CIMPA-UNESCO-VIETNAM
LECTURES: HANOÏ 2001

Control Theory and Integrable Systems

Introduction to Differential Algebra and Differential Galois Theory

Jacques-Arthur WEIL
LACO, département de mathématiques,
Faculté des sciences
123 avenue Albert Thomas, 87060 Limoges CEDEX, France.
weil@unilim.fr
and
INRIA, Projet CAFÉ,
2004 route des Lucioles, B.P 93, F-06902 Sophia Antipolis CEDEX, France
jacques-arthur.weil@inria.fr

December 3-7 2001

Contents

Part i
Preparatory Lectures

1 Algebraic Numbers, Algebraic Functions

Throughout this lecture, k denotes a field on which we assume that one can perform the four operations $+, -, *, /$ and one can tell when an element is equal to zero (i.e a computable field). All fields and rings are assumed to be commutative in this lecture.

We will study polynomial rings and show how to construct fields that contains (unknown) roots of polynomial equations. Properties of this fields will be adressed through Galois theory.

1.1 Polynomial Rings and the Euclidean Algorithm

Let $k[X]$ denote the ring of polynomials in one variable over k. An *ideal* I is a subring of $k[X]$ such that: for all p in I and $q \in k[X]$, we have $pq \in k[X]$. A central tool in studying polynomial ideals is the Euclidean division.

Definition 1 *Euclidean division: Let $P_1, P_2 \in k[X]$ with $P_2 \neq 0$.*
There exists a unique pair $(Q, R) \in k[X]$ such that $P_1 = QP_2 + R$ and $\deg(R) < \deg(P_2)$.

We say that $k[X]$ is a Euclidean ring. *Proof.* Exercise ◯

Exercise 2.

1. Principality:
   Recall that an Ideal is *principal* if it is generated by a single element P (i.e all elements of the ideal are multiples of P). Show that any ideal of $k[X]$ is principal.

2. Euclidean algorithm:
   Let $R_0 = P_1$, $R_1 = P_2$, and perform successive Euclidean divisions: $R_0 = Q_1R_1 + R_2$, $R_1 = Q_2R_2 + R_3$,...,$R_{n-2} = Q_{n-1}R_{n-1} + R_n$ and $R_{n-1} = Q_nR_n$ (i.e R_n is the last non-zero remainder in the sequence of divisions). Show that R_n is the greatest common divisor of P_1 and P_2.

3. Use the Euclidean algorithm to prove *Bézout's relation*: If D is the greatest common divisor of P_1 and P_2, there exists polynomials S and T such that $SP_1 + TP_2 = D$.
   Using the Euclidean algorithm, give an algorithm to compute S and T. Prove that S can be chosen of degree less than P_2 and that, in this case, it is unique.

◇

Exercise 3. Let $K \subset L$ be fields. Let $F, G \in K[X]$ and let D be their greatest common divisor. Using Bézout's relation, prove that D is also the greatest common divisor of F and G viewed as polynomials in $L[X]$. ◇

This Bézout relation and the Euclidean structure will allow us to work modulo polynomial ideals effectively.

1.2 Algebraic Extensions

Definition 2 *We say that an element α is* algebraic *over k if there exists a nonzero $P \in k[X]$ such that $P(\alpha) = 0$. Otherwise, α is said to be transcendental over k.*

Let α be algebraic over k. Then $I := \{Q \in k[X] | Q(\alpha) = 0\}$ is a (prime) ideal. By exercise 2.1, we know that I is generated by some polynomial P. If we further ask that P is monic, then it is uniquely defined and it is called the *minimum polynomial* of α.

Exercise 4. Show that I is prime (i.e if $ab \in I$ for $a, b \in k[X]$ then either $a \in I$ or $b \in I$). Check that P is the monic polynomial of lowest degree such that $P(\alpha) = 0$. Deduce from this that P is irreducible. $\diamond$

Example. The following simple example can lead you in what follows. The element $\sqrt{2}$ is a zero of $P = X^2 - 2$ so it is algebraic over $\mathbb{Q}$ (prove that it does not belong to $\mathbb{Q}$). You can easily check that any element in $\mathbb{Q}[\sqrt{2}]$ can be written as $a + b\sqrt{2}$ for a, b in $\mathbb{Q}$. So $\mathbb{Q}[\sqrt{2}]$ is also a vector space of dimension 2 over $\mathbb{Q}$ (basis: $1, \sqrt{2}$). Moreover, any non zero element in $\mathbb{Q}[\sqrt{2}]$ has an inverse in $\mathbb{Q}[\sqrt{2}]$ because $(a + b\sqrt{2}).\frac{a-b\sqrt{2}}{a^2-2b^2} = 1$ so $\frac{a-b\sqrt{2}}{a^2-2b^2} \in Q[\sqrt{2}]$ is the desired inverse. We conclude that $\mathbb{Q}[\sqrt{2}]$ is in fact also a field. $\diamond$

In general, if P is an irreducible polynomial of degree n in $k[X]$, we can give a precise meaning to the expression "let α be a root of P" using the Euclidean division. Let $I := (P)$ denote the ideal generated by P in $k[X]$. Because P is irreducible, I is a maximal ideal in $k[X]$ (prove this). Consider the map

$$\phi : \begin{array}{ccc} k[X] & \to & k[X] \\ \tilde{P} & \mapsto & R \end{array} \quad \text{such that} \tilde{P} = QP + R, \deg(R) < \deg(P)$$

This map induces the canonical ring morphism from $k[X]$ to the quotient ring $k[X]/I$ (i.e R is a canonical representant for the class of $\tilde{P}$ modulo I). One can then define a generic root α of P the image of X under this canonical ring morphism, so $k[\alpha] = k[X]/I$.
This construction shows that $k[X]/I$ is also a vector field of dimension n, generated by $1, \alpha, \ldots, \alpha^{n-1}$.
As in the case of $\mathbb{Q}(\sqrt{2})$, we now give a constructive proof that $k[X]/I$ is actually a field (this also follows from the fact that I is a maximal ideal, of course). Let $R(\alpha)$ be a non-zero element in $k[\alpha]$. Because $R(\alpha) \neq 0$, R is not a multiple of P. Now P is irreducible so it is prime with R and Bézout's relation shows that there exists a unique pair of polynomials $(S, T) \in k[X]^2$ such that $\deg(S) < \deg(P)$ and $SR + TP = 1$. Specializing in α, we see that $S(\alpha)R(\alpha) = 1$ and hence $R(\alpha)$ admits the inverse $S(\alpha)$ in $k[\alpha]$. We conclude that $k[\alpha]$ is equal to the field $k(\alpha)$.
If k is a number field (e.g $\mathbb{Q}, \mathbb{R}, \ldots$), then α is called an algebraic number. If k is a function field in one variable (e.g $\mathbb{Q}(z), \mathbb{C}(z)$), then α is (a bit abusively) called an algebraic function.

A field extension $k \subset K$ is called a *finite extension* if K is a finite dimensional vector space over k. Its dimension is denoted by $[K : k]$ and is called the degree of the extension. An algebraic element α is called separable over k if it is either transcendental over k or a zero of a polynomial with no multiple roots in k. An algebraic extension of k is called separable if all its elements are separable over k. In characteristic zero, all algebraic elements are separable.

Exercise 5. Composite algebraic extensions.
Let L be a finite extension of k of degree n and M be a finite extension of L of degree m. Show that M is a finite extension of k of degree mn.
Deduce that if v is an element of an algebraic extension L of k, then the degree of v over k is a divisor of the degree $[L : k]$ of L over k. $\diamond$

2 A Short Introduction to Galois Theory

Let P be a polynomial of degree n in $k[X]$. The goal of Galois theory is to describe the roots of P and the algebraic relations among them. We will first introduce a field that contains all roots of P and then show how the automorphisms of this field allow one to measure the relations among the roots.

2.1 Splitting Fields

Definition 3 *Let $P \in k[X]$. A field F is called a* splitting field *for P if*

1. *F contains all roots of P, i.e P factors as a product of linear factors in $F[X]$.*
2. *If L is another field extension of k containing all roots of P, then we can embed F in L.*

This definition means that F is the field extension of k generated by all roots of P. One can show iteratively that splitting fields can be constructed. Let α_1 be a root of P. Then, P factors as $P = (X - \alpha_1)P_2P_3 \ldots$ with the P_i being irreducible polynomials in $k(\alpha_1)[X]$. If the P_i are linear, we are done. Otherwise, let α_2 be a root of P_2, factor the P_i over $k(\alpha_1, \alpha_2)[X]$ and iterate the construction until the P_i are linear. The process will stop (in at most n steps) because at each step the degree of at least one of the P_i is strictly

lowered.

We may also view the construction of a splitting field another way. Let $P = X^m - p_1X^{m-1} + p_2X^{m-2} + \ldots + (-1)^m p_m$ be an irreducible polynomial. Let σ_j denote the j-th symmetric function of the roots. Consider the ring $k[X_1, \ldots, X_m]$ in m indeterminates X_j and let I denote the ideal generated by $(\sigma_1(X_1, \ldots, X_m) - p_1, \ldots, \sigma_m(X_1, \ldots, X_m) - p_m)$ in $k[X_1, \ldots, X_m]$. We would like to view the zeroes of I as "models" of the roots of P. However, we may miss some additional relations satisfied by the relation this way. So, let J denote a proper (proper means different from $k[X_1, \ldots, X_m]$) maximal ideal of $k[X_1, \ldots, X_m]$ containing I and let $F := k[X_1, \ldots, X_m]/J$. Because J is maximal, this is now a field and it can be checked that this indeed is a splitting field for P. The ideal J is sometimes called the *ideal of relations* among the roots.
Exercise 6.

1. Show that the splitting field is unique, i.e any two splitting fields are isomorphic.
2. Show that if $k \subset L \subset M$ with M a spliting field for $P \in k[X]$, then M is also a splitting field for P viewed as a polynomial in $L[X]$.

$\diamond$

Exercise 7.

1. Find the splitting field over $\mathbb{Q}$ for the polynomial $x^4 + 4$.
2. Let p be a prime number. Find the splitting field over $\mathbb{Q}$ for $x^p - 1$.

$\diamond$

A field extension is a Galois extension if it is the splitting field of some polynomial.

2.2 Galois Groups

Let P denote a polynomial of degree n over k.

Definition 4 *Let F be an extension field of k. The set $Gal(F/k)$ of field automorphisms of F, that leave every element of k fixed, is called the* Galois group *of F over k.*
If $P \in k[x]$ and F is a splitting field for P over k, then $Gal(F/k)$ is called the Galois group of P over k.

The fact that elements of the Galois group leave the elements of k fixed means that they will preserve all algebraic relations between the roots of P. In particular, if $P(\alpha) = 0$ and $\sigma \in Gal(P)$, we see that $P(\sigma(\alpha)) = \sigma(P(\alpha)) = \sigma(0) = 0$ so the Galois group maps roots to other roots. This gives $Gal(P)$ a representation as a group of permutation on n letters (the n roots). The properties of these permutations will mirror the algebraic relations between the roots.

In fact, let J denote the ideal of relations as in the second construction of splitting fields above. Then the Galois group is the set of permutations of the roots that preserve the ideal J. For example, let $P = x^4 + 4$ and follow the second construction of the splitting field. We have the following generators for the ideal I.

$$I = (x_1+x_2+x_3+x_4-0, x_1x_2+\ldots+x_3x_3-0, x_1x_2x_3+x_1x_2x_4+x_2x_3x_4-0, x_1x_2x_3x_4-4)$$

Additional relations are given by $x_2 = -x_1, x_3^2 + x_1^2 = 0, x_4 = -x_3$ so $J = (I, x_2 + x_1, x_3^2 + x_1^2, x_4 + x_3)$. The Galois group is the set of permutations of the roots that preserve the (ideal of) additional relations (the symmetric ones are automatically preserved by a permutation), and you may (and should) verify that there are exactly eight such permutations.

