J. Symbolic Computation (1999) **28**, 441–473
Article No. jsco.1999.0310
Available online at http://www.idealibrary.com on IDEAL

Galois Theory of Differential Equations, Algebraic Groups and Lie Algebras

MARIUS VAN DER PUT[†]

Department of Mathematics, P.O. Box 800, 9700 AV Groningen,The Netherlands

The Galois theory of linear differential equations is presented, including full proofs. The connection with algebraic groups and their Lie algebras is given. As an application the inverse problem of differential Galois theory is discussed. There are many exercises in the text.

1. Introduction

The aim of this paper is to provide several things:

(1) A quick and elementary introduction to differential Galois theory.
(2) The relations between differential equations and algebraic Lie algebras.
(3) Complete proofs for the differential Galois theory.
(4) An introduction to the inverse problem and, in particular, a sketch of the solution of this problem by M. F. Singer and C. Mitschi.
(5) A collection of exercises for topics (1), (2) and (4).

As a consequence the level of exposition varies considerably. In particular, some proofs (marked by ¶) and the Appendix require more mathematical background than the main body of the text. The reader is advised to study the paper without paying too much attention to those technical details. This gives sufficient information to complete the exercises. We hope that this introduction might motivate the reader to continue and study the rest of the paper.

The exposition of differential Galois theory, especially the geometric approach, seems to be relatively new. The use of torsors goes back to Kolchin (1973, Chapters V and VI). The results and theorems are known with a few minor exceptions. A more powerful approach to differential Galois theory is given in Deligne (1990). We have not followed his ideas since it involves a long and technical discussion of Tannakian categories. The link between the Tannakian approach and Picard–Vessiot theory (as presented here) is given in the Appendix.

[†] E-mail: mvdput@math.rug.nl

0747–7171/99/100441 + 33 $30.00/0

2. Linear Differential Equations

A *scalar linear differential equation* is an equation of the form

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y^{(1)} + a_0 y = b.$$

Here $y^{(k)}$ denotes the kth derivative of y. For $y^{(1)}$, $y^{(2)}$ and $y^{(3)}$ we will also use the notations y', y'' and y'''. The $a_0, \ldots, a_{n-1}, b$ are supposed to lie in a field K of "functions". The equation is called *homogeneous* of order n if $b = 0$. Otherwise the equation is called *inhomogeneous of order n*. An nth-order inhomogeneous equation can be transformed into a homogeneous equation of order $n + 1$.

Example 2.1. The equation $y' = ay + b$, with $b \neq 0$, is transformed into the homogeneous equation of order two $(b^{-1}y' - b^{-1}ay)' = 0$.

A *matrix differential equation* over K is an equation of the form $y' = Ay$, where A is an $n \times n$-matrix with coefficients in K and where y is a vector of length n. The derivative y' of a vector y is defined by componentwise differentiation. Likewise, the derivative of a matrix $A = (a_{i,j})$ is defined by $A' = (a'_{i,j})$.

There is a standard way to transform a homogeneous scalar differential equation of order n into a matrix differential equation of size n.

Example 2.2. $y'' + ay' + by = 0$ is transformed into the matrix equation

$$\begin{pmatrix} y \\ y' \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \begin{pmatrix} y \\ y' \end{pmatrix}.$$

Let $y' = Ay$ be a matrix equation. A matrix equation $v' = \tilde{A}v$ is called *equivalent to $y' = Ay$* if there is a $B \in \mathrm{GL}(n, K)$ such that the substitution $y = Bv$, which leads to $v' = (B^{-1}AB - B^{-1}B')v$, has the property $\tilde{A} = B^{-1}AB - B^{-1}B'$. One can show (see Katz, 1987) that any matrix differential equation is equivalent to a matrix equation derived from a scalar equation. In the sequel we will use both scalar equations and matrix equations.

Our first concern is to give a precise definition for the type of fields K that we will work with. All the rings, considered in this paper, are supposed to be commutative, to have a unit element and to contain $\mathbf{Q}$. A *differentiation or derivation* on a ring R is a map $D : R \to R$ having the properties $D(a + b) = D(a) + D(b)$ and $D(ab) = D(a)b + aD(b)$. An element $a \in R$ will be called *constant* if $D(a) = 0$. A ring R equipped with a differentiation is called a differential ring. Often, we will denote the differentiation of a differential ring by $a \mapsto a'$. *The field K is supposed to be a differential field. Its set of constants is denoted by C. It is supposed that $C \neq K$.* According to Exercise (1), the set of constants C of K is a subfield. One calls C the field of constants of K. In later sections we will add the technical assumption that C is an algebraically closed field.

Examples 2.3. (Differential Fields). Let $C \supset \mathbf{Q}$ denote a field.

(1) $C(z)$, with derivation $f \mapsto f' = \frac{df}{dz}$.
(2) The field of formal Laurent series $C((z))$ with derivation $f \mapsto f' = \frac{df}{dz}$.
(3) The field of convergent Laurent series $\mathbf{C}(\{z\})$ with derivation $f \mapsto f' = \frac{df}{dz}$.

(4) The field of all meromorphic functions on any open connected subset of the extended complex plane $\mathbf{C} \cup \{\infty\}$, with derivation $f \mapsto f' = \frac{df}{dz}$.

(5) $\mathbf{C}(z, e^z)$ with derivation $f \mapsto f' = \frac{df}{dz}$.

In Examples (1) and (2), the field of constants is C. In the other examples the field of constants is $\mathbf{C}$. For the last example this follows from the inbedding of $\mathbf{C}(z, e^z)$ in the field of the meromorphic functions on $\mathbf{C}$.

LEMMA 2.4. *Let K be a differential field, with field of constants $C \neq K$. Consider the matrix equation $y' = Ay$ over K. Let $V = \{v \in K^n \mid v' = Av\}$ be its solution space over K. Then V is a vector space over C of dimension $\leq n$.*

PROOF. It is clear that V is a vector space over C. We will show the following statement:

(*) *If the vectors $v_1, \ldots, v_k \in V$ are linearly dependent over K then they are linearly dependent over C.*

Any $n+1$ vectors in V are linearly dependent over K. According to (*), they are also linearly dependent over C. Thus the dimension of V over C is $\leq n$.

Statement (*) is proved by induction on k. The case $k = 1$ is trivial. The induction step is proved as follows. Let $k > 1$ and let the $v_1, \ldots, v_k$ be linearly dependent over K. We may suppose that any proper subset of $\{v_1, \ldots, v_k\}$ is linearly independent over K. Then there is a unique relation $v_1 = \sum_{i=2}^k a_i v_i$ with all $a_i \in K$. Now

$$0 = v_1' - Av_1 = \sum_{i=2}^k a_i' v_i + \sum_{i=2}^k a_i(v_i' - Av_i) = \sum_{i=2}^k a_i' v_i.$$

Thus all $a_i' = 0$ and all $a_i \in C$. □

Suppose that the solution space $V \subset K^n$ of $y' = Ay$ has dimension n over C and that an explicit basis of V is known, then we have not much left to ask about the equation $y' = Ay$. This situation can be translated in terms of matrices as follows: Let $v_1, \ldots, v_n$ denote a basis of V. Let $B \in \mathrm{GL}(n, K)$ be the matrix with columns $v_1, \ldots, v_n$. Then $B' = AB$. This brings us to the following definition.

DEFINITION 2.5. Let R be a differential ring, containing the differential field K and having C as its set of constants. An invertible matrix $B \in \mathrm{GL}(n, R)$ is called a *fundamental matrix for the equation $y' = Ay$* if $B' = AB$ holds.

Suppose that $B, \tilde{B} \in \mathrm{GL}(n, R)$ are both fundamental matrices. Define M by $\tilde{B} = BM$. Then $A\tilde{B} = \tilde{B}' = B'M + BM' = ABM + BM'$ and thus $M' = 0$. We conclude that $M \in \mathrm{GL}(n, C)$. In other words, the set of all fundamental matrices (inside $\mathrm{GL}(n, R)$) for $y' = Ay$ is equal to $B \cdot \mathrm{GL}(n, C)$.

This brings us to our first problem. Suppose that the solution space of $y' = Ay$ over K is too small, i.e., its dimension is strictly less than n or equivalently there is no fundamental matrix in $\mathrm{GL}(n, K)$. How can we produce enough solutions in a larger differential ring or differential field? This is the subject of Section 3: Picard–Vessiot theory. A second, related problem, is to make the solutions as explicit as possible.

The situation is somewhat analogous to the case of an ordinary polynomial equation $P(X) = 0$ over a field K. Suppose that P is separable polynomial of degree n. Then one can construct a splitting field $L \supset K$ which contains precisely n solutions $\{\alpha_1, \ldots, \alpha_n\}$. Explicit information on the α_i can be obtained from the action of the Galois group on $\{\alpha_1, \ldots, \alpha_n\}$.

The following exercises might help the reader to become familiar with derivations and the algebraic point of view concerning differential equations.

Exercises.

(1) *Constructions with rings and derivations.* Let R be any differential ring. The differentiation is denoted by $r \mapsto D(r)$. (We note that the assumption $\mathbf{Q} \subset R$ is not needed in this exercise.)

(a) Prove that the set of constants C of R is a subring containing 1.

(b) Let $t, n \in R$ and suppose that n is invertible. Prove the formula
$$D\left(\frac{t}{n}\right) = \frac{D(t)n - tD(n)}{n^2}.$$

(c) Prove that C is a field if R is a field.

(d) Let $I \subset R$ be an ideal. Prove that D induces a differentiation on R/I if and only if $D(I) \subset I$.

(e) Let the ideal $I \subset R$ be generated by $\{a_j\}_{j \in J}$. Prove that $D(I) \subset I$ if $D(a_j) \in I$ for all $j \in J$.

(f) Let $S \subset R$ be a multiplicative subset, i.e., $0 \notin S$ and for any two elements $s_1, s_2 \in S$ one has $s_1 s_2 \in S$. We recall that the "localization of R with respect to S" is the ring RS^{-1}, defined as the set of equivalence classes of pairs (r, s) with $r \in R,\ s \in S$. The equivalence relation is given by $(r_1, s_1) \sim (r_2, s_2)$ if there is a $s_3 \in S$ with $s_3(r_1 s_2 - r_2 s_1) = 0$. The symbol $\frac{r}{s}$ denotes the equivalence class of the pair (r, s). Prove that there exists a unique derivation D on RS^{-1} such that the canonical map $R \to RS^{-1}$ commutes with D. (Hint: use that $tr = 0$ implies $t^2 D(r) = 0$.)

(g) Consider the polynomial ring $R[X_1, \ldots, X_n]$ and let $S \subset R[X_1, \ldots, X_n]$ be a multiplicative subset. Let $a_1, \ldots, a_n \in R[X_1, \ldots, X_n]S^{-1}$ be given. Prove that there exists a unique derivation D on $R[X_1, \ldots, X_n]S^{-1}$ such that the canonical map $R \to R[X_1, \ldots, X_n]S^{-1}$ commutes with D and $D(X_i) = a_i$ for all i.

(2) *Lie algebras of derivations.* Let F be any field and let $C \subset F$ be a subfield. Let $\mathrm{Der}(F/C)$ denote the set of all derivations D of F such that D is the zero map on C. Prove that $\mathrm{Der}(F/C)$ is a vector space over F. Prove that for any two elements $D_1, D_2 \in Der(F/C)$, the map $D_1 D_2 - D_2 D_1$ is again in $\mathrm{Der}(F/C)$. Conclude that $\mathrm{Der}(F/C)$ is a Lie algebra over C.

(3) *Derivations on field extensions.* Let F be a field (of characteristic 0) and let D be a differentiation on F. Prove the following statements.

(a) Let $F \subset \tilde{F}$ be a finite extension, then D has a unique extension to a derivation of $\tilde{F}$. Hint: $\tilde{F} = F(a)$, where a satisfies some irreducible polynomial over F. Use Exercise (1).

(b) D has a unique extension to a derivation of the algebraic closure $\bar{F}$ of F.

(c) Let $F \subset F(X)$ be a transcendental extension of F. Choose an $a \in F(X)$. There is a unique derivation $\tilde{D}$ of $F(X)$, extending D, such that $\tilde{D}(X) = a$.

(4) *Some order-one equations over $C(z)$.* Let C denote an algebraically closed field of characteristic 0. Let $K = C(z)$ be the differential field with differentiation $' = \frac{d}{dz}$. Prove the following statements.

(a) $y' = a$ has a solution in K if and only if the residue of adz at every point $z = c$ with $c \in C$ is zero.

(b) $y' = ay$ has a solution $y \in K$, $y \neq 0$ if and only if adz has at most poles of order 1 at $C \cup \{\infty\}$ and its residues are integers.

(c) $y' = ay$ has a solution $y \neq 0$ which is algebraic over K if and only if adz has at most poles of order 1 at $C \cup \{\infty\}$ and its residues are rational numbers.

(5) *Some order-one equations over $C((z))$.* Let C be an algebraically closed field of characteristic 0. The differential field $K = C((z))$ is defined by $' = \frac{d}{dz}$. Let $a \in K$, $a \neq 0$.

(a) When does $y' = a$ have a solution in K?
(b) When does $y' = a$ have a solution in $\bar{K}$?
(c) When does $y' = ay$ have a non-zero solution in K?
(d) When does $y' = ay$ have a non-zero solution in $\bar{K}$?

We note that every finite algebraic extension of K has the form $C((z^{1/n}))$. This could be used for the exercise.

(6) *Regular matrix equations over $C((z))$ and $\mathbf{C}(\{z\})$.* Let $C[[z]]$ denote the ring of all formal power series with coefficients in the field C. The field of fractions of $C[[z]]$ is the field $C((z))$ consisting of all formal Laurent series with coefficients in C. Let $\mathbf{C}\{z\} \subset \mathbf{C}[[z]]$ denote the ring of all convergent power series. The field of fractions of $\mathbf{C}\{z\}$ is denoted by $\mathbf{C}(\{z\})$. It is the subfield of $\mathbf{C}((z))$ consisting of all convergent Laurent series.

(a) Prove that a matrix differential equation $y' = Ay$ with $A \in \mathrm{M}(n, C[[z]])$ has a unique fundamental matrix B of the form $1 + \sum_{n>0} B_n z^n$ with all $B_n \in \mathrm{M}(n, C)$.

(b) A matrix equation $y' = Ay$ over $C((z))$ is called *regular* if the equation is equivalent to an equation $v' = \tilde{A}v$ with $\tilde{A} \in \mathrm{M}(n, C[[z]])$. Prove that an equation $y' = Ay$ is regular if and only if there is a fundamental matrix with coefficients in $C((z))$.

(c) A matrix equation $y' = Ay$ over $\mathbf{C}(\{z\})$ is called *regular* if it is regular as an equation over $\mathbf{C}((z))$. Prove that $y' = Ay$ is regular if and only if there exists a fundamental matrix with coefficients in $\mathbf{C}(\{z\})$.

(7) *Regular singular matrix equations over $C((z))$ and $\mathbf{C}(\{z\})$.* A matrix differential equation $y' = Ay$ over $C((z))$ is called *regular singular* if the equation is equivalent to a differential equation $v' = \tilde{A}v$ such that $z\tilde{A}$ has coefficients in $C[[z]]$. We note that a regular equation is also considered as a regular singular equation. The first part of this exercise will prove the statement:

Any regular singular equation $y' = Ay$ over $C((z))$ is equivalent to $v' = Dz^{-1}v$ with D a constant matrix.

