DIFFERENTIAL GALOIS THEORY

MOSHE KAMENSKY

1. Introduction

We are interested in the following kind of statements:

proposition 1. *The integral $\int e^{-t^2} dt$ can not be solved by elementary functions.*

proposition 2. *The differential equation $x'' + tx = 0$ can not be solved by elementary functions and integration.*

The aim of the talk is to explain how to make these statements precise and prove them, using differential Galois theory. The reference to all of the material here is [vdPS03].

By *solving* a differential equation we mean obtaining a solution via a finite number of operations of the following kind (starting with a rational function):

- Adding a function algebraic over the functions we already have.
- Adding the exponential of (the integral of) a function we have.
- For the second problem, adding the integral of a function we have (alternatively, allowing logarithms)

At each stage, after adding the functions we are allowed to take any rational combinations of them, as well as their derivatives.

We first explain that the problem is completely algebraic. To this end, we define

definition 3. A *differential field* is a field K (of characteristic 0), endowed with a derivation $D : K \to K$. This means that D is additive and satisfies the Leibniz rule: $D(xy) = D(x)y + xD(y)$ for any $x, y \in K$. $D(x)$ will also be denoted by x'.

The set of elements of K satisfying $Dx = 0$ is a subfield of K called the *field of constants*, and is denoted C_K. D is thus a linear operator over C_K.

Examples of differential fields include the fields rational functions over the real or complex numbers, and more generally the field of meromorphic functions on a region in $\mathbb{P}^1(\mathbb{C})$, and subfields of such fields, all with the usual derivative.

Given a differential field K, it makes sense to consider differential equations with coefficients in K. Solutions of such equations will generally lie in (differential) field extensions of K. The first operation described above corresponds to forming algebraic field extensions of the field K (the derivation extends uniquely to such extensions.)

Adjoining an integral of a function amounts to passing to a field generated by the solution of an equation $x' = b$, where $b \in K$, or equivalently, by a non-constant solution of $x'' - (b'/b)x' = 0$. Similarly, the exponential of b is obtained as the solution of $x' - b'x = 0$. In both cases, as well as in the propositions we wish to prove, we are concerned with linear differential equations.

definition 4. Let K be a differential field. A *linear differential equation* over K is an equation of the form $L(x) = 0$, where L is an operator of the form $a_n D^n + \cdots + a_1 D + a_0$, with $a_i \in K$. n is called the *order* of L (and of the equation.)

A system of (first order) linear differential equations is an equation of the form $\bar{y}' = A\bar{y}$, where A is a matrix over K, and $\bar{y}$ is a column vector of variables, where the derivation acts coordinate wise. The order of such an equation is the dimension of A.

Any linear differential equation can be transformed to a system of first order equations of the same order by means of a simple change variables. This system is equivalent to the original equation in the sense that the set of solutions in any differential field extensions is canonically the same. We will mostly use the language of first order systems.

In any case, the following claim is easy:

proposition 5. *Let V be the set of solutions (in K) of a linear differential equation of order n over a field K. Then V is a vector space over C_K, of dimension at most n.*

The original statements can thus be reformulated by saying that a differential field extension of $\mathbb{C}(t)$ containing the solution of a particular equation can not be obtained as sequence of extensions of a particular kind. This is an analogue of the claim, in usual Galois theory, that certain algebraic extensions can not be obtained as sequence of a certain kind of algebraic extensions (radical ones.) The proof of these statements is also obtained analogously, by developing Galois theory for linear differential equations. To motivate the constructions, we shall recall the basic definitions of usual Galois theory.

2. Algebraic Galois theory

Let K be a field of characteristic 0, p an irreducible polynomial over it. The Galois group of the equation $p(x) = 0$ can be obtained as the automorphism group of the *splitting field* of the equation, which is the minimal field containing all solutions to the equation. This field can be constructed as follows: We consider the polynomial ring $K[x_1, \ldots, x_n]$, where n is the degree of p. The x_i stand for the solutions. To ensure that these solutions are distinct, we localise this ring by the polynomials $x_i - x_j$ (for $i \neq j$) to obtain a new ring A. We consider the ideal I in this ring generated by the polynomials $p(x_i)$, for all i. The quotient of A by any maximal ideal extending I is the splitting field L (as explained below, they are all isomorphic.) The Galois group G of p is defined to be the automorphism group of L.

