Computing the Lie algebra of the differential Galois group of a linear differential system (1/2)

## Thomas Cluzeau

University of Limoges ; CNRS; XLIM (France)


In collaboration with M. Barkatou, J.-A. Weil and L. Di Vizio (CNRS, UVSQ)

Functional Equations in LIMoges 2016

## Motivation

$\diamond k=\mathbb{C}(z)$ (for actual computations $\mathbb{C}$ is replaced by a computable subfield of $\overline{\mathbb{Q}}), A \in \mathbb{M}_{n}(k)$, y vector of unknown functions, ${ }^{\prime}=\frac{d}{d z}$

$$
\text { Linear differential system }[A]: \mathbf{y}^{\prime}=A \mathbf{y}
$$

$\diamond$ Important object for studying $[A]$ : its differential Galois group $G$
$\rightarrow G$ measures everything that algebra can see about the solutions
$\diamond$ Direct problem in diff. Galois theory: given [A], compute $G$

- Many theoretical algorithms: Compoint-Singer'99, Hrushovski'02 and Feng'15, van der Put-Singer'03, van der Hoeven'07
- None of them are either practical or implemented


## Objective

## Philosophy of our work (see also Nguyen-van der Put'10)

$\rightarrow$ For a large class of problems, computing the Lie algebra $\mathfrak{g}$ of the linear algebraic group $G$ is enough
$\diamond$ For the computation of $\mathfrak{g}$, not much is known (Aparicio's PhD thesis'10, Aparicio-Compoint-Weil'13)

$$
\text { Goal of this talk AND the next one by } \mathrm{T} \text {. Dreyfus }
$$

Provide a full algorithm for computing the Lie algebra $\mathfrak{g}$ of $G$

- This talk (1/2): irreducible and completely reducible systems
- Next talk (2/2): reducible systems


## I

Differential systems/modules/Galois group and Lie algebra

## Differential modules

$\diamond$ A differential module $\mathcal{M}$ over $k$ is a finite dimensional vector space over $k$ equipped with an additive $\operatorname{map} \partial: \mathcal{M} \rightarrow \mathcal{M}$ s.t.
$\forall f \in k, \forall m \in \mathcal{M}, \partial(f m)=f^{\prime} m+f \partial(m)$
A differential submodule of $\mathcal{M}$ is then a sub-vector space of $\mathcal{M}$ which is stable under the action of $\partial$
$\diamond$ A differential module $\mathcal{M}$ is

- irreducible if it has no non-trivial differential submodule
- absolutely irreducible if $\bar{k} \otimes_{k} \mathcal{M}$ is irreducible
- decomposable if $\mathcal{M}=\mathcal{M}_{1} \oplus \mathcal{M}_{2}$
- completely reducible if it is a direct sum of irreducible modules
$\diamond$ Krull-Schmidt: $\mathcal{M}=\mathcal{M}_{1} \oplus \mathcal{M}_{2} \oplus \cdots \oplus \mathcal{M}_{r}$, with $\mathcal{M}_{i}$ indecomposable. It is called a maximal decomposition of $\mathcal{M}$ ( $\mathbf{R} \mathbf{k}$ : if $\mathcal{M}$ is completely reducible, then the $\mathcal{M}_{i}$ are irreducible)