(a) We may suppose that zA has coefficients in $C[[z]]$. Write A as $A_{-1}z^{-1} + A_0 + A_1z + a_2z^2 + \cdots$ where the $A_i \in \mathrm{M}(n, C)$. We are looking for a $B \in \mathrm{GL}(n, C((z)))$ such that $B^{-1}AB - B^{-1}B'$ is Dz^{-1} for some constant matrix D.

(i) As a first attempt we take B of the form $1 + B_1z + B_2z^2 + \cdots$ with all $B_i \in \mathrm{M}(n, C)$. Then D must be A_{-1} and we have to solve the B_i's step by step from the equation $AB = B' + BA_{-1}z^{-1}$. Show that there is a unique solution for the B_i's under the assumption that the eigenvalues of A_{-1} do not differ by a non-zero integer. Hint: take $E \in \mathrm{M}(n, C)$ with eigenvalues $\lambda_1, \ldots, \lambda_n$. Prove that the eigenvalues of the linear map $\mathrm{M}(n, C) \to \mathrm{M}(n, C)$, given by $B \mapsto [E, B] := EB - BE$, are the $\lambda_i - \lambda_j$.

(ii) Suppose now that A_{-1} does not satisfy the condition of (i). Let λ be any eigenvalue of A_{-1}. The space C^n can be written as a direct sum $E \oplus F$, where E is the generalized eigenspace for λ and F is the direct sum of the generalized eigenspaces for the other eigenvalues of A_{-1}. Consider the element $B \in \mathrm{GL}(n, C((z)))$, which is multiplication by z on E and the identity on F. Prove that $\tilde{A} = B^{-1}AB - B^{-1}B'$ has again the form $\tilde{A}_{-1}z^{-1} + \tilde{A}_0 + \tilde{A}_1z + \cdots$. Show that the eigenvalues of $\tilde{A}_{-1}$ are the same as the ones for A_{-1}, with the exception that λ is replaced by $\lambda - 1$. Use this to transform $y' = Ay$ into an equation satisfying the condition in (i).

(b) Consider a matrix differential equation $y' = Ay$ over $\mathbf{C}(\{z\})$. Suppose that $y' = Ay$ is regular singular as a differential equation over $\mathbf{C}((z))$.

(i) Show that there is also a $B \in \mathrm{GL}(n, \mathbf{C}(\{z\}))$ such that $\tilde{A} = B^{-1}AB - B^{-1}B'$ satisfies $z\tilde{A}$ has its coefficients in $\mathbf{C}\{z\}$. Hint: truncate a suitable matrix in $\mathrm{GL}(n, \mathbf{C}((z)))$.

(ii) Show that $y' = Ay$ is also over $\mathbf{C}(\{z\})$ equivalent to an equation $v' = Dz^{-1}v$ with D a constant matrix.

(iii) The (*local*) *topological monodromy* of an equation $y' = Ay$ can be defined as follows. The equation has no singularities above a set of the form $\{z \in \mathbf{C} \mid 0 < |z| < \epsilon\}$ for some positive ϵ. In particular there is a fundamental matrix W for the equation defined in a neighbourhood of $\epsilon/2$. Analytic continuation along a circle around 0 in a positive direction changes W into $W \cdot M$ for some $M \in \mathrm{GL}(n, \mathbf{C})$. The matrix M is called the (*local*) *monodromy matrix* of the equation. This matrix is only determined up to conjugation (why?). Prove that the monodromy matrix of the regular singular equation $y' = Ay$ is conjugated to the monodromy matrix of the equivalent equation $y' = Dz^{-1}y$. Prove that the monodromy matrix of the latter equation is $e^{2\pi iD}$. Hint: $e^{D\log(z)}$ is a fundamental matrix in a neighbourhood of 1.

(iv) Show that $y' = D_1z^{-1}y$ and $y' = D_2z^{-1}y$ (with constant matrices D_1, D_2) are equivalent (over $\mathbf{C}(\{z\})$) if and only if the monodromy matrices $e^{2\pi iD_1}$ and $e^{2\pi iD_2}$ are conjugated (in $\mathrm{GL}(n, \mathbf{C})$). Hint: suppose that $e^{2\pi iD_1} = e^{2\pi iD_2}$. Consider in a neighbourhood of the point 1 the fundamental matrices $W_1 = e^{D_1 \log(z)}$ and $W_2 = e^{D_2 \log(z)}$ for $y' = D_1 z^{-1} y$ and $y' = D_2 z^{-1} y$. Define $B = W_1 W_2^{-1}$. Show that $B \in \mathrm{GL}(n, \mathbf{C}(\{z\}))$ and that B "transform" $y' = D_1 z^{-1} y$ into $y' = D_2 z^{-1} y$.

3. Picard–Vessiot Theory

From now on K is a differential field with an algebraically closed field of constants C. In the sequel we will need the following definitions:

Definitions 3.1. A *differential ring over* K is a commutative K-algebra R with a unit element, together with a differentiation $'$ extending the differentiation on K. If R is a field, then R is called a *differential field over* K. A *differential ideal* I in a differential ring R is an ideal satisfying $f' \in I$ for all $f \in I$. We note that for a differential ring R over K and a differential ideal $I \subset R$, $I \neq R$, the factor ring R/I is again a differential ring over K. (See Exercise (1).) A *simple differential ring* R (over K) is a differential ring whose only differential ideals are (0) and R. A *Picard–Vessiot ring* for the equation $y' = Ay$, with $A \in \mathrm{M}(n, K)$, is a differential ring over K satisfying:

(1) R is a simple differential ring.
(2) There exists a fundamental matrix B for $y' = Ay$ with coefficients in R, i.e., the matrix $B \in \mathrm{GL}(n, R)$ satisfies $B' = AB$.
(3) R is generated as a ring by K, the coefficients of a fundamental matrix B and the inverse of the determinant of B.

Lemma 3.2. *Let R be a simple differential ring over K.*

(1) *R has no zero divisors.*
(2) *Suppose that R is finitely generated over K, then the field of fractions of R has C as set of constants.*

Proof. (1) We will first show that any non-nilpotent element $a \in R, a \neq 0$ is non-zero divisor. Consider the ideal $I = \{b \in R |$ there exists a $n \geq 1$ with $a^n b = 0\}$. This is a differential ideal not containing 1. Thus $I = (0)$ and a is not a zero divisor.
Let $a \in R, a \neq 0$ be nilpotent. Then we will show that a' is also nilpotent. Let $n > 1$ be minimal with $a^n = 0$. Differentiation yields $a' n a^{n-1} = 0$. Since $n a^{n-1} \neq 0$ we have that a' is a zero divisor and thus a' is nilpotent. Finally, the ideal J consisting of all nilpotent elements is a differential ideal and thus equal to (0).
(2) See the Appendix. □

Definition 3.3. A *Picard–Vessiot field* for the equation $y' = Ay$ over K is the field of fractions of a Picard–Vessiot ring for this equation.

Example 3.4. Consider $y' = a$ with $a \in K$. This inhomogeneous scalar equation can be rewritten as the matrix equation

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}' = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

If K contains a solution b of the scalar equation then $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ is a fundamental matrix and $R = K$ is a Picard–Vessiot ring for the equation.

We suppose now that the scalar equation has no solution in K. Define the differential ring $R = K[Y]$ with the derivation "extending" on K and $Y' = a$ (see Exercise (1)). Then R contains an obvious solution of the scalar equation and $\left(\begin{smallmatrix} 1 & Y \\ 0 & 1 \end{smallmatrix}\right)$ is a fundamental matrix for the matrix equation.

The minimality of the ring $R = K[Y]$ is obvious. We want to show that R has only trivial differential ideals. Let I be a proper ideal of $K[Y]$. Then I is generated by some $F = Y^n + \cdots + f_1Y + f_0$ with $n > 0$. The derivative of F is $F' = (na + f'_{n-1})Y^{n-1} + \cdots$. If I is a differential ideal then $F' \in I$ and thus $F' = 0$. In particular, $na + f'_{n-1} = 0$ and $\frac{-f_{n-1}}{n}' = b$. This contradicts our assumption. We conclude that $R = K[Y]$ is a Picard–Vessiot ring for $y' = a$.

Example 3.5. Consider $y' = ay$ with $a \in K^*$. Define the differential ring $R = K[T, T^{-1}]$ with the derivation "extending" on K and $T' = aT$. Then R contains a non-zero solution of $y' = ay$. The minimality of R is clear and the ring R would be the answer to our problem if R has only trivial differential ideals. For the investigation of this we have to consider two cases:

(a) Suppose that K contains no non-zero solution of $y' = nay$ for all $n \in \mathbf{Z}$, $n \neq 0$. Let $I \neq 0$ be a differential ideal. Then I is generated by some $F = T^m + a_{m-1}T^{m-1} + \cdots + a_0$, with $m \geq 0$ and $a_0 \neq 0$. The derivative $F' = maT^m + ((m-1)aa_{m-1} + a'_{m-1})T^{m-1} + \cdots + a'_0$ of F belongs to I. This implies $F' = maF$. For $m > 0$ one obtains the contradiction $a'_0 = maa_0$. Thus $m = 0$ and $I = R$. We conclude that $R = K[T, T^{-1}]$ is a Picard–Vessiot ring for the equation $y' = ay$.

(b) Suppose that $n > 0$ is minimal with $y' = nay$ has a solution $y_0 \in K^*$. Then $R = K[T, T^{-1}]$ has a non-trivial differential ideal (F) with $F = T^n - y_0$. Indeed, $F' = naT^n - nay_0 = naF$. The differential ring $K[T, T^{-1}]/(T^n - y_0)$ over K will be written as $K[t]$, where t is the image of T. One has $t^n = y_0$ and $t' = at$. Every element of $K[t]$ can uniquely be written as $\sum_{i=0}^{n-1} a_it^i$. We claim that $K[t]$ is a Picard–Vessiot ring for $y' = ay$. The minimality of $K[t]$ is obvious. We have to prove that $K[t]$ has only trivial differential ideals. Let $I \subset K[t]$, $I \neq 0$ be a differential ideal. Let $0 \leq d < n$ be minimal such that I contains a non-zero F of the form $\sum_{i=0}^{d} a_it^i$. Suppose that $d > 0$. We may assume that $a_d = 1$. The minimality of d implies $a_0 \neq 0$. Consider $F' = dat^d + ((d-1)aa_{d-1} + a'_{d-1})t^{d-1} + \cdots + a'_0$. The term $F' - daF$ belongs to I and is 0, since d is minimal. Then $a'_0 = daa_0$ contradicts our assumption. Thus $d = 0$ and $I = K[t]$.

Proposition 3.6. *Let the equation $y' = Ay$ over K be given.*

(1) *There exists a Picard–Vessiot ring for the equation.*
(2) *Any two Picard–Vessiot rings for the equation are isomorphic.*
(3) *The field of constants of a Picard–Vessiot field is again C.*

PROOF. (1) Let $(X_{i,j})$ denote a $n \times n$-matrix of indeterminates and let det denote the determinant of $(X_{i,j})$. Consider the differential ring $R_0 = K[X_{i,j}, \frac{1}{\det}]$ with the differentiation, extending the one of K, given by $(X'_{i,j}) = A(X_{i,j})$. Exercise (1) shows the existence and unicity of such a differentiation. Let $I \subset R_0$ be a maximal differential ideal. Then $R = R_0/I$ is easily seen to be a Picard–Vessiot ring for the equation.
(2) See the Appendix.
(3) Follows from Lemma 3.2. □

REMARK 3.7. We note that the maximal differential ideal I of R_0 in the above proof is in general not a maximal ideal of R_0. (See Examples 3.4 and 3.5.)

REMARK 3.8. In the literature there is a slightly different definition of the Picard–Vessiot field of a differential equation. The equivalence of the two definitions is stated in the next proposition.

PROPOSITION 3.9. *Let $y' = Ay$ be a differential equation over K and let $K \subset L$ be an extension of differential fields. Then L is a Picard–Vessiot field for the equation if and only if the following conditions are satisfied.*

(1) *The field of constants of L is C.*
(2) *There exists a fundamental matrix $B \in \mathrm{GL}(n, L)$ for the equation.*
(3) *L is generated over K by the coefficients of B.*

PROOF. The conditions (1)–(3) are necessary, according to Proposition 3.6 and the definitions of Picard–Vessiot ring and field. Suppose that L satisfies the three conditions. As in the proof of part (1) of Proposition 3.6, we consider the differential ring $R_0 = K[X_{i,j}, \frac{1}{\det}]$ with $(X'_{i,j}) = A(X_{i,j})$. Consider the differential rings $R_0 \subset L \otimes_K R_0 = L[X_{i,j}, \frac{1}{\det}]$. Define a set of n^2 new variables $Y_{i,j}$ by $(X_{i,j}) = B \cdot (Y_{i,j})$. Then $L \otimes_K R_0 = L[Y_{i,j}, \frac{1}{\det}]$ and $Y'_{i,j} = 0$ for all i, j. One can identify $L \otimes_K R_0$ with $L \otimes_C R_1$ where $R_1 := C[Y_{i,j}, \frac{1}{\det}]$. Let $\underline{p}$ be a maximal differential ideal of R_0. Then $\underline{p}$ generates an ideal in $L \otimes_K R_0$ which is denoted by $(\underline{p})$. Since $L/(\underline{p}) \cong L \otimes R_0/\underline{p} \neq 0$, the ideal $(\underline{p})$ is a proper differential ideal. Define the ideal $\underline{r} \subset R_1$ by $\underline{r} = (\underline{p}) \cap R_1$. According to Lemma 5.8 of the Appendix, the ideal $(\underline{p})$ is generated by $\underline{r}$. Take a maximal ideal $\underline{m}$ of R_1 containing $\underline{r}$. Then $R_1/\underline{m} = C$. The corresponding homomorphism of C-algebras $R_1 \to C$ extends to a differential homomorphism of L-algebras $L \otimes_C R_1 \to L$. Its kernel contains $(\underline{p}) \subset L \otimes_K R_0 = L \otimes_C R_1$. Thus we have found a K-linear differential homomorphism $\psi : R_0 \to L$ with $\underline{p} \subset \ker(\psi)$. The kernel of ψ is a differential ideal and so $\underline{p} = \ker(\psi)$. The subring $\psi(R_0) \subset L$ is isomorphic to $R_0/\underline{p}$ and is therefore a Picard–Vessiot ring. The matrix $(\psi X_{i,j})$ is a fundamental matrix in $\mathrm{GL}(L)$ and must have the form $B \cdot (c_{i,j})$ with $(c_{i,j}) \in \mathrm{GL}(n, C)$, because the field of constants of L is C. Since L is generated over K by the coefficients of B one has that L is the field of fractions of $\psi(R_0)$. Therefore, L is a Picard–Vessiot field for the equation. □

Definitions 3.10. *The differential Galois group* G of an equation $y' = Ay$ over K is defined as the group $\mathrm{Aut}(R/K)$ of the automorphisms of a Picard–Vessiot ring R for the equation. More precisely, G consists of the K-algebra automorphisms σ of R satisfying $\sigma(f') = \sigma(f)'$ for all $f \in R$. The elements of G are also called the *differential K-automorphisms of R.*

Observations 3.11. Consider the matrix differential equation $y' = Ay$ over K. Let R be a Picard–Vessiot ring for the equation, L its field of fractions, $B \in \mathrm{GL}(n, R)$ a fundamental matrix and $G = \mathrm{Aut}(R/K)$. Write $\mathrm{Aut}(L/K)$ for the group of the K-automorphisms of L satisfying $\sigma(f') = \sigma(f)'$ for all $f \in L$. Then:

(1) For any $\sigma \in \mathrm{Aut}(L/K)$ one has $\sigma(B) = BC(\sigma)^{-1}$ with $C(\sigma) \in \mathrm{GL}(n, C)$.
(2) G coincides with $\mathrm{Aut}(L/K)$.
(3) The map $G \to \mathrm{GL}(n, C)$, given by $\sigma \mapsto C(\sigma)$, induces an isomorphism of G with a subgroup of $\mathrm{GL}(n, C)$.