Let H be a subgroup of $Gal(F/k)$. The fixed field of F under H, noted F^H is the field $F^H = \{v \in F | \forall h \in H, h(v) = v\}$. We will admit the following very important theorem of Galois theory:

Theorem 1 (Normality) *Let G be the Galois group of F over k. Then k is the fixed field of F under G: $k = F^G$.*

This means that an element in F is indeed in k if and only if it is fixed by G. This way, we can relate the degree of an element v of F to the number of its conjugates under the action of G. Let $Q := \prod_{g\in G}(Y - g(v))$. If we let any $h \in G$ act on the coefficients of Q, we have $h(Q) = \prod_{hg\in G}(Y - hg(v)) = \prod_{g\in G}(Y - g(v)) = Q$ because left multiplication by h is a bijection on G: hence, the above theorem shows that Q has coefficients in k. Now assume that v has exactly m conjugates corresponding to elements $g_1, \ldots, g_m$ of G. Then we see that Q must be a power of $\prod_{i=1,\ldots,m}(Y - g_i(v))$ and hence this polynomial has coefficients in k so v is algebraic of degree at most m. Now it can't be less than m otherwise v would have less than m conjugates, so finally we see that v is algebraic of degree m.

Exercise 8. Let F be a splitting field over $\mathbb{Q}$ for $x^4 + 1$

1. Show that $[F : \mathbb{Q}] = 4$. Show that the Galois group has four elements
2. Show that $i \in F$ and $\sqrt{2} \in F$. Find automorphisms of F that have fixed field $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ respectively.
3. Compute the Galois group of F over $\mathbb{Q}$. Show that the groups computed in the previous question are normal subgroups.

$\diamond$

The normality theorem implies that, for any subgroup H of G, we have $H = Gal(F/F^H)$. The above reasoning (and the primitive element theorem) then show that $[F : F^H] = |H|$ (in particular, $[F : k] = |G|$). Consequently, $[F^H : k] = |G/H|$. Conversely, for any subfield E of F, we see that $Gal(F/E)$ is a subgroup of G and $E = F^{Gal(F/E)}$.

One can further show that F^H is a Galois extension of k if and only if H is a normal subgroup.

Exercise 9. Show that $\mathbb{Q}(i, \sqrt{2})$ is a splitting field (a Galois extension). Compute its Galois group over $\mathbb{Q}$ and describe all intermediate subgroups and subfields. $\diamond$

The set of roots of unity, the complex roots of $x^n - 1 = 0$, form a cyclic group of order n. There are $\phi(n)$ generators for this group (check that $\phi(n)$ is the number of integers in $\{1, \ldots, n\}$ that are prime with n). If d divides n, elements of order d generate a subgroup of order $\phi(d)$ (thus there are exactly $\phi(d)$ elements).

Exercise 10. Let $k = \mathbb{C}(x)$. Show that, for $f \in k$ non zero, the Galois group of $Y^n - f$ is a cyclic group whose order is (a divisor of) n. $\diamond$

Exercise 11. Let $P \in k[X]$ be irreducible and let F be a splitting field for P over k. Assume that $Gal(F/k)$ is abelian. Show that $F = k(\alpha)$ for any root α of P. $\diamond$

Exercise 12. We say that an element $f \in F$ is *radical* over k if there exist an integer m and $a \in k$ such that $f^m = a$. Let F be the splitting field of $X^m - a$. Prove that the Galois group of F is abelian and isomorphic to the group of m-th roots of unity. $\diamond$

We say that P is solvable by radicals if the roots of f can be expressed by compositions of radicals. This is equivalent with saying that we can construct the splitting field via a tower of fields $k = F_0 \subset F_1 \subset \ldots \subset F_i \subset \ldots \subset F_r = F$ where each F_i is a galois extension, generated over F_{i-1} by a radical. if G_i is

the Galois group of F over F_i. We then have a tower of normal subgroups such that G_{i+1} is normal in G_i and G_{i+1}/G_i is the Galois group of a cyclic extension, hence an abelian group. We conclude that G is solvable. We will admit the converse,hence

Theorem 2 *A polynomial P is solvable by radicals if and only if its Galois group is solvable.*

Part ii
Introduction to Differential Algebra and Differential Galois Theory

A Differential Algebra

Let k be a field of caracteristic 0. Our most common examples will be the field $\mathbb{C}(x)$ of rational functions, the field $\mathbb{C}((x))$ of Laurent series (quotients of power series), and the field $\mathbb{C}(\{x\})$ of convergent power series.

Definition 5 *A* derivation *on k is an operator ∂ satisfying*

1. $\forall a, b \in k, \qquad \partial(a+b) = \partial(a) + \partial(b)$. *(additivity)*
2. $\forall a, b \in k, \qquad \partial(a.b) = \partial(a)b + a\partial(b)$. *(Leibniz rule)*

A field k (resp. a ring) equipped with such a derivation ∂ will be called a differential field *(resp. a differential ring) and will be noted (k, ∂) unless the context is clear.*

For $\mathbb{C}(x)$, it is customary to consider the derivation $\partial = \frac{d}{dx}$ and for $\mathbb{C}((x))$ it is customary to use the derivation $\delta = x.\frac{d}{dx}$.
The elements whose derivative is equal to zero are called *constants*. The constants of a field (resp. ring) form a field (resp. ring).
If (k_1, ∂_1) is a differential field, we say that it is *differential extension of k* if $k \subset k_1$ and if the restriction of ∂_1 to k coincides with ∂.

A.1 Differential Polynomials

We now would like to mimic the construction that we gave on algebraic functions to give models of a wider class of functions. We follow the construction of Ritt in [Rit50]. Given an infinite set of indeterminates Y_i, indexed by $\mathbb{N}$, we may extend the derivation of K to $K[Y_i]_{i\in\mathbb{N}}$ by letting $\delta(Y_i) = Y_{i+1}$. We will write $Y_1 = Y'$, $Y_i = Y^{(i)}$; we then say that Y is a *differential indeterminate*. The ring of differential polynomials in Y is $k\{Y\} = K[Y, Y', Y'', \ldots]$.

If we wish to consider partial differential equations, we may consider several (commuting) derivations $\partial_1, \ldots, \partial_s$ and let our set of indeterminates be indexed by $\mathbf{N}^s$. However, in this lecture, we will focus on the ordinary case, i.e we work with only one derivation ∂.
Recall that the usual functions ($\exp(x)$, $\log(x)$, $\sin(x)$ or the special functions) are defined as solutions of differential equations. We now would like to mimic the construction of algebraic numbers or algebraic functions to give an *algebraic model* for the usual functions. First note that we a function is a solution of a differential equation, it is also a solution of all the equations obtained by successive derivations of the initial one. So a model for our functions should be a zero not only of a differential polynomial but also of all its derivatives.
Given a differential polynomial P, we thus will call *differential ideal generated by* P, noted $[P]$, the set of all combinations $\sum_{i\geq 1} A_i P^{(i)}$ (where the A_i are differential polynomials, and $P^{(i)}$ are the successive derivatives of P) : The functions solutions of $P = 0$ are also solutions of all these differential equations $\sum_{i\geq 1} A_i P^{(i)} = 0$. More generally, we will say that an ideal I of $k\{Y\}$ is a *differential ideal* if $\partial(I) \subset I$. Note that $k\{Y\}$ is Not principal any more, ideals are generally not generated by a single polynomial.
Now it is as simple to construct a model of $\exp(x)$ as it was to model $\sqrt{2}$. Let $I = [Y' - Y]$ the differential ideal generated by $Y' - Y$. One can show that I is prime and even maximal. Let $\phi : \mathbb{C}(x)\{Y\} \mapsto \mathbb{C}(x)\{Y\}/[Y' - Y]$ be the canonical morphism. If we set $y = \phi(Y)$, then $y' - y = 0$. We thus have constructed a differential extension of $(\mathbb{C}(x),')$ (because $[Y' - Y]$ is maximal, so $\mathbb{C}(x)\{Y\}/[Y' - Y] = \mathbb{C}(x, y)$. Of course, this construction does not give us *The* exponential function, but models the whole class of solutions of $y' - y = 0$. What we have constructed is a field that "looks" like $\mathbb{C}(x, \exp(x))$ in the sense that any property which is true in $\mathbb{C}(x, y)$ is also true in $\mathbb{C}(x, \exp(x))$.
Functions obtained in this way are called *differentially algebraic.*
Exercise 13. Show that the derivation on the field $\mathbb{C}(x, y)$ just constructed is $\frac{d}{dx} + y\frac{d}{dy}$. ◇
Exercise 14.[Ros72] Let $(K,')$ be a differential field whose constant field C is of characteristic zero and $y' = fy$, where $f \in K$, a differential equation with no solution algebraic over K. Let T be a differential indeterminate and t the solution of $t' = ft$ constructed as the image of T in the quotient $k\{T\}/[T' - fT]$. Check that $k[t]$ is a differential ring.

Let $P \in k[T]$ be an irreducible monic polynomial such that $P(t)$ divides $P(t)'$. Show that $P = T$. $\diamond$

Proposition 1 *Let (k, ∂) be a differential field and let y be transcendental over k Then, for all $a \in k(y)$, there exists a unique derivation Δ of $k(y)$ which extends ∂ and such that $\Delta(y) = a$.*

Proof. Expressions in $k(y)$ are rational functions in y with no relation satisfied by y over k. Let ∂_k be the derivation of $k(y)$ that coincides with ∂ on k and sends y to 0. Then, we must have $\Delta = \partial_k + a\frac{d}{dy}$. $\bigcirc$

Proposition 2 *Let (k, ∂) be a differential field and let y be algebraic over k. Then there is only one derivation Δ on $k(y)$ which extends ∂.*

Proof. We may give a constructive proof for this. It is necessary and sufficient to find the image of y under Δ to specify Δ. Let P be the minimum polynomial of P over k. Then $P(y) = 0$ so $\Delta(P(y)) = \Delta(0)$. Now, $\Delta(P(y)) = \partial_k(P)(y) + \Delta(y)\frac{dP}{dy}(y)$. As P is irreducible, $\frac{dP}{dy}$ is prime with P so there exist $S, T \in k[X]$ so that $S\frac{dP}{dy} + TP = 1$. Specializing in y, we have $S(y)\frac{dP}{dy}(y) = 1$ so $\Delta(y) = -S(y)\partial_k(P)(y) \in k[y]$. The latter relation defines Δ uniquely. $\bigcirc$

A.2 Models for the Usual Functions

We now introduce some terminology for functions that we will use a lot in the rest of these lectures.

Definition 6 *Let (k, ∂) be a differential field and (K, Δ) be a differential field extension. Let $a \in K$.*

1. *We say that a is* rational *if a is in the base field k.*
2. *We say that a is a* logarithm *on k if there exists u in k such that $a' = \frac{u'}{u}$. More generally, we will say that a is an* integral *over k if there exists u in k such that $a' = u$.*

3. *We say that* a *is* exponential[1] *over* k *if there exists* $u \in k$ *such that* $a' = ua$.

With our differential algebraic setting, we may, starting from $\mathbb{C}(x)$, construct iteratively exponentials and integrals. The resulting class is the class of *Liouvillian* functions, i.e the functions that are found in a tower of fields that can be constructed by adjoining successively exponentials, integrals, or algebraic elements.