## Differential module $\leftrightarrow$ Differential system

$\diamond$ Via a choice of basis, a differential module $\mathcal{M}$ is associated with a linear differential system $[A]$ and vice versa
$\diamond$ Change of basis in $\mathcal{M} \leftrightarrow$ gauge transfo. $P \in \mathrm{GL}_{n}(k)$ in $[A]$ leading to equivalent system $[P[A]]$ with $P[A] \triangleq P^{-1}\left(A P-P^{\prime}\right)$
$\rightarrow \mathcal{M}$ reducible: $\exists P, P[A]=\left(\begin{array}{cc}A_{11} & 0 \\ A_{21} & A_{22}\end{array}\right)$ block triangular
$\rightarrow \mathcal{M}$ decomposable: $\exists P, P[A]=\left(\begin{array}{cc}A_{1} & 0 \\ 0 & A_{2}\end{array}\right)$ block diagonal
$\diamond \mathcal{M}=\mathcal{M}_{1} \oplus \cdots \oplus \mathcal{M}_{r} \leftrightarrow \exists P, P[A]=\left(\begin{array}{llll}A_{1} & & & \\ & A_{2} & & \\ & & \ddots & \\ & & & A_{r}\end{array}\right)$
Maximal dec. $\leftrightarrow\left[A_{i}\right]$ indec. ( $\mathbf{R} \mathbf{k}$ : irred. if $\mathcal{M}$ is completely red.)

## The differential module $\mathcal{M} \otimes_{k} \mathcal{M}^{\star}$

$\diamond \mathcal{M}$ differential module, $[A]$ associated differential system
$\diamond$ Its dual $\mathcal{M}^{\star} \triangleq \operatorname{Hom}_{k}\left(\mathcal{M}, \mathbb{1}_{k}\right)$ is associated with $\left[-A^{T}\right]$
$\diamond$ Consider $\mathcal{M} \otimes_{k} \mathcal{M}^{\star}$ : elements viewed in $\mathbb{M}_{n}(k)$
$\rightarrow \mathcal{M} \otimes_{k} \mathcal{M}^{\star}$ is associated with the matrix differential system

$$
F^{\prime}=[A, F] \triangleq A F-F A
$$

Using the classical Kronecker product of matrices:

$$
F^{\prime}=[A, F] \Longleftrightarrow \operatorname{Vect}(F)^{\prime}=\left(A \otimes I_{n}-I_{n} \otimes A^{T}\right) \operatorname{Vect}(F)
$$

with $\operatorname{Vect}(F)=\left(F_{1 \bullet}^{T} \ldots F_{n \bullet}^{T}\right)^{T} \in k^{n^{2}}$ and $F_{i \bullet}$ the $i$-th row of $F$
$\diamond \mathcal{M}$ completely reducible $\Rightarrow \mathcal{M} \otimes_{k} \mathcal{M}^{\star}$ is completely reducible

## The differential Galois group

$\diamond \mathcal{M}$ differential module associated with a differential system $[A]$
$\diamond K$ Picard-Vessiot extension for $\mathcal{M}$ : diff. field ext. of $k$
$\rightarrow[A]$ admits a fundamental matrix of solutions $U \in \mathrm{GL}_{n}(K)$
$\diamond$ The differential Galois group $G$ of $\mathcal{M}$ is the group $\operatorname{Aut}_{\partial}(K / k)$ of differential $k$-algebra automorphisms of $K$ :
$\forall g \in G, \forall f \in K, \quad g\left(f^{\prime}\right)=g(f)^{\prime}, \quad f \in k \Rightarrow g(f)=f$
$\diamond G$ viewed as a subgroup of $\mathrm{GL}_{n}(\mathbb{C})$ is a linear algebraic group:
There exists a polynomial ideal $\mathcal{I} \subset \mathbb{C}\left[X_{1,1}, X_{1,2}, \ldots, X_{n, n}, \operatorname{det}^{-1}\right]$, where $\operatorname{det}^{-1}$ is the inverse of $\operatorname{det}\left(\left(X_{i, j}\right)_{i, j}\right)$, such that

$$
G \cong\left\{M=\left(m_{i, j}\right)_{i, j} \in \mathrm{GL}_{n}(\mathbb{C}) \mid \forall P \in \mathcal{I}, P\left(m_{i, j}\right)=0\right\}
$$

