PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 55-62

Lucia Di Vizio

Direct Problem In Differential Galois Theory

Written by Alejandro Alberto Villa Isaza

1 Introduction

Galois theory of differential equations attaches an algebraic group to any linear differential system (over a differential field with an algebraically closed field of constants). Such a group provides algebraic information on the differential system. Unfortunately, the calculation of such a Galois group is quite complicated in general and we do not have an effective algorithm to accomplish this task. We present here an algorithm to calculate the Lie algebra of the Galois group, which works when the system is absolutely irreducible. The algorithm is being implemented in MAPLE.

1.1 A quick introduction to differential Galois theory

Let us consider the field $k := \mathbb{C}(x)$ of rational functions with complex coefficients, equipped with the derivation $\partial := \frac{d}{dx}$ acting trivially on $\mathbb{C}$ and such that $\partial(x) = 1$. We consider a linear differential system associated with the matrix A in the ring $M_n(k)$ of square matrix of

order n, with entries in k:

$$[A] : \partial(Y) = AY \tag{1}$$

Definition 1 *A Picard-Vessiot extension for the differential system* (1) *is a field extension L/k, equipped with an extension of the derivation ∂, such that:*

1. *there exists $U \in \mathrm{GL}_n(L)$, verifying $\partial(U) = AU$, whose entries generate L over k;*
2. *the fields of constants L^∂ of L is $\mathbb{C}$.*

An important point in the theory is that, when the field of constants is algebraically closed, as in our case, a Picard-Vessiot extension always exists. The differential Galois group G of $\partial(y) = Ay$ is defined as

$$G := \mathrm{Gal}^\partial(L/k) := \{\varphi \text{ is a field automorphim of } L/k, \text{ commuting to } \partial\}.$$

Any automorphism $\varphi \in G$ sends U to another invertible matrix of solutions of $\partial y = Ay$, so that $U^{-1}\varphi(U) \in \mathrm{GL}_n(\mathbb{C})$. This gives a representation $G \to \mathrm{GL}_n(\mathbb{C})$ of G as a group of matrices. It turns out that G coincide with (the $\mathbb{C}$-points of) an algebraic group defined over $\mathbb{C}$. Notice that the choice of another invertible matrix of solutions leads to a conjugated representation of G.

One can define a Galois correspondence among the intermediate fields of L/k stable by ∂ and the linear algebraic subgroups of G defined over $\mathbb{C}$: to each closed algebraic subgroup H of G, one associates the field L^H of elements stable by H; to each intermediate field M of L/k, stable under ∂, one associates the group $\mathrm{Gal}^\partial(L/M)$. The relative algebraic closure $\tilde{k}$ of k in L corresponds to the connected component G_0 of the identity, so that $G_0 = \mathrm{Gal}^\partial(L/\tilde{k})$. By definition, the Lie algebra $\mathfrak{g}$ of G is the tangent space to G, or to G_0, at 1.

This is a sketch of an outline of difference Galois theory. For an extended reference, see [8].

1.2 The direct problem

The algebraic group G encodes a lot of information about the system (1), as the many applications of differential Galois theory show. For instance, the dimension of G as a variety over $\mathbb{C}$ is equal to the transcendence degree of L/k (see [8, Corollary 1.30]). Another example is the following: the connected component G_0 of G is solvable if and only if L/k is Liouvillian, that is L is obtained from k as a result of a tower of extensions of the form $K(u)/K$ such that either u is algebraic over K, or $\partial(u) \in K$ or $\partial(u)/u \in K$ (see [8, §1.5]).

The examples above show the interest of being able to calculate the differential Galois group of a differential system. The reader will also notice that, in both examples, the information needed on G can be read on G_0 or on its Lie algebra $\mathfrak{g}$.

There exist some algorithms to calculate differential Galois groups. For instance we can effectively calculate the Galois group of a differential system of rank 2, using Kovacic's algorithm [6]. There are some "theoretic" algorithms that do not make any assumption on the rank of the system: [2], [4], [7], [3]. None of them is implemented.

