Lecture 3: Introduction to Galois theory of linear differential equations

Andrei Tsyganov

Yanqi Lake Beijing Institute of Mathematical Sciences and Applications,

2024.

At approximately the same time that were published the works of Kovaleskaya and Lyapunov on the rigid body and motivated by the classical Galois theory of algebraic equations, Picard and, in a more clear way Vessiot in his Ph.D.Thesis, created and developed the differential Galois Theory of linear differential equations.

Then this theory is also called the Picard-Vessiot Theory and was also worked by Kolchin from the forties to the sixties along this century, who introduced the modern algebraic abstract terminology and obtained new important results.

Sauloy, J. Differential Galois Theory through Riemann-Hilbert Correspondence: An Elementary Introduction, American Mathematical Soc., 2016.

Linear Differential Equation

1) A differential ring (R, Δ) is a ring R with a set $\Delta = \{\partial_1, \dots, \partial_m\}$ of maps (derivations) $\partial_i : R \to R$, such that

1. $\partial_i(a+b) = \partial_i(a) + \partial_i(b), \quad \partial_i(ab) = \partial_i(a)b + a\partial_i(b)$ for all $a, b \in R$, and
2. $\partial_i\partial_j = \partial_j\partial_i$ for all i, j.

2) The ring $C_R = \{c \in R \mid \partial(c) = 0 \ \forall\, \partial \in \Delta\}$ is called the ring of constants of R.

When $m = 1$, we say R is an ordinary differential ring (R, ∂).

We frequently use the notation a' to denote $\partial(a)$ for $a \in R$.

A differential ring that is also a field is called a differential field. If k is a differential field, then C_k is also a field.

Examples

- $(C^\infty(\mathbb{R}^m), \Delta = \{\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_m}\})$ = infinitely differentiable functions on $\mathbb{R}^m$.
- $(\mathbb{C}(x_1, \dots, x_m), \Delta = \{\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_m}\})$ = field of rational functions
- $(\mathbb{C}[[x]], \frac{\partial}{\partial x})$ = ring of formal power series

  $\mathbb{C}((x)) =$ quotient field of $\mathbb{C}[[x]] = \mathbb{C}[[x]][\frac{1}{x}]$
- $(\mathbb{C}\{\{x\}\}, \frac{\partial}{\partial x})$ = ring of germs of convergent series

  $\mathbb{C}(\{x\}) =$ quotient field of $\mathbb{C}\{\{x\}\} = \mathbb{C}\{\{x\}\}[\frac{1}{x}]$
- $(\mathcal{M}_{\mathcal{O}}, \Delta = \{\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_m}\})$ = field of functions meromorphic on $\mathcal{O}^{\text{open,connected}} \subset \mathbb{C}^m$

Many examples are reduced to Example 5) because

> Any differential field k, finitely generated over $\mathbb{Q}$, is isomorphic to a differential subfield of some $\mathcal{M}_{\mathcal{O}}$.

There are three different versions of the notion of a linear differential equation.

Let (k, ∂) be a differential field.

1. A scalar linear differential equation is an equation of the form

$$L(y) = a_n y^{(n)} + \dots + a_0 y = 0, \; a_i \in k.$$

2. A matrix linear differential equation is an equation of the form

$$Y' = AY, \; A \in \mathrm{gl}_n(k)$$

   where $\mathrm{gl}_n(k)$ denotes the ring of $n \times n$ matrices with entries in k.

3. A differential module of dimension n is an n-dimensional k-vector space M with a map $\partial : M \to M$ satisfying

$$\partial(fm) = f'm + f\partial m \text{ for all } f \in k, m \in M.$$

From scalar to matrix equations

Given

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0 y = 0,$$

put $y_1 = y, y_2 = y', \ldots y_n = y^{(n-1)}$, then we have

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n-1} \\ y_n \end{pmatrix}' = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{n-1} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n-1} \\ y_n \end{pmatrix}$$

We shall write this last equation as $Y' = A_L Y$ and refer A_L as the companion matrix of the scalar equation and the matrix equation as the companion equation.

Clearly any solution of the scalar equation yields a solution of the companion equation and vice versa.

From matrix equations to differential modules

Given $Y' = AY, \ A \in \mathrm{gl}_n(k)$, we construct a differential module in the following way:

Let $M = k^n, \ e_1, \dots, e_n$ the usual basis. Define $\partial e_i = -\sum_j a_{j,i} e_j$, i.e., $\partial e = -A^t e$. Note that if $m = \sum_i f_i e_i$ then $\partial m = \sum_i (f_i' - \sum_j a_{i,j} f_j) e_i$.