Proof. Since $\sigma \in \mathrm{Aut}(L/K)$ commutes with differentiation, $\sigma(B)$ is again a fundamental matrix and thus $B^{-1}\sigma(B) \in \mathrm{GL}(n, C)$. (See Section 2.) This proves (1). From (1) it follows that any $\sigma \in \mathrm{Aut}(L/K)$ leaves R invariant and (2) follows easily. If this constant matrix $C(\sigma)$ is the identity, then σ is the identity, since R is generated by the coefficients of B and $\frac{1}{\det B}$. Now (3) follows. □

The Epsilon Trick. Let W be an algebraic variety over a field F. For any F-algebra R (as before R is commutative and has a unit element) one defines $W(R)$ as the set of points of W with coordinates in R. In other words, $W(R)$ consists of the set of morphisms $\mathrm{Spec}(R) \to W$ over $\mathrm{Spec}(F)$. For a homomorphism of F-algebras $f : R_1 \to R_2$ one has an induced map $W(f) : W(R_1) \to W(R_2)$. The F-algebra $F[\epsilon]$ is defined by the relation $\epsilon^2 = 0$. Choose a point $p \in W(F)$. Consider the canonical homomorphism $F[\epsilon] \to F$, given by $\epsilon \mapsto 0$ and the induced caninical map $W(F[\epsilon]) \to W(F)$. Then $\{w \in W(F[\epsilon]) |\ w \text{ maps to } p \in W(F)\}$ can be identified with the tangent space of W at the point p.

Proof. ¶In Shafarevich (1974, p. 227), one finds the following definition of the tangent space of W at the point $p \in W(F)$. Let O_p denote the local ring at p and m its maximal ideal. Then O_p is an F-algebra, $O_p/m = F$ and m/m^2 is a vector space over F. The tangent space $T_{W,p}$ of W at p is defined by $T_{W,p} = \mathrm{Hom}_F(m/m^2, F)$.

Consider a $q \in W(F[\epsilon])$ with image p. Then q induces an F-algebra homomorphism $q : O_p \to F[\epsilon]$ such that $q : O_p \to F[\epsilon] \to F$ is the canonical map $O_p \to F$. Clearly, q maps m to ϵF and m^2 to 0. Thus q induces an F-linear map $m/m^2 \to F$.

Conversely, let an F-linear map $k : m/m^2 \to F$ be given. The F-algebra O_p/m^2 can be written as $F\oplus(m/m^2)$. The map $\tilde{q} : F\oplus(m/m^2) \to F[\epsilon]$ is defined by $\tilde{q}(f+v) = f+\epsilon k(v)$, for $f \in F$ and $v \in m/m^2$. It is clear that $\tilde{q}$ is a homomorphism of F-algebras. One defines the point $q \in W(F[\epsilon])$ by $q : O_p \to O_p/m^2 \xrightarrow{\tilde{q}} F[\epsilon]$. It is easily seen that the two maps defined above are each others inverses. This gives the identification of $\{w \in W(F[\epsilon])|w \text{ maps to } p \in W(F)\}$ with $T_{W,p}$. □

A special case is the following. Let $G \subset \mathrm{GL}(n)_F$ be an algebraic group defined over F. Then $\underline{g} := \{A \in \mathrm{M}(n,F)|1+\epsilon A \in G(F[\epsilon])\}$ is identified with the tangent space of G at the point $1 \in G(F)$. The F-linear subspace $\underline{g}$ of the space of all $n \times n$ matrices $\mathrm{M}(n,F)$ with coefficients in F is in fact a Lie subalgebra of $\mathrm{M}(n,F)$. The Lie algebra of G is defined as $\underline{g}$ with this structure as Lie algebra.

Proof. ¶We want to show that $\underline{g}$ is a Lie subalgebra of $\mathrm{M}(n,F)$. For this purpose we have to extend the epsilon trick to the case of $F[\alpha]$ with $\alpha^3 = 0$. Since the point $1 \in G(F)$ is smooth, one can lift any point of $G(F[\epsilon])$, which maps to $1 \in G(F)$, to a point of $G(F[\alpha])$. Thus for $A, B \in \underline{g}$ there are elements $a := 1+\alpha A+\alpha^2 A_1$ and $b := 1+\alpha B+\alpha^2 B_1$ in $G(F[\alpha])$. The commutator $aba^{-1}b^{-1}$ is equal to $1+\alpha^2(AB-BA)$. Thus $AB-BA \in \underline{g}$. □

Proposition 3.12. *Let $L \supset K$ be a Picard–Vessiot field with differential Galois group G. Then:*

1. *G considered as subgroup of $\mathrm{GL}(n,C)$ is an algebraic group.*
2. *The Lie algebra of G coincides with the Lie algebra of the derivations of L/K, which commute with the differentiation on L.*
3. *The field L^G of the G-invariants elements of L is equal to K.*

Proof. ¶(1) and (2). L is the field of fractions of $R := K[X_{i,j}, \frac{1}{\det}]/q$, where q is a maximal differential ideal. For any C-algebra A (as always A is commutative and has a unit element) one defines the differential rings $K\otimes_C A$, $R\otimes_C A$ and $L\otimes_C A$ with the derivation given by $(f \otimes a)' = f' \otimes a$ for $f \in K$, R, or L and $a \in A$. The ring of the constants of the three differential rings is A. The group $\mathcal{G}(A) := \mathrm{Aut}(L \otimes A/K \otimes A)$ is defined in the obvious way, namely as the group of the differential $K \otimes A$-automorphisms of $L \otimes A$. For $M \in \mathrm{GL}(n,A)$ one defines the $K \otimes A$-automorphism σ_M of $K[X_{i,j}, \frac{1}{\det}] \otimes A$, given by the formula $(\sigma_M X_{i,j}) = (X_{i,j})M^{-1}$. One observes that σ_M induces a $K \otimes A$-linear automorphism of $R \otimes A$ (and thus an element of $\mathcal{G}(A)$) if and only if σ_M leaves the ideal $qK[X_{i,j}, \frac{1}{\det}] \otimes_C A$ invariant. Moreover, every element of $\mathcal{G}(A)$ is obtained in this way for a unique M. Thus $\mathcal{G}(A)$ can be indentified with a subgroup of $\mathrm{GL}(n,A)$.

For a C-algebra homomorphism $f : A_1 \to A_2$ there is an induced group homomorphism $\mathcal{G}(f) : \mathcal{G}(A_1) \to \mathcal{G}(A_2)$. In other words, $\mathcal{G}$ is a covariant functor from the category of the C-algebras to the category of groups. $\mathrm{GL}(n)_C$ can also be seen as a covariant functor from the category of C-algebras to the category of groups and $\mathcal{G}$ is a subfunctor of $\mathrm{GL}(n)_C$.

Let the C-algebra $C[\epsilon]$ be defined by $\epsilon^2 = 0$. Consider the canonical map $C[\epsilon] \to C$ and the induced map $\mathcal{G}(C[\epsilon]) \to \mathcal{G}(C)$. The kernel of $\mathcal{G}(C[\epsilon]) \to \mathcal{G}(C)$ is equal to the set of the elements in $\mathrm{Aut}(L[\epsilon]/K[\epsilon])$ of the form $1+\epsilon D$ with D a map from L to L. The D's with the above property are the K-linear derivations on L commuting with $'$, as one easily verifies.

We will now show that there is an ideal $I \subset C[Y_{i,j}, \frac{1}{\det}]$ such that for any C-algebra A,

$$\mathcal{G}(A) = \{M \in \mathrm{GL}(n, A) | f(M) = 0 \text{ for all } f \in I\}.$$

Take for B the C-algebra $C[Y_{i,j}, \frac{1}{\det}]$. Let $M \in \mathrm{GL}(n, B)$ be the matrix $(Y_{i,j})$ and consider the map σ_M on $K[X_{i,j}, \frac{1}{\det}] \otimes_C B$. Let $q_1, \dots, q_r$ denote generators of the ideal q. Let $\{e_j\}$ denote a basis of R as vector space over C. The image of $\sigma_M(q_i)$ in $R \otimes_C B$ can be written as a finite sum $\sum_j e_j \otimes F(i,j)$ with $F(i,j) \in B$. Let $I \subset B = C[Y_{i,j}, \frac{1}{\det}]$ denote the ideal generated by all $F(i,j)$. We claim that the ideal I has the required property.

Let A be any C-algebra and $M \in \mathrm{GL}(n, A)$. The map σ_M is defined as above. Then $M \in \mathcal{G}(A)$ if and only if σ_M maps every q_i to an element of q. The image of $\sigma_M(q_i)$ in $R \otimes_C A$ has the form $\sum e_j \otimes F(i,j)(M)$. This proves the claim.

We will now prove that the ideal I is a radical ideal. We replace K by its algebraic closure $\bar{K}$. The ideal I and the functor $\mathcal{G}$ remain unchanged. The ideal q changes into a radical ideal $\tilde{q} = q\bar{K}[X_{i,j}, \frac{1}{\det}]$. We will write $W \subset \mathrm{GL}(n)_{\bar{K}}$ for the reduced subset defined by $\tilde{q}$ and V for the reduced set $\cap_{E \in W(\bar{K})} E^{-1}W$. Let $\tilde{r}$ be the radical ideal of V. Define the radical ideal $r \subset K[Y_{i,j}, \frac{1}{\det}]$ as the preimage of $\tilde{r}$ under the C-algebra homomorphism $C[Y_{i,j}, \frac{1}{\det}] \to \bar{K}[X_{i,j}, \frac{1}{\det}]$, given by $Y_{i,j} \mapsto X_{i,j}$. We want to prove that $r = I$ and thus show that I is a radical ideal. For this we have to verify that for any C-algebra A, the group $\mathcal{G}(A)$ is equal to $\{M \in \mathrm{GL}(n, A) | \forall f \in r : f(A) = 0\}$.

Let $M \in \mathrm{GL}(n, A)$. Then $M \in \mathcal{G}(A)$ if and only if σ_M leaves the ideal generated by $\tilde{q}$ invariant. This is equivalent to $DM^{-1} \in W(A \otimes_C \bar{K})$ for all $D \in W(\bar{K})$. The latter is equivalent to $M \in V(A \otimes_C \bar{K})$ and then also equivalent to $f(M) = 0$ for all $f \in r$.

Define the reduced algebraic subset G of $\mathrm{GL}(n)_C$ by the radical ideal I. Then G represents the functor $\mathcal{G}$. Since $\mathcal{G}$ is a functor with values in the category of groups, G is a reduced algebraic subgroup of $\mathrm{GL}(n)_C$. The field C is algebraically closed and we may identify G with the subgroup $G(C) \subset \mathrm{GL}(n, C)$. The group $G(C)$ is by construction equal to $\mathrm{Aut}(L/K)$. This proves the first statement. The second statement follows from the above calculation of the kernel of $\mathcal{G}(C[\epsilon]) \to \mathcal{G}(C)$.

(3) See the Appendix. □

Proposition 3.13. (The Galois Correspondence) *Let $L \supset K$ be the Picard–Vessiot field of the equation $y' = Ay$ over K. Let $G := \mathrm{Aut}(L/K)$ be the differential Galois group of the equation. Consider the two sets $\mathcal{S}$ = the closed subgroups of G and $\mathcal{L}$= the differential fields M with $K \subset M \subset L$. Let $\alpha : \mathcal{S} \to \mathcal{L}$ and $\beta : \mathcal{L} \to \mathcal{S}$ be the maps defined by $\alpha(H) = L^H$, where L^H is the subfield of L consisting of the H-invariant elements, and $\beta(M) = \mathrm{Aut}(L/M)$, the set of automorphisms of L/M commuting with the differentiation on L. Then:*

(1) *The two maps α and β are inverse to each other.*
(2) *Suppose that $H \in \mathcal{S}$ is a normal subgroup of G. Put $M = L^H$. Then $\mathrm{Aut}(M/K)$ is isomorphic to G/H. Moreover M is a Picard–Vessiot field for some linear differential equation over K.*
(3) *Let G^o denote the identity component of G. Then $L^{G^o} \supset K$ is a finite Galois extension with Galois group G/G^o.*

Proof. See the Appendix. □

For the next important result we will need some definitions. Suppose that the differential field K is $C(z)$ and consider an equation $y' = Ay$ over K. The field K is seen as the function field of the projective line $\mathbf{P}^1(C) = C \cup \{\infty\}$ over C. A *point of K* is by definition a point of this projective line. For every point p of K one considers the "completion" $\hat{K}_p$ of the field K at that point. For a finite point $c \in C$, this is the Laurent series field $\hat{K}_c := C((z-c))$. For the infinite point this is $\hat{K}_\infty := C((z^{-1}))$. Those fields are in an obvious way differential fields.

The equation can be considered locally at a point p, which means that we consider the equation over the field $\hat{K}_p$. The equation is called *regular at a finite point c* if there is a $B \in GL(n, \hat{K}_c)$ such that the equivalent equation $v' = \tilde{A}v$, with $\tilde{A} := B^{-1}AB - B^{-1}B'$, has no poles. In other words $\tilde{A} \in M(n, C[[z-c]])$. The equation is called *regular singular* at $z = c$ if there is a $B \in GL(n, \hat{K}_c)$, such that $(z-c)\tilde{A}$ has no poles at $z = c$, i.e., $(z-c)\tilde{A} \in M(n, C[[z-c]])$ (see also Exercise (7)). Similar definitions can be given for the point ∞.

It is a standard fact that a point p is regular for the equation $y' = Ay$ if and only if there is a fundamental matrix with coefficients in $\hat{K}_p$. (See Exercise (6).)

Suppose that $K = C(z) \subset F$ is a finite field extension of degree n. The geometric picture corresponding to this is a non-constant morphism $m : X \to \mathbf{P}^1$, of degree n, between non-singular connected projective curves over C with function fields F and $C(z)$. A point of $C(z)$ is called *unramified* if its preimage in X consists of n points.

We are interested in the case where F is a Galois extension of K. One can prove (in that case) the following.

Proposition 3.14. *A point p is unramified if and only if the field F can be embedded into $\hat{K}_p$.*

Proof. ¶For a point $q \in X$ with $m(q) = p$, one has an inclusion of the fields $\hat{K}_p \subset \hat{F}_q$. The ramification index $e(q)$ of q is defined as the degree $[\hat{F}_q : \hat{K}_p]$. The point q is (by definition) unramified if and only if $e(q) = 1$. Take a point $p \in \mathbf{P}^1$ and let $q_1, \ldots, q_s$ denote the points $q \in X$ with $m(q) = p$. Then the formula $\sum e(q_i) = n$ holds. In particular, p is unramified if and only if all $e(q_i) = 1$. Thus, p is unramified if and only if $s = n$.