In fact, G is an algebraic group over K, and $spec(L)$ is a *torsor* over G. To see this, and to identify the different constructions of the splitting field, we note that, given two such splitting fields L_1 and L_2, and given a maximal ideal m of $L_1 \otimes_K L_2$, the map $L_1 \to L_1 \otimes_K L_2/m$ is an isomorphism, since p splits to linear factors over L_1. Thus, the set of prime (or maximal) ideals of $L_1 \otimes_K L_2$ corresponds canonically with K-algebra isomorphisms between L_1 and L_2. In particular, we get a K-algebra isomorphism $L \otimes_K L \to L \otimes_K K[G]$, where $K[G]$, the dual space to the group algebra of G, is the algebra of functions on G (this morphism described explicitly by the map $G \to Hom(L \otimes_K L, L)$ given by $g \mapsto (a \otimes b \mapsto ag(b))$, corresponding to the identification above.)

To summarise, the Galois group can be obtained by first constructing the torsor $spec(L)$ (or the splitting field), and then recovering the group from it.

3. The Galois group associated with a linear differential equation

We are going to mimic the algebraic construction. Thus, we shall first construct the analogue of the splitting field. We will be working over a base differential field K. **We assume that the field C_K of constants is algebraically closed.** An example is $\mathbb{C}(t)$.

definition 6. A *differential algebra* over K is a K-algebra together with a derivation extending the derivation on K. A *differential ideal* in such an algebra is an ideal closed under the derivation. The quotient by such an ideal again has the structure of a differential algebra. A differential algebra is called *simple* if it has no non-trivial differential ideals.

Analogously to the usual Galois theory, we would like to construct a minimal differential algebra containing all possible solutions of a differential equation $y' = Ay$. As explained above, "all solutions", in this case, means that the dimension of the set of solutions is n, the dimension of A. We thus start with the algebra $K[X]$, where X is a matrix of variables of dimension n, whose columns correspond to solutions. This fact is ensured by giving this algebra a differential structure determined by $D(X) = AX$. To ensure that these columns are linearly independent, we localise by the determinant $det(X)$. Analogously to the algebraic case, we now divide the resulting algebra $K[X, X^{-1}]$ by a maximal differential ideal, to obtain a simple differential ring. Such a ring is called a *Picard-Vessiot* ring for the given equation.

lemma 7.
(1) *A maximal differential ideal is prime*
(2) *Let R be a Picard-Vessiot extension. Then $C_{K(R)} = C_K$.*
(3) *Any two Picard-Vessiot rings of the same equation are isomorphic.*

We may now ask more precisely the question we started with:

definition 8. Let $K \subseteq L$ be the Picard-Vessiot extension of an equation $y' = Ay$.
(1) The equation is called *Liouvillian* if there is a (finite) sequence of field extensions $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$ such that $K_{i+1} = K_i(t_i)$ where one of the following holds:
   (a) $t_i' \in K_i$ (*extension by integral*)
   (b) $t_i'/t_i \in K_i$ (*extension by exponential*)
   (c) t_i is algebraic over K_i (*algebraic extension*)
(2) If algebraic extensions are not allowed, the equation is called *solvable by quadratures*
(3) If only integrals (resp. exponentials) are allowed, the equation is said to be solvable by integrals (resp. exponentials.)

Thus, proposition 2 becomes the statement "The equation $x'' + tx = 0$ is not solvable by quadratures", and proposition 1 says "The equation $x'' + 2tx' = 0$ is not solvable by exponentials" (both over $\mathbb{C}(t)$.)

The Picard-Vessiot extension $K(R)$ is the analogue of the splitting field. Accordingly, we define the Galois group of the equation $y' = Ay$ as the group of differential automorphisms of a Picard-Vessiot extension $K(R)$ over K. This group is, in fact,

the group of C_K points of an affine algebraic group over C_K. The situation is analogous to the algebraic case:

theorem 9. *Let R be a Picard-Vessiot ring for the equation $y' = Ay$. There is a K-algebra isomorphism*

$$R \otimes_K R \to R \otimes_{C_K} H$$

where H is the algebra of functions of an affine algebraic group G over C_K. The group G acts on spec(R) via this map, making it into a G-torsor. The group of C_K points of G are identified via this action with the full group of automorphisms of R. G is called the Galois group of the equation.