Exercise 15. Show that $\log(x)$, $\cos(x)$, $\sqrt{\exp(x^2)+1}$, $\int \exp(-x^2)$ are liouvillian functions. ◇

We will see later that, for solving differential equations, the liouvillian functions play a role somewhat analogous to the role played by radicals for solving polynomials equations.

B Introduction to Differential Galois Theory

Differential Galois theory is, as in the clasical case, a tool to study the algebraic relations among solutions of linear differential equations; as we will see in the lectures of J.P Ramis on integrability of Hamiltonian systems, it can also be used to study dynamical properties on solutions of some non-linear systems. A general reference for differential Galois theory is the forthcoming fundamental book [PS02]. Many other introduction exist in the litterature, for example [Beu92, Kap57, Put97, Sin98, Tou90] (see also the notes of M. Canalis-Durand and the notes of J.P Ramis). The links between differential Galois theory and Hamiltonian mechanics have been developped in many papers, among which we may mention [Zig82a, Zig82b, Mor99, CRS95, BCRS96, MR01a, MR01b]; lovely introductions to these aspects are also found in [Aud00, Chu98, Aud01, Mor00] and of course [Ram01].

B.1 Differential Equations and Differential Systems

We consider a differential field k with a derivation that we note $'$ or ∂ if the context is not clear. For the rest of these notes, we assume that the field of

[1] This is a frequent abuse of notations in the litterature, as we should really say that a is the exponential of an integral

constants C of k is algebraically closed (i.e any polynomial over C has all its roots in C) and of characteristic zero. Typical examples are $\overline{\mathbb{Q}}$ or $\mathbb{C}$.

B.1.1 Equivalent differential systems and differential modules

A linear differential equation is an equation of the form

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

with the a_i being functions in k (not constants). Solving this equation is equivalent to solving the companion system

$$\begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_{n-1} \\ y_n \end{pmatrix}' = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_{n-1} \\ y_n \end{pmatrix}$$

Conversely, suppose that $(y_1, y_2, \cdots, , y_n)$ satisfy a homogeneous first order linear differential system $Y' = AY$ of size n. To find an equation associated with $Y' = AY$, we would like to find a system in companion form whose solutions are *equivalent* (or "isomorphic") to the ones of the original system (precisely: obtained with a change of variables $Y = PZ$ with P an invertible matrix with coefficients in k). This is done by the following cyclic vector process (see e.g [MRa89, PS02, Wei95] for references and other methods). Consider $\Lambda \in k^n$ and let $z_1 = \Lambda Y = \lambda_1 y_1 + \ldots + \lambda_n y_n$. We compute $z_2 = z_1', \ldots, z_{n+1} = z_1^{(n)}$ by using the relation $Y' = AY$. We obtain $n+1$ linear expressions in the n variables y_i and so they are linearly dependant: this provides a linear differential equation $\mathcal{L}(z_1) = 0$ for z_1. Letting $Z = (z_1, \cdots, z_n)^t$, we now have a relation $Z = PY$ and $Z' = BY$; If the matrix P is invertible, Λ is called a *cyclic vector* for the system and $Z' = (BP^{-1})Z$ is a companion system, equivalent to the first one. It can be shown that the cyclic vectors form a Zariski open set, and almost all choices of Λ will fit [PS02].

Thus, in the following, everything that is stated for first order systems is valid for n-th order equations and vice-versa.

A useful tool to describe an equivalence class of differential systems (intrinsically) is the notion of differential module:

Definition 7 *A* differential module *over* (k, ∂) *is finite-dimensional* k*-vector space* $M \simeq k^n$ *with an operator* D *satisfying a Leibniz rule:*

$$\forall f \in k, v \in M : \qquad D(f.v) = \partial(f).v + f.D(v)$$

Differential modules are sometimes also called "modules with a connection" in the litterature. To a differential system $Y' = AY$, one may cannonically associate a differential module with a basis $e = (e_1, \ldots, e_n)$ and the operator D acting by $D(e_i) = \sum_{j=1}^{n} -a_{j,i}e_j$. This way, a solution $Y = y_1e_1 + \ldots + y_ne_n$ of $Y' = AY$ is caracterized by the relation $D(Y) = 0$ (check this) so that we may write $D =' -A$.
It can be checked that two differential systems are equivalent if and only if they are associated to the same differential module (in fact, the change of variable that sends a system to the other can be viewed as a change of basis in the differential module).
The cyclic vector method above amounts to finding an element v such that $v, D(v), \ldots, D^(n-1)(v)$ are a basis of the differential module M (hence the term "cyclic").

B.1.2 First integrals of linear differential systems

Let U denote a fundamental matrix of solutions of $Y' = AY$ (i.e U is invertible and its collumns are solutions of $Y' = AY$). A *linear first integral* of the system is a linear function $\mathbf{R}$ such that $\mathbf{R}(Y)$ is a constant whenever Y satisfies $Y' = AY$. Let Y_i denote the columns of U and R_i denote the rows of U^{-1}. As $U^{-1}U = 1$, we see that $R_i.Y_j = \delta_{i,j}$ (where $\delta_{i,j}$ is the kronecker symbol, $\delta_{i,i} = 1$ and $\delta_{i,j} = 0$ when $i \neq j$). It follows that the rows R_i define linear first integrals of the system. We see that the columns of ${}^tU^{-1}$ are coefficients of linear first integrals; they are also solutions of the *adjoint system* $Z' = -{}^tAZ$. We see that solutions of the adjoint (or *dual*) system yield first integrals of the system. This simple fact is useful in the Morales-Ramis theory of non-integrability of Hamiltonian systems (see the notes of Ramis).

B.2 The Differential Galois Group

We will proceed as in classical Galois theory: first, we construct a field generated by all the solutions (and their derivatives)

Definition 8 *A differential field extension* $K \supset k$ *is said to be a* Picard-Vessiot extension *of* k *(for* $L(y) = 0$*) if*

1. *$K = k(y_1, y_1', \ldots, y_i^{(j)}, \ldots, y_n^{(n-1)})$, where the y_i are a basis of solutions of $L(y) = 0$ (i.e K is the differential field generated[2] by the solutions of L.*

2. *K and k have the same field of constants.*

As the constant field of k is algebraically closed of characteristic 0, one can show that Picard-Vessiot extensions exist and are unique up to differential isomorphism ([PS02], [Kol48b] for the original proof). In the sequel, the term "solution" will always denote a solution in the Picard-Vessiot extension K.

Example. Let $k = \mathbb{C}(x)$ and consider the equation $L(y) = y' - \frac{1}{3x}y$. We know that the solution is $x^{\frac{1}{3}}$ but let's construct the Picard-Vessiot extension (hence the solution) like we did in the the preliminary lecture on Galois groups.
We consider the ring $k[y]$ with the derivation $D = \frac{d}{dx} + \frac{1}{3x}\frac{d}{dy}$, where y is an indeterminate. In this construction, y satisfies $D(y) - \frac{1}{3x}y = 0$. However, it is easily checked that $D(\frac{y^3}{x}) = 0$ so this ring contains a new constant. Take the ideal $I = (y^3 - x)$; it is prime (in fact, it is maximal) and stable under the derivation. We now let $K = k[y]/I$. This is now a differential field and it now has no new constant (the "new constant" is included in the relation defined by I). This is now a Picard-Vessiot extension.
Note the similarity with the second construction of the splitting field in the preliminary Galois lecture. ◇
In fact, the existence of Picard-Vessiot extension can be achieved through this construction (see [PS02, Mag94, Put98]). Consider the ring $R := k[X_{1,1}, \ldots, X_{n,n}, W]$ where the $X_{i,j}$ are indeterminates and

$$W.\det \begin{pmatrix} X_{1,1} & \ldots & X_{1,n} \\ \vdots & & \vdots \\ X_{n,1} & \ldots & X_{n,n} \end{pmatrix} = 1.$$

Extend the derivation on k to a derivation D on R by letting $D(X_{i,j}) = X_{i,j+1}$ for $1 \leq j < n$ and $D(X_{i,n}) = -sum_{l=0}^{n-1} a_l X_{i,l+1}$. This way, we have formally realized that $L(X_{i,1}) = 0$. Let J denote a differential ideal in R (i.e $D(J) = J$) which is maximal among differential ideals. It can be shown that then J is

[2]Note that as $L(y_i) = 0$, we have $y_i^{(n)}$ and the higher derivatives in K, which really makes it a differential field

a prime ideal. So R/J has no zero-divisor and we may let $K := Frac(R/J)$. Now K has no new constant: if $\frac{P}{Q}$ was a new constant, then $(P - Q)$ would be a differential ideal in R/J, contradicting the maximality of J. It follows that this construction yields a Picard-Vessiot extension K. The ideal J is called the *ideal of relations* among solutions.

Definition 9 *We call a* differential k-automorphism *of K an automorphism g of K which leaves k fixed et which commutes with the dérivation,i.e:*

1. $\forall y \in K,\ g(y)' = g(y')$
2. $\forall y \in k,\ g(y) = y$

The differential Galois group $G = Gal_\partial(K/k)$ *of a differential extension $K \supset k$ is the group of differential k-automorphisms of K.*
The differential Galois group G *of $L(y) = 0$ is defined as the differential Galois group of K/k, where K is a Picard-Vessiot extension of k for L.*

Consider the n-dimensional C-vector space V of solutions of $L(y) = 0$ in K, generated by the y_i over C. Let $g \in G$ and let y denote a solution of $L(y) = 0$. Then, $g(y)$ is also a solution. Indeed, as $a_i \in k$, we have $g(a_i) = a_i$ and :

$$\begin{aligned} L(g(y)) &= g(y)^{(n)} + a_{n-1}g(y)^{(n-1)} + \ldots + a_0 g(y) \\ &= g(y^{(n)}) + g(a_{n-1})g(y^{(n-1)}) + g(a_0)g(y) \\ &= g(L(y)) = g(0) = 0. \end{aligned}$$

As any solution is a linear combination of the y_i, we deduce that there exists constants $c_{i,j}$ such that $g(y_j) = \sum_i c_{i,j} y_i$. As an automorphism is fully determined by its action on the generators y_i of K, this gives us a faithful representation of G as a subgroup of the group $GL(n, C)$ of invertible $n \times n$ matrices. In fact, one can show ([PS02, Beu92, Kov86]), that G is a *linear algebraic group*, i.e the entries $c_{i,j}$ of the matrices are defined as solutions of a set of algebraic equations; the reason for this is the fact (intuitively clear, but still deep) that G can also be viewed as the set of such automorphisms that preserve all the relations among the solutions.
Recall the construction of the Picard-Vessiot extension; G can be viewed as the set of matrices with a right action on the $X_{i,j}$ that preserve the ideal of relations J, and this is what makes it a linear algebraic group. In what follows, we will identify G to this representation as a group of matrices acting on solutions.

A little bit on linear algebraic groups Before proceeding with Galois theory, a quick incursion (see e.g [CLO97, Spr81, PS02, Kap57] for more) into linear algebraic groups.
Recall that an affine algebraic variety V over C is defined as the set of solution of some polynomial equations (e.g straight lines, a circle, conics,etc..). The ideal $I(V)$ associated to the variety is the set of polynomials that vanish at every point of the variety. Conversely, to any ideal we associate the variety of points that annul all polynomials of the ideal. The variety is called irreducible if $I(V)$ is prime. As every ideal is the intersection of a finite number of prime ideals, we see that any affine variety is the union of a finite number of irreducible varieties.