Suppose that $F \supset C(z)$ is a Galois extension with Galois group G. Then G acts transitively on the set $\{q_1, \ldots, q_s\} = m^{-1}(p)$ for any $p \in \mathbf{P}^1$. Thus all $e(q_i)$ are equal. Suppose that F can be embedded into $\hat{K}_p$. Then for some i one has $\hat{F}_{q_i} \subset \hat{K}_p$ and thus $\hat{F}_{q_i} = \hat{K}_p$ and $e(q_i) = 1$. Therefore all $e(q_j) = 1$ and p is unramified.

Conversely, suppose that p is unramified. Then $\hat{K}_p = \hat{F}_{q_1} \supset F$. □

Corollary 3.15.

(1) *Consider a differential equation $y' = Ay$ over the field $K = C(z)$ with Picard–Vessiot field L and differential Galois group G. Then the set of the ramification points of the finite Galois extension $K \subset L^{G^o}$ is contained in the set of the singular points of the equation.*

(2) *Suppose that the equation has at most one singular point. Then G is connected.*
(3) *Suppose that the equation has at most two singular points, then G/G^o is a cyclic group.*

Proof. (1) Let p be a regular point for the differential equation. There is a fundamental matrix B with coefficients in $\hat{K}_p$. According to Proposition 3.9, the subfield $L \subset \hat{K}_p$, generated over K by the coefficients of B, is a Picard–Vessiot field for the equation over K. Then $K \subset L^{G^o}$ is a finite Galois extension of K, lying inside $\hat{K}_p$. Thus p is unramified for the extension $K \subset L^{G^o}$.
(2) The Riemann–Hurwitz–Zeuthen genus formula shows that a finite extension $K = C(z) \subset F$ with $C(z) \neq F$ is ramified at two or more points.
(3) This follows again from the Riemann–Hurwitz–Zeuthen formula.□

Examples 3.16. The algebraic subgroups of SL(2) and SL(3)
We give here the rather useful lists of (the conjugacy classes of) the algebraic subgroups of $\mathrm{SL}(2,C)$ and $\mathrm{SL}(3,C)$. The lists are used in Kovacic's algorithm (Kovacic, 1986) for order two equations and the extension of this algorithm to order three equations by Singer and Ulmer (1993). In Section 5, the lists are used again for the explicit constructions of differential equations with differential Galois groups SL(2) and SL(3). For $\mathrm{SL}(2,C)$ the list reads:

(1) Reducible subgroups G, i.e., there exists a G-invariant line. In other terms, the subgroups of $\left\{\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix} |a \in C^*, b \in C\right\}$.
(2) Irreducible and imprimitive groups G, i.e., there is no G-invariant line but there is a pair of lines invariant under G. In other terms G is an irreducible subgroup of the infinite dihedral group, consisting of all $A \in \mathrm{SL}(2,C)$ such that A permutes the two lines $C(1,0), C(0,1)$ in C^2.
(3) Three finite primitive groups: the tetrahedral, the octahedral and the icosahedral group.
(4) $\mathrm{SL}(2,C)$.

For $\mathrm{SL}(3,C)$ the list is:

(1) G is reducible, i.e., G fixes a proper linear subspace of C^3. There are two cases:
 (a) 1-reducible groups G, i.e., G fixes a line in C^3.
 (b) 2-reducible groups G, i.e., G fixes a plane in C^3.
(2) G is irreducible and imprimitive, i.e., G permutes the three lines $C(1,0,0), C(0,1,0)$, and $C(0,0,1)$, and is irreducible.
(3) G is irreducible and primitive. The possibilities are:
 (a) $\mathrm{PSL}(2,C)$. This group is obtained from the natural action of $\mathrm{SL}(2,C)$ on the second symmetric power $C^2 \otimes_s C^2 \cong C^3$.
 (b) $\mathrm{PSL}(2,C) \times C_3$, where $C_3 = \{\lambda\, id | \lambda^3 = 1\}$.
 (c) Eight finite primitive groups.

(d) $\mathrm{SL}(3, C)$.

Exercises.

(8) Calculate the differential Galois group and its Lie algebra for Examples 3.4 and 3.5.

(9) $K = C(z)$ with C algebraically closed. Consider the equation $y'' = c^2 y$ with $c \in C^*$. Show that the differential ring $K[Y, Y^{-1}]$, given by $Y' = cY$, is a Picard–Vessiot ring for the equation. Calculate the differential Galois group and its Lie algebra.

(10) Consider $y'' = ry$ over $K = C(z)$, with C algebraically closed.

(a) Prove that the differential Galois group G is contained in $\mathrm{SL}(2, C)$. Hint: Let L be a Picard–Vessiot field. Take a basis y_1, y_2 of the solution space $V \subset L$ of the equation. Prove that $y_1 y_2' - y_1' y_2$ has derivative 0. Conclude from this that any $\sigma \in G$ has determinant 1.

(b) Suppose that $r \in C[z]$. Prove that G is connected.

(c) Suppose that $r \in C[z]$ has odd degree. Show that G is an irreducible group. Hint: let $L \supset K$ be a Picard–Vessiot extension for the equation and let $V \subset L$ be the solution space for the equation. If $G \subset \mathrm{GL}(V)$ is reducible, then there is a line $Cy \subset V$ fixed by G. Prove that $u := \frac{y'}{y}$ lies in K and satisfies $u' + u^2 = r$. Expand u at $z = \infty$ and show that this gives a contradiction.

(d) Suppose again that $r \in C[z]$ has odd degree. Prove that $G = \mathrm{SL}(2, C)$ and give an explicit description of the Picard–Vessiot ring.

(e) In the special case $r = z$, the equation is called the Airy equation (studied by Airy and Stokes). Two independent solutions of the equation are called the Airy functions Ai, Bi. They can be seen as entire functions on the complex plane. What can one say about the algebraic relations between z, Ai, Ai', Bi, Bi'?

(11) *The differential Galois group of a regular singular equation over* $\mathbf{C}(\{z\})$. According to Exercise (7), we may write such an equation as $y' = Dz^{-1}y$ with $D \in M(n, \mathbf{C})$. For the construction of a Picard–Vessiot field we introduce a new complex variable t. The functions in t that we will consider are meromorphic functions, defined on some upper half plane $H_b := \{t \in \mathbf{C} | \; im(t) > b\}$ (with $b \in \mathbf{R}$). Two meromorphic functions f_1, f_2 on H_{b_1} and H_{b_2} will be identified if f_1 and f_2 coincide on an upper half plane H_{b_3} with $b_1, b_2 \leq b_3$. The collection of all meromorphic functions defined on some upper half plane is a field, denoted by $\mathcal{H}$. The differentiation on this field is defined by $\frac{1}{2\pi i} e^{-2\pi i t} \frac{d}{dt}$. The field of constants of $\mathcal{H}$ is clearly $\mathbf{C}$. The field $\mathcal{H}$ has a nice automorphism σ, given by $f(t) \mapsto f(t+1)$. This automorphism commutes with the differentiation on $\mathcal{H}$. The field $\mathbf{C}(\{z\})$ is identified with as subfield of $\mathcal{H}$ by the substitution $z = e^{2\pi i t}$. Thus $\sum a_n z^n \in \mathbf{C}(\{z\}) \mapsto \sum a_n e^{2\pi i n t} \in \mathcal{H}$. It is easily seen that $\mathbf{C}(\{z\})$ is a differential subfield of $\mathcal{H}$.

(a) Prove that $e^{2\pi i t D}$ is a fundamental matrix for $y' = Dz^{-1}y$ with coefficients in $\mathcal{H}$ and conclude that $\mathcal{H}$ contains a Picard–Vessiot field L for the equation.

(b) Prove that $\sigma(L) = L$ and conclude that σ lies in the differential Galois group G.

(c) Prove that $L^\sigma = \mathbf{C}(\{z\})$. Hint: any $f \in L^\sigma$ has the form $f(t) = g(e^{2\pi i t})$ where $g(z)$ is holomorphic on $\{z \in \mathbf{C} | \; 0 < |z| < \epsilon\}$ for some positive ϵ and $|g(z)| \leq c|z|^n$ holds for some $n \in \mathbf{Z}$ and some positive constant c.

(d) Conclude from (c) and Proposition 3.13 that the subgroup $<\sigma>\subset G$, generated by σ, has Zariski closure G.

(e) Show that G is the smallest algebraic subgroup of $\mathrm{GL}(n, \mathbf{C})$, containing the monodromy matrix $e^{2\pi i D}$.

4. Geometric Approach

For the construction of the Picard–Vessiot ring of an equation $y' = Ay$ over K we have used the differential ring $K[X_{i,j}, \frac{1}{\det}]$ with $(X'_{i,j}) = A(X_{i,j})$. This ring is the coordinate ring of the group $\mathrm{GL}(n)_K$. Let I denote a radical ideal of $K[X_{i,j}, \frac{1}{\det}]$ and let W denote the closed subspace of $\mathrm{GL}(n)_K$ defined by I. We will call a (non-empty) reduced subspace $W \subset \mathrm{GL}(n)_K$ *differentially invariant* if its (radical) ideal I is a differential ideal. In the following lemma a criterion for W to be differentially invariant is established. For the formulation of this criterion we need the algebraic closure $\bar{K}$ of K and the K-algebra $\bar{K}[\epsilon]$ over $\bar{K}$, defined by the relation $\epsilon^2 = 0$. As before, we denote for any K-algebra S the set of points of W with coordinates in S by $W(S)$.

Lemma 4.1. *The reduced subspace $W \subset GL(n)_K$ is differentially invariant if and only if for every $B \in W(\bar{K})$ the element $B + \epsilon(B' - AB)$ lies in $W(\bar{K}[\epsilon])$. In other terms, $B' - AB$ lies in the tangent space of W at the point $B \in W(\bar{K})$.*

Proof. For any $f \in K[X_{i,j}, \frac{1}{\det}]$ and $B \in \mathrm{GL}(n, \bar{K})$ one has the formula:

$$f(B + \epsilon(B' - AB)) = f(B) + \epsilon(f(B)' - f'(B)).$$

The verification of this formula is straightforward. For convenience we introduce another differentiation, denoted by $f \mapsto \partial_K f$, on $K[X_{i,j}, \frac{1}{\det}]$ by the requirements ∂_K is identical with $'$ on K and $\partial_K X_{i,j} = 0$ for all i, j. Then one finds:

$$f(B + \epsilon(B' - AB)) = f(B) + \sum_{i,j} \epsilon(B' - AB)_{i,j} \frac{\partial f}{\partial X_{i,j}}(B),$$

$$f(B)' = \partial_K f(B) + \sum_{i,j} B'_{i,j} \frac{\partial f}{\partial X_{i,j}}(B), \qquad \text{and}$$

$$\begin{aligned} f'(B) &= \partial_K f(B) + \sum_{i,j} \left(X'_{i,j} \frac{\partial f}{\partial X_{i,j}} \right)(B) \\ &= \partial_K f(B) + \sum_{i,j} \sum_k A_{i,k}(X_{k,j} \left(\frac{\partial f}{\partial X_{i,j}} \right)(B) \\ &= \partial_K f(B) + \sum_{i,j} (AB)_{i,j} \frac{\partial f}{\partial X_{i,j}}(B). \end{aligned}$$

Let I be the radical ideal of W. Suppose that I is a differential ideal. Then for any $B \in W(\bar{K})$ and any $f \in I$ one has $f(B + \epsilon(B' - AB)) = 0$ since also $f' \in I$. On the other hand suppose that for every $B \in W(\bar{K})$ the element $B + \epsilon(B' - AB)$ lies in $W\bar{K}[\epsilon]$. The formula implies that for any $f \in I$ and all $B \in W(\bar{K})$ one has $f'(B) = 0$. Since I is a radical ideal one finds $f' \in I$. □

Observations 4.2.

(1) Let $y' = Ay$ over K be given. There is a bijective correspondence between the maximal differential ideals of $K[X_{i,j}, \frac{1}{\det}]$ and the minimal differentially invariant subspaces of $\mathrm{GL}(n)_K$.
(2) Let Z be a minimal differentially invariant subspace of $\mathrm{GL}(n)_K$ (corresponding to the maximal differential ideal I). Then the differential Galois group G of the equation is equal to $\{M \in \mathrm{GL}(n, C) | ZM \subset Z\}$.

Proof. The first statement is obvious. For the second statement we observe that for any $\sigma \in G$ there is a matrix $M \in \mathrm{GL}(n, C)$ such that the K-automorphism σ_M of $K[X_{i,j}, \frac{1}{\det}]$, defined by $(\sigma_M X_{i,j}) = (X_{i,j})M^{-1}$, has the property: $\sigma_M I \subset I$ and σ_M induces σ on $K[X_{i,j}, \frac{1}{\det}]/I$. □

Corollary 4.3. *Let $H \subset \mathrm{GL}(n, C)$ be an algebraic group with Lie algebra $\underline{h} \subset \mathrm{M}(n, C)$. Suppose that the differential equation $y' = Ay$ over K has the property $A \in \underline{h}(K)$. Then the differential Galois group G of the equation is contained in (a conjugate of) the group H.*

Proof. It suffices to show that H_K is differentially invariant. Indeed, there is then a minimal differentially invariant $Z \subset H_K$. For $M \in G$ one has $ZM \subset Z$. Take a $B \in Z(\bar{K}) \subset H_K(\bar{K})$. Then $BM \in Z(\bar{K}) \subset H_K(\bar{K})$ and thus $M \in H_K(\bar{K}) \cap GL(n, C) = H(C)$.

Consider a $B \in H(\bar{K})$. Then $(1 - \epsilon A)(B + \epsilon B') = B + \epsilon(B' - AB)$. The term $(1 - \epsilon A)$ belongs to $H(\bar{K}[\epsilon])$ since $A \in \underline{h}(\bar{K})$. We verify now that $B + \epsilon B' \in H(\bar{K}[\epsilon])$. For any f in the ideal $J \subset C[X_{i,j}, \frac{1}{\det}]$ of H one has

$$f(B + \epsilon B') = f(B) + \sum_{i,j} \epsilon B'_{i,j} \left(\frac{\partial f}{\partial X_{i,j}} \right)(B) = f(B) + \epsilon f(B)'.$$

Therefore, $f(B + \epsilon B') = 0$ for $B \in H_K(\bar{K})$ and $f \in J$ and so $B + \epsilon B' \in H(\bar{K}[\epsilon])$. This proves finally that $B + \epsilon(B' - AB) \in H_K(\bar{K}[\epsilon])$. □

The following theorem can be seen as a converse of Corollary 4.3.

Theorem 4.4. *Let $y' = Ay$ be a differential equation over $K = C(z)$ with differential Galois group G. Let $\underline{g}$ denote the Lie algebra of G. Let H be a connected algebraic subgroup of $\mathrm{GL}(n)_C$ with Lie algebra $\underline{h}$. Suppose that:*

(1) *The differential Galois group is connected.*
(2) *$A \in \underline{h}(K)$.*

Then there exists a $B \in H(K)$ such that the equivalent equation $v' = \tilde{A}v$, with $y = Bv$ and $\tilde{A} = B^{-1}AB - B^{-1}B'$, satisfies $\tilde{A} \in \underline{g}(K)$.

The proof of this theorem is quite involved. It is given in the Appendix. We note that Kovacic (1969) and Mitchi and Singer (1996) give (different) proofs for Corollary 4.3 and Theorem 4.4. For the application of this theorem we recall that an *algebraic Lie subalgebra* $M \subset \mathrm{M}(n, C)$ is defined as the Lie algebra of a linear algebraic subgroup of $\mathrm{GL}(n, C)$.

