Linear Differential Equations and Liouvillian Solutions

Felix Ulmer
Université de Rennes I

May 30, 1994

[summary by Jacques-Arthur Weil]

Let k be a differential field (e.g. $k = \mathbb{Q}(x)$ or $k = \mathbb{C}(x)$) with derivation $\frac{d}{dx}$. We review the methods of differential Galois theory used for solving the equation $L(y) = a_n y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0 y = 0$ (with $a_i \in k$). For effectivity and simplicity, we take $k = \overline{\mathbb{Q}}(x)$ in the sequel.

1. Classes of solutions

1.1. A solution is *rational* if it belongs to k. For example, the equation $a_2 y'' + xy' - y = 0$ has the solution $y = x$ which is in k. Algorithms for computing such solutions have been known for long. The first one is due to Liouville (1833). Some faster or more general versions have been given by Abramov [1], Bronstein [2], and Singer [4] (for the case when k contains a wider class of functions).

If there is no rational solution, then one must perform a field extension to find a solution. Let K be a differential field which is an extension of k, and Δ be the derivation on K (resp. δ on k). We say K is a differential field extension of k if Δ and δ coincide on k.

1.2. A solution y of L is *algebraic* if it belongs to an algebraic extension of k. In other words, there is an irreducible polynomial P with coefficients in k such that $P(y) = 0$. For example, if we define y as a zero of the polynomial $y^2 - x$, then y is a solution of $2xy' = y$. Work on characterising such solutions has been performed for example by Pépin, Klein, Jordan, Fuchs, Baldassari & Dwork, Singer (see e.g. [3, 6, 7] for further references).

1.3. A solution that is not algebraic is transcendental. An interesting class of solutions corresponds to the notion of "integrability by quadratures". A solution y of L is *Liouvillian* if it belongs to a field K such that:

(1) $K = K_n \supseteq \cdots \supseteq K_1 \supseteq K_0 = k$;
(2) $K_i = K_{i-1}(\eta_i)$ for $i = 1, \ldots, n$ and:
  (a) η_i is algebraic over K_{i-1}, or
  (b) $\eta_i' \in K_{i-1}$ (case of an integral), or
  (c) $\eta_i'/\eta_i \in K_{i-1}$ (case of exponential of an integral).

For example, if we take $L(y) = y'' - \frac{1}{2(x+1)}y' - (x+1)y = 0$, then $\{\exp[\int \sqrt{1+x}], \exp[-\int \sqrt{1+x}]\}$ forms a basis of liouvillian solutions.

1.4. There is a very important subclass of the liouvillian solutions: we say that a solution y is *exponential* if its logarithmic derivative is in k, i.e. $y'/y \in k$. For example, the equation $y'' - (2 + 4x^2)y = 0$ has the solution $y = e^{x^2}$ ($y'/y = 2x$). Methods for computing such solutions have been given, for example, by Singer or Bronstein [2, 4].

2. Differential Galois theory

The main known tool to compute liouvillian solutions of linear differential equations is differential Galois theory. Roughly, the idea is to look at the group of transformations that send a solution of the equation to another solution of the equation; from the knowledge of this group, one can derive algebraic properties of the solutions. We now outline this formalism.

2.1. Picard-Vessiot extensions. To a given vector space of solutions of L, one associates a field extension the following way. Since we work in a differential context, in order to adjoin an element y to k we must also add all its derivatives. We write $k\langle y\rangle := k(y, y', y'', \ldots)$. We say that $K \supset k$ is a *Picard-Vessiot extension* if $K = k\langle y_1, \ldots, y_n\rangle$, where $\{y_1, \ldots, y_n\}$ is a basis of the solution space of $L(y) = 0$, and K and k have the same field of constants C (elements with zero-derivative).

Then, we proceed as in classical Galois theory: The *differential Galois group* of L is the set $\mathrm{Gal}(L)$ of the automorphisms of K that let k point-wise fixed *and that commute with the derivation* (this definition does not depend on K). As in classical Galois theory, an element is in k if and only if it is left fixed by $\mathrm{Gal}(L)$; also, the subfields of K appear as fixed fields of some algebraic subgroup of $\mathrm{Gal}(L)$.