A linear algebraic group G is a group of $n \times n$ matrices whose entries form an algebraic variety of C^{n^2+1}. The reason for adding one dimension is to include the condition that the determinant is not zero: if we add one variable, the condition $\det(g) \neq 0$ is rephrased as $u.\det(g) - 1 = 0$ which is now a polynomial equation. This way, we see that $GL(n, C)$ is a linear algebraic group.

If G is a linear algebraic group and G is irreducible as a variety, we will say that it is *connected* (for the Zariski topology). If G is not connected, then G is the finite union of irreducible ("connected") varieties. Among those, the one that contains the identity element is called the *connected component of the identity* in G, and denoted by G°. One can show that G° is a normal subgroup of finite index in G.
A linear algebraic group is said to *virtually* have a property if G° has that property; for example, G is called *virtually abelian* if G° is abelian (as a group).
The *dimension* of G is defined as the transcendence degree of G° over C.

Example. Here are classical examples of linear algebraic groups.

1. $GL(n, C)$ and $SL(n, C)$ (defined by $\det(g) = 1$).
2. The group of upper triangular matrices T (defined by $T_{i,j} = 0$ for $j < i$).
3. Let I_n denote the identity matrix of size n and the standard symplectic matrix
$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

The set of matrices M that satisfy ${}^tM.J.M = J$ (this relation induces a finite set of polynomial relations on the entries of M) is called the *Symplectic* group $Sp(2n, C)$ and will be central in the applications to symplectic mechanics.

4. Any finite group of matrices (check this!)

$\diamond$

To measure properties of the connected component of the identity G°, one uses its Lie algebra. The Lie algebra of a linear algebraic group is the tangent space at the identity (this makes sense: the group is an algebraic variety, so there is a natural tangent space). This is simply computed with the epsilon-trick (see [Put98, PS02]) as follows. Let ϵ denote an object satisfying $\epsilon^2 = 0$ (think of ϵ as being ideally small). A matrix M is in the tangent space at the identity if and only if $Id + \epsilon M$ satisfies the equations of the group (or "is a $C[\epsilon]$-point of the variety"). This defines the Lie algebra $Lie(G)$.
The dimension of G as a variety equals the dimension of $Lie(G)$ as a vector space. If you compute the Lie algebra for the groups in the above examples (easy computation), you will find that $sl(n, C) := Lie(SL(n, C))$ is the set of matrices with zero trace, that the Lie algebra of T is T itself, that $sp(2n, C) := Lie(Sp(2n, C))$ is the set of matrices M satisfying ${}^tMJ + JM = 0$ (or $M = JS$, with S any symmetrical matrix), and that the Lie algebra of a finite group is equal to 0.

B.3 Some Essential Properties

As in classical Galois theory, there is a Galois correspondence between algebraic subgroups of G and differential subfields of K. We will admit here a weak version of this correspondence which will be enough for our purposes (see e.g [PS02] for a full proof).

Theorem 3 (Galois normality) *Let K denote a Picard-Vessiot extension of k, let G be its differential Galois group, and let $z \in K$. Then:*

$$z \in k \iff \forall g \in G,\ g(z) = z.$$

A first application of this concerns unimodularity of the Galois group: recall that a matrix is called unimodular if its determinant is equal to 1, and

that the group of unimodular matrices is denoted by $SL(n, C)$.
Define the *Wronskian* matrix $W = (y_i^{(j-1)})_{i,j=1..n}$ and the Wronskian determinant $w = \det(W)$.
Exercise 16.

1. Show that $y_1, \ldots, y_n$ are linearly independent over C if and only if the Wronskian determinant w is not equal to zero.
2. Show that $w' = a_1 w$
3. Show that, $\forall g \in G$, $g(w) = w.\det(g)$ (Hint: show that g acts on W by multiplication on the right).

$\diamond$

Lemma 1 *There exists $f \in k$ such that $a_{n-1} = \frac{f'}{f}$ if and only if $G \subset SL(n, C)$.*

Proof. Assume that $G \subset SL(n, C)$. By the above exercise, we have $g(w) = w$ for all g in G hence the normality theorem shows that $w \in k$ and it is thus a solution in k of $w' = a_{n-1}w$.
Conversely, if there exists f in k such that $a_{n-1} = \frac{f'}{f}$, then we must have $w = c.f$ with $c \in C$ (because K contains no new constants) so $w \in k$ and thus the relation $g(w) = w.\det(g)$ implies that $\det(g) = 1$. $\bigcirc$

Note that we can always arrange that the Galois group be unimodular by letting $y = z.e^{\int \frac{a_{n-1}}{n}}$, we see that z satisfies a linear differential over k where we have no term in $z^{(n-1)}$ any more, hence the wronskian is a constant (necessarily in k) and the Galois group is unimodular.

If $z \in K$, the *orbit of z under G*, noted $\mathrm{Orb}_G(z)$ is the set of elements of the form $g(z)$ for some g in G.

Proposition 3 *Let $z \in K$. Then z is algebraic of degree m over k if and only if $\mathrm{Orb}_G(z)$ has exactly m elements.*
All solutions of $L(y) = 0$ are algebraic if and only if G is a finite group.

Proof. Assume that z is algebraic; let Q be its minimum polynomial. Let

$$P = \prod_{g \in G} (Y - g(z)) \in K[Y].$$

Of course, $P(z) = 0$ and we now show that the coefficients are in k. Let $g_0 \in G$. As left multiplication by g_0 is a bijection of G, we have

$$\prod_{g\in G} (Y - g_0.g(y)) = \prod_{\tilde{g}\in G} (Y - \tilde{g}(y)) .$$

So the coefficients of P are fixed by the group and hence, by Galois normality, they are all in k. The roots of P are exactly $\mathrm{Orb}_G(z)$ by construction. As Q is the minimum polynomial of z, Q is a divisor of P so the roots of Q are in $\mathrm{Orb}_G(z)$. Now, the image of a root of Q (here: z) by any element of G is again a root of Q. We conclude that there are as many roots of Q as elements in $\mathrm{Orb}_G(z)$, hence $\deg(Q) = \mathrm{card}\,(\mathrm{Orb}_G(z))$.
Conversely, if $\mathrm{Orb}_G(z)$ has exactly m elements, call $g_1, \ldots, g_m$ elements of G such that $\mathrm{Orb}_G(z) = \{g_1(z), \ldots, g_m(z)\}$. As above, we form $P = \prod_{i=1..m} (Y - g_i(z))$. Let $g \in G$; as it is an automorphisms, $g(g_i(z)) \neq g(g_j(z))$ when $i \neq j$ so g acts as a transitive permutation on the $g_i(z)$. It follows that P has coefficients in k. Now, if it was reducible, z would be a zero of a factor and its orbit would hence have less than m element. We conclude that z is algebraic of degree m.
Now, if G is a finite group, the above shows that any element in the Picard-Vessiot extension is algebraic; conversely, if all solutions are algebraic, then the y_i have only a finite number of possible images under G so, as an automorphism of K is defined by its action on the generators of K, the group G must be finite. ◯

Exercise 17. Let $z \in K$ be algebraic of degree m. Let $Stab_G(z) := \{g \in G, g(z) = z\}$ denote the stabilizer of z in G. Show that m is the index in G of $Stab_G(z)$ (i.e the cardinal of the quotient). ◇

Proposition 4 *An non-zero element z of K is exponential over k if and only if, for all $g \in G$, there exists a constant $c_g \in C$ such that $g(y) = c_g.y$.*

Proof. Let $g \in G$.

$$\left(\frac{g(z)}{z}\right)' = \frac{g(z')}{z} - \frac{z'}{z^2}g(z) = \frac{g(z)}{z}\left(g(\frac{z'}{z}) - \frac{z'}{z}\right).$$

So, $g(z)/z$ is a constant for all $g \in G$ if and only if z'/z is left fixed by all $g \in G$. By Galois normality, this is indeed equivalent with the fact that

$z'/z \in k$. ○

Note that in fact, this means that an element z of K is exponential if and only if the straight-line $z.k$ is globally invariant under G.

Exercise 18.[Put97]
We consider the equation $y' = ay$ with $a \in \mathbb{C}(x)$.

1. Show that any proper algebraic subgroup of $\mathbb{C}^*$ is finite and cyclic.
2. By considering the possible Galois groups, show that an algebraic solution $y' = ay$ must satisfy $y^m = f$ where $f \in \mathbb{C}(x)$ (i.e y is *radical* over $\mathbb{C}(x)$). Show that the equation $y' = ay$ has an algebraic solution if and only if there exists a positive integer m such that the equation $f' = maf$ has a solution $f \in \mathbb{C}(x)$.
3. For $m \in \mathbb{N}$, show that the equation $f' = maf$ has a rational solution if and only if $a = \sum_i \frac{n_i}{m(x-x_i)}$ with $n_i \in \mathbb{Z}$ having their gcd prime to m. What is the Galois group in this case.
4. Deduce from this a method which decides if the equation $y' = ay$ has an algebric solution, computes it, and gives the differential Galois group.
5. Application: compute the Galois group for $y' = y$, for $y' = \frac{1}{4x}y$, and for $y' = \frac{\alpha}{x}y$.

◇

Exercise 19.[Logarithms]

1. Consider the field $K = \mathbb{C}(x, \log(x))$. Show that K is a Picard-Vessiot extension of $\mathbb{C}(x)$ corresponding to a homogeneous linear differential equation of order 2 and that its Galois group is conjugate to $G_a = \{\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, c \in \mathbb{C}\}$.
2. Show that G_a is abelian, isomorphic to the additive group $(\mathbb{C}, +)$, and that its only algebraic subgroups are itself and $\{Id\}$.
3. Show that the reasonning of (i) applies for any element f such that $f' = a \in \mathbb{C}(x)$. Deduce from this that either f is transcendental or f is in $\mathbb{C}(x)$ (theorem of Liouville).

◇

These two exercises show that when one adjoins to k an exponential or an integral, the Galois group of the extension is abelian. Recall that the Liouvillian functions are the elements of fields obtained by adjoining successively exponentials, integrals, or algebraic elements to $\mathbb{C}(x)$.

Exercise 20. We say that a field K is a purely Liouvillian extension of $\mathbb{C}(x)$ if it is constructed via a tower of fields $\mathbb{C}(x) = K_0 \subset K_1 \subset \ldots \subset K_N = K$ where K_{i+1} is obtained from K_i by adjoining either an exponential or an integral.

Show that the differential Galois group of a purely Liouvillian extension K is solvable. ◇

If we allow arbitrary algebraic extensions, their Galois group G is finite and needs not be abelian any more (in general, it is not!). However, G° is then reduced to the identity. This gives us the first step to the following theorem of Kolchin (which we will admit)

Theorem 4 ([Kol48]) *A linear differential has a basis of liouvillian solutions if and only if its differential Galois group G is virtually solvable.*

In [Kol48], Kolchin actually proved the Lie-Kolchin theorem: G° is solvable if and only if its matrices can be put simultaneously in triangular form. The above theorem then follows without too many difficulties. To get convinced, you may study an exemple of this situation where a linear differential equation has a solvable differential Galois group.

Exercise 21. Consider the differential equation

$$L(y) = y'' + (-g(x) - 2)\, y' + (g(x) + 1)\, y = 0$$

with g a non-zero rational function in $\mathbb{C}(x)$.

1. Show that it admits $y_1 = e^x$ as a solution.
2. Using variation of constants, show that it admits $y_2 = e^{x + \int g(x)}$ as a second solution.
3. Show that the differential Galois group of L is solvable.

4. Show that the differential Galois group of L is either

$$\left\{\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}, c \in \mathbb{C}^*\right\} \qquad \text{or} \qquad \left\{\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}, c \in \mathbb{C}^*, d \in \mathbb{C}\right\}$$

and give a criterion to decide between either case.