Remark 4.5. The condition that G is connected is necessary for Theorem 4.4. Indeed, let G denote again the differential Galois group of the equation. Let G^o denote the component of $1 \in G$. Suppose that one can find a $\tilde{A} \in \underline{g}(K)$ with $\tilde{A} = B^{-1}AB - B^{-1}B'$ and $B \in \mathrm{GL}(n, K)$. According to Corollary 4.3, the differential Galois group G is contained in the *connected* algebraic group with Lie algebra $\underline{g}$. Thus $G \subset G^o$ and therefore $G = G^o$ and G is connected.

Corollary 4.6. *With the notations and assumptions of* Theorem 4.4, *one has:*

(1) $\underline{g}$ *is a minimal algebraic Lie algebra such that there is an equivalent equation* $v' = \tilde{A}v$ *with* $\tilde{A} \in \underline{g}(K)$.
(2) *The Picard–Vessiot ring of* $y' = Ay$ *is isomorphic to* $K \otimes_C C[G]$, *where* $C[G]$ *is the coordinate ring of* G.

Proof. (1) is a direct consequence of Theorem 4.4 and Corollary 4.3.
(2) After applying Theorem 4.4, we may suppose that $A \in \underline{g}(K)$. Let $Z \subset G$ be a minimal differentially invariant subset. By Observation 4.2 one has $ZM \subset M$ for all $M \in G(C)$. The same holds for the points in the algebraic closure $\bar{K}$, i.e., $Z(\bar{K})M \subset Z(\bar{K})$ for every $M \in G(\bar{K})$. Therefore $Z = G_K$ and this proves (2).□

Exercises.

(12) *Algebraic solutions of the Riccati equation.* Consider the equation $y'' = ry$ over the field $C(z)$ with $r = \frac{5}{16}z^{-2} + z$. Associated to this equation is the non-linear equation $u' + u^2 = r$, which is called the *Riccati equation.* Let A denote a Picard–Vessiot ring for the equation.

(a) Choose $y \in A, y \neq 0$ with $y'' = ry$ and put $u := \frac{y'}{y}$. Verify that u is a solution of the Riccati equation.
(b) Let $u \in A$ be a solution of the Riccati equation and let $y \in A$ satisfy $y' = uy$. Prove that $y'' = ry$.
(c) The field extension $C(t) \supset C(z)$ is defined by $t^2 = z$. Verify that $u_1 = -\frac{1}{4}z^{-1} + t \in C(t)$ is a solution of the Riccati equation. Find a second solution $u_2 \in C(t)$ of the Riccati equation.
(d) Prove that the differential ring $R = C(t)[y_1, y_1^{-1}]$, defined by $y_1' = u_1 y_1$, is a Picard–Vessiot ring for the equation. Hint: verify that R is a simple differential ring. Prove that R is generated over $C(z)$ by the coefficients of a fundamental matrix for the equation.
(e) Determine the differential Galois group G of the equation.

(f) Verify that the Lie algebra of G is equal to the Lie algebra of the K-linear derivations $D : R \to R$ that commute with $'$.

(13) Consider the matrix differential equation $y' = \begin{pmatrix} 1 & 1 \\ 0 & d \end{pmatrix} y$ over $C(z)$ with $d = \frac{1}{3z}$.

(a) Prove that $R = C(z)[Y_1, Y_1^{-1}, Y_2, F]/(Y_2^3 - z)$, with the differentiation given by $Y_1' = Y_1$, $Y_2' = \frac{1}{3z}Y_2$, $F' = F + Y_2$, is a well-defined differential ring.

(b) We write y_1, y_2, f for the images of Y_1, Y_2, F in R. Prove that $\begin{pmatrix} y_1 & f \\ 0 & y_2 \end{pmatrix}$ is a fundamental matrix.

(c) Prove that the subring $R_0 := C(z)[y_1, y_1^{-1}, y_2] \subset R$ is a simple differential ring.

(d) Prove that the equation $H' = H + y_2$ has no solution in R_0.

(e) Prove that R is a simple differential ring. Hint: let $I \subset R$, $I \neq 0$ be a differential ideal. Define $n \geq 0$ to be the minimal integer for which there exists a non-zero element of I with degree n in the variable f. Prove that the set

$$\{a \in R_0 \mid \text{ there is an element of the form } af^n + *f^{n-1} + \cdots \in I\}$$

is a differential ideal of R_0.

(f) Conclude that R is a Picard–Vessiot ring for the equation. Calculate the differential Galois group and its Lie algebra.

(14) Let $\mathrm{diag}(a_1, \ldots, a_n)$ denote the diagonal matrix with entries $a_1, \ldots, a_n$. Consider the matrix differential equation $y' = \mathrm{diag}(a_1, \ldots, a_n)y$ over K with all $a_i \in K$. The subgroup $\Lambda \subset \mathbf{Z}^n$ is defined as

$$\{\underline{m} = (m_1, \ldots, m_n) \in \mathbf{Z}^n \mid \exists f \in K^* \text{ with } f' = (m_1a_1 + \cdots + m_na_n)f\}.$$

Prove the following statements:

(a) $K[E_1, \ldots, E_n, E_1^{-1}, \ldots, E_n^{-1}]/I$ is the Picard–Vessiot ring for the equation, with the differentiation given by $E_i' = a_iE_i$ for all i and where the ideal I is generated by the elements $E_1^{m_1} \cdots E_n^{m_n} - 1$ with $\underline{m} = (m_1, \ldots, m_n) \in \Lambda$.

(b) The differential Galois group G of the equation is

$$\{\mathrm{diag}(t_1, \ldots, t_n) \mid t_1, \ldots, t_n \in C^* \text{ and } t_1^{m_1} \cdots t_n^{m_n} = 1 \text{ for all } \underline{m} \in \Lambda\}.$$

(c) The Lie algebra of G is

$$\{\mathrm{diag}(d_1, \ldots, d_n) \mid d_1, \ldots, d_n \in C \text{ and } \sum m_id_i = 0 \text{ for all } \underline{m} \in \Lambda\}.$$

(d) What are the algebraic Lie algebras contained in the (commutative) Lie algebra of all diagonal matrices in $\mathrm{M}(n, C)$?

(e) Consider the example $K = \mathbf{C}(z)$ and the $a_i \in \mathbf{C}$. What can one conclude about the complex functions e^{a_iz}?

5. Inverse Problems

In this section the differential field will be $C(z)$, with C algebraically closed and differentiation $' = \frac{d}{dz}$. The *inverse problem* is:

Let an algebraic subgroup $G \subset \mathrm{GL}(n, C)$ be given. Is there a differential equation $y' = Ay$ with G as differential Galois group?

For the case $C = C$, the field of complex numbers, the answer is "yes". The (complex analytic) proof, given by C. Tretkoff and M. Tretkoff (1979), is easy and non-constructive. To some extent this analytic result can be used for the inverse problem over any algebraically closed field C (see Singer, 1993). In the recent work of J.-P. Ramis, the inverse problem is solved for differential equations over the field of convergent power series $\mathbf{C}(\{z\})$ and for differential on a compact Riemann surface with prescribed number and type of singularities (see van der Put, 1998).

A constructive, algebraic solution of the inverse problem for connected groups G is developed by C. Mitschi and M. F. Singer. In the sequel of this section we will explain a certain part of their work. (See also van der Put (1998) for a slightly different presentation.)

Let a connected algebraic group $G \subset \mathrm{GL}(n)_C$ be given and let $\underline{g}$ denote its Lie-algebra. Then one tries to find a matrix $A \in \underline{g}(K)$ satisfying the following two properties:

(a) The differential Galois group of the equation $y' = Ay$ is connected.
(b) There is no $B \in G(K)$ such that $\tilde{A} := B^{-1}AB - B^{-1}B'$ lies in $\underline{n}(K)$ for a proper algebraic Lie subalgebra $\underline{n}$ of $\underline{g}$.

If A satisfies both conditions then we know by Theorem 4.4 that the differential Galois group of the equation is G.

A first step for the inverse problem is the reduction to the case of semi-simple connected groups G. We will not go into this. We recall that a connected linear algebraic group G is semi-simple if and only if its Lie algebra $\underline{g}$ is semi-simple (see Humphreys, 1981). The proof of the inverse problem for semi-simple groups G runs as follows.

Step 1. Construct an injective representation $\rho : G \to GL(V)$ such that:

(a) G leaves no line of V invariant.
(b) Any proper connected closed subgroup $H \subset G$ has an invariant line in V.

Step 2. Then one looks at the Cartan decomposition (or root space decompostion) of $\underline{g}$. This decomposition reads (Jacobson, 1962; Fulton and Harris, 1991):

$$\underline{g} = \underline{h} \oplus (\oplus_\alpha \underline{g}_\alpha),$$

where $\underline{h}$ is a Cartan subalgebra and the one dimensional spaces $\underline{g}_\alpha = CX_\alpha$ are the eigenspaces for the adjoint action of $\underline{h}$ on $\underline{g}$ corresponding to the non-zero roots $\alpha : \underline{h} \to C$. More precisely, the adjoint action of $\underline{h}$ on $\underline{h}$ is zero and for any $\alpha \neq 0$ one has $[h, X_\alpha] = \alpha(h)X_\alpha$ for all $h \in \underline{h}$. One takes a "general" element $A_1 \in \underline{h}$. Further $A_0 := \sum_{\alpha \neq 0} X_\alpha$.

Step 3. The action of $\underline{g}$ on V will also be denoted by ρ. Consider the differential equation $y' = (\rho(A_0) + z\rho(A_1))y$. For notational convenience we will omit the symbol ρ. The equation has a connected differential Galois group, contained in G. If the differential Galois group is a proper subgroup of G, then by Theorem 4.4. there is $B \in G(K) \subset \mathrm{GL}(K \otimes V)$ such that $B^{-1}(A_0 + zA_1)B - B^{-1}B' \in \underline{n}(K)$ with $\underline{n}$ is the Lie algebra of some connected, proper algebraic subgroup $N \subset G$. The assumptions on ρ imply that there is a $v \in V$, $v \neq 0$ with $(B^{-1}(A_0 + zA_1)B - B^{-1}B')v \in Kv$. The vector

$w = Bv \in K \otimes V$ has the property $[\frac{d}{dz} - (A_0 + zA_1)]w \in Kw$. We note that the operator $\frac{d}{dz}$ on $K \otimes V$ is defined by $\frac{d}{dz}(f \otimes v) = f' \otimes v$. After multiplication of w with a non-zero element of K we may suppose that $w \in C[z] \otimes V$ and that the coordinates of w with respect to a basis of V have g.c.d. 1. This leads to the equation $[\frac{d}{dz} - (A_0 + zA_1)]w = cw$ with $c \in K$. Clearly $c \in C[z]$ and by comparing the degrees one finds that the degree of c is at most 1.

Step 4. One considers now the equation

$$\left[\frac{d}{dz} - (A_0 + zA_1)\right] w = (c_0 + c_1 z)w \text{ with } w = w_m z^m + \cdots + w_1 z + w_0,$$

with all $w_i \in V$ and $w_m \neq 0$. Comparing the coefficients of z^{m+1}, z^m, z^{m-1} one obtains the relations

$$\begin{aligned} A_1(w_m) &= -c_1 w_m, \\ A_0(w_m) + A_1(w_{m-1}) &= -c_0 w_m - c_1 w_{m-1}, \\ -m w_m + A_0(w_{m-1}) + A_1(w_{m-2}) &= -c_0 w_{m-1} - c_1 w_{m-2}. \end{aligned}$$

A careful analysis of the equations leads to a choice of A_1 such that the three above equations have no solution.

Exercise 15. Prove that SL(2) is a differential Galois group along the lines of the above proof. Hint:

(a) Show that the ordinary representation of $\mathrm{SL}(2, C)$ on $V = C^2$ has already the properties required in Step 1.

(b) Show that

$$\underline{sl(2)} = C\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \oplus C\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \oplus C\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

is the Cartan decomposition of Step 2.

(c) Take $A_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $A_1 = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$. Carry out the calculations of Step 4, which will lead to the non-existence of the vector w.

Lemma 5.1. (Mitchi and Singer, 1996) *Let G be a connected semi-simple linear algebraic group. There exists an injective representation $\rho : G \to \mathrm{GL}(V)$ such that:*

(1) *G leaves no line of V invariant.*

(2) *Any proper connected closed subgroup $H \subset G$ has an invariant line in V.*

Proof. ¶We will call a space V with a representation $\rho : G \to \mathrm{GL}(V)$ a G-module. The G-module is called faithful if ρ is injective. Let $G \subset \mathrm{GL}(n, C)$ be given. Chevalley's theorem (see Humphreys, 1981) states that for any proper algebraic subgroup H there is a G-module V and a line $L \subset V$ such that H is the stabilizer of that line. Since G is semi-simple, V is a direct sum of irreducible modules. The projection of L to one of these irreducible components is again a line. Thus we find that H stabilizes a line in some irreducible G-module V of dimension > 1. Any subgroup of G, conjugated to H, also stabilizes a line in V. Dynkin's theorem (Dynkin, 1957) implies that there are only finitely many conjugacy classes of maximal connected proper algebraic subgroups of G. One chooses an irreducible G-module V_i, $i = 1, \ldots, m$ for each class and one chooses an irreducible faithful module V_0. Then $V = V_0 \oplus \cdots \oplus V_m$ has the required properties. □

Exercise 16. Let $G = \mathrm{SL}(3, C)$ act in the usual way upon $W = C^3$. Show that the induced representation on

$$V = W \oplus (\Lambda^2 W) \oplus (W \otimes_s W) = W \oplus (W \otimes W)$$

has the properties of Lemma 5.1. Here $\Lambda^2 W$ is the second exterior power and $W \otimes_s W$ is the second symmetric power. Hint: use the classification of the closed subgroups of $\mathrm{SL}(3, C)$ and that $W \otimes_s W$ has an invariant line for the induced action of the group $\mathrm{PSL}(2, C)$.

Theorem 5.2. (Mitchi and Singer, 1996) *Every connected semi-simple linear algebraic group is a differential Galois group over the field $C(z)$.*

Proof. We use the notations, introduced for the explanation of the steps in the proof. Lemma 5.1 provides a G-module V with the required properties. The action of $\underline{h}$ on V gives a decomposition of $V = \oplus V_\beta$ into eigenspaces for a collection of linear maps $\beta : \underline{h} \to C$. The β's are called the weights of the representation. The first conditions on $A_1 \in \underline{h}$ are:

(a) The $\alpha(A_1)$ are distinct and different from 0 (for the non-zero roots α of $\underline{g}$).
(b) The $\beta(A_1)$ are distinct and different from 0 (for the non-zero weights β of the representation).

It is clear that A_1 with these properties exists. Choose such an A_1. We want A_1 to satisfy the more technical condition:

(c) If the integer m is an eigenvalue of the operator $\sum_{\alpha \neq 0} \frac{1}{-\alpha(A_1)} X_{-\alpha} X_\alpha$ on V, then $m = 0$.

If A_1 does not yet satisfy this last condition then a suitable multiple cA_1, with $c \in C^*$, satisfies all three conditions. We take such an A_1.

The eigenspaces for the action of A_1 on V will be denoted by V_b with $b = \beta(A_1)$ the corresponding eigenvalue of A_1. Any element $v \in V$ is written as $v = \sum_b v_b$, with $v_b \in V_b$. The relation $[A_1, X_\alpha] = \alpha(A_1) X_\alpha$ implies that $X_\alpha(V_d) \subset V_{d+\alpha(A_1)}$. This implies that A_0 has the property $A_0(V_d) \subset \oplus_{b \neq d} V_b$. Consider the three equations of Step 4.