2 Why calculating $\mathfrak{g}$ rather than G?

2.1 Reduced forms

We denote $\bar{k}$ the algebraic closure of k. Given $A = (a_{ij}) \in M_n(\bar{k})$, we fix a basis $\alpha_1, \alpha_2, \ldots, \alpha_r \in \bar{k}$ of the $\mathbb{C}$-vector space spanned by the a_{ij}'s. Then there exist $M_1, M_2, \ldots, M_r \in M_n(\mathbb{C})$ such that $A = \sum_{h=1}^{r} \alpha_h M_h$. The matrices $M_1, M_2, \ldots, M_r$ are a Wei-Norman decomposition of A. We define $\mathrm{Lie}(A)$ as the smallest algebraic Lie sub-algebra of $M_n(\mathbb{C})$ containing $M_1, M_2, \ldots, M_r$. The Lie algebra $\mathrm{Lie}(A)$ does not depend on the choice of $\alpha_1, \alpha_2, \ldots, \alpha_r$.

Theorem 1 (Kolchin-Kovacic, [8, Corollary 1.32]) *For any differential system* (1)*, we have the inclusion* $\mathfrak{g} \subset \mathrm{Lie}(A)$*. Moreover there exists*

$P \in GL_n(\bar{k})$ *such that* $P[A] := \partial(P)P^{-1} + PAP^{-1} \in \mathfrak{g}(\bar{k})$

The statement above is not very precise. Indeed, it is not $\mathfrak{g}$ which contains $P[A]$, but a conjugated algebra of $\mathfrak{g}$. In fact, we are conjugating the representation of $\mathfrak{g}$ by changing the system. However the theorem means that, up to conjugation, we have $\mathfrak{g} \subset \mathrm{Lie}(P[A])$, and hence that $\mathfrak{g} = \mathrm{Lie}(P[A])$.

Definition 2 *In the notation of the theorem above, we say that* $\partial Z = P[A]Z$ *is a reduced form of* $\partial Y = AY$.

2.2 Characterization of reduced forms

A differential module $\mathcal{M} = (M, \nabla)$ over k is a finite dimensional k-vector space M, say of dimension n, equipped with a $\mathbb{C}$-linear map $\nabla : M \to M$, such that $\nabla(fm) = \partial(f)m + f\nabla(m)$ for all $f \in k$ and $m \in M$. For any basis $\underline{e}$ of M over k, we have $\nabla(\underline{e}) = \underline{e}(-A)$, for some $A \in M_n(k)$. Hence an element $m \in M$, that is written as $m = \underline{e}y$, for some $y \in k^n$, verifies $\nabla(m) = 0$ if and only if $\partial(y) = Ay$. We say that $\partial(y) = Ay$ is the differential system associated to $\mathcal{M}$ in the basis $\underline{e}$. If $\underline{f}$ is another basis of M such that $\underline{e} = \underline{f}P$, then a direct calculation shows that $\nabla(\underline{f}) = \underline{f}(-P[A])$. This means that finding a reduced form is equivalent to finding a convenient basis of $\mathcal{M}$ over k.

We denote by $\mathrm{Constr}(M)$ an algebraic construction of M, i.e., a vector space obtained from M by taking duals, tensor products, direct sums and subquotients. Any such $\mathrm{Constr}(M)$ is endowed with a natural action of ∇ (see [8, §2.2] for a detailed description of the action of ∇). We denote by $\mathrm{Constr}(\mathcal{M})$ the corresponding differential module and by $\partial(y) = \mathrm{Constr}(A)y$ the system associated to $\mathrm{Constr}(\mathcal{M})$ in the basis induced by $\underline{e}$.

Notice that, if $x_0 \in \mathbb{C}$ is an ordinary point for $\partial y = Ay$, i.e., if A does not have any pole at x_0, then it is an ordinary point for any $\partial y = \mathrm{Constr}(A)y$.