## The Lie algebra $\mathfrak{g}$ of $G$

$\diamond$ The Lie algebra $\mathfrak{g}$ of $G$ is the tangent space of $G$ at the point id $\in G: \mathfrak{g}$ can be represented as a Lie sub-algebra of $\mathfrak{g l}_{n}(\mathbb{C})$

$$
\mathfrak{g} \cong\left\{N \in \mathbb{M}_{n}(\mathbb{C}) \mid I_{n}+\epsilon N \in G(\mathbb{C}[\epsilon]) \text { with } \epsilon \neq 0 \text { and } \epsilon^{2}=0\right\}
$$

where $G(\mathbb{C}[\epsilon])$ set of $\mathbb{C}[\epsilon]$-points of $G$
$\diamond$ Adjoint action of $G$ on $\mathfrak{g}: G \times \mathfrak{g} \rightarrow \mathfrak{g},(g, h) \mapsto g h g^{-1}$
$\diamond V \triangleq \mathbb{C}$-vector space of solutions of $[A]$ in $K^{n}, \operatorname{End}(V)$ endowed with a Lie algebra structure $\mathfrak{g l}(V)$ identified with $\mathfrak{g l}_{n}(\mathbb{C})$ $\Rightarrow$ We have a representation of $\mathfrak{g}$ in $\operatorname{End}(V)$
$\diamond U \operatorname{sing} \operatorname{End}(V) \cong V \otimes V^{\star}, \mathfrak{g}$ can then be viewed as a sub-vector space of $V \otimes V^{\star}$ stable under the adjoint action of $G$

## Tannakian correspondence and characterization of $\mathfrak{g}$

$\diamond$ Tannakian correspondence: 1-1 correspondence (compatible with all constructions of linear algebra) between sub-vector spaces of $V$ stable under the action of $G$ and differential submodules of $\mathcal{M}$
$\rightarrow$ The representation of $\mathfrak{g}$ in $\operatorname{End}(V)$ corresponds to the differential submodule $\mathfrak{g}^{s} \triangleq\left(K \otimes_{\mathbb{C}} \mathfrak{g}\right)^{G}$ of $\mathcal{M} \otimes_{k} \mathcal{M}^{*}$
( $\mathbf{R k}: \mathfrak{g}^{s}$ is the Lie algebra considered by Katz in his works)
$\rightarrow \mathfrak{g}^{\boldsymbol{s}}$ (and thus $\mathfrak{g}$ ) can be investigated by studying differential submodules of $\mathcal{M} \otimes_{k} \mathcal{M}^{*}$ which can all be obtained from a maximal decomposition if $\mathcal{M}$ is completely reducible

## Sketch of our algorithm

1. Compute a maximal decomposition of $\mathcal{M} \otimes_{k} \mathcal{M}^{\star}$ (tools: eigenring techniques \& use specific structure)
2. Find a candidate for $\mathfrak{g}^{s}$
(tools: modular approach based on Grothendieck-Katz p-curvature conjecture)
3. Validation of the candidate (tools: reduced form \& conjugation between Lie algebras)
$\diamond$ For the ease of presentation, in the following, we assume $\mathcal{M} /[A]$ absolutely irreducible (it can be checked: Compoint-Weil'04)
$\rightarrow$ Completely reducible case quite similar (only small modif.)
$\rightarrow$ Reducible case: see next talk by T. Dreyfus

## II

## Maximal decomposition of $\mathcal{M} \otimes_{k} \mathcal{M}^{\star}$

## Maximal decomposition: general method

Problem: given $[\mathrm{A}]$, find $P \in \mathrm{GL}_{n}(k)$ s.t. $P[A]$ block diagonal
$\diamond$ Already studied in computer algebra: Singer'96, Barkatou'07
$\rightarrow$ Compute the eigenring (rational solutions - Barkatou'99)

$$
\mathcal{E}(A) \triangleq\left\{F \in \mathbb{M}_{n}(k) \mid F^{\prime}=[A, F]=A F-F A\right\}
$$

$\diamond$ If $F \in \mathcal{E}(A), P^{-1} F P=\operatorname{diag}\left(F_{1}, \ldots, F_{r}\right)\left(F_{i}\right.$ constant matrices with distinct eigenvalues), then $P[A]=\operatorname{diag}\left(A_{1}, \ldots, A_{r}\right)$
$\diamond$ This corresponds to $\mathcal{M}=\mathcal{M}_{1} \oplus \cdots \oplus \mathcal{M}_{r}$, where the bases of the submodules $\mathcal{M}_{i}$ are given by the columns of $P$
$\diamond$ Maximal dec. given by a random element of $\mathcal{E}(A)$ (Barkatou'07)

## Maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^{\star}$ : specific methods (1)

$\diamond$ We can apply the previous method to $\mathcal{A} \triangleq A \otimes I_{n}-I_{n} \otimes A^{T}$
$\rightarrow$ Computing $\mathcal{E}(\mathcal{A})$ : rational solutions of $\mathcal{A} \otimes I_{n^{2}}-I_{n^{2}} \otimes \mathcal{A}^{T}$ of size $n^{4}$ ! BarkatouCluzeauEIBachaWeil' $12 \rightarrow O\left(n^{20}\right)$ arithm. op.
$\rightarrow$ We should take into account the specific form of $\mathcal{A}$
$\diamond$ Problem: compute rational solutions of $\overline{\mathcal{A}} \triangleq \mathcal{A} \otimes I_{n^{2}}-I_{n^{2}} \otimes \mathcal{A}^{T}$
$\diamond$ First approach: algorithm in Barkatou'99 proceeds in two steps:

1. Local data at each singularity $\rightarrow$ universal denominator
2. Polynomial solutions of an auxiliary system

Adapt ideas of BarkatouPfluegel' $98 \Rightarrow$ local datas needed for rational solutions of $\overline{\mathcal{A}}\left(\right.$ size $\left.n^{4}\right)$ can be computed from $[A]$ (size $n$ )
( $\mathbf{R k}$ : the second step can also be accelerated)

Maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^{\star}$ : specific methods (2)
$\diamond$ Second approach: use structural decompositions
$[\overline{\mathcal{A}}]$ associated with $\operatorname{End}(\operatorname{End}(\mathcal{M})) \triangleq\left(\mathcal{M} \otimes \mathcal{M}^{\star}\right) \otimes\left(\mathcal{M} \otimes \mathcal{M}^{\star}\right)^{\star}$
$\rightarrow$ Decompose $\operatorname{End}(\operatorname{End}(\mathcal{M}))$ and rational sol. of smaller systems
Theorem 1 (BCdVW'16): we have $\mathcal{M} \otimes \mathcal{M}^{\star}=\mathbb{1}_{k} \oplus \mathcal{W}$ and the explicit iso.

$$
\operatorname{End}(\operatorname{End}(\mathcal{M})) \cong \underbrace{\mathbb{1}_{k} \oplus \mathcal{W} \oplus \operatorname{Sym}^{2}(\mathcal{W})}_{\operatorname{Sym}^{2}\left(\mathbb{1}_{k} \oplus \mathcal{W}\right)} \oplus \underbrace{\mathcal{W} \oplus \Lambda^{2}(\mathcal{W})}_{\Lambda^{2}\left(\mathbb{1}_{k} \oplus \mathcal{W}\right)}
$$

Theorem 2 (BCdVW'16): we have the explicit iso.
$\operatorname{End}(\operatorname{End}(\mathcal{M})) \cong \underbrace{\mathbb{1}_{k} \oplus \mathcal{N}_{\mathrm{S}^{2}}}_{\operatorname{End}\left(\mathrm{S}^{2}\right)} \oplus \underbrace{\mathbb{1}_{k} \oplus \mathcal{N}_{\Lambda^{2}}}_{\operatorname{End}\left(\Lambda^{2}\right)} \oplus \operatorname{Hom}\left(\mathrm{S}^{2}, \Lambda^{2}\right) \oplus \operatorname{Hom}\left(\Lambda^{2}, S^{2}\right)$
$\rightarrow$ Rational solutions of systems of smaller size still having specific structures ( $\mathrm{Sym}^{2}, \Lambda^{2}$, Hom) that can be used for rational solutions (AparicioBarkatouSimonWeil'11, BarkatouPfluegel'98)