2.2. Galois group. Call V the vector space of solutions of L. As $\mathrm{Gal}(L)$ acts on V, we can decompose its action on a basis of V. The image of a solution of L is still a solution of L, so the image of an element of K is completely characterised by the images of the y_i in the basis $\{y_1, \ldots, y_n\}$. This provides a faithful matrix representation of degree n of the Galois group: $\mathrm{Gal}(L)$ can be viewed as a subgroup of $GL(n, C)$ (the group of invertible $n \times n$ matrices with entries in C).

In fact, $\mathrm{Gal}(L)$ is a *linear algebraic group* (its entries are solutions of a set of polynomial equations). So, the group has a structure of an algebraic variety. In particular, there is a component of this variety in which lies the origin; we denote it by $\mathrm{Gal}(L)^\circ$. A key fact is that L has a liouvillian solution if and only if $\mathrm{Gal}(L)^\circ$ is solvable (Picard-Vessiot, Kolchin). In this sense, finding liouvillian solutions is the differential analog of searching for solutions by radicals in the classical case.

2.3. Ricatti equation. A theorem of Lie-Kolchin on triangularization of matrix groups implies that $\mathrm{Gal}(L)^\circ$ is solvable if the elements of $\mathrm{Gal}(L)^\circ$ have a common eigenvector y: $\forall \sigma \in \mathrm{Gal}(L)^\circ, \exists c_\sigma \in C, \sigma(y) = c_\sigma y$. As a consequence $\sigma(\frac{y'}{y}) = \frac{\sigma(y')}{\sigma(y)} = \frac{c_\sigma y'}{c_\sigma y} = \frac{y'}{y}$, which means that y'/y is in the fixed field K° of $\mathrm{Gal}(L)^\circ$. This in turn implies that y'/y is algebraic over k.

As a consequence, there exists a $u = y'/y$ that is a solution of $P(u) = u^N + b_{N-1}u^{N-1} + \cdots + b_0 = 0$ and conversely, $y = \exp[\int u]$ is a solution of $L(y) = 0$. If we let $y' = uy$, then $y^{(i)} = R_i(u, u', \ldots)y$, with $R_i = R'_{i-1} + uR_{i-1}$. Replacing in L, we get that $\sum a_i R_i(u, u', \ldots) = 0$: this is a non-linear differential equation of order $n-1$ satisfied by u, called the *Ricatti equation.* For example, if $L = y'' - ry$, then the Ricatti equation is $u' + u^2 - r = 0$.

Finding a liouvillian solution is thus reduced to finding an algebraic solution of the Ricatti equation, which again splits into two subproblems: (1) find a bound for the degree N of P; (2) given N, compute the coefficients of a polynomial P such that its zeroes are logarithmic derivatives of solutions of L.

Problem (1) is solved by group-theoretic considerations. It follows from works of Kovacic or Singer that there is a function $f(n)$ such that $N \leq f(n)$ (e.g., $f(2) = 60, f(3) = 360, f(4) \leq 5040, f(5) \leq 25920, f(6) \leq 604800, \ldots$). Recent works of Ulmer and Singer & Ulmer show that sharp bounds are $N \leq 12$ for $n = 2$ and $N \leq 36$ for $n = 3$. We shall come back to this point later and we now focus on the actual computation of the coefficients of the polynomial P.

3. Computing a solution

3.1. Symmetric powers. Suppose for a moment that we work in an algebraic closure of k. There, P has N zeroes $u_1, \ldots, u_N$, and $P(u) = \prod(u - u_i)$. Since all zeroes of P are logarithmic derivatives of solutions of $L(y) = 0$, there are N solutions y_i such that the coefficient b_{N-1} satisfies $b_{N-1} = \frac{y_1'}{y_1} + \cdots + \frac{y_N'}{y_N} = \frac{(y_1 \cdots y_N)'}{y_1 \cdots y_N}$. For any integer m, one can construct a linear differential equation $L^{\circledS m}$, called the *m-th symmetric power of* L, whose solution space is spanned by all monomials of degree m in the $y_1, \ldots, y_n$. In particular, b_{N-1} is the logarithmic derivative of a solution of $L^{\circledS N}$: our problem is now reduced to finding exponential solutions of $L^{\circledS N}$. Similar techniques yield the other coefficients.

