra*, second ed., Hermann, Paris, 1976.

[Ko] KOLCHIN, E., *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.

[M] MAGID, A., *Lectures on Differential Galois Theory*, University Lecture Series, vol. 7, American Mathematical Society, Providence, RI, 1997, second printing with corrections.

[S] SINGER, M., Direct and inverse problems in differential Galois theory, *Selected Works of Ellis Kolchin with Commentary* (H. Bass, et al., eds.), American Mathematical Society, Providence, RI, 1999, pp. 527–554.

[7] *F. Ulmer and van der Put, MSRI Preprint #1998–058, have shown that once one knows that finite groups are Galois groups over $\mathbb{C}(t)$, then there are good methods to construct a linear differential equation having a given finite subgroup G of $GL_n(\mathbb{C})$ as a differential Galois group.*