III

## Candidate for $\mathfrak{g}^{5}$

## Candidate for $\mathfrak{g}^{s}$ : reduction modulo $p$

Problem: In the max. dec. $\mathcal{M} \otimes_{k} \mathcal{M}^{\star}=\bigoplus_{i=1}^{r} \mathcal{W}_{i}$, find $\mathfrak{g}^{s}$
$\rightarrow$ Idea: use a modular approach to find a candidate for $\mathfrak{g}^{s}$
$\diamond$ Crucial object for studying diff. systems $\left[A_{p}\right] / \operatorname{modules}\left(\mathcal{M}_{p}, \partial\right)$ in characteristic $p>0$ : the $p$-curvature $\chi_{p} \triangleq \partial^{p}$ acting on $\mathcal{M}_{p}$ $\diamond$ In terms of matrices: $\chi_{p}$ is given by the $p$ th iterate of the sequence $\chi_{1}=A_{p}$ and, for $i>1, \chi_{i+1}=\chi_{i}^{\prime}-A_{p} \chi_{i}$
$\rightarrow$ Algorithms: Katz'82, van der Put'95-96, Cluzeau'03 and recently BostanCarusoSchost'15 for a fast algorithm

Grothendieck-Katz p-curvature conjecture: The Lie algebra $\mathfrak{g}^{s}$ is the smallest (algebraic) Lie sub-algebra of $\mathfrak{g l}_{n}(k)$ whose reduction modulo $p$ contains the $p$-curvature $\chi_{p}$ for almost all $p$.

## Candidate for $\mathfrak{g}^{s}$ : algorithm ModularSelection

$\diamond \mathcal{M} \otimes_{k} \mathcal{M}^{\star}=\bigoplus_{i=1}^{r} \mathcal{W}_{i}$ given by gauge transfo. $T \in \mathrm{GL}_{n^{2}}(k)$ (the columns $T_{\bullet j}$ of $T$ provide bases of the submodules $\mathcal{W}_{i}$ )

1. Choose a prime $p \rightarrow \bigoplus_{i=1}^{r} \mathcal{W}_{i, p}$ given by $T_{p}=T \bmod p$;
2. Compute the $p$-curvature $\chi_{p}$ of $\left[A_{p}\right]$;
3. Compute $V=T_{p}^{-1} \operatorname{Vect}\left(\chi_{p}\right)$;
4. From the non-zero entries of $V$, deduce a basis of the submodule of $\bigoplus_{i=1}^{r} \mathcal{W}_{i}$ whose reduction mod $p$ contains $\chi_{p}$.
$\diamond$ From G-K conjecture, the submodule found can be used as a reasonable guess for $\mathfrak{g}^{5}$
$\diamond$ Remark: this may select a bigger or smaller submodule
$\rightarrow$ we need to check whether our guess is correct or not

## Validation of the candidate

## Reduced form of a linear differential system

$\diamond$ Definition: $[A]$ in reduced form if $A \in \bar{k} \otimes \mathfrak{g}$.
$\rightarrow \mathfrak{g}$ viewed as a $\mathbb{C}$-vector space generated by $N_{1}, \ldots, N_{d} \in \mathbb{M}_{n}(\mathbb{C})$
$\rightarrow$ reduced form iff $\exists f_{1}, \ldots, f_{d} \in \bar{k}$ s.t. $A=f_{1} N_{1}+\cdots+f_{d} N_{d}$
Theorem (Kolchin-Kovacic): There exists a reduction matrix $P \in \mathrm{GL}_{n}(\bar{k})$ such that $[P[A]]$ is in reduced form.
$\diamond$ Reduced forms $\Rightarrow$ invariants ( $\approx$ rational sol. of "constructions") have constant coefficients in $\mathbb{C}$ : Aparicio-Compoint-Weil'13

Theorem (Aparicio-Compoint-Weil'13): For all ordinary point $z_{0} \in \mathbb{C}$ of $[A]$, there exists a reduction matrix $P \in \mathrm{GL}_{n}(\bar{k})$ for $[A]$ that sends every invariant $\mathbf{f}$ of $[A]$ to its evaluation at $z_{0}$.