It is important to stress that it is the algebraic group structure that is important, rather than just the group structure on the set of points. This becomes apparent in the next stage: to pursue further the analogy with the algebraic case, we require Galois correspondence. Such correspondence exists, when we replace fields by differential fields, and sub-groups by closed subgroups.

theorem 10. *Let L be a Picard-Vessiot extension of K, G the corresponding Galois group. There is a Galois correspondence between closed subgroups of G and differential subfields $L \supset M \supset K$, given by $H \mapsto L^H$, $M \mapsto Aut(L/M)$. Picard-Vessiot extensions correspond to normal subgroups.*

Before stating the final result, we recall some definitions regarding affine groups.

4. Affine algebraic groups

Since the Galois group of differential equation is an algebraic group, the study of solubility will require some facts about them. The following can be found in any book on algebraic groups, for example [Wat79]. We recall the following definitions:

definition 11. Let G be an affine algebraic group.

1. G is called *solvable* if there is a sequence of closed subgroups $G = G_n \supset \cdots \supset G_0 = 1$ with G_i normal in G_{i+1} with an abelian quotient.
2. G is called *unipotent* if any representation of G contains a trivial representation
3. G is called *diagonalisable* if any representation of G is a sum of one-dimensional representations. It is a *torus* if it is diagonalisable and connected.

We need a description of solvable group in terms of representations. This is possible when the group is connected, over an algebraically closed field of characteristic 0, and is called the Lie-Kolchin theorem:

theorem 12 (Lie-Kolchin)**.** *Let G be a connected group over an algebraically closed field of characteristic 0. Then G is solvable if and only if every representation of G contains a one-dimensional sub representation.*

(Recall that we are working with groups over such a field, so only the connectedness is an issue.)

The following corollary, summarising the facts we need, mostly follows directly from the definitions and the theorem.

corollary 13.
1. *A diagonalisable or unipotent group is solvable*
2. *Let $1 \to H \to G \to A \to 1$ be an exact sequence of algebraic groups.*

(a) *If H is solvable and A is abelian then G is solvable.*
(b) *If H and A are unipotent, so is G.*
(c) *If H and A are tori, so is G.*

(3) *G_a is unipotent, G_m is a torus.*
(4) *Let G be connected. G is solvable if and only if there is a sequence $G = G_n \supset \cdots \supset G_0 = H_l \supset \cdots \supset H_0 = 1$, where G_{i+1}/G_i is G_m and H_{i+1}/H_i is G_a. It is unipotent if and only if $n = 0$ and is a torus if and only if $l = 0$.*

Proof. (1) Such groups stabilise a full flag in a faithful representation
(2) (a) Obvious.
(b) Given a representation V of G, let V_0 be the (nontrivial) subspace of elements fixed by H. Since H is normal in G, V_0 is a sub-representation of G, and hence a representation of A. Any vector fixed by A will be fixed by G.
(c) We already know that G is solvable, so by the Lie-Kolchin theorem, V has a 1-dimensional sub-representation L. Consider $V \otimes \check{L}$.
(3) G_a is isomorphic to U_2. Representations of G_m are $\mathbb{Z}$-graded vector spaces.
(4) Assume G is solvable. If it has a non-trivial one-dimensional representation, then this is a morphism onto G_m (since G is connected), with a solvable kernel H. Replacing H by its connected component, we still get G_m as a quotient, so we may continue by induction. Assume now that any one-dimensional representation is trivial. By the Lie-Kolchin theorem, G is unipotent. Let V be a non-trivial representation, $v \in V$ a fixed vector, $V_1 = V/\langle v \rangle$, u a lifting of a fixed vector in V_1 to V. Since V is non-trivial, we may assume that u is not a fixed vector in V. Hence, for any $g \in G$, $g(u) - u = \alpha(g)v$ for some field element $\alpha(g)$. It is easy to see that this is a homomorphism to G_a, which is non-trivial since u is not fixed.