In particular, we have that $\partial m = 0$ if and only if

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}' = A \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

Conversely, given a differential module (M, ∂), select a basis $e = (e_1, \dots, e_n)$. Define $A_M \in \mathrm{gl}_n(k)$ by $\partial e_i = \sum_j a_{j,i} e_j$.

This yields a matrix equation $Y' = AY$.

If $\bar{e} = (\bar{e}_1, \dots, \bar{e}_n)$ is another basis, we get another equation $Y' = \bar{A} Y$.

Galois theory of polynomials

The idea behind the Galois theory of polynomials is to associate to a polynomial a group of symmetries of the roots that preserve all the algebraic relations among these roots and deduce properties of the roots from properties of this group.

Let $P(X) \in k[X]$ be a polynomial of degree n without repeated roots (i.e., $\mathsf{GCD}(P.P') = 1$) over field k of characteristic 0 for siplicity. Let

$$S = k\left[X_1, \dots, X_n, \frac{1}{\prod(X_i - X_j)}\right]$$

and $I = (P(X_1), \dots, P(X_n)) \triangleleft S$ be the ideal generated by the $P(X_i)$.

The ring S/I is generated by n distinct roots of P but does not yet reflect the possible algebraic relations among these roots. We therefore consider any maximal ideal M in S containing I.

This ideal can be thought of as a maximally consistent set of algebraic relations among the roots.

Galois group

1) The splitting ring of the polynomial P over k is the ring

$$R = S/M = k\left[X_1, \dots, X_n, \frac{1}{\prod(X_i - X_j)}\right]/M .$$

2) The Galois group of P (or of R over k) is the group of automorphisms $\mathtt{Aut}(R/k)$.

Because M is a maximal ideal, R is actually a field and since S contains $\frac{1}{\prod(X_i - X_j)}$, the images of the X_i in R are distinct roots of P.

So, in fact, R coincides with the usual notion of a splitting field (a field generated over k by the distinct roots of P) and as such, is unique up to k-isomorphism.

As sequence, R is independent of the choice of maximal ideal M containing I!

Galois theory of linear differential equations

Let (k, ∂) be a differential field and $Y' = AY, A \in \mathrm{gl}_n(k)$ a matrix differential equation over k. We now want the Galois group to be the group of symmetries of solutions preserving all algebraic and differential relations. We proceed in a way similar to the above.

Let

$$S = k\left[Y_{1,1}, \dots, Y_{n,n}, \frac{1}{\det(Y_{i,j})}\right]$$

where $Y = (Y_{i,j})$ is an $n \times n$ matrix of indeterminates.

We define a derivation on S by setting $Y' = AY$.

The columns of Y form n independent solutions of the matrix linear differential equation $Y' = AY$ but we have not yet taken into account other possible algebraic and differential relations.

To do this, let M be any maximal differential ideal and let $R = S/M$.

Definition

Let (k, ∂) be a differential field and $Y' = AY, A \in \mathfrak{gl}_n(k)$ a matrix differential equation over k.

A Picard-Vessiot ring (PV-ring) for $Y' = AY$ is a differential ring R over k such that

1. R is a simple differential ring (i.e., the only differential ideals are (0) and R).
2. There exists a fundamental matrix $Z \in \mathrm{GL}_n(R)$ for the equation $Y' = AY$.
3. R is generated as a ring by k, the entries of Z and $\frac{1}{\det Z}$.

If C_k is algebraically closed then any PV-rings for the same equation are k-isomorphic as differential rings and $C_k = C_R$.

Since a PV-ring is a domain we define a PV-field K to be the quotient field of a PV-ring.

Example

Let

$$k = \mathbb{C}(x), \qquad x' = 1, \quad \alpha \in \mathbb{C}, \quad Y' = \frac{\alpha}{x} Y$$

so that

$$S = k[Y, \frac{1}{Y}].$$

Suppose that

$$\alpha = \frac{n}{m}, \quad GCD(n, m) = 1.$$

In this case

$$\mathcal{R} = k[Y, \frac{1}{Y}]/[Y^m - x^n] = k(x^{\frac{m}{n}}).$$

To see this note that the ideal $(Y^m - x^n) \triangleleft k[Y, \frac{1}{Y}]$ is a maximal ideal and closed under differentiation since

$$(Y^m - x^n)' = \frac{n}{x}(Y^m - x^n).$$

Definition of differential Galois group

Let (k, ∂) be a differential field and R a PV-ring over k. The differential Galois group of R over k, $\mathsf{DGal}(R/k)$ is the group $\{\sigma : R \to R \mid \sigma \text{ is a differential } k\text{-isomorphism}\}$.

Let R be a PV-ring for the equation $Y' = AY$ over k and $\sigma \in \mathsf{DGal}(R/k)$.

Fix a fundamental solution matrix Z and let $\sigma \in \mathsf{DGal}(R/k)$.