## A Lie algebra conjugation problem

$\diamond$ Definition: Two Lie sub-algebras $\mathfrak{g}_{1}, \mathfrak{g}_{2} \subset \mathfrak{g l}_{n}(k)$ are conjugated if $\exists$ a conjugation matrix $P \in \mathrm{GL}_{n}(\bar{k})$ s.t. $\mathfrak{g}_{2}=P^{-1} \mathfrak{g}_{1} P$.

Theorem (BCdVW'16):

- $M_{i}(i=1, \ldots, d)$ basis of candidate Lie algebra $\mathfrak{g}^{s}$,
- $z_{0}$ ordinary point of $[A]$,
- $\mathfrak{g}^{t}$ Lie sub-algebra of $\mathfrak{g l} l_{n}(\mathbb{C})$ with basis $M_{i}\left(z_{0}\right)(i=1, \ldots, d)$.

Then, there exists a reduction matrix $P \in \mathrm{GL}_{n}(\bar{k})$ for $[A]$ that is a conjugation matrix between the Lie algebra $\mathfrak{g}^{s}$ and $\mathfrak{g}^{t}$.
$\rightarrow$ A reduction matrix can be found among the conjugation matrices between $\mathfrak{g}^{t}$ and $\mathfrak{g}^{s}$

## Semi-simple Lie algebras

$\diamond \mathcal{M}$ absolutely irreducible $\Rightarrow \mathfrak{g}^{t}$ and $\mathfrak{g}^{s}$ semi-simple Lie algebras
$\diamond$ Central objects in the study of a semi-simple Lie algebra $\mathfrak{g}$ : set of canonical generators (and Chevalley bases)
$\rightarrow$ Matrices $H_{1}, \ldots, H_{r}, X_{1}, \ldots, X_{r}, Y_{1}, \ldots, Y_{r}$ which satisfies:
$\left[H_{i}, H_{j}\right]=0,\left[X_{i}, Y_{j}\right]=\delta_{i, j} H_{i},\left[H_{i}, X_{j}\right]=c_{j, i} X_{j},\left[H_{i}, Y_{j}\right]=-c_{j, i} Y_{j}$

- This is associated with a root space decomposition of $\mathfrak{g}$
- $H_{1}, \ldots, H_{r}$ are generators of a Cartan sub-algebra of $\mathfrak{g}$
- $C=\left(c_{i, j}\right)_{1 \leq i, j \leq r}$ is a Cartan matrix of $\mathfrak{g}\left(c_{i, i}=2\right)$
$\rightarrow$ Algorithms for computing set of canonical generators and
Chevalley bases: deGraaf'00


## Algorithm ConjugationMatrices

Input: $\left\{M_{i}\right\}_{i}$ basis of $\mathfrak{g}^{s},\left\{M_{i}\left(z_{0}\right)\right\}$ basis of $\mathfrak{g}^{t}$
Ouput: Conjugation matrices $P$ between $\mathfrak{g}^{t}$ and $\mathfrak{g}^{s}$

1. Compute a set of canonical generators $\left\{H_{i}^{t}, X_{i}^{t}, Y_{i}^{t}\right\}$ of $\mathfrak{g}^{t}$;
2. Compute generators $\tilde{H}_{i}^{s}$ of a "split" Cartan sub-algebra $\mathfrak{h}^{5}$ of $\mathfrak{g}^{s}$ s.t. $\chi\left(\tilde{H}_{i}^{s}\right)=\chi\left(H_{i}^{t}\right)$ (ansatz $\rightarrow$ solving algebraic equations)
3. Compute a set of canonical generators $\left\{H_{i}^{s}, X_{i}^{s}, Y_{i}^{s}\right\}$ of $\mathfrak{g}^{s}$ having the same Cartan matrix as $\left\{H_{i}^{t}, X_{i}^{t}, Y_{i}^{t}\right\}$;
4. Compute the matrices $P \in \mathrm{GL}_{n}(\bar{k})$ such that $\forall i, P X_{i}^{t}=X_{i}^{s} P$ and $P Y_{i}^{t}=Y_{i}^{s} P$ (overdetermined linear system).