The converse follows from the previous items. □

5. Solvable differential equations

We may now state the main result, connecting solubility of differential equations with their Galois groups:

theorem 14. *Let $y' = Ay$ be a differential equation over a field K (with algebraically closed field of constants), and let G be its Galois group.*

(1) *The equation is Liouvillian if and only if G^0 (the connected component of G) is solvable.*
(2) *The equation is solvable by quadratures if and only if G is solvable.*
(3) *The equation is solvable by exponentials if and only if G is diagonalisable.*
(4) *The equation is solvable by integrals if and only if G is unipotent.*

We start by proving a special case:

lemma 15. *Let L be a Picard-Vessiot extension of K with a connected Galois group G. Then $G = G_a$ if and only if $L = K(t)$ with $t' \in K$. $G = G_m$ if and only if $L = K(t)$ with $t'/t \in K$.*

Proof. Let V be the set of solutions. It is a faithful representation of G. Assume $G = G_m$, and let t_1 be a non-trivial eigenvector. Then $t_1'/t_1 \in K$ (by Galois theory.)

Let t be such that generates a maximal subfield of L. Then $K(t) = L$, again by Galois theory.

Now assume that $G = G_a$, let v be a fixed vector, and let u be a non-fixed lift of a fixed vector in $V/\langle v\rangle$. Then $t = u/v$ satisfies the requirement.

□

The theorem is now a consequence of the last lemma and corollary 13:

Proof of theorem 14. Assume first that the equation satisfies the said condition, and let L be the Picard-Vessiot extension, so $L = K(t_1, \dots, t_n)$. We do induction on n. Since L is a Picard-Vessiot extension over $K(t_1)$, this field extension corresponds to a closed subgroup $H \subseteq G$. By induction, H is of the required form. If t_1 is an exponential or an integral, then G fixes $K(t_1)$ as a set, and so H is normal, and G/H is either G_a or a subgroup of G_m. In any case, corollary 13 gives the result. Otherwise, t_1 must be algebraic (and we are in the Liouvillian case), and this extension disappears when passing to the connected component.

Conversely, assume that the Galois group is of the prescribed form. If G is unipotent it is connected. If we are in the Liouvillian then we may pass to the connected component. In the other two cases, the quotient is a finite solvable group, so by usual Galois theory, the corresponding extension is obtained by adjoining roots, which can be realised as exponentials. In any case, we may assume that G is connected. The last part of corollary 13 now gives a quotient which is either G_a or G_m. We now use the lemma, and proceed by induction on the dimension of G. □

6. Galois groups of particular equations

The theorem allows us to immediately prove 1: One shows directly that there is no element of $F = \mathbb{C}(t, e^{-t^2})$ whose derivative is e^{-t^2}. Therefore, the Galois group of this integral over F is G_a, which is not diagonalisable. To show 2, we need to consider the Galois group of the equation $x'' + tx = 0$.

Let V be the space of solution of a linear differential equation inside its Picard-Vessiot extension. It is a vector space over C, the field of constants, and so has an associated projective space $\mathbb{P}(V)$. This space is not affine, but it is "differentially affine". The map from V to $\mathbb{P}(V)$ is given by $x \mapsto x'/x$. The Galois group G acts on $\mathbb{P}(V)$ by automorphisms. The Borel fixed point theorem says that if a connected solvable group G acts on a projective variety, then it has a fixed point. Thus, to show that such an equation is not solvable, it is enough to show that the connected component of G does not fix any point of $\mathbb{P}(V)$, which, using Galois theory, amounts to showing that the differential equation for $\mathbb{P}(V)$ does not have solutions algebraic over the fixed field.

In the case where the base field is $\mathbb{C}(t)$ and the equation is $x'' + r(t)x = 0$ ($r(t) \in \mathbb{C}(t)$), the equation for the projective space is $u' + u^2 = r$ (this is called the *Riccati equation.*) If r is a polynomial, it can be shown that the linear equation has a connected Galois group (the solutions, and hence any function in the field they generate, can only have ramification points where r is singular; and $\mathbb{P}^1$ has no cover with ramification only at ∞.) Let u be a meromorphic solution of the Riccati equation. A direct calculation shows that the order of $u' + u^2$ at ∞ is either positive or even. In particular, if r is a polynomial of odd degree, the group is not solvable.

References

[vdPS03] Marius van der Put and Michael F. Singer, *Galois theory of linear differential equations*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 328, Springer-Verlag, Berlin, 2003, `http://www4.ncsu.edu/~singer/papers/dbook2.ps`. MR MR1960772 (2004c:12010) 1

[Wat79] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979. MR MR547117 (82e:14003) 4

Department of Maths, University of East-Anglia, Norwich, NR4 7TJ, England
E-mail address: `mailto:m.kamensky@uea.ac.uk`
URL: `http://mkamensky.notlong.com`