$\diamond$

C Second Order Differential Equations

We will now show how to use the differential Galois group for solving linear differential equations. For simplicity, we focus on second order equations. The idea is to first classify the possible Galois groups and then, on the basis of this classification, to study the corresponding properties of the solutions. We consider the differential equation $L(y) = y'' - a_1 y' - a_0 y = 0$.

C.1 Subgroups of $SL(2, C)$

Recall from lemma 1 that we can assume that the differential Galois group is unimodular, i.e a subgroup of $SL(2, \mathbb{C})$. The subgroups of $SL(2, \mathbb{C})$ are classified and we now go through this construction.

C.1.1 Case I: Reducible Case

Definition 10 *Let G be a linear group acting on a vector space. We say that (the action of) G is* reducible *if there exists a non-trivial subspace $W \subset V$ such that $G(W) \subset W$.*

In our case, $\dim(V) = 2$ so W has to be of dimension 1 and the matrices in the Galois group are triangular (or diagonal). By proposition 4 (and the remark right after it), this is equivalent with the fact that the differential equation has an exponential solution. We also see that the group is diagonal if there are (at least) two exponential solutions (this case is handled further in exercise 23). In this case, W admits a complement subspace that is also stable under G and the group is then said to be *completely reducible.*

To the equation $L(y) = 0$, we associate the Riccati equation, i.e the equation satisfied by $u = \frac{y'}{y}$. Simple computation shows that $u' = a_0 + a_1 u - u^2$.

We see that the equation is reducible if and only if the Riccati equation has a rational solution.

If G is reducible, then L itself is reducible, in the sense that it can be written as a composition of two operators (check this in exercise 21); you may check that L has a right factor $\partial - u$ if and only if u is a solution of the Riccati equation.

If G does not act reducibly, it is called *irreducible.*

C.1.2 Case II: Imprimitive Case

Definition 11 *Let G be an irreducible group acting on a vector space V. We say that G is* imprimitive *if there exist subspaces V_i such that $V = V_1 \oplus \ldots \oplus V_r$ and G permutes transitively the V_i :*

$$\forall i = 1, \ldots, r \; \forall g \in G, \qquad \exists j \in \{1, \ldots, r\} : \; g(V_i) = V_j.$$

We then say that $V_1, \ldots, V_r$ form a system of imprimitivity for G.

In our case, we must have $r = 2$ and $\dim(V_1) = \dim(V_2) = 1$. The matrices have the form

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix} \qquad \text{with } \; a, b \in C^*.$$

Lemma 2 *Assume that G is irreducible. Then the Riccati equation has an algebraic solution of degree 2 if and only if G is imprimitive.*

Proof. Let P denote the minimum polynomial of an algebraic Riccati solution of degree 2. Let u_1, u_2 be the roots of P. As u_1, u_2 satisfy the Riccati equation, there exists solutions y_i of $L(y) = 0$ such that $y_i'/y_i = u_i$. As G permutes the u_i, it permutes the lines $V_i = C. < y_i >$ and the V_i form a system of imprimitivity.
Reciprocally, let $V_i = C. < y_i >$ be a system of imprimitivity. If we let $u_i = y_i'/y_i$, then G permutes the u_i and proposition 3 shows that they are algebraic of degree 2 and conjugate (you may also check that the symmetric functions in the u_i are left fixed by G). ◯

C.1.3 Case III: Primitive case

Definition 12 *If G is irreducible and not imprimitive, we say that it is primitive.*

One can show ([SUl93b]) that an equation whose Galois group is an infinite primitive subgroup of $SL(n, C)$ does not have Liouvillian solutions; And if the group is finite, all solutions are algebraic (proposition 3) and hence Liouvillian.

In the case of $SL(2, C)$, there are three primitive groups (see [SUl93a, SUl93b] or the lovely survey [Kov01] by Kovacic himself which we follow here): The tetraedral group ($A_4^{SL_2}$) of order 24, the octaedral group ($S_4^{SL_2}$) of order 48, and the icosaedral group ($A_5^{SL_2}$) of order 120. We will now review them

The tetraedral group $A_4^{SL_2}$ of order 24 is generated by matrices

$$M_1 = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \qquad \text{and} \qquad M_2 = \frac{1}{3}(2\xi - 1) \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}$$

where ξ denotes a primitive sixth root of unity, i.e $\xi^2 - \xi + 1 = 0$. The subgroup $< M_1 >$ generated by M_1 has order 6. Assume the second order operator L has $A_4^{SL_2}$ as its Galois group. Let y_1, y_2 denote a basis of the solution space on which these matrices act and have this form. We see that the line generated by y_1 is left fixed by $< M_1 >$; this imposes that $u_1 := \frac{y_1'}{y_1}$ is left fixed by $< M_1 >$ (recall proposition 4) so its orbit under G has length at most 4 (in fact, direct computation shows that it has length exactly 4). By the Galois correspondenc (proposition 3), it follows that u_1 is algebraic of degree 4. We conclude that when the Galois group is $A_4^{SL_2}$, the Riccati equation has a solution which is algebraic of degree 4.
Another way to see this result is the following. Computing the conjugates of y_1 under G shows that the polynomial $Y_1 \left(2\,Y_2 + Y_1\right) \left(4\,{Y_2}^2 - 2\,Y_1\,Y_2 + {Y_1}^2\right)$ is a semi-invariant of the Galois group (i.e it is sent to a multiple of itself by the group acting by linear substitution, right action). It can also be checked that its cube is an invariant. We will use this below to compute the minimum polynomial of u_1.

The octaedral group $S_4^{SL_2}$ of order 48, is generated by matrices

$$M_1 = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \qquad \text{and} \qquad 1/2\,\xi\,\left(\xi^2+1\right)\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

where ξ denotes a primitive eighth root of unity, i.e $\xi^4+1=0$. The subgroup $< M_1 >$ generated by M_1 has order 8 and reasoning as above shows that the riccati solution u_1 is algebraic of degree $6 = \frac{48}{8}$.
The group admits the semi-invariant $Y_1^5 Y_2 - Y_1 Y_2^5$, whose square is an invariant.

The icosaedral group $A_5^{SL_2}$ of order 120. is generated by matrices

$$M_1 = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} \phi & \psi \\ \psi & -\phi \end{pmatrix}$$

where ξ denotes a primitive tenth root of unity, i.e $\xi^4 - \xi^3 + \xi^2 - \xi + 1 = 0$, and $\phi = \frac{1}{5}(\xi^3 - \xi^2 + 4\xi - 2)$ and $\psi = \frac{1}{5}(\xi^3 + 3\xi^2 - 2\xi + 1)$. The subgroup $< M_1 >$ generated by M_1 has order 10 and reasoning as above shows that the riccati solution u_1 is algebraic of degree $12 = \frac{120}{10}$.
The group admits the invariant $Y_1^{11} Y_2 - 11 Y_1^6 Y_2^6 - Y_1 Y_2^{11}$.

In the cases of these three groups, all solutions are algebraic and hence all solutions of the Riccati equation are of course also algebraic. By developping on propositions 3 et 4, the study of those groups (see [UWe96, Kov86] or push further the above calculations) shows that :

- For $A_4^{SL_2}$: The Riccati has algebraic solutions of degrees 4,6 ou 12.
- For $S_4^{SL_2}$: The Riccati has algebraic solutions of degrees 6,8,12, ou 24.
- For $A_5^{SL_2}$: The Riccati has algebraic solutions of degrees 12,20,30, ou 60.

Lastly, if $G = SL(2,C)$, the differential equation does NOT have liouvillian solutions. In view of the applications to hamiltonian mechanics ([Ram01]), we see that the only subgroup(s) of $SL(2,C)$ that will yield obstructions to integrability are ... only $SL(2,C)$ itself.

This classification work is summarized in Kovacic's theorem

Theorem 5 ([Kov86]) *Let $L(y) = 0$ be a linear differential equation with coefficients in k It has Liouvillian solutions if and only if it has solutions of the form $y = e^{\int u}$ where u is an algebraic solution of degree 1 (reducible case I), degree 2 (Imprimitive case II), or degree in $\{4, 6, 12\}$ (Primitive case III) of the associated Riccati equation.*

C.2 The Kovacic algorithm

We now give a (simplified) version of the algorithm of Kovacic for solving second order linear differential equations.

C.2.1 Symmetric powers

Let $P = U^m + b_{m-1}U^{m-1} + \ldots b_0$ be the minimum polynomial of an algebraic solution of the Riccati equation. Let $u_1, \ldots, u_m$ be the roots of P, and y_i the solutions of $L(y) = 0$ of which they are logarithmic derivatives. We then have

$$b_{m-1} = -(u_1 + \ldots + u_m) = -(\frac{y_1'}{y_1} + \ldots y_m' y_m) = -\frac{(\prod y_i)'}{\prod y_i}.$$

The coefficient $-b_{m-1}$ is thus the logarithmique derivative of a product of m solutions of $L(y) = 0$.

Lemma 3 *Let y_1, y_2 be a basis of solutions of $L(y) = 0$. There exists a linear differential equation $L^{\circledS m}$ whose solution space is the set of homogeneous polynomials of degree m in y_1, y_2 with coefficients in C.*

Proof. Let y be a generic solution of $L(y) = 0$. Let $z = y^m$. Compute z', z'',...,z^{m+1} by always replacing y'' by its expression given by $L(y) = 0$. The $z^{(i)}$ are linear combinations of monomials of degree m in y, y'. These monomials form a k-vector space of dimension $m + 1$; if we have $m + 2$ elements of such a space, they are linearly dependent, so z,z', z'',...,z^{m+1} satisfy a linear dependence relation over k that we note $L^{\circledS m}(z) = 0$: what we know is that it has order at most $m + 1$.
Let A be the differential ring $K[X_1, X_2]$ where the derivation is given by $X_1' = X_2' = 0$. By construction, we have $L^{\circledS m}((X_1 y_1 + X_2 y_2)^m) = 0$. We easily infer that any monomial of degree m en y_1, y_2 is a solution of $L^{\circledS m}(z) = 0$. But, if these monomials were linearly dependent, then y_1, y_2 would be linearly dependent (any homogeneous polynomial in two variables factors as a product of linear factors over C) : So they form a vector space

of dimension $m+1$, then $L^{\circledS m}(z)$ is order $m+1$, and its solution space is precisely that vector space. ◯

We can calculate the linear dependence between z and z' using standard linear algebra, but a faster method is the following:
Exercise 22.[[BMW97]] Let $L(y) = y'' + ay' + by = 0$. we define recursively a sequence of operators L_i by :

$$\begin{cases} L_0(y) &= y, \\ L_1(y) &= y', \\ L_{i+1}(y) &= L_i(y)' + iaL_i(y) + i(m-i+1)bL_{i-1}(y). \end{cases}$$

1. Let y be a solution of $L(y) = 0$. Show by induction that

$$L_i(y^m) = m(m-1)\cdots(m-i+1)y^{m-i}(y')^i.$$

2. Deduce that $L_{m+1} = L^{\circledS m}$.

◇

C.2.2 Algebraic Solutions of the Riccati Equation

Theorem 6 *The Riccati equation has a solution algebraic of degree at most m if and only if the symmetric power $L^{\circledS m}(z) = 0$ has an exponential solution.*

Proof. If the Riccati equation has an algebraic solution of degree m, we have seen that the coefficient b_{m-1} of its minimum polynomial is the logarithmic derivative of an exponential solution of $L^{\circledS m}(z) = 0$.
Conversely, let z be an exponential solutions of $L^{\circledS m}(z) = 0$. Lemma 3 shows that there exists a polynomial $Q(y_1, y_2)$ homogeneous of degree m such that $z = Q(y_1, y_2)$. Let v be the logarithmic derivative of z. As $Q(y_1, y_2)$ factors as a product of linear factors over C, let $u_1, \ldots, u_m$ be the logarithmic derivatives of these factors. A linear combination of solutions is a solution so the u_i are Riccati solutions. For any $g \in G$, as $g(v) = v$, $g(u_i)$ must be one of the u_j : by proposition 3, it follows that the u_i are algebraic of degree at most m. ◯

If the u_i do not have degree m, you may check that the product P of their minimum polynomials will be of degree m and its coefficient b_{m-1} will be given by $b_{m-1} = -v'/v$.