Theorem (BCdVW'16): If our choice for $\mathfrak{g}^{s}$ is correct, then output of the form $P=c \tilde{P}$, with $\tilde{P} \in \mathrm{GL}_{n}(\bar{k}), c$ arbitrary element of $\bar{k}$

## Algorithm ReductionMatrix

$\diamond$ Let $P=c \tilde{P}$ and $\left(N_{i}^{t}\right)_{i=1, \ldots, d}$ be a Chevalley basis of $\mathfrak{g}^{t}$
$\diamond \exists f_{i} \in \bar{k}$ such that $P[A]=\sum_{i=1}^{d} f_{i} N_{i}^{t}$ implies:

$$
\begin{gather*}
\tilde{P}^{-1} A \tilde{P}-\frac{c^{\prime}}{c} I_{n}-\tilde{P}^{-1} \tilde{P}^{\prime}=\sum_{i=1}^{d} f_{i} N_{i}^{t}  \tag{1}\\
\frac{c^{\prime}}{c}=\frac{1}{n}\left(\operatorname{Tr}(A)-\frac{\operatorname{det}(\tilde{P})^{\prime}}{\operatorname{det}(\tilde{P})}-\sum_{i=1}^{d} f_{i} \operatorname{Tr}\left(N_{i}^{t}\right)\right) \tag{2}
\end{gather*}
$$

1. Plug (2) into (1) and solve the linear system for the $f_{i} \in \bar{k}$. If the system has no solution, then Return "Fail".
2. Plug the solution found into (2) and solve the scalar order one linear differential equation for $c$. If algebraic solution, then Return $P=c \tilde{P}$, Else Return "Fail".

IV
Full algorithm and example

## Full algorithm and remarks

1. Compute a maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^{\star}$;
2. Apply ModularSelection to get a candidate for $\mathfrak{g}^{s}$;
3. Apply ConjugationMatrices; If it fails, go back to Step 2 and choose another prime $p$
4. Compute a Chevalley basis $\left(N_{i}^{t}\right)_{i}$ of $\mathfrak{g}^{t}$;
5. Apply ReductionMatrix.

If it fails, go back to Step 2 and choose another prime $p$, Else Return $\left(N_{i}^{t}\right)_{i}$.
$\diamond$ Remarks on the successive choices of $p$ :

- There may exist an infinite number of "bad" primes: good strategy for choosing prime numbers $\rightsquigarrow$ deterministic algo.
- if $\mathcal{W}_{1}, \mathcal{W}_{2}$ are proved not correct: try $\mathcal{W}_{1}+\mathcal{W}_{2}$ before new $p$
- If candidate decomposable: check each submodule


## Remark on complexity / Implementation

$\diamond$ Arithmetic complexity polynomial in $n$ except algebraic systems solved in ConjugationMatrices
$\rightarrow$ Significant diff. compared to the exponential (several levels) complexity obtained in Feng'15 for computing the Galois group
$\diamond$ We have a prototype Maple implementation
$\diamond$ We manage to apply it to many examples up to order $n=7$
$\diamond$ In practice, the most costly step is the dec. of $\mathcal{M} \otimes \mathcal{M}^{\star}$

## Example (1)

$\diamond$ Consider the system given by

$$
A:=\left[\begin{array}{ccc}
\frac{x-1}{x} & x & -1 \\
-x^{3}+1 & 0 & -1 \\
\frac{x-1}{x}+x^{2} & x+1 & -1
\end{array}\right]
$$