The first equation can only be solved with $w_m \in V_d, w_m \neq 0$ and $d = -c_1$. The second equation, which can be read as $c_0 w_m = -A_0(w_m) + (-A_1 - c_1) w_{m-1}$, imposes $c_0 = 0$. Indeed, the two right-hand side terms $-A_0(w_m)$ and $(-A_1 - c_1) w_{m-1}$ have no component in the eigenspace V_d for A_1 to which w_m belongs. Furthermore,

$$w_{m-1} = \sum_{b \neq d} \frac{1}{-b+d} A_0(w_m)_b + v_d = \sum_{\alpha \neq 0} \frac{1}{-\alpha(A_1)} X_\alpha(w_m) + v_d$$

for some $v_d \in V_d$.

The third equation can be read as

$$-mw_m + A_0(w_{m-1}) = (-A_1 - c_1)w_{m-2}.$$

A necessary condition for this equation to have a solution w_{m-2} is that the left-hand side has 0 as component in V_d. The component in V_d of the left-hand side is easily calculated to be

$$-mw_m + (A_0(w_{m-1}))_d = \left(-m + \sum_{\alpha \neq 0} \frac{1}{-\alpha(A_1)} X_{-\alpha} X_\alpha\right)(w_m).$$

Since this is zero, m is an eigenvalue of the operator $\sum_{\alpha \neq 0} \frac{1}{-\alpha(A_1)} X_{-\alpha} X_\alpha$. It follows from our assumption on A_1 that $m = 0$.

This leaves us with the equation $[\frac{d}{dz} - (A_0 + zA_1)]w = c_1 zw$ and $w \in V$. Since $\frac{d}{dz} w = 0$, one finds that Cw is invariant under A_0 and A_1. The Lie algebra $\underline{g}$ is generated by A_0 and A_1. Thus Cw is invariant under $\underline{g}$ and under G. Our assumptions on the G-module V imply that $w = 0$. □

Exercise 17. Find an explicit differential equation over $K = C(z)$ with differential Galois group $\mathrm{SL}(3, C)$. Hint: use Exercise (14) and the construction in the proof of Theorem 5.2.

Appendix A

5.1. appendix A.1. proofs

Lemma 3.2 Part (2). *Suppose that R is a finitely generated simple differential ring over the differential field K. Then the set of constants of the field of fractions L of R is equal to C.*

Proof. Suppose that $a \in L, a \neq 0$ has derivative $a' = 0$. We have to prove that $a \in C$. The non-zero ideal $\{b \in R \mid ba \in R\}$ is a differential ideal and thus equal to R. Hence $a \in R$. We suppose that $a \notin C$. Then for every $c \in C$, the non-zero ideal $(a - c)R$ is a differential ideal. This implies that $a - c$ is an invertible element of R for every $c \in C$. Now we consider $a \in R$ as a regular function on the affine scheme $Z := \mathrm{Spec}(\bar{K} \otimes_K R)$ of finite type over the algebraic closure $\bar{K}$ of K. The image of the morphism $a : Z \to \bar{K}$ is either finite or contains a Zariski open subset of $\bar{K}$. (See Humphreys, 1981, Section 4.3.) Since $a - c$ is invertible for every $c \in C$ it follows that the intersection of C with the image of a is empty. Therefore, the image of a is finite and so there is a polynomial $P = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ such that $K[a] = K[X]/(P)$. Differentiation of the equality $P(a) = 0$ yields $a'_{d-1}a^{d-1} + \ldots a'_1 a + a'_0 = 0$. The minimality of P implies that all $a'_i = 0$ and so all $a_i \in C$. Since C is algebraically closed, P is linear and we have obtained a contradiction. □

Proposition 3.6 Part (2). *Any two Picard–Vessiot rings for the equation $y' = Ay$ over K are isomorphic.*

Proof. Let R_1, R_2 denote two Picard–Vessiot rings for the equation. Let B_1, B_2 denote the two fundamental matrices. Consider the differential ring $R_1 \otimes_K R_2$ with differentiation given by $(r_1 \otimes r_2)' = r_1' \otimes r_2 + r_1 \otimes r_2'$. Choose a maximal differential ideal $I \subset R_1 \otimes_K R_2$ and define $R_3 := (R_1 \otimes_K R_2)/I$. There are obvious morphisms of differential rings $\phi_i : R_i \to R_3$, $i = 1, 2$. Since R_i is simple, the morphism $\phi_i : R_i \to \phi_i(R_i)$ is an isomorphism. The image of ϕ_i is generated over K by the coefficients of $\phi_i(B_i)$. The matrices $\phi_1(B_1)$ and $\phi_2(B_2)$ are fundamental matrices over the ring R_3. Since the set of constants of R_3 is C one has $\phi_1(B_1) = \phi_2(B_2)M$, where M is an invertible matrix with coefficients in C. This implies that $\phi_1(R_1) = \phi_2(R_2)$ and so R_1 and R_2 are isomorphic. □

Proposition 3.12 Part (3). *The field L^G of the G-invariant elements of a Picard–Vessiot field L, for $y' = Ay$ over K, is equal to K.*

Proof. Write $a \in L \setminus K$ as $\frac{b}{c}$ with $b, c \in R$. Put $d = b \otimes c - c \otimes b \in R \otimes_K R$. Then $d \neq 0$. The ring $R \otimes_K R$ has no nilpotent elements since the charateristic of K is zero. Let J be a maximal differential ideal in the differential ring $(R \otimes R)[\frac{1}{d}]$. As in the proof of Proposition 3.6 we consider the two morphisms $\phi_i : R \to N := (R \otimes_K R)[\frac{1}{d}]/J$. Their images are equal to a certain subring $S \subset N$ and the maps $\phi_i : R \to S$ are isomorphisms. This induces a $\sigma \in G$ with $\phi_1 = \phi_2 \sigma$. The image of d in N is equal to $\phi_1(b)\phi_2(c) - \phi_1(c)\phi_2(b)$. Since the image of d in N is non-zero, one finds $\phi_1(b)\phi_2(c) \neq \phi_1(c)\phi_2(b)$. Then $\phi_2((\sigma b)c) \neq \phi_2((\sigma c)b)$ and $(\sigma b)c \neq (\sigma c)b$ and finally $\sigma(\frac{b}{c}) \neq \frac{b}{c}$. □

5.2. appendix A.2. torsors

We note that the use of torsors in differential Galois theory was initiated in Kolchin (1973, Chapters V and VI). Let G be a linear algebraic group over a field C. A *G-torsor Z over a field $K \supset C$* is an algebraic variety over K with a G-action, i.e., a morphism $G \times_C Z \to Z$ denoted by $(g, z) \mapsto zg$, such that:

(1) $z1 = z$; $z(g_1 g_2) = (zg_1)g_2$.
(2) The morphism $G \times_C Z \to Z \times_K Z$, given by $(g, z) \mapsto (zg, z)$, is an isomorphism.

A torsor is often refered to as a *principal homogeneous space over G*. The *trivial G-torsor over K* is defined by $Z = G_K := G \otimes_C K$ and $G \times_C G_K \to G_K$ is the multiplication map $(g, z) \mapsto z \cdot g$. Any G-torsor over K, isomorphic to the trivial one, is called trivial.

Suppose that Z has a K-rational point b, i.e., $b \in Z(K)$. We note that $G \times_C Z = G_K \times_K Z$. The map $G_K \to Z$, given by $g \mapsto bg$, is an isomorphism. It follows that Z is a trivial G-torsor over K. Thus the torsor Z is trivial if and only if Z has a K-rational point.

Let Z be any G-torsor over K. Choose a point $b \in Z(\bar{K})$, where $\bar{K}$ is the algebraic closure of K. Then $Z(\bar{K}) = bG(\bar{K})$. For any $\sigma \in \mathrm{Gal}(\bar{K}/K)$ one has $\sigma(b) = bc(\sigma)$ with $c(\sigma) \in G(\bar{K})$. The map $\sigma \mapsto c(\sigma)$ from $\mathrm{Gal}(\bar{K}/K)$ to $G(\bar{K})$ satisfies the relation

$$c(\sigma_1) \cdot \sigma_1(c(\sigma_2)) = c(\sigma_1 \sigma_2).$$

A map $c : \mathrm{Gal}(\bar{K}/K) \to G(\bar{K})$ with this property is called a *1-cocycle for* $\mathrm{Gal}(\bar{K}/K)$ *acting on* $G(\bar{K})$. Two 1-cocycles c_1, c_2 are called *equivalent* if there is an element $a \in G(\bar{K})$ such that

$$c_2(\sigma) = a^{-1} \cdot c_1(\sigma) \cdot \sigma(a) \text{ for all } \sigma \in \mathrm{Gal}(\bar{K}/K).$$

The set of all equivalence classes of 1-cocycles is, by definition, *the cohomology set* $H^1(\mathrm{Gal}(\bar{K}/K), G(\bar{K}))$. This set has a special point 1, namely the image of the trivial 1-cocycle. Take another point $\tilde{b} \in Z(\bar{K})$. This defines a 1-cocycle $\tilde{c}$. Write $\tilde{b} = ba$ with $a \in G(\bar{K})$. Then one finds that $\tilde{c}(\sigma) = a^{-1} \cdot c(\sigma) \cdot \sigma(a)$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Thus $\tilde{c}$ is equivalent to c and the torsor Z defines a unique element c_Z of $H^1(\mathrm{Gal}(\bar{K}/K), G(\bar{K}))$.

Lemma 5.3. *The map $Z \to c_Z$ induces a bijection between the set of isomorphism classes of G-torsors over K and $H^1(\mathrm{Gal}(\bar{K}/K), G(\bar{K}))$.*

Proof. The map $Z \to c_Z$ is injective. Indeed, let Z_1 and Z_2 be torsors, $b_1 \in Z_1(\bar{K})$ and $b_2 \in Z_2(\bar{K})$ two points defining equivalent 1-cocycles. After changing the point b_2 we may suppose that the two 1-cocycles are identical. One defines $f : Z_1(\bar{K}) \to Z_2(\bar{K})$ by $f(b_1 g) = b_2 g$ for all $g \in G(\bar{K})$. It is clear that f defines an isomorphism $(Z_1)_{\bar{K}} \to (Z_2)_{\bar{K}}$. By construction f is invariant under the action of $\mathrm{Gal}(\bar{K}/K)$. Therefore f is induced by an isomorphism $\tilde{f} : Z_1 \to Z_2$ of G-torsors.

Let an element of $H^1(\mathrm{Gal}(\bar{K}/K), G(\bar{K}))$ be represented by a 1-cocycle c. The group G is an algebraic subgroup of $\mathrm{GL}(n)_C$. According to Serre (1968, p. 159), one has that

$$H^1(\mathrm{Gal}(\bar{K}/K), \mathrm{GL}(n, \bar{K})) = \{1\}.$$

Thus there is a $B \in \mathrm{GL}(n, \bar{K})$ with $c(\sigma) = B^{-1}\sigma(B)$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. The subset $BG(\bar{K}) \in \mathrm{GL}(n, \bar{K})$ is Zariski closed and defines an algebraic variety $Z \subset \mathrm{GL}(n)_{\bar{K}}$. For $\sigma \in \mathrm{Gal}(\bar{K}/K)$ one has $\sigma(BG(\bar{K})) = \sigma(B)G(\bar{K}) = Bc(\sigma)G(\bar{K}) = BG(\bar{K})$. Thus Z is defined over K. It is rather clear that Z is a G-torsor over K. Further $B \in Z(\bar{K})$ defines the 1-cocycle c. This shows the map $Z \mapsto c_Z$ is also surjective. □

For the formulation of the next theorem we need a definition.

Definition 5.4. A field F is called a *C_1-field* if every homogeneous polynomial $f \in F[X_1, \dots, X_n]$ of degree less than n has a non-trivial zero in F^n.

It is known that the fields $C(z)$, $C((z))$, $\mathbf{C}(\{z\})$ are C_1-fields if C is algebraically closed. The field $C(z, e^z)$, with C algebraically closed, is not a C_1-field.

Theorem 5.5. (T. A. Springer; see Serre, 1964, p. 150) *Let G be a connected linear algebraic group over the field K. Suppose that K is a C_1-field. Then*

$$H^1(\mathrm{Gal}(\bar{K}/K), G(\bar{K})) = \{1\}.$$

Now we return to the matrix differential equation $y' = Ay$ over the differential field K. The Picard–Vessiot ring for this equation has the form $K[X_{i,j}, \frac{1}{\det}]/q$, where q is a maximal differential ideal. We recall that $K[X_{i,j}, \frac{1}{\det}]$ is the coordinate ring of the group $\mathrm{GL}(n)_K$ and that $Z := \mathrm{Spec}(K[X_{i,j}, \frac{1}{\det}]/q)$ is an irreducible and reduced Zariski-closed subset of $\mathrm{GL}(n)_K$. Let L denote the field of fractions of $K[X_{i,j}, \frac{1}{\det}]/q$. As in the proof of Proposition 3.12 we will make a distinction between $\mathrm{Aut}(L/K)$ and the reduced algebraic group $G \subset \mathrm{GL}(n)_C$, defined in the proof of Proposition 3.12. One has of course $G(C) = \mathrm{Aut}(L/K)$. There is a natural morphism $G \times_C Z \to Z$, defined by $(g, z) \mapsto z \cdot g$. The following result is quite powerful, as we will see.

Theorem 5.6. *Z is a G-torsor over K.*

The proof is quite involved. We have to show that $f : G \times_C Z \to Z \times_K Z$, where f is the morphism given by $(g, z) \mapsto (zg, z)$, is an isomorphism of algebraic varieties over K. In terms of rings, we have to show that the K-algebra homomorphism $f^* : O(Z) \otimes_K O(Z) \to O(G) \otimes_C O(Z)$, where $O(Z)$ and $O(G)$ are the coordinate rings of Z and G, is an isomorphism. It suffices to find a field extension F of K such that $1_F \otimes_K f^*$ is an isomorphism. Thus we want to show that for some field extension $F \supset K$, the induced morphism of varieties over F, namely $G \times_C Z_F \to Z_F$, makes Z_F into a trivial G-torsor over F. For F we will take a Picard–Vessiot field L.

Consider the following rings

$$K\left[X_{i,j}, \frac{1}{\det}\right] \subset L\left[X_{i,j}, \frac{1}{\det}\right] = L\left[Y_{i,j}, \frac{1}{\det}\right] \supset C\left[Y_{i,j}, \frac{1}{\det}\right],$$

where the relation between the variables $X_{i,j}$ and the variables $Y_{i,j}$ is given by $(X_{i,j}) = (r_{i,j})(Y_{i,j})$. The $r_{a,b} \in L$ are the images of $X_{a,b}$ in $K[X_{i,j}, \frac{1}{\det}]/q \subset L$. The three rings have a differentiation and a $\mathrm{Aut}(L/K)$-action. The differentiation is given by the known differentiation on L and by $(X'_{i,j}) = A(X_{i,j})$. Since $(r_{i,j})$ is a fundamental matrix for the equation, we find that $(Y'_{i,j}) = 0$ and the differentiation is trivial on $C[Y_{i,j}, \frac{1}{\det}]$. The $\mathrm{Aut}(L/K)$-action is induced by the $\mathrm{Aut}(L/K)$-action on L. Thus $\mathrm{Aut}(L/K)$ acts trivially on $K[X_{i,j}, \frac{1}{\det}]$. For $\sigma \in \mathrm{Aut}(L/K)$ we have $(\sigma r_{i,j}) = (r_{i,j})M$ for a certain $M \in G(C)$. Then $(\sigma Y_{i,j}) = M^{-1}(Y_{i,j})$. Let us admit for the moment the next two lemmata.