3.2. Reducible operators. Let $D = \frac{d}{dx}$. Then, $L(y)$ can be viewed as the action of the operator $\sum a_i D^i$ on y. Such operators form a non-commutative multiplicative ring $\mathcal{D} = k[D]$ in the following way: for $a \in k$, we have $D(ay) = aD(y) + a'y$, which give the multiplication rule on $\mathcal{D}$: $Da = aD + a'$ ($\mathcal{D}$ is called an Ore ring of type "derivation"). Before searching for solutions, one should first search if L factors in $\mathcal{D}$. For example, we have $D^2 = D.D = (D + 1/x)(D - 1/x)$. Algorithms performing such factorizations (or detecting reducibility) exist on $\mathbb{C}(x)$. The classical algorithm dates back to Beke/Schlesinger (1895); Grigor'ev, Singer, or Van Hoeij have recently proposed alternative methods.

In terms of solution space, $\mathrm{Gal}(L)$ has an invariant subspace of dimension m if and only if L has a factor of order m. In that case, we say that $\mathrm{Gal}(L)$ (resp. L) is *reducible.*

3.3. Irreducible operators. Assume that $\mathrm{Gal}(L)$ is irreducible. We say that $\mathrm{Gal}(L)$ is *imprimitive* if V is a direct sum of subspaces that are permuted transitively under the action of $\mathrm{Gal}(L)$. Otherwise, it is *primitive.* In general, if $\mathrm{Gal}(L)$ is irreducible then: either $\mathrm{Gal}(L)$ is imprimitive and $\exists y$ with $[k(y'/y) : k]$ small, or $\mathrm{Gal}(L)$ is primitive finite and $\exists y$ with $[k(y'/y) : k]$ big, or $\mathrm{Gal}(L)$ is primitive infinite and there is no liouvillian solution. This is made precise by the following theorems.

THEOREM 1 (KOVACIC, 1986). *Let L be of order 2 and* $\mathrm{Gal}(L) \subseteq SL(2, \mathbb{C})$*, then:*

(1) $\mathrm{Gal}(L)$ *is reducible, or*
(2) $\mathrm{Gal}(L)$ *is imprimitive and then* $\exists y$ *with* $[k(y'/y) : k] = 2$*, or*
(3) $\mathrm{Gal}(L)$ *is primitive and* $\exists y$ *with* $[k(y'/y) : k] = 4, 6, 12$*, or*
(4) $\mathrm{Gal}(L) = SL(2, \mathbb{C})$ *and* $L(y) = 0$ *has no liouvillian solution.*

THEOREM 2 (SINGER-ULMER, 1993). *Let L be of order 3 and* $\mathrm{Gal}(L) \subseteq SL(3, \mathbb{C})$*, then:*

(1) $\mathrm{Gal}(L)$ *is reducible and* $L = L_1(L_2)$ *or*
(2) $\mathrm{Gal}(L)$ *is imprimitive and then* $\exists y$ *with* $[k(y'/y) : k] = 3$*, or*
(3) $\mathrm{Gal}(L)$ *is primitive finite and* $\exists y$ *with* $[k(y'/y) : k] = 6, 9, 21, 36$*, or*
(4) *Else,* $L(y) = 0$ *has no liouvillian solutions.*

3.4. Algebraic solutions of L. In general, it is difficult to compute y from the knowledge of y'/y (Abel's problem), but one can compute y directly in the case of a known finite primitive group because y is then algebraic. It follows that y is algebraic over $k(y'/y)$, and one can show that there is an integer m such that $y^m \in k(y'/y)$. Thus, if d is one of the possible degrees for $[k(y'/y) : k]$, the minimum polynomial of y is of the form $P(y) = y^{m.d} + a_{d-1} y^{m.(d-1)} + \cdots + a_1 y^m + a_0$. This polynomial has the same number of coefficients as the minimum polynomial of an algebraic solution of the Ricatti equation. To show that the Ricatti equation had an algebraic solution, we showed that there was a subgroup of L with a common eigenvector. Such a subgroup is called