We then have that $\sigma(Z)$ is again a fundamental solution matrix of $Y' = AY$ and, a calculation shows that $(Z^{-1}\sigma(Z))' = 0$.

Therefore, $\sigma(Z) = Zm_\sigma$ for some $m_\sigma \in \mathrm{GL}_n(C_k)$. This gives an injective group homomorphism $\sigma \mapsto m_\sigma$ of $\mathsf{DGal}(R/k)$ into $\mathrm{GL}_n(C_\sigma)$.

If we select a different fundamental solution matrix, the images of the resulting maps would be conjugate.

Fundamental Theorem of Differential Galois Theory

Let k be a differential field with algebraically closed constants C_k.

Let K be a Picard-Vessiot field with differential Galois group G.

1) There is a bijective correspondence between Zariski-closed subgroups $H \subset G$ and differential subfields F, $k \subset F \subset K$ given by

$$H \subset G \quad \mapsto \quad K^H = \{a \in K \mid \sigma(a) = a \text{ for all } \sigma \in H\}$$

$$k \subset F \subset K \quad \mapsto \quad \mathrm{DGal}(K/F) = \{\sigma \in G \mid \sigma(a) = a \text{ for all } a \in F\}$$

2) A differential subfield $k \subset F \subset K$ is a Picard-Vessiot extension of k if and only if $\mathrm{DGal}(K/F)$ is a normal subgroup of G, in which case $\mathrm{DGal}(F/k) \simeq \mathrm{DGal}(K/k)\mathrm{DGal}(K/F)$.

The Zariski closed sets form the collection of closed sets of a topology on GL_n and in this topology each linear algebraic group G may be written (uniquely) as the finite disjoint union of connected closed subsets.

With the identification above $\mathsf{DGal}(R/k) \subset \mathrm{GL}_n(C_k)$ we have

Proposition

$\mathsf{DGal}(R/k) \subset \mathrm{GL}_n(C_k)$ is a linear algebraic group.

The differential Galois group measures the algebraic relations among solutions of the linear differential equations.

In general, it is not easy to compute Galois groups, although there is a complete algorithm due to Hrushovski

E. Hrushovski. Computing the Galois group of a linear differential equation. In T. Crespo and Z. Hajto, editors,Differential Galois Theory, volume 58 of Banach Center Publications, pages 97-138. Institute of Mathematics, Polish Academy of Sciences, Warszawa, 2002.

Below we will study some partial cases and, of course, matrix linear differential equations associated with the Hamiltonian systems.

Monodromy

We will need the definition of the monodromy group of a linear differential equation.

Consider differential equations over the complex numbers, so let $k = \mathbb{C}(x),\ x' = 1$ and

$$\frac{dY}{dx} = A(x)Y,\ A(x) \in \mathrm{gl}_n(\mathbb{C}(x)) \qquad (*)$$

Definition

A point $x_0 \in \mathbb{C}$ is an ordinary point of equation (*) if all the entries of $A(x)$ are analytic at x_0, otherwise x_0 is a singular point.

Example: Equation

$$\frac{dy}{dx} = \frac{\alpha}{x}y$$

has the singular points are $\{0, \infty\}$.

Let $S = \mathbb{CP}^1$ be the Riemann Sphere,

$$X = S^2 - \{\text{singular points of } (*)\}\,, \qquad x_0 \in X.$$

From standard existence theorems, we know that in a small neighborhood $\mathcal{O}$ of x_0, there exists a fundamental matrix Z whose entries are analytic in $\mathcal{O}$.

Let $\boldsymbol{\gamma}$ be a closed curve in X based at x_0. Analytic continuation along $\boldsymbol{\gamma}$ yields a new fundamental solution matrix Z_γ at x_0 which must be related to the old fundamental matrix as

$$Z_\gamma = Z D_\gamma\,, \qquad D_\gamma \in \mathrm{GL}_n(\mathbb{C}).$$

One can show that D_γ just depends on the homotopy class of $\boldsymbol{\gamma}$. This defines a homomorphism

$$\begin{array}{rcl} \mathtt{Mon} : \pi_1(X, x_0) & \to & \mathrm{GL}_n(\mathbb{C}) \\ \boldsymbol{\gamma} & \mapsto & D_\gamma \end{array}$$

This homomorphism carries the group structure of $\pi_1(S, x_0)$, and thus its image is also a group.

Definition

The homomorphism $\mathtt{Mon}$ is called the monodromy map and its image is called the monodromy group.

Note that the monodromy group depends on the choice of Z so it is only determined up to conjugation. Since analytic continuation preserves analytic relations, we have that the monodromy group is contained in the differential Galois group.