Lemma 5.7. *The map $I \mapsto (I)$ from the set of ideals of $K[X_{i,j}, \frac{1}{\det}]$ to the set of the $\mathrm{Aut}(L/K)$-invariant ideals of $L[X_{i,j}, \frac{1}{\det}]$ is a bijection. The inverse map is given by $J \mapsto J \cap K[X_{i,j}, \frac{1}{\det}]$.*

Lemma 5.8. *Let M be any differential field, e.g., $M = L$, with field of constant C. The map $I \mapsto (I)$ from the set of ideals of $C[Y_{i,j}, \frac{1}{\det}]$ to the set of the differential ideals of $M[Y_{i,j}, \frac{1}{\det}]$ is a bijection. The inverse map is given by $J \mapsto J \cap C[Y_{i,j}, \frac{1}{\det}]$.*

Combining the two lemmata, one finds a bijection between the differential ideals of $K[X_{i,j}, \frac{1}{\det}]$ and the $\mathrm{Aut}(L/K)$-invariant ideals of $C[Y_{i,j}, \frac{1}{\det}]$. A maximal differential ideal of the first ring corresponds then with a maximal $\mathrm{Aut}(L/K)$-invariant ideal of the second ring. Thus $r := qL[X_{i,j}, \frac{1}{\det}] \cap C[Y_{i,j}, \frac{1}{\det}]$ is a maximal $\mathrm{Aut}(L/K)$-invariant ideal. By maximality r is a radical ideal and its zero set W in $\mathrm{GL}(n, C)$ is minimal with respect to $\mathrm{Aut}(L/K)$-invariance. Thus W is a right coset for $\mathrm{Aut}(L/K)$ in $\mathrm{GL}(n, C)$. After changing $(r_{i,j})$ into $(r_{i,j})M$ for a suitable $M \in G(C)$ one obtains that $W = \mathrm{Aut}(L/K)$ and r is the ideal defining $\mathrm{Aut}(L/K) \subset \mathrm{GL}(n)_C$. In the notation of the proof of Proposition 3.12 this means that $r = I$.

This leads to $L \otimes_K (K[X_{i,j}, \frac{1}{\det}]/q) \cong L \otimes_C (C[Y_{i,j}, \frac{1}{\det}]/r) = L \otimes_C O(G)$, where $O(G)$ is the coordinate ring of G. In other words, we found an isomorphism $h : Z_L \cong G_L$. We still have to verify that Z_L as G torsor over L is, via h, isomorphic to the trivial torsor $G \times_C G_L \to G_L$.

Take a $M \in G(C)$. The action of M on the rings, considered above, is given by $(X_{i,j}) \mapsto (X_{i,j})M$, $(r_{i,j}) \mapsto (r_{i,j})$ and thus $(Y_{i,j}) \mapsto (Y_{i,j})M$. This verifies that the

G-torsors Z_L and the trivial G-torsor G_L are isomorphic via h. The proofs of the two lemmata will conclude the proof of Theorem 5.6.

Proof of Lemma 5.7. From the flatness of L/K it follows that for any ideal I of $K[X_{i,j}, \frac{1}{\det}]$ one has $(I) \cap K[X_{i,j}, \frac{1}{\det}] = I$. It suffices to prove that any $\mathrm{Aut}(L/K)$-invariant ideal J of $L[X_{i,j}, \frac{1}{\det}]$ is generated by $I := J \cap K[X_{i,j}, \frac{1}{\det}]$. Choose a basis $\{e_a\}_{a \in A}$ of $K[X_{i,j}, \frac{1}{\det}]$. Any $f \in J$ can uniquely be written as a finite sum $f = \sum l_a \otimes e_a$, with all $l_a \in L$. The length $l(f)$ is defined as $\#\{a \in A | l_a \neq 0\}$. By induction on the length we will show that $f \in (I)$.

For $l(f) = 0, 1$ this is trivial. Suppose $l(f) > 1$. We may, after mutiplying f with a non-zero element of L suppose that $l_{a_1} = 1$ for some a_1. If all l_a belong to K then $f \in K$. If not, then there exists a a_2 with $l_{a_2} \in L \setminus K$. For any $\sigma \in \mathrm{Aut}(L/K)$, the length of $\sigma(f) - f = \sum((\sigma(l_a) - l_a) \otimes e_a$ is less than $l(f)$. Thus $\sigma(f) - f \in (I)$.

According to Proposition 3.12, there exists a $\sigma \in \mathrm{Aut}(L/K)$ with $\sigma(l_{a_2}) \neq l_{a_2}$. As above one finds that $\sigma(l_{a_2}^{-1} f) - l_{a_2}^{-1} f \in I$. Then

$$\sigma(l_{a_2}^{-1} f) - l_{a_2}^{-1} f = \sigma(l_{a_2}^{-1})(\sigma(f) - f) + (\sigma(l_{a_2}^{-1}) - l_{a_2}^{-1})f.$$

Since $\sigma(l_{a_2}^{-1}) - l_{a_2}^{-1} \in L^*$, it follows that $f \in (I)$. □

Proof of Lemma 5.8. The proof is rather similar to the one of Lemma 5.7. The only thing that we need to verify is that every differential ideal J of $M[Y_{i,j}, \frac{1}{\det}]$ is generated by $I := J \cap C[Y_{i,j}, \frac{1}{\det}]$. One takes a basis $\{e_a\}_{a \in A}$ of $C[Y_{i,j}, \frac{1}{\det}]$ over C. Any element $f \in J$ can uniquely be written as a finite sum $\sum_a m_a \otimes e_a$ with all $m_a \in M$. By induction on the length of f we will show that $f \in (I)$. Again $l(f) = 0, 1$ are trivial cases. Suppose $l(f) > 1$. We may suppose that $m_{a_1} = 1$ for some $a_1 \in A$ and $m_{a_2} \in M \setminus C$ for some $a_2 \in A$. Then $f' = \sum_a m'_a \otimes e_a$ has a length smaller then $l(f)$ and belongs therefore to (I). Similarly $(m_{a_2}^{-1} f)' \in (I)$. Write $(m_{a_2}^{-1} f)' = (m_{a_2}^{-1})' f + m_{a_2}^{-1} f' \in (I)$. Since C is the field of constants of M, one has $(m_{a_2}^{-1})' \neq 0$ and it follows that $f \in (I)$. □

Corollary 5.9. *Let R be a Picard–Vessiot ring for the equation $y' = Ay$ over K. Put $Z = \mathrm{Spec}(R)$. Let G denote the differential Galois group. Then:*

1. *There is a finite extension $\tilde{K}$ of K such that $Z_{\tilde{K}} \cong G_{\tilde{K}}$. Let $O(G)$ denote the coordinate ring of G then $\tilde{K} \otimes_K R \cong \tilde{K} \otimes_C O(G)$.*
2. *Z is smooth and connected.*
3. *The transcendence degree of L/K is equal to the dimension of the group G.*

Proof. (1) Take $B \in Z(\bar{K})$. Then B is defined over a finite extension $\tilde{K}$ of K whence the torsor $Z_{\tilde{K}}$ is trivial.

(2) We know already that Z is connected. Smoothness follows from (1).

(3) The transcendence degree is the dimension of Z and according to (1) equal to the dimension of G.□

Corollary 5.10. *Let the differential field K be a C_1-field. Suppose that the differential Galois group G of the equation $y' = Ay$ is connected. Let the Lie algebra of G be denoted by $\underline{g}$. Let $H \supset G$ be a connected algebraic group with Lie algebra $\underline{h} \supset \underline{g}$. Suppose that $A \in \underline{h}(K)$. Then there is a $B \in H(K)$ such the the equivalent equation $v' = \tilde{A}v$, with $y = Bv$ and $\tilde{A} = B^{-1}AB - B^{-1}B'$, satisfies $\tilde{A} \in \underline{g}(K)$.*

Proof. The Picard–Vessiot ring for the equation can be taken to be $K[X_{i,j}, \frac{1}{\det}]/q$, where the maximal differential ideal q contains the differential ideal which defines H_K. In other words $Z = \mathrm{Spec}(K[X_{i,j}, \frac{1}{\det}]/q)$ is a minimal differentially invariant subset inside the differentially invariant subset H_K. We know that Z is a trivial G-torsor and contains a rational point $B \in Z(K) \subset H(K)$. The equivalent equation $v' = \tilde{A}v$ has minimal differential ideal $B^{-1}Z = G_K$. According to Lemma 4.1 one has for any $D \in G(\bar{K})$ that $D + \epsilon(D' - \tilde{A}D) \in G_K(\bar{K}[\epsilon])$. For $D = 1$ this yields $(1 - \epsilon\tilde{A}) \in G(K)$ and thus $\tilde{A} \in \underline{g}(K)$. □

5.3. appendix A.3. the Galois correspondence

We start by proving a special case of the Galois correspondence.

Lemma 5.11. *Let L/K be a Picard–Vessiot extension for $y' = Ay$ over K with differential Galois group G. Let $H \subset G$ be a proper closed subgroup of G then $L^H \neq K$.*

Proof. $R \subset L$ denotes a Picard–Vessiot ring and $\tilde{K}$ is a finite extension of K such that $\tilde{K} \otimes_K R \cong \tilde{K} \otimes_C O(G)$, where $O(G)$ is the coordinate ring of G. Let $Qt(O(G))$ denote the total ring of fractions of $O(G)$. This ring is the ring of the rational functions on G. The total rings of fractions of $\tilde{K} \otimes_K R$ and $\tilde{K} \otimes_C O(G)$ are $\tilde{K} \otimes_K L$ and $\tilde{K} \otimes_C Qt(O(G))$. They are again isomorphic. Taking H-invariants leads to an isomorphism between $\tilde{K} \otimes_K L^H$ and $\tilde{K} \otimes_C Qt(O(G))^H$. The ring $Qt(O(G))^H$ consists of the H-invariant rational functions on G. It is known that for $H \neq G$ the ring $Qt(O(G))^H$ contains a non constant element (i.e., not in C) (see Humphreys, 1981). This proves $L^H \neq K$. □

We note, in passing, that $O(G)^H$ can be reduced to C for $H \neq G$. An example is $G = \mathrm{GL}(2)$ and H is a Borel subgroup. This shows that one cannot formulate the Galois correspondence with Picard–Vessiot rings instead of Picard–Vessiot fields.

Proposition 3.13. (The Galois Correspondence) *Let $L \supset K$ be the Picard–Vessiot field of the equation $y' = Ay$ over K. Let $G := \mathrm{Aut}(L/K)$ be the differential Galois group of the equation. Consider the two sets $\mathcal{S}$ = the closed subgroups of G and $\mathcal{L}$= the differential fields M with $K \subset M \subset L$. Let $\alpha : \mathcal{S} \to \mathcal{L}$ and $\beta : \mathcal{L} \to \mathcal{S}$ be the maps defined by $\alpha(H) = L^H$, where L^H is the subfield of L consisting of the H-invariant elements, and $\beta(M) = \mathrm{Aut}(L/M)$, the set of automorphisms of L/M commuting with the differentiation on L. Then:*

1. *The two maps α and β are inverse to each other.*
2. *Suppose that $H \in \mathcal{S}$ is a normal subgroup of G. Put $M = L^H$. Then $\mathrm{Aut}(M/K)$ is isomorphic to G/H. Moreover M is a Picard–Vessiot field for some linear differential equation over K.*
3. *Let G^o denote the identity component of G. Then $L^{G^o} \supset K$ is a finite Galois extension with Galois group G/G^o.*

Proof. We note that $\beta(M) = \mathrm{Aut}(L/M)$ is in fact the differential Galois group of the equation $y' = Ay$ over M. Thus $\beta(M)$ is a closed subgroup of G and belongs to $\mathcal{S}$.

(1) For $M \in \mathcal{L}$ one has $\alpha\beta(M) = L^{\mathrm{Aut}(L/M)}$. The last field is equal to M, because we can apply Proposition 3.12 to the Picard–Vessiot extension L/M for $y' = Ay$ over M. For $H \in \mathcal{S}$ the inclusion $H \subset H_1 := \mathrm{Aut}(L/L^H) = \beta\alpha(H)$ is obvious. Apply now Corollary 5.9, with G replaced by H_1 and K replaced by $L^H = L^{H_1}$. If $H \neq H_1$, then we find the contradiction $L^H \neq L^{H_1}$.

(2) There is an obvious injective homomorphism $G/H \to \mathrm{Aut}(L^H/K)$. For proving the surjectivity we have to show that any $\sigma \in \mathrm{Aut}(L^H/K)$ extends to an element of $\mathrm{Aut}(L/K)$.

Consider, more generally, $M \in \mathcal{L}$ and a K-homomorphism of differential fields $\psi : M \to L$. The Picard–Vessiot field for $y' = Ay$ over M is L. The Picard–Vessiot field for $y' = \psi(A)y$ (note that $\psi(A) = A$) over $\psi(M)$ is also L. The unicity of the Picard–Vessiot field yields a K-isomorphism of differential fields $\tilde{\psi} : L \to L$, extending ψ.

It is more difficult to see that M is a Picard–Vessiot field for some linear differential equation over K. A "natural" proof will be given in Remark 5.14. Here we give a proof which does not use Tannakian arguments. Take a finite Galois extension $\tilde{K}$ of K with (ordinary) Galois group U, such that the torsor corresponding to R is becomes trivial over $\tilde{K}$. This means that $\tilde{K} \otimes_K R \cong \tilde{K} \otimes_C O(G)$, where $O(G)$ is the coordinate ring of G. We note that this implies that for every $f \in R$, the G-orbit $\{g(f)|g \in G\}$ of f spans a finite-dimensional vector space over C. Indeed, this holds for $O(G)$ (see Humphreys, 1981) and therefore also for $\tilde{K} \otimes_C O(G)$.

It is known that $O(G)^H = O(G/H)$, which is the coordinate ring of the linear algebraic group $G' := G/H$ (see Humphreys, 1981). Let $Qt(O(G))$ denote the total ring of fractions of $O(G)$. Moreover, $Qt(O(G))^H$ is the total ring of fractions of $O(G)^H$. Thus $\tilde{K} \otimes_K R^H \cong \tilde{K} \otimes_C O(G')$, which is a finitely generated $\tilde{K}$-algebra. Moreover $\tilde{K} \otimes_K L^H$ is equal to $\tilde{K} \otimes_C Qt(O(G))^H$. Taking invariants under U, one finds that R^H is a finitely generated K-algebra with field of fractions L^H. The G'-orbit of any element $f \in R^H$ spans a finite-dimensional vector space over C. We conclude that there is a finite-dimensional C-vector space $V \subset R^H$, which is G'-invariant and generates R^H as a K-algebra.

Take a basis $v_1, \ldots, v_s$ of V over C. Let $\mathcal{D}_M = M[\partial]$ denote the ring of differential operators with coefficients in the differential field $M = L^H$. This ring is left- and right Euclidean and so the left ideal $\mathcal{D}_M(\partial - \frac{v_1'}{v_1}) \cap \cdots \cap \mathcal{D}_M(\partial - \frac{v_s'}{v_s})$ has the form $\mathcal{D}_M P$, where P is a monic operator of order $\leq s$. The operator P is unique, every v_i lies in the kernel of P. Hence P has order s and its kernel on R^H is V. Since V is G'-invariant the operator P is invariant under G'. By Proposition 3.6 part (3), P lies in $K[\partial]$. The field L^H is generated as an extension of K by the elements of V and their derivatives. The constants of L^H are C. From Proposition 3.9 it follows that L^H is a Picard–Vessiot field of the scalar differential equation $P(y) = 0$.