In [UWe96], it is shown how, in many cases, one can also ask for rational solutions of $L^{\circledS m}(y)$, which simplifies the algorithm.

Recall that the Riccati equation associated with $y'' + a_1 y' + a_0 y$ is $u' = -a_0 - a_1 u - u^2$. Differentiating the identity $P(u) = 0$ and replacing u' by its expression, we obtain a polynomial relation of degree $m+1$ for u. The remainder of the Euclidean division of this polynomial of degree $m+1$ by P must be zero which gives us the following recursion to obtain all coefficients b_i once b_{m-1} is known.

$$(\sharp)_m : \qquad \begin{cases} b_m = 1 \\ b_{i-1} = \dfrac{-b_i' + b_{m-1} b_i + a_1 (i-m) b_i + a_0 (i+1) b_{i+1}}{m-i+1}, \quad m-1 \geq i \geq 0 \\ b_{-1} = 0 \end{cases}$$

Finally, we obtain the following algorithm to calculate algebraic solutions of Riccati equations:

For $m \in \{1, 2, 4, 6, 12\}$:

- Compute $L^{\circledS m}(y)$
- Seek exponential solutions f
- If there are some: let $b_{m-1} = -\frac{f'}{f}$, compute the other coefficients b_i of P by using $(\sharp)_m$, and return P
  else, proceed with next m.

If no solution is found this way, there are no Liouvillian solutions.

Exercise 23. Consider the differential equation $L(y) = y'' - ry = 0$.

1. Write the Riccati equation $R(u) = 0$ satisfied by $u = y'/y$.
2. Show that $L^{\circledS 2}(y) = y''' - 4ry' - 2r'y''$.
3. We assume that R has an algebraic solution of degree 2.

(a) Show that its minimum polynomial has the form

$$P = u^2 - \frac{f'}{f}u + \frac{f''}{2f} - r$$

where $L^{\circledS 2}(f) = 0$.

(b) Show that $f\, disc(P) = c$ where c is a constant.

(c) We assume that $L^{\circledS 2}(f) = 0$ has a solution $f \in \mathbb{C}(x)$ and that $disc(P) \neq 0$. Show that the Riccati equation has one or two rational solutions; Compute them, and deduce that L admits the liouvillian solutions $y = \sqrt{f}e^{\pm\int \frac{\sqrt{c}}{2f}}$.

(d) Conversely, show that if $L(y) = 0$ has two linearly independent exponential solutions, then the matrices of the Galois group are diagonal matrices and $L^{\circledS 2}(y) = 0$ has a rational solution (recall that the Galois group is unimodular)

(e) Application : solve $y'' - \frac{c}{16x^2}y = 0$ où $c \in \mathbb{C}$.

$\diamond$

D Local and Global Differential Galois Theory

In the lectures of Canalis-Durand [CaD01] and Ramis [Ram01], it is shown how *local* information gives indications on the structure of the differential Galois group. We will now explain some (easiest) algebraic aspects of this local approach, and how to realize actual computations with it.

D.1 Local Solutions

D.1.1 Power Series Solutions

We make the coefficients of our differential equation polynomials: $L(y) = a_n y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_n y = 0$ where the a_i are now polynomials (in fact, analytic would be enough). If $a_n(x_0) \neq 0$, then Cauchy's theorem shows that the equation has a basis of analytic solutions around zero.

Computing these power series is achieved the following way. Let $T = x - x0$ if $x_0 \in \mathbb{C}$ of $T = \frac{1}{x}$ if $x_0 = \infty$. Perform the change of variables

$x \mapsto T$ in the equation and plug $\sum_i c_i T^i$ into the equation: you will obtain a recurrence relation for the c_i and they will be uniquely determined by their first n terms (exercise: prove this cleanly).
To fix notations, let's make this recursion explicit. The operator L can be viewed as an endomorphism of the infinite dimensional vector space $\mathbb{C}[[x]]$. Assume that $a_i = \sum_{i=1}^{m_i} a_{i,j} x^j$. We write the action of L on a basis of $\mathbb{C}[[x]]$: we get $L(x^N) = \sum_{i=0}^{n} \sum_{j=0}^{m_i} N(N-1)\dots(N-i+1) a_{i,j} x^{N+j-i}$. Now,

$$L(\sum_{N=0}^{\infty} c_N x^N) = \sum_{N=0}^{\infty} \sum_{i=0}^{n} \sum_{j=0}^{m_i} N(N-1)\dots(N-i+1) c_N a_{i,j} x^{N+j-i}. \quad (1)$$

So, grouping powers of x, we obtain a recurrence relation

$$(\mathcal{R}_N) : \sum_{l=0}^{m} E_l(N) c_{N-l} = 0 \quad (2)$$

with E_l being a polynomial. In particular, if ν is the *valuation* of the power series (the smallest integer such that $c_\nu \neq 0$), we must have $E_0(\nu) = 0$ (all the $c_{\nu-l}$ are zero).
If $a_n(x_0) \neq 0$, then direct computation shows that $E_0(N) = N(N-1)\dots(N-(n-1))$.
Exercise 24. Use this to show the formal part of Cauchy's theorem i.e the existence of a basis of solutions in power series. ◇

D.1.2 Exponents and Quasi-Series

We now turn to the singular case. For notational convenience, we assume that the considered singular point is zero (i.e $a_n(0) = 0$).
We say that a solution y is a *quasi-series* if it is of the form $y = x^\alpha \phi$ with ϕ analytic and $\alpha \in \mathbb{C}$. If $\alpha \in \mathbb{Z}$, this is a *Laurent* series; if $\alpha \in \mathbb{Q}$, this is a *Puiseux* series. If further ϕ has valuation zero (i.e its constant term is not zero), then α is well defined and we call it the *exponent* of the quasi-series y.

Example. The Euler homogeneous equation ([Ince]).
Consider the equation $L(y) = x^2 y'' + c_1 x y' + c_2 y = 0$ with c_1, c_2 constants (this equation is often called, as many other equations, an Euler equation). Computation shows that $L(x^\alpha) = E_0(\alpha) x^\alpha$ with $E_0(\alpha) = \alpha(\alpha-1) + c_1\alpha + c_0$. We see that there is a solution of the form x^α if and only if $E_0(\alpha) = 0$.
If E_0 has two distinct roots α_1, α_2, then we have distinct solutions x_1^α and x_2^α (check that they are linearly independent over C).

If E_0 has a double root α_1, we have $E_0(\alpha_1) = E_0'(\alpha_1) = 0$. We differentiate the relation $L(x^\alpha) = E_0(\alpha)x^\alpha$ with respect to α (note that $\frac{\partial}{\partial\alpha}(x^\alpha) = x^\alpha \log(x)$):
we obtain $L(x^\alpha \log(x)) = (E_0'(\alpha) + \log(x)E_0(\alpha))x^\alpha$, from which it follows that $L(x_1^\alpha \log(x)) = 0$ so a second solution is $x_1^\alpha \log(x)$. ◇

Exercise 25. Show that the equation $L(y) := 2xy'' + 3y' + 2y = 0$ has a basis of quasi-series solutions at $x = 0$. Hint: Compute $L(x^{\alpha+N})$ for an arbitrary integer N and show that $L(\sum_{N=0}^{\infty} c_N x^{\alpha+N}) = 0$ if and only if we both have that $E_0(\alpha) = 0$ for some polynomial E_0 and the c_N are solutions of a recursion relation (compute it). ◇

To make this general, look at equation 1 and replace N by $\alpha+N$ in there. Relation 2 then becomes

$$(\mathcal{R}_N) : \sum_{l=0}^{m} E_l(\alpha + N)c_{N-l} = 0 \tag{3}$$

A necessary condition for the existence of a quasi-series solution with exponent α is that $E_0(\alpha) = 0$ (from the case $N = 0$ in recursion 3).

Definition 13 .
The polynomial E_0 is called the indicial polynomial *of L at zero.*
The roots of E_0 are called the exponents *of L at zero.*
If E_0 has degree exactly n, then zero is called a regular singularity*; otherwise, E_0 has degree strictly less than n and zero is an* irregular singularity.

Exercise 26. Let α be an exponent at zero such that, for all $i \in \mathbb{N}$, $\alpha + i$ is Not an exponent. Prove that L admits a quasi-series solution of exponent α. ◇

More generally, if the singularity is regular singular, then (see [Ram01] or [Ince]) either there is a basis of quasi-series solutions, or there is a basis formed of quasi-series and of solutions of the form $x^{\alpha_1}\phi_1, x^{\alpha_1-n_1}(\phi_2 + x^{n_1}\phi_1 \log(x)), \ldots$ (this may happen in the case when two exponents differ by an integer). Moreover, the power series ϕ_i are analytic. So in this case, the formal theory and the analytical theory coincide.

D.1.3 Generalised Exponents

If the singularity zero is not regular, then quasi-series and logarithms are clearly not enough to define solutions. For example, consider the equation

$x^2y' + y = 0$: the solution $e^{\frac{1}{x}}$ can not be written as a quasi-series at zero, so we need to add exponentials to our formal local objects.

Definition 14 *An element* $e_i \in \mathbb{C}[x^{-\frac{1}{r}}]$ *is called a* generalized exponent *if there is a formal solution of the form* $e^{\int \frac{e_i}{x}}\phi_i$ *where* $\phi_i \in \mathbb{C}[[x]][e_i, \log(x)]$ *and the valuation (with respect to* x*, not counting the* log*) of* ϕ_i *is equal to zero. If* $r > 1$*, then* r *is called the* ramification index *of the generalized exponent.*

Note that exponents themselves are generalized exponents: indeed $x^\alpha = e^{\int \frac{\alpha}{x}}$. To compute generalized exponents, one looks for formal Puiseux series solutions for the Riccati equation associated with L (i.e solutions in $C((x^{\frac{1}{r}}))$ for some $r \in \mathbb{N}$) and keeps only the parts of such solutions whose valuation is less or equal to -1; the degrees of the generalized exponents can be measured from the *Newton polygon* of L at zero.

One can show ([PS02, Hoe97]) that one can compute a basis of formal solutions of the form $e^{\int \frac{e_i}{x}}\phi_i$ where $\phi_i \in \mathbb{C}[[x]][e_i, \log(x)]$.

D.1.4 The Formal Local Galois group

We still assume that we work at zero (otherwise, take a local parameter $t = x - x_0$ at $x_0 \in \mathbb{C}$ or $t = \frac{1}{x}$ at infinity and work with t). We consider the field $\mathbb{C}((x))$ as our base field. The *formal local Galois group* $\hat{G}_0$ at zero is defined as the differential Galois group of a Picard-Vessiot extension of $\mathbb{C}((x))$ for L.