Theorem 2 ([1]) *In the notation above, let x_0 be an ordinary point for $\partial y = Ay$. Then we have:*

1. *$\partial Y = AY$ is in reduced form if and only if for all algebraic construction $Constr(\mathcal{M})$ and all vectors of solution y of $\partial y = Constr(A)y$ with coefficients in k, the vector y has its coefficients in $\mathbb{C}$.*

2. *If $\partial y = AY$ is not a reduced form, then there exists a matrix $P \in GL_n(\bar{k})$ such that $\partial Z = P[A]Z$ is in reduced form and that any solution y of $\partial Y = Constr(A)Y$ with coefficients in k is sent to its value $y(x_0)$ at x_0 by the basis change associated to P.*

The theorem above says that $y(x_0)$ is solution of $\partial Y = P[\mathrm{Constr}(A)]Y$ and that $P[\mathrm{Constr}(A)] = \mathrm{Constr}(P[A])$

3 Some properties of $\mathfrak{g}$

In this paragraph, we are going to state some properties of $\mathfrak{g}$ that we use in the algorithm. The statements below are non trivial, but their proof is beyond the scope of this short exposition.

Let L be a Picard-Vessiot extension for the system $\partial y = Ay$, associated to a differential module $\mathcal{M}$, in a fixed basis. The action of ∇ extends naturally to $M \otimes_k L$, since L comes equipped with an extension of ∂. We set $V := (M \otimes_k L)^{\nabla} := \{m \in M \otimes_k L : \nabla(m) = 0\}$. By construction of L, V is a $\mathbb{C}$-vector space of dimension n and it is endowed with an action of G. We have a representation $G \to \mathrm{GL}(V)$, which allows to see $\mathfrak{g}$ as a sub-Lie algebra of $\mathrm{End}(V)$, invariant under the adjoint action of G, namely $G \times \mathrm{End}(V) \to \mathrm{End}(V)$, $(g, \psi) \mapsto g\psi g^{-1}$.

There exist two one-to-one correspondences between:

1. the subspaces of the algebraic constructions of V that are stable by the action of G,

2. the sub-differential modules of all the algebraic constructions of $\mathcal{M}$, i.e., all the sub-k-vector space of all the algebraic constructions of $\mathcal{M}$ that are stable by ∇.

They are defined by:

$$W \mapsto (W \otimes_{\mathbb{C}} L)^G, \quad (N, \nabla) \mapsto (N \otimes_k L)^{\nabla},$$

and are inverse of each other. The action of ∇ on $(W \otimes_{\mathbb{C}} L)^G$ is defined using the fact that W is a vector space of solution of a linear differential system.

As we have pointed out, the Lie algebra $\mathfrak{g}$ is a G-invariant sub-$\mathbb{C}$-vector space of $\mathrm{End}(V)$, hence $\mathfrak{g}^k := (\mathfrak{g} \otimes_{\mathbb{C}} L)^G$ is a sub-Lie algebra of $\mathrm{End}(\mathcal{M}) \cong \mathcal{M} \otimes \mathcal{M}^*$.[1]

The algorithm that we are presenting here, is articulated in two parts: first it calculates $\mathfrak{g}^k$ and then deduces $\mathfrak{g}$ from $\mathfrak{g}^k$, constructing the matrix P mentioned in Theorem 2. Indeed, $\mathfrak{g}^k$ is a sub-module of $\mathcal{M} \otimes_k \mathcal{M}^*$, stable by ∇. Hence it is generated by some matrices $M_i(x) \in M_n(k)$, for $i = 1, \ldots, s$. Then $\mathfrak{g}$ will be generated by their values $M_i(x_0)$ in an ordinary point x_0.