(3) G/G^o is a finite group. The property $(L^{G^o})^{G/G^o} = K$ implies that $L^{G^o} \supset K$ is a Galois extension with Galois group G/G^o. □

5.4. appendix A.4. the Tannakian point of view

In this subsection we will explain in short the connection between the Picard–Vessiot theory, differential Galois theory and Tannakian categories. Let C be a field and G a linear algebraic group over C. A representation (T, ρ) is a finite-dimensional vector space over C together with a homomorphism $\rho : G \to \mathrm{GL}(T)$ of algebraic groups over C. The category of all representations of G is denoted by Repr_G. The set $\mathrm{Hom}((T_1,\rho_1),(T_2,\rho_2))$ consists of the C-linear maps $f : T_1 \to T_2$ such that $\rho_2 \circ f = f \circ \rho_1$. Thus each Hom is a vector space over C. One can form finite direct sums of representations, kernels and cokernels. Further for any two representations $(T_1,\rho_1),(T_2,\rho_2)$ one defines the tensor product $(T_1 \otimes_C T_2, \rho)$ by the formula $\rho(g)(t_1 \otimes t_2) = (\rho_1(g)t + 1) \otimes (\rho_2(g)t_2)$. There is a unit object $\mathbf{1}$, i.e., the trivial representation of G on a one-dimensional vector space over C. For every object (T,ρ) there is a dual (T^*,ρ^*) with T^* is the dual vector space and ρ^* is the dual action of G on T^*.

Let K be a differential field. The field of constants C of K is supposed to be algebraically closed and to have characteristic 0. A differential module $M = (M,\partial)$ is a finite-dimensional vector space over K equipped with a C-linear map $\partial : M \to M$ such that $\partial(fm) = f'm + f\partial(m)$ for all $f \in K$ and $m \in M$. Let Diff_K denote the category of all differential modules over K. For two differential modules $(M_1,\partial_1),(M_2,\partial_2)$ one defines $\mathrm{Hom}(M_1,M_2)$ as the set of the K-linear $f : M_1 \to M_2$ with $\partial_2 \circ f = f \circ \partial_1$. Each Hom is a vector space over C. There are direct sums, kernels and cokernels. For every two differential modules $(M_1,\partial_1),(M_2,\partial_2)$ one defines the tensor product $(M_1 \otimes_K M_2, \partial)$ by $\partial(m_1 \otimes m_2) = (\partial_1 m_1) \otimes m_2 + m_1 \otimes (\partial_2 m_2)$. There is a unit object $\mathbf{1}$, this is the one-dimensional vector space K with $\partial(f) = f'$ for all $f \in K$. For every object (M,∂) one can define a dual (M^*,∂^*) by M^* is the dual of the K-vector space M and $\partial^*(m^*)$ is the element of M^*, given by $\partial^*(m^*)(m) = m^*(\partial m) - (m^*(m))'$.

For a given differential module M over K one considers the full subcategory $\{\{M\}\}$ of Diff_K, whose objects are isomorphic to finite direct sums of subquotients of some $M \otimes M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*$ (i.e., M_1/M_2 where $M_2 \subset M_1$ are submodules of this tensor product). The link between the Tannakian approach and the Picard–Vessiot theory is the following result.

Proposition 5.12. *Let M be a differential module over K with differential Galois group G. There is an equivalence $\{\{M\}\} \to \mathrm{Repr}_G$ which respects the structures on the two categories (i.e., C-linear isomorphism between* Hom*'s, direct sums, kernels, cokernels, tensor products, unit objects, duals).*

Proof. Let $E \supset K$ be a Picard–Vessiot ring for M. For any object N of $\{\{M\}\}$ we consider the kernel $\mathcal{F}(N) := \ker(\partial, E \otimes_K N)$, which is a vector space over C, and the canonical E-linear map $E \otimes_C \mathcal{F}(N) \to E \otimes_K N$. By definition, this map is an isomorphism in the case $N = M$. It follows that the map is also an isomorphism for any tensor product $M \otimes M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*$ and for its subquotients. Thus the map is for every object N of $\{\{M\}\}$ an isomorphism. The action of G on E extends to an action on $E \otimes_K N$ by $g(e \otimes n) = (ge) \otimes n$. This action commutes with ∂ on $E \otimes_K N$ and thus induces an action of G on $\mathcal{F}(N)$. It is easily seen that this makes $\mathcal{F}(N)$ into a representation of G. A morphism $N_1 \to N_2$ between objects of $\{\{M\}\}$ induces in an obvious way a morphism $\mathcal{F}(N_1) \to \mathcal{F}(N_2)$. Thus $\mathcal{F}$ is a functor. It is obvious that $\mathcal{F}$ respects all the structures on the two categories. In order to show that $\mathcal{F}$ is an equivalence we have to verify that the map $\mathrm{Hom}(N_1,N_2) \to \mathrm{Hom}(\mathcal{F}N_1, \mathcal{F}N_2)$ is an isomorphism and that every object of Repr_G is isomorphic to some $\mathcal{F}(N)$. In proving the first statement, it suffices to show that $\mathrm{Hom}(\mathbf{1},N) \to \mathrm{Hom}(\mathbf{1},\mathcal{F}(N))$ is bijective, because $\mathrm{Hom}(N_1,N_2) = \mathrm{Hom}(\mathbf{1}, N_1^* \otimes N_2)$. The left-hand side consists of the elements $n \in N$ with $\partial n = 0$. The right-hand side consists of the elements in $\ker(\partial, E \otimes_K N)$ which are invariant under G. From $E^G = K$ the bijection follows.

Put $V = \mathcal{F}(M)$. The group G is given as an algebraic subgroup of $\mathrm{GL}(V)$. It is known that (see Deligne and Milne, 1982) every representation of G is isomorphic to a finite direct sum of subquotients of the tensor products $V \otimes V \otimes \cdots \otimes V \otimes V^* \otimes \cdots \otimes V^*$. This shows that every representation of G is isomorphic to some $\mathcal{F}(N)$. □

Remark 5.13. In the terminology of Deligne and Milne (1982) a category (with additional structures as above) is called a neutral Tannakian category if it is isomorphic to Repr_G for some affine group scheme over C. In the case of the above proposition G is actually a linear algebraic group. The work of Deligne (1990) proves "abstractly" that Diff_K and $\{\{M\}\}$ are neutral Tannakian categories. The Picard–Vessiot theory (including the statements on torsors) is then an easy consequence.

Remark 5.14. For an object N of $\{\{M\}\}$ the differential Galois group is the image of G in $\mathrm{GL}(T)$, with $T = \mathcal{F}(N)$. This implies at once that for every closed normal subgroup $N \subset G$ the linear algebraic group G/N is a differential Galois group. Indeed, according to the above proposition, it suffices to produce a representation $\rho : G \to \mathrm{GL}(T)$ with kernel N.

5.5. appendix A.5. characterization of Picard–Vessiot rings and fields

The inspiration for this subsection is Chapter V of Magid (1994). We note that most of the contents of that chapter follows from Lemma 5.15 and Theorem 5.6. A Picard–Vessiot ring or field resembles closely the splitting field of a polynomial equation. Splitting fields of separable polynomials and finite Galois extensions are identical, however the definition of a finite Galois extension is more intrinsic. In this subsection, we will give an intrinsic characterization of Picard–Vessiot rings and fields which does not refer to a specific linear differential equation. The first result characterizes the Picard–Vessiot ring inside the Picard–Vessiot field.

Lemma 5.15. *Let $L \supset K$ be a Picard–Vessiot field for a linear differential equation $y' = Ay$ over K. Let $R \subset L$ be the Picard–Vessiot ring and G the differential Galois group. The following properties of $f \in L$ are equivalent:*

1. *$f \in R$.*
2. *The C-vector space $< Gf >_C$ spanned by the orbit $Gf = \{g(f) | g \in G\}$ has dimension $m < \infty$.*
3. *The K-vector space $< f, f', f'', \ldots >_K$ spanned by f and all its derivatives has dimension $m < \infty$.*

Proof. (1)⇒(2). For some finite extension $\tilde{K}$ of K one has $\tilde{K} \otimes_K R \cong \tilde{K} \otimes_C O(G)$. The orbit of any element of $O(G)$ spannes a finite-dimensional vector space over C (see Humphreys, 1981). This property is inherited by $\tilde{K} \otimes_C O(G)$ and R.

(2)⇒(3). Choose a basis $v_1, \ldots, v_m$ of $< Gf >_C$. In the ring of differential operators

$L[\partial]$ one considers the left ideal $L[\partial](\partial - \frac{v_1'}{v_1}) \cap \cdots \cap L[\partial](\partial - \frac{v_m'}{v_m})$. Since $L[\partial]$ is a left- and right Euclidean domain this left ideal is equal to $L[\partial]P$ where P is a monic operator of degree $\leq m$. From $P(v_i) = 0$ for all i, it follows that the degree of P is m and that the kernel of P on L is $< Gf >_C$. The G-invariance of this space, the uniqueness of P and $L^G = K$ implies that $P \in K[\partial]$. From $P(f) = 0$ it follows that $< f, f', f'', \ldots >_K$ has dimension $\leq m$. Suppose that f satisfies a monic differential operator $Q(f) = 0$ with $Q \in K[\partial]$ and the degree of Q is $n \leq m$. Then the kernel of Q on L is a G-invariant vector space of dimension $\leq n$ and contains f. Thus $n = m$ and $Q = P$.

(3)⇒(1). The K-vector space $W := < f, f', f'', \ldots >_K$ is supposed to have dimension $m < \infty$. The minimal monic differential operator $P \in K[\partial]$ has degree m. Consider the non-zero ideal $I \subset R$ consisting of the elements $a \in R$ such that $aW \subset R$. For $a \in I$ and $w \in W$, one has $a'w = (aw)' - aw'$. Since both R and W are invariant under differentiation, one finds $a'w \in R$. Thus I is a differential ideal. Moreover the differential ring R is simple. Thus $I = R$ and $f \in R$. □

An element f (in some differential ring containing K) is called *differentially finite over* K if the dimension of the K-vector space $< f, f', f'', \ldots >_K$ is finite. An example which illustrates the equivalence between (1) and (3) in the lemma is: $K = C(z) \subset L = C(z, l)$ with $l' = z^{-1}$ and $f = l^{-1}$. A simple calculation shows that f is not differentially finite.

Proposition 5.16. *Let $K \subset L$ be an extension of differential fields. Then L is a Picard–Vessiot field of some linear differential equation over K, if and only if the following conditions are satisfied:*

1. *$L \supset K$ is a finitely generated field extension.*
2. *The field of constants of L is C.*
3. *Let $f \in L$ be differentially finite over K and let $P \in K[\partial]$ be the monic operator of minimal degree with $P(f) = 0$. Then the dimension over C of the kernel of P on L is equal to the degree of P.*
4. *L is generated over K by differentially finite elements.*

Proof. The conditions are necessary, according to the definitions and Lemma 5.15. Suppose that the conditions are satisfied. Let the differentially finite elements $f_1, \ldots, f_s$ generate L over K. The minimal monic differential operator of f_i is denoted by $P_i \in K[\partial]$. The left ideal $\cap_{i=1}^s K[\partial]P_i$ is equal to $K[\partial]P$ for some monic P of degree m. The kernel of P on L has dimension m over C. It follows from Proposition 3.9 that L is a Picard–Vessiot field for the equation $P(y) = 0$ over K. □

Remarks.

1. From Lemma 5.15 and Proposition 5.16 one can derive a characterization of Picard–Vessiot rings.
2. Condition (3) in the proposition can be seen as an analogue of normality for a finite field extension.

Acknowledgements

In preparing this manuscript and the exercises I was greatly helped by Wim R. Oudshoorn. I would also like to thank the referees for their useful comments.

References

Deligne, P. (1990). Catégories Tannakiennes. In *The Grothendieck Festschrift 2*, pp. 111–195; *Prog. Math.*, **87**, Basel, Birkhäuser.

Deligne, P., Milne, M. (1982). In *Tannakian Categories*, SLNM **900**, pp. 101–228.

Dynkin, E. (1957). Maximal subgroups of the classical groups. *Trudy Moskov. Mat. Obschetsva*, **1**, 39–160. *Am. Math. Soc. Transl. Ser. 2*, **6**, 245–378.

Fulton, W., Harris, J. (1991). In *Representation Theory,* volume 129*,* Graduate Texts in Mathematics, New York, Springer Verlag.

Humphreys, J. E. (1981). *Linear Algebraic Groups,* 2$^{\text{nd}}$ edn, New York, Springer Verlag.

Jacobson, N. (1962). *Lie Algebras*, New York, Dover.

Kaplansky, I. (1976). *An Introduction to Differential Algebra,* 2$^{\text{nd}}$ edn, Paris, Hermann.

Katz, N. (1987). A simple algorithm for cyclic vectors. *Am. J. Math.*, **109**, 65–70.

Kolchin, E. R. (1973). *Differential Algebra and Algebraic Groups*, New York, Academic Press.

Kovacic, J. J. (1969). The inverse problem in the Galois theory of differential equations. *Ann. Math.*, **89**, 583–608.

Kovacic, J. J. (1986). An algorithm for solving second order linear homogeneous differential equations. *J. Symb. Comput.*, **2**, 3–43.

Magid, A. (1994). *In Lectures on Differential Galois Theory, volume 7, University Lecture Series*, Providence, RI, American Mathematical Society.

Mitschi, C., Singer, M. F. (1996). Connected linear groups as differential Galois Groups. *J. Algbra*, **184**, 333–361.

van der Put, M. (1998). Recent work on differential Galois theory, Séminaire Bourbaki, exp849, volume 1997/98, Astérisque 252, 1998.

Ramis, J.-P. (1996). About the inverse problem in differential galois theory: the differential Abhyankar conjecture. In *The Stokes Phenomenon and Hilbert's 16th Problem*, Braaksma, B. L. J., Immink, G. K., van der Put, M. eds., Singapore, World Scientific.

Ramis, J.-P. (1996). About the inverse problem in differential Galois theory: the differential Abhyankar conjecture. In *The Stokes Phenomenon and Hilbert's 16th Problem*, Bram, B. L. J., Im, G. K., van der Put, M. eds., Singapore, World Scientific.

Serre, J.-P. (1964). In *Cohomologie Galoisienne,* LNM **5**, New York, Springer Verlag.

Serre, J.-P. (1968). *Corps Locaux*, Paris, Hermann.

Shafarevich, I. R. (1974). Basic algebraic geometry. In *Die Grundlehren der Mathematischen Wissenschaften, Band 213*, Berlin, Heidelberg, New York, Springer Verlag.

Singer, M. F. (1993). Moduli of linear differential equations on the Riemann sphere with fixed Galois groups. *Pac. J. Math.*, **106**, 343–395.

Singer, M. F., Ulmer, F. (1993). Galois groups of second and third order differential equations. *J. Symb. Comput.*, **16**, 9–36.

Tretkoff, C., Tretkoff, M. (1979). Solution of the inverse problem of differential Galois theory in the classical case. *Am. J. Math.*, **101**, 1327–1332.

Received 18 May 1998