Because we know the structure of the formal solutions, we may describe the structure of the formal local Galois group: for each i, we may write $e^{\int \frac{e_i}{x}} = x^{\alpha_i}e^{P_i}$ (with P_i of negative degree in x).
The *formal local monodromy* is defined as the Galois group over $\mathbb{C}((x))$ of

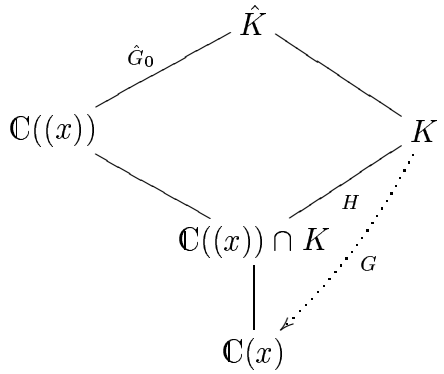
1. either $\mathbb{C}((x))(x^{\alpha_1}, \ldots, x^{\alpha_n})$ if there are no logarithms in the solutions (in which case it is a torus)

2. or $\mathbb{C}((x))(x^{\alpha_1}, \ldots, x^{\alpha_n}, \log(x))$ if there are logarithms in the solutions (in this case, it contains a unipotent element)

The *exponential Torus* is defined as the Galois group of $\mathbb{C}((x))(e^{P_1}, \ldots, e^{P_n})$. One readily sees that these two groups generate the formal local Galois group; moreover, they can be easily computed from the given of local solutions.

Lemma 4 *The formal local Galois group can be embedded into a subgroup of the differential Galois group of L over $\mathbb{C}(x)$.*

Proof. We use the fact that $\mathbb{C}(x)$ can be embedded in $\mathbb{C}((x))$ so we view it as a subfield. Consider the following Kaplansky diagram:



where H is the differential Galois group of K. Galois theory shows that H is a subgroup of K. Then, the above diagram shows ([Kap57]) that the Galois groups H and $\hat{G}_0$ are isomorphic. Thus, $\hat{G}_0$ can be viewed as a subgroup of G. ◯

If we now take for our base field the field $\mathbb{C}(\{x\})$ of convergent power series, we define the *local Galois group* G_0 as the differential Galois group of a Picard-Vessiot extension of $\mathbb{C}(\{x\})$. A Kaplansky diagram again shows that $\hat{G}_0 \subset G_0 \subset G$.

At a regular singularities, we have $\hat{G}_0 = G_0$ and the Schlesinger density theorem ([Ram01]) shows that the global Galois group is generated by its local Galois groups.

At irregular singularities, though, then new phenomena may occur (Stokes phenomenon) and in this case $\hat{G}_0 \subsetneq G_0$. This subject is adressed in the notes of M. Canalis-Durand [CaD01].

A very simple illustration of a link between local and global information is given in the following

Proposition 5 *Assume that the Global galois group is finite. Then the exponents at all singularities are rational.*

Proof. The local Galois group is embedded in the global Galois group and hence finite. The exponential torus is infinite so there cannot be irregular

points and all points must be regular. Now, if there are logarithms, the monodromy contains an additive subgroup and is infinite (alternatively: a logarithm is transcendental hence not algebraic, contradicting the fact that the group is finite). So the monodromy must be diagonal. But, because it is finite, it is cyclic and hence the exponents must be rational. ◯
We note that this result is proved more naturally using Puiseux expansions of algebraic functions, but this proof gives light on the power of the Galois theoretic tools.

D.2 Local and Global Algorithms

D.2.1 Rational Solutions

Let $\mathcal{S}$ denote the set of singular points (i.e the zeroes of a_n and possibly infinity). We search for a method to check if our differential equation has a rational solution. Let y be a rational function. Then y can be written as $y = \prod_{x_i \in \mathcal{S}} (x - x_i)^{\alpha_i} . (p_m x^m + p_{m-1} x^{m-1} + \ldots + p_0)$. So to compute y, we need to find the α_i, the degree m, and the coefficients p_i. Expansion in Laurent series (or partial fraction decomposition) shows that the α_i must be exponents of L at x_i. Now, expansion at infinity (expand in powers of $\frac{1}{x}$) shows that there must exist an integer exponent α_∞ at infinity such that $m = -\alpha_\infty - \sum_{x_i \in \mathcal{S}} \alpha_i$. We thus obtain the following algorithm, whose solutions are a basis of rational solutions (if any) of $L(y) = 0$:

1. Select the minimal integer exponents α_i at all singularities, including ∞. If one singularity does not have integer exponents, then STOP.
2. Let $m := -\alpha_\infty - \sum_{x_i \in \mathcal{S}} \alpha_i$. if m is not positive, then STOP.
   Plug $y = \prod_{x_i \in \mathcal{S}} (x - x_i)^{\alpha_i} . (p_m x^m + p_{m-1} x^{m-1} + \ldots + p_0)$ into the equation
3. solve the resulting linear system in the p_i.

D.2.2 Radical and Global Solutions

The same reasoning applies to radical solutions, i.e the exponents may be used also to compute solutions having some power which is rational: one can similarly prove (see e.g [Hoe97]) that there is a radical solution only if there are rational exponents e_i at all singular points $x_i \in \mathcal{S}$ such that $m := -e_\infty - \sum_{x_i \in \mathcal{S}} e_i$ is a positive integer. The solution would again be $y = P . \prod_{x_i \in \mathcal{S}} (x - x_i)^{e_i}$ with P of degree m. Pluging this expression $L(y) = 0$

with indeterminate coefficients of P gives a linear system for the coefficients of P, any (non-zero) solution of this system leading to a solution of L;
Note that unlike the case of rational solutions, there may be different combinations of the e_i to be tested. Also, note that if some factors of a_n are irreducible polynomials, then we may have to compute with a splitting field of those to check for combinations, and this can make the algorithm more costly.

For the more general case of exponential solutions, the process is similar, though a little bit more technical, see [Hoe97] or [PS02].

Now we would like to see how to use these tools in the Kovacic algorithm. We introduce the following useful trick from [Hoe97]:
Note that if we have two formal solutions $e^{\int \frac{e_i}{x}}\phi_i$, then their product is $e^{\int \frac{e_1+e_2}{x}}\phi_1\phi_2$, hence e_1+e_2 is a generalized exponent for the symmetric square of L. In general, it is easy to verify that the expressions $ie_1+(m-i)e_2$ form the generalized exponents of $L^{\circledS m}$. So we can check necessary conditions on rational (or radical) solutions of $L^{\circledS m}$ without having to compute this equation.

D.2.3 The Art of Computing Galois Groups

We now have all tools to smoothly use and apply the Kovacic algorithm (and generalisations like [SUl96, HRUW99]). We will show on examples how to combine all these tools together to obtain differential Galois groups.

Example. Consider the Airy equation $L(y) = y'' - xy = 0$. The only singularity is infinity. The local (generalised) exponents are $-\frac{1}{4} \pm 2\sqrt{x}^3$ at infinity. Because of the ramification at infinity, we see that the equation cannot have exponential solutions. Now we look at the second symmetric power.
Looking at sums of the exponents, we see that the only rational exponent of the second symmetric power $L^{\circledS 2}$ will be $(\frac{1}{2})$ at infinity. This cannot be the degree of a polynomial. so there cannot exists a radical solution the the second symmetric power.
Now, as the equation is irregular at infinity, the group cannot be finite by proposition 5: this excludes case 3 of the Kovacic algorithm. Finally, the only possibility is that the Galois group is $SL(2, C)$. ◇

Example. Consider the equation (from the notes of J.P Ramis [Ram01])

$$L(y) = y'' + \left(1/4\ (x-1)^{-1} + 5/4\ (x-1)^{-2} + 3/16\, x^{-2}\right)\ y\ = 0$$

The local (generalised) exponents are $(\frac{1}{4}, \frac{3}{4})$ at zero, the roots of $X^2 - 2X + 5$ at 1 and $-\frac{1}{4} \pm 2\sqrt{-x}$ at infinity. Because of the ramification at infinity, we see that the equation cannot have exponential solutions. Now we look at the second symmetric power.
Looking at sums of the exponents, we see that the only rational exponents of the second symmetric power $L^{\circledS 2}$ will be $(\frac{1}{2}, 1, \frac{3}{2})$ at zero, (1) at 1 and $(-\frac{1}{2})$ at infinity. Taking the lowest e_0, e_1, e_∞ possible, we have $-e_\infty - e_1 - e_0 = -1 < 0$ and the latter cannot be the degree of a polynomial so there cannot exists a radical solution the the second symmetric power.
Now, as the equation is irregular at infinity (and does not have rational exponents at 1), the group cannot be finite by proposition 5: this excludes case 3 of the Kovacic algorithm. Finally, the only possibility is that the Galois group is $SL(2, C)$. ◇

Exercise 27. Consider the equation $L(y) = x^3 y'' + (x^2 + x)y' - y = 0$ (from the notes of M. Canalis-Durand [CaD01]).

1. Show that the exponents at ∞ are $(0, 0)$ and that the generalized exponents at 0 are $(1, -\frac{1}{x})$.

2. Show that $e^{\frac{1}{x}}$ is an exponential solution, the only one (up to scalar multiplication).
   Show that there is a unique power series solution at zero, and that it is divergent (and Gevrey). Compute the formal local Galois group at 0.

3. Show that the formal solutions at infinity are of the form $y_{1,\infty}^{\hat{}}$ and $y_{1,\infty}^{\hat{}} \log(x) + y_{2,\infty}^{\hat{}}$ where the $y_{i,\infty}^{\hat{}}$ are power series in $\frac{1}{x}$. Compute the formal local Galois group at infinity.

4. Compute the global Galois group, and compare it with the formal local Galois groups.

◇

Exercise 28. The Whittaker equation $L(y) = y'' - (\frac{1}{4} + \frac{12}{\lambda})y\ = 0$. The exponents at zero are the roots of $\lambda X^2 - \lambda X - 12$ and at infinity $\pm\frac{x}{2}$.

1. Show (using the above examples) that for generic values of λ the Galois group is $SL(2, C)$.

2. Show that the exponents at zero are rational if and only if $\lambda = \frac{12}{n(n-1)}$ with $n \in \mathbb{Q}$.

3. In this case, the equation is $y'' - \frac{1}{4} - \frac{n(n-1)}{x^2}$. Show that the exponents at zero are $(n, 1-n)$ and $\pm\frac{x}{2}$ at infinity. Prove that the Galois group is $SL(2, C)$ unless n is an integer.

4. Perform the change of variables $y(x) = e^{\frac{x}{2}} f(x)$. Search for f as a power series: its coefficients u_N satisfy the recursion $Nu_N - (n+N) * (n-1-N)u(N+1) = 0$ and $u(0) = 0$. Conclude that when n is an integer, f is a polynomial and hence L has one (in fact, two) exponential solutions.

$\diamond$

In this exercise, we see that these tools give strong necessary conditions. However, question (4) shows that when there are parameters and the necessary conditions are satisfied, then it is not that easy to decide if there actually exists a solution. In this case, it was feasible; in general, it is not (see [Bou99]) and even sometimes undecidable.
Still, in the applications to Hamiltonian mechanics, we encounter many systems where "mysteriously" reasonings like the above (and many other tricks) allow one to say a lot about non-integrability of entire families of equations. This last topic is an active field of research.

References

[Aud00] Audin, Michele - *Les systèmes Hamiltoniens et leur intégrabilité*, Cours Spécialisés Soc. Math. France, 2001.

[Aud01] Audin, Michele - *Intégrabilité et non-intégrabilité de systèmes hamiltoniens (d'après S. Ziglin, J. Morales-Ruiz, J.P. Ramis,....* Séminaire Bourbaki exposé numéro 884, Paris, mars (2001).