Example:

$$y' = \frac{\alpha}{x} y \,, \quad (y = e^{\alpha \log x} = x^{\alpha}) \quad \text{singular points} = \{0, \infty\}$$

$$\mathtt{Mon}(\pi_1(X, x_0)) = \{(e^{2\pi i \alpha})^n \mid n \in \mathbb{Z}\}$$

If $\alpha \in \mathbb{Q}$ this image is finite and so equals the differential Galois group.

If $\alpha \notin \mathbb{Q}$, then this image is infinite and so Zariski dense in $\mathrm{GL}_1(\mathbb{C})$.

Since analytic continuation preserves analytic relations, the monodromy group is a subset of the differential Galois group over the base field of meromorphic functions on S; in particular, it is included in the differential Galois group over the base field of rational functions.

For Fuchsian systems (all singularities are regular singularities, i.e. the growth at singularities of solutions is at most polynomials), we have moreover the following:

Schlesinger density theorem

Let $(*): \; Y' = AY$ be a Fuchsian differential linear equation with coefficients in $\mathbb{C}(x)$ and let Π be its monodromy group.

Then Π is dense for the Zariski topology in the Galois group of the Picard-Vessiot extension of $(*)$ over the base field of rational functions: $\overline{\Pi} = \mathrm{Gal}(A)$.

Suppose that a system of ODE

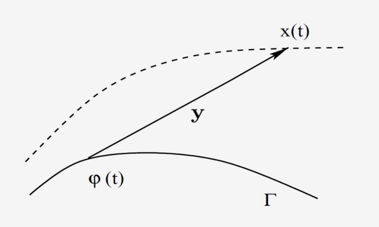
$$\frac{d}{dt}x = v(x_1, \dots, x_m)\,, \qquad (*)$$

has a known non-stationary particular solution $\varphi(t)$. Substitute

$$x = \varphi(t) + y$$

and obtain the so-called variational equation which we will study instead of (*)

$$\frac{d}{dt}y = A(t)y\,, \qquad A(t) = \frac{\partial v}{\partial x}(\varphi(t))\,.$$



Moralès-Ramis Theorem

Let H be an analytic Hamiltonian on a complex analytic symplectic manifold and Γ be a non constant solution. If H is integrable in the Liouville sense with meromorphic first integrals, then the first order variational equation along Γ has a virtually Abelian Galois group over the base field of meromorphic functions on Γ.

Definition

Algebraic group G is said to be virtually Abelian if its connected component containing the identity is an Abelian subgroup of G.

The main idea behind this theorem is that if H is Liouville integrable, then so are the linearized equations near a non constant solution Γ. More precisely the first integrals of H can be transformed in such a way that their first non trivial term in their series expansion near Γ are functionally independent.

Ziglin's Lemma

Let $\Phi_1, \dots, \Phi_r \in k(x_1, \dots, x_n)$ be functionally independent functions. We consider $\Phi_1^0, \dots, \Phi_r^0$ the lowest degree homogeneous term for some fixed positive weight homogeneity in $x_1, \dots, x_n$. Assume $\Phi_1^0, \dots, \Phi_{r-1}^0$ are functionally independent. Then there exists a polynomial Ψ such that the lowest degree homogeneous term Ψ^0 of $\Psi(\Phi_1, \dots, \Phi_r)$ is such that $\Phi_1^0, \dots, \Phi_{r-1}^0, \Psi^0$ are functionally independent.

Applying this Lemma recursively, we prove that if a Hamiltonian system admits a set of commuting, functionally independent meromorphic first integrals on a neighbourhood of a curve, then their first order terms, after possibly polynomial combinations of them, are also commuting, functionally independent meromorphic first integrals of the linearized system along the curve.

Moralès-Ramis precisely proved that symplectic linear differential systems having such first integrals have a Galois group whose identity component is Abelian. This result can be expected knowing that the Galois group leaves invariant every first integral, so the more first integrals, the smaller the Galois group.

References:

Kolchin E., Differential algebra and algebraic groups. Academic Press, New York, 1973.

Beukers F., Differential Galois Theory, From Number Theory to Physics, W.Waldschmidt, P.Moussa, J.-M.Luck, C.Itzykson Ed., Springer-Verlag, Berlin 1995, 413-439.

Morales Ruiz, J. J., Differential Galois theory and non-integrability of Hamiltonian systems, volume 179 of Progress in Mathematics, Birkhäuser Verlag, Basel, 1999.

Audin, M., Les systèmes hamiltoniens et leur intégrabilité, Cours Spécialisés 8, Collection SMF, SMF et EDP Sciences, Paris, 2001.

Singer, M. F. Introduction to the Galois Theory of Linear Differential Equations, Algebraic Theory of Differential Equations, Cambridge University Press, 357:1–82, 2009.