4 The algorithm

The algorithm works under the following assumption: the differential module $\mathcal{M}$ is absolutely irreducible, that is, the differential module $\mathcal{M} \otimes_k \bar{k}$ does not have any non trivial sub-differential module. This ensures that $\mathfrak{g}$ acts irreducibly on V and that $\mathcal{M} \otimes_k \mathcal{M}^*$ is a direct sum of irreducible differential modules.

We also make the more innocent assumption, to whom one can always reduce, that $\mathfrak{g}$ is contained in $\mathfrak{sl}_n(\mathbb{C})$, which implies that $\mathfrak{g}$ is semi-simple.

The algorithm proceeds as follow:

[1] The Lie algebra $\mathfrak{g}^k$ is nothing else than the Lie algebra introduced by N. Katz in [5].

1. One decomposes $\mathcal{M} \otimes_k \mathcal{M}^*$ using the properties of the eigenring (see [8, Proposition 2.40]). This boils down to finding the rational solutions of a differential system of rank n^4, which increases considerably the complexity of the algorithm. Fortunately, there are some canonical decompositions of $\mathcal{M} \otimes_k \mathcal{M}^*$ that allow, for instance, to consider two differential systems of rank $(n^2-1)n^2/2$ and $(n^2-1)(n^2-2)/2$, rather than of rank n^4. In spite of the appearances, it is quite a gain since for $n = 3$ one has to solve two systems of rank 36 and 28, which is already much faster than solving a system of rank 81.

2. One has to select the pieces of the decomposition of $\mathcal{M} \otimes_k \mathcal{M}^*$ containing $\mathfrak{g}^k$. This is done systematically, testing all the proper submodules of $\mathcal{M} \otimes_k \mathcal{M}^*$. So, the algorithm selects a maximal submodule $\mathfrak{g}^{guess}$ and it goes to the next step to test it.

3. The test consists in trying to find the matrix P. There are two possibilities:
   a) It can find P: it means that $\mathfrak{g}^k \subset \mathfrak{g}^{guess}$. Then it goes back to step 2 and tests of all the proper maximal submodules of $\mathfrak{g}^{guess}$ to see if it has to replace $\mathfrak{g}^{guess}$ by a smaller candidate or if we have found $\mathfrak{g}^k$ and P, and therefore $\mathfrak{g}$.
   b) It cannot find P: it means that $\mathfrak{g}^k \not\subset \mathfrak{g}^{guess}$, so it goes back to step 2 and picks another candidate.

References

[1] A. Aparicio Monforte, E. Compoint, and J.-A. Weil. A characterization of reduced forms of linear differential systems. *Journal of Pure and Applied Algebra*, 217(8):1504–1516, 2013.

[2] E. Compoint and M. F. Singer. Computing Galois groups of completely reducible differential equations. *J. Symbolic Computation*, 28(4-5):473–494, 1999.

[3] R. Feng. Hrushovski's algorithm for computing the Galois group of a linear differential equation. *Advances in Applied Mathematics*, 65:1 – 37, 2015.

[4] E. Hrushovski. Computing the Galois group of a linear differential equation. In *Differential Galois theory (Bedlewo, 2001)*, volume 58 of *Banach Center Publ.*, pages 97–138. Polish Acad. Sci., Warsaw, 2002.

[5] N. M. Katz. A conjecture in the arithmetic theory of differential equations. *Bull. Soc. Math. France*, 110(2):203–239, 1982.

[6] J. J. Kovacic. An algorithm for solving second order linear homogeneous differential equations. *J. Symbolic Comput.*, 2(1):3–43, 1986.

[7] J. van der Hoeven. Around the numeric-symbolic computation of differential Galois groups. *J. Symbolic Comput.*, 42(1-2):236–264, 2007.

[8] M. van der Put and M. F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.

Alejandro Alberto Villa Isaza
Dipartimento Di Matematica e Fisica
Università Degli Studi Di Roma Tre
Largo San Leonardo Murialdo 1
00145, Rome, Italy.
email: villaisaza@mat.uniroma3.it