[BCRS96] Baider, A.; Churchill, R. C.; Rod, D. L.; Singer, M. F. - *On the infinitesimal geometry of integrable systems.* Mechanics day (Waterloo, ON, 1992), 5–56, Fields Inst. Commun., 7, Amer. Math. Soc., Providence, RI, 1996.

[BDw79] Baldassarri, Francesco.; Dwork, Bernard - *On second order linear differential equations with algebraic solutions.* Amer. J. Math. 101 (1979), no. 1, 42–76.

[BaP98] Barkatou, Moulay; Pflügel, Eckhard - *On the equivalence problem of linear differential systems and its application for factoring completely reducible systems.* Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (Rostock), 268–275 (electronic), ACM, New York, 1998.

[Ber86] Bertrand D. *Théorie de Galois différentielle* Cours de DEA, Notes rédigées par R. Lardon, Université de Paris VI, 1986

[BBH88] Beukers, Frits; Brownawell, W. Dale; Heckman, Gert - *Siegel normality.* Ann. of Math. (2) 127 (1988), no. 2, 279–308.

[Beu92] Beukers, Frits - *Differential Galois theory.* From number theory to physics (Les Houches, 1989), 413–439, Springer, Berlin, 1992.

[Bou99] Boucher, Delphine - *About the polynomial solutions of homogeneous linear differential equations depending on parameters.* Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC), 261–268 (electronic), ACM, New York, 1999

[Bro97] Bronstein, Manuel **Symbolic integration. I. Transcendental functions.** With a foreword by B. F. Caviness. Algorithms and Computation in Mathematics, 1. Springer-Verlag, Berlin, 1997

[Bro94] Bronstein, Manuel - *An improved algorithm for factoring linear ordinary differential operators,* Proceedings of the international symposium on Symbolic and algebraic computation ISSAC'94, p.336-340, July 20-22, 1994, Oxford, England

[BMW97] Bronstein, Manuel; Mulders, Thom; Weil, Jacques-Arthur - *On symmetric powers of differential operators.* Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI), 156–163 (electronic), ACM, New York, 1997

[CaD01] Canalis-Durand, Mireille - *Gevrey Asymptotics*, CIMPA School, Hanoï 2001

[CRS95] Churchill, R. C.; Rod, D. L.; Singer, M. F. - *Group-theoretic obstructions to integrability.* Ergodic Theory Dynam. Systems 15 (1995), no. 1, 15–48.

[Chu98] Churchill, R. C. - *Galoisian obstructions to the Integrability of Hamiltonian Systems.* The Kolchin Seminar in Differential Algebra, May, (1998).

[Chu99] Churchill, R. C. - *Two generator subgroups of* $\mathrm{SL}(2,\mathbb{C})$ *and the hypergeometric, Riemann, and Lam equations.* Differential algebra and differential equations. J. Symbolic Comput. 28 (1999), no. 4-5, 521–545.

[CLO97] Cox, David; Little, John; O'Shea, Donal - **Ideals, varieties, and algorithms.** *An introduction to computational algebraic geometry and commutative algebra.* Second edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[CSi98] Compoint, Élie; Singer, Michael F. - *Relations linaires entre solutions d'une quation diffrentielle.* Ann. Fac. Sci. Toulouse Math. (6) 7 (1998), no. 4, 659–670.

[CSi99] Compoint, Élie; Singer, Michael F. - *Computing Galois groups of completely reducible differential equations.* Differential algebra and differential equations. J. Symbolic Comput. 28 (1999), no. 4-5, 473–494.

[Cor01] Cormier, Olivier - *On Liouvillian Solutions of Linear Differential Equations of Order 4 and 5.* Proceedings of International Symposium on Symbolic and Algebraic Computation ISSAC'2001, ACM Press, London - Ontario, 2001.

[Fak97] Fakler, Winfried - *On second order homogeneous linear differential equations with Liouvillian solutions.* Computer algebra (Saint-Louis, 1996). Theoret. Comput. Sci. 187 (1997), no. 1-2, 27–48.

[GCL92] Labahn G Geddes O, Czapor S.R - **Algorithms for computer algebra**, 1992.

[Har01] Hartmann, Julia - *Invariants and Differential Galois Groups in Degree Four.* Preprint, Univ. Heidelberg, 2001

[Hes01] Hessinger, Sabrina A. - *Computing the Galois group of a linear differential equation of order four.* Appl. Algebra Engrg. Comm. Comput. 11 (2001), no. 6, 489–536.

[Hoe97] van Hoeij, Mark - *Factorization of differential operators with rational functions coefficients.* J. Symbolic Comput. 24 (1997), no. 5, 537–561.

[HWe97] van Hoeij, Mark; Weil, Jacques-Arthur - *An algorithm for computing invariants of differential Galois groups.* Algorithms for algebra (Eindhoven, 1996). J. Pure Appl. Algebra 117/118 (1997), 353–379.

[HRUW99] van Hoeij, Mark; Ragot, Jean-François; Ulmer, Felix; Weil, Jacques-Arthur - *Liouvillian solutions of linear differential equations of order three and higher.* In: Differential algebra and differential equations. J. Symbolic Comput. 28 (1999), no. 4-5, 589–609.

[Ince] Ince, E.L -**Ordinary Differential Equations**, Dover Publications, New-York (1956).

[Kap57] Kaplanski I, An introduction to differential Algebra, 1957.

[Kol48] Kolchin E. R, *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations.* Ann. of Math. (2) 49, (1948). 1–42.

[Kol48b] Kolchin, E. R, *Existence theorems connected with the Picard-Vessiot theory of homogeneous linear ordinary differential equations.* Bull. Amer. Math. Soc. 54, (1948). 927–932.

[Kov86] Kovacic, Jerald - *An algorithm for solving second order linear homogeneous differential equations* J. Symbolic Comput. **2** (1986) pp 3-43.

[Kov01] Kovacic, Jerald - *An algorithm for solving second order linear homogeneous differential equations* CCNY Colloquium lecture, Sept. 20, 2001. Available at `http://members.bellatlantic.net/ jkovacic/algorithm.dvi`

[Lang] Lang, Serge - **Algebra**, Third edition, Addison-Wesley 1992.

[Mag94] MAGID, ANDY R. - **Lectures on differential Galois theory.** University Lecture Series, 7. American Mathematical Society, Providence, RI, 1994.

[MRa89] RAMIS, J.-P.; MARTINET - J. THORIE DE GALOIS DIFFRENTIELLE ET RESOMMATION. Computer algebra and differential equations [Tou90], 117–214, Comput. Math. Appl., Academic Press, London, 1990.

[Ram01] RAMIS, JEAN-PIERRE - *Integrability of Hamiltonian Systems and Differential Galois Theory.* CIMPA school, Hanoï 2001.

[Mor99] MORALES RUIZ, JUAN J. - **Differential Galois theory and non-integrability of Hamiltonian systems.** Progress in Mathematics, 179. Birkhuser Verlag, Basel, 1999.

[Mor00] MORALES-RUIZ, J. J. - *Kovalevskaya, Liapounov, Painlev, Ziglin and the differential Galois theory.* Regul. Chaotic Dyn. 5 (2000), no. 3, 251–272.

[MR01a] MORALES RUIZ, JUAN J.; RAMIS, JEAN PIERRE - *Galoisian obstructions to integrability of Hamiltonian systems*, Methods and Applications of Analysis **8** (2001)

[MR01b] MORALES RUIZ, JUAN J.; RAMIS, JEAN PIERRE - *Galoisian obstructions to integrability of Hamiltonian systems II*, Methods and Applications of Analysis **8** (2001)

[Pfl97] PFLÜGEL, ECKHARDT - *An algorithm for computing exponential solutions of first order linear differential systems.* Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI), 164–171 (electronic), ACM, New York, 1997.

[Put97] PUT, MARIUS VAN DER. - *Symbolic analysis of differential equations*, in **Some tapas of Computer algebra**, Eds A.Cohen, H. Cuypers, H. Sterk, Springer 1997.

[Put98] VAN DER PUT, MARIUS - *Galois theory of differential equations, algebraic groups and Lie algebras.* Differential algebra and differential equations. J. Symbolic Comput. 28 (1999), no. 4-5, 441–472.

[Put99] VAN DER PUT, MARIUS - *Recent work on differential Galois theory.* Séminaire Bourbaki. Vol. 1997/98. Astérisque No. 252 (1998), Exp. No. 849, 5, 341–367.

[PS02] VAN DER PUT, MARIUS; SINGER, MICHAEL F. - **Differential Galois Theory.** Book to appear.

[PU00] VAN DER PUT, MARIUS; ULMER, FELIX - *Differential equations and finite groups.* J. Algebra 226 (2000), no. 2, 920–966.

[Ros72] ROSENLICHT, MAXWELL - *Integration in finite terms.* Amer. Math. Monthly 79 (1972), 963–972.

[Rit50] RIT50, J.F - *Differential Algebra*, American Mathematical Society Colloquium Publications, Vol. XXXIII, American Mathematical Society, New York, N. Y., 1950. Reprinted: Dover Publications, Inc., New York 1966 viii+184 pp.

[Sin81] SINGER, MICHAEL F. - *Liouvillian Solutions of n^{th} Order Linear Differential Equations* Am. J. Math. **103**, pp. 661–682.

[Sin96] SINGER, MICHAEL F. - *Testing reducibility of linear differential operators: a group-theoretic perspective.* Appl. Algebra Engrg. Comm. Comput. 7 (1996), no. 2, 77–104.

[Sin98] SINGER, MICHAEL F. - *Direct and Inverse Problems in Differential Galois Theory.* In: Selected works of Ellis Kolchin with commentary. Ed: H. Bass, A. Buium and P. Cassidy. American Mathematical Society, Providence, RI, 1999.

[SUl93a] SINGER, MICHAEL F.; ULMER, FELIX - *Galois groups of second and third order linear differential equations.* J. Symbolic Comput. 16 (1993), no. 1, 9–36.

[SUl93b] SINGER, MICHAEL F.; ULMER, FELIX - *Liouvillian and algebraic solutions of second and third order linear differential equations.* J. Symbolic Comput. 16 (1993), no. 1, 37–73.

[SUl96] SINGER, MICHAEL F.; ULMER, FELIX - *Linear differential equations and products of linear forms.* In: Algorithms for algebra (Eindhoven, 1996). J. Pure Appl. Algebra 117/118 (1997), 549–563.

[Spr81] Springer, Tonny Albert - **Linear Algebraic Groups.** Progress in Math. 9, Birkhäuser, second edition, 1998.

[Tou90] **Computer algebra and differential equations**. Edited by E. Tournier. Computational Mathematics and Applications. Academic Press, Inc. London, 1990

[Ulm92] Ulmer, Felix - *On Liouvillian solutions of linear differential equations.* Appl. Algebra Engrg. Comm. Comput. 2 (1992), no. 3, 171–193.

[UWe96] Ulmer, Felix; Weil, Jacques-Arthur - *Note on Kovacic's algorithm.* J. Symbolic Comput. 22 (1996), no. 2, 179–200.

[Wei95] Weil, Jacques-Arthur - *First integrals and Darboux polynomials of homogeneous linear differential systems.* Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), 469–484, Lecture Notes in Comput. Sci., 948, Springer, Berlin.

[Zig82a] Ziglin, S.L. - *Branching of solutions and non existence of first integrals in Hamiltonian mechanics I*, Funct. Anal. Appl. **16** (1982).

[Zig82b] Ziglin, S.L. - *Branching of solutions and non existence of first integrals in Hamiltonian mechanics II*, Funct. Anal. Appl. **17** (1982).