1-reducible. To find the group or a solution, we must therefore find a 1-reducible subgroup H of $\mathrm{Gal}(L)$ of minimal index. Suppose we have found such an H and let $\mathfrak{S} = \{\sigma_1, \ldots, \sigma_d\}$ be a system of representatives of $\mathrm{Gal}(L)/H$. If y_0 is the eigenvector of H, then

$$P(y) = \prod_{\sigma \in \mathfrak{S}} (y^m - \sigma(y_0)^m).$$

Now, as the a_i are rational, they are invariant under $\mathrm{Gal}(L)$. So, one can decompose the a_i in terms of invariants (or semi-invariants) of the group. Recall that a homogeneous polynomial $M(y_1, \ldots, y_n)$ is called an *invariant* of the group if it is left invariant under the action of the group ($\sigma(M)(y_i) = M(\sigma(y_i)) = M(y_i)$). Now, to detect if the group has invariants of degree m (resp. semi-invariants), one just has to search for rational solutions (resp. exponential solutions) of $L^{\circledS m}$, and we are almost done: as these solutions are given up to multiplication by constants, we just adjust the constants so as to really obtain the desired polynomials. Examples and more precise descriptions of this process are given in [5, 6].

4. Symmetric powers

The whole philosophy was to reduce the computation of Liouvillian solutions to the computation of exponential (and sometimes rational) solutions of some symmetric powers of L. In fact, group-theoretic considerations show that one can reduce the presence of liouvillian solutions to the reducibility of some symmetric powers. Conversely, reducibility of some symmetric powers helps finding the Galois group of a given linear differential equation.

THEOREM 3 (SINGER-ULMER). *Liouvillian solutions and symmetric powers are linked the following way:*

- *The equation $y'' - ry$ has a liouvillian solution if and only if $L^{\circledS 6}$ is reducible.*
- *The equation $L(y) = y''' - a_1 y' - a_0 y = 0$ has a Liouvillian solution if and only if $L^{\circledS 4}$ has order less than 5 or is reducible* AND *(a) $L^{\circledS 2}$ has order 6 and is irreducible* OR *(b) $L^{\circledS 3}$ has a factor of order 4.*

Bibliography

[1] Abramov (S. A.) and Kvashenko (K. Yu.). – Fast algorithms for the search of the rational solutions of linear differential equations with polynomial coefficients. In Watt (Stephen M.) (editor), *Symbolic and algebraic computation.* pp. 267–270. – New York, 1991. Proceedings ISSAC'91, Bonn, Germany.

[2] Bronstein (M.). – On solutions of linear ordinary differential equations in their coefficient field. *Journal of Symbolic Computation*, vol. 13, 1992, pp. 413–439.

[3] Singer (M. F.). – Liouvillian solutions of n-th order homogeneous linear differential equations. *American Journal of Mathematics*, vol. 103, n° 4, 1981, pp. 661–682.

[4] Singer (M. F.). – Liouvillian solutions of linear differential equations with Liouvillian coefficients. *Journal of Symbolic Computation*, vol. 11, 1991, pp. 251–273.

[5] Singer (Michael F.) and Ulmer (Felix). – Galois groups of second and third order linear differential equations. *Journal of Symbolic Computation*, vol. 16, 1993, pp. 1–36.

[6] Singer (Michael F.) and Ulmer (Felix). – Liouvillian and algebraic solutions of second and third order linear differential equations. *Journal of Symbolic Computation*, vol. 16, 1993, pp. 37–73.

[7] Ulmer (Felix). – On Liouvillian solutions of linear differential equations. *Applicable Algebra in Engineering, Communication and Computing*, vol. 2, 1992, pp. 171–193.