$\diamond \mathcal{M} \otimes \mathcal{M}^{\star}=\mathbb{1}_{k} \oplus \mathcal{W}_{1} \oplus \mathcal{W}_{2}$, with $\mathcal{W}_{1}, \mathcal{W}_{2}$ of resp. dim. 3 and 5
$\diamond p$-curvature $\rightarrow$ candidate for $\mathfrak{g}^{s}$ is $\mathcal{W}_{1}$ irred with basis

$$
M_{1}=\left[\begin{array}{ccc}
-1 & 0 & 1 \\
0 & 0 & 0 \\
-x^{2}-1 & 0 & 1
\end{array}\right], M_{2}=\left[\begin{array}{ccc}
0 & 1 & 0 \\
-x^{2} & 0 & 0 \\
0 & 1 & 0
\end{array}\right], M_{3}=\left[\begin{array}{ccc}
0 & 1 & 0 \\
-x^{2}-1 & 0 & 1 \\
0 & 0 & 0
\end{array}\right]
$$

## Example (2)

$\diamond x_{0}=1$ ordinary point for $[A]$ : set of canonical gen. of $\mathfrak{g}^{t}$ :

$$
H^{t}=\left[\begin{array}{ccc}
2 i & 0 & -2 i \\
0 & 0 & 0 \\
4 i & 0 & -2 i
\end{array}\right], X^{t}=\left[\begin{array}{ccc}
0 & -i & 0 \\
1+i & 0 & -1 \\
0 & 1-i & 0
\end{array}\right], Y^{t}=\left[\begin{array}{ccc}
0 & -i & 0 \\
-1+i & 0 & 1 \\
0 & -1-i & 0
\end{array}\right]
$$

$\diamond$ Computing an "aligned" set of canonical gen. of $\mathfrak{g}^{s}$, we get:
$H^{s}=\left[\begin{array}{ccc}\frac{-2 i}{x} & 0 & \frac{2 i}{x} \\ 0 & 0 & 0 \\ \frac{-2 i\left(x^{2}+1\right)}{x} & 0 & \frac{2 i}{x}\end{array}\right], X^{s}=\left[\begin{array}{ccc}0 & \frac{i}{x} & 0 \\ -i x+1 & 0 & -1 \\ 0 & \frac{i+x}{x} & 0\end{array}\right], Y^{s}=\left[\begin{array}{ccc}0 & \frac{i}{x} & 0 \\ -i x-1 & 0 & 1 \\ 0 & \frac{i-x}{x} & 0\end{array}\right]$.
$\diamond$ Conjugation matrices $P$ s.t. $X^{t} P=P X^{s}$ and $Y^{t} P=P Y^{s}$ :

$$
P=c \tilde{P}, \quad c \in \bar{k}, \quad \tilde{P}=\left[\begin{array}{ccc}
1 & 0 & 0 \\
0 & -x & 0 \\
x+1 & 0 & -x
\end{array}\right] .
$$

## Example (3)

$\diamond$ Solving linear system obtained from $P[A]=f_{1} H^{t}+f_{2} X^{t}+f_{3} Y^{t}$

$$
\left\{f_{1}=\frac{i}{2 x}, f_{2}=-\frac{i}{2}\left(x^{2}+i\right), f_{3}=\frac{i}{2}\left(-x^{2}+i\right)\right\}
$$

$\diamond$ Solving the scalar diff. equation for $c$, we get $c=a / x, a \in \mathbb{C}^{*}$
$\rightarrow$ Reduction matrix $P$ and reduced form $R$ given by:

$$
P=\left[\begin{array}{ccc}
\frac{a}{x} & 0 & 0 \\
0 & -a & 0 \\
\frac{(x+1) a}{x} & 0 & -a
\end{array}\right], \quad R=\left[\begin{array}{ccc}
-x & -x^{2} & x \\
x^{2}+1 & 0 & -1 \\
-2 x & -x^{2}+1 & x
\end{array}\right] .
$$

$\rightarrow$ The Lie algebra $\mathfrak{g}$ viewed as a Lie sub-algebra of $\mathfrak{g l}_{3}(\mathbb{C})$ admits the basis $H^{t}, X^{t}, Y^{t}$

