

Introduction to the Galois Theory of Linear Ordinary Differential Equations

R.C. Churchill

Hunter College and the Graduate Center of CUNY,
and the University of Calgary

Address for Correspondence

Department of Mathematics

Hunter College

695 Park Avenue, New York, NY 10021, USA

September 17, 2006

Introduction to the Galois Theory of Linear Ordinary Differential Equations

R.C. Churchill

Prepared for the

Kolchin Seminar on Differential Algebra

Graduate Center, City University of New York

8 September 2006

Originally given 9 and 16 September 2005. Corrected 19 September 2005 and 7 September 2006.

Abstract

We define the differential Galois group of a linear homogeneous ordinary differential equation and illustrate the type of information about solutions packaged within. The initial format is classical; at the end we indicate how the results can be conceptualized geometrically.

Contents

- §1. An Extrinsic Definition of the Differential Galois Group
- §2. Closed-Form Solutions
- §3. The Connection with Algebraic Groups
- §4. Equations of Second Order
- §5. Examples of Differential Galois Group Calculations
- §6. A Brief Digression on Derivations
- §7. Differential Structures
- §8. Extensions of Differential Structures
- §9. An Intrinsic Definition of the Differential Galois Group

Bibliography

1. An Extrinsic Definition of the Differential Galois Group

Consider an n^{th} -order linear homogeneous differential equation

$$(1.1) \quad y^{(n)} + a_1(z)y^{(n-1)} + \cdots + a_{n-1}(z)y' + a_n(z)y = 0$$

with coefficients (for simplicity) in the field $\mathbb{C}(z)$ of rational functions on the Riemann sphere $\mathbb{P}^1 \simeq \mathbb{C} \cup \{\infty\}$. Fix a point $z_0 \in \mathbb{C}$ which is a regular point for all coefficients and henceforth identify $\mathbb{C}(z)$ with the field K of associated germs at z_0 : this enables us to work with function fields while avoiding the ambiguities of “multi-valued” functions. Note that K is a “differential field”, i.e., the operator d/dz passes to the germ level and defines a derivation¹ thereon which we again denote by d/dz .

Pick a basis $\{y_j\}_{j=1}^n$ of solution germs of (1.1) at z_0 and form the field extension $L \supset K$ generated by these elements. This is again a differential field, and the derivation, also denoted by d/dz , extends that on K . $L \supset K$ is the *Picard-Vessiot extension* of K corresponding to (1.1); it is the analogue of the splitting field of a polynomial in ordinary Galois theory.

The *differential Galois group* of (1.1) is the group $G_{\text{dg}}(L/K)$ of field automorphisms of L which commute with d/dz and fix K pointwise. We will be interested in what information this group provides about the solutions of (1.1), and how it can be computed. Our first result addresses the information question.

Theorem 1.2 : *For the differential Galois group $G := G_{\text{dg}}(L/K)$ defined above the following statements are equivalent :*

- (a) G is finite;
- (b) the field extension $L \supset K$ is finite, Galois in the usual sense, and G is the usual Galois group; and
- (c) all solutions of (1.1) are algebraic over $K \simeq \mathbb{C}(z)$.

In (b) “usual sense” means: in the sense of the classical Galois theory of polynomials. A more precise statement of (c) is: all germs of solutions of (1.1) at z_0 are germs of algebraic functions over $\mathbb{C}(z)$.

¹A *derivation* on a field K is an additive mapping $\delta : k \in K \mapsto k' \in K$ satisfying the *Leibniz rule* $(k\ell)' = k\ell' + k'\ell$. The concept will be generalized in §6.

Proof :

(a) \Rightarrow (b) : It is a fact² that K is the fixed field of L under the action of G (i.e., to any $\ell \in L \setminus K$ there corresponds at least one element $g = g(\ell) \in G$ such that $g \cdot \ell \neq \ell$). (This does not require the finiteness hypothesis.) However, by a result of E. Artin³ (and the finiteness hypothesis) the extension $L \supset K$ must then be Galois, G must be the usual Galois group, and $[L : K]$ must be the order of G .

(b) \Rightarrow (c) : Galois extensions (in the usual sense) are algebraic.

(c) \Rightarrow (a) : Let $M \supset L$ be a splitting field of the irreducible polynomials (in $K[z]$) of the y_j . Then the extension $M \supset K$ is finite and Galois; let H denote the (necessarily finite) Galois group. Since any field automorphism of L over K extends to an automorphism⁴ of M over K the differential Galois group $G_{\text{dg}}(L/K)$ is contained in the image of the restriction mapping $h \in H \mapsto h|_L$, and (a) follows.

q.e.d.

The search for algebraic solutions of linear differential equations (as in (1.1)) was a major mathematical activity in the late nineteenth century. Consider, for example, the *hypergeometric equation*⁵

$$(1.3) \quad y'' + \frac{\gamma - (\alpha + \beta + 1)z}{z(1-z)} y' - \frac{\alpha\beta}{z(1-z)} y = 0,$$

wherein α, β, γ are complex parameters. In 1873 H.A. Schwarz⁶ used a beautiful geometric argument involving spherical triangles to enumerate those parameter values for which all solutions were algebraic over $\mathbb{C}(z)$. This example will recur later in the notes.

²See, e.g., [Kap, Chapter V, Theorem 5.7, p. 36].

³See, e.g., [Lang, Chapter VI, §1, Theorem 1.8, p. 264].

⁴Let K^a be an algebraic closure of K containing M (and therefore L). Then any field automorphism $\sigma : L \rightarrow L$ over K extends to a field embedding $\hat{\sigma} : M \rightarrow K^a$ by standard algebra (e.g., see [Lang, Chapter V, §2, Theorem 2.8, p. 233]), and this extension must be an automorphism of M by normality (e.g., see [Lang, Chapter V, §3, Theorem 3.3, p. 237]).

⁵Which is more commonly written

$$z(1-z)y'' + [\gamma - (\alpha + \beta + 1)z]y' - \alpha\beta y = 0.$$

⁶See, e.g., [Poole, Chapter VII, particularly the table on p. 128].

2. Closed-Form Solutions

Let $K \simeq \mathbb{C}(z)$ be as in the previous section and let $L \supset K$ be a field extension generated by germs of meromorphic functions such that the operator d/dz defines a derivation on L . The extension is *Liouvillian* if there is a finite sequence of intermediate fields

$$\mathbb{C}(z) = K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

such that d/dz restricts to a derivation on each K_j , and for $j = 1, \dots, n$ the field K_j has the form $K_{j-1}(\ell)$ where either:

- (a) $\ell'/\ell \in K_{j-1}$;
- (b) $\ell' \in K_{j-1}$; , or
- (c) ℓ is algebraic over K_{j-1} .

An element $\ell \in K_j$ as in (a) is an *exponential of an integral over K_{j-1}* . Indeed, one often writes ℓ as $e^{\int k}$, where $k := \ell'/\ell \in K_{j-1}$. An element $\ell \in K_j$ as in (b) is an *integral over K_{j-1}* , and is often expressed as $\int k$ when $k := \ell' \in K_{j-1}$.

A function (germ) is *Liouvillian* if it is contained in some Liouvillian extension of K . Such functions are regarded as “elementary”, or as being of “closed-form”: they are obtained from rational functions by a finite sequence of adjunctions of exponentials, indefinite integrals, and algebraic functions. Logarithms, being indefinite integrals, are included, as are the elementary trigonometric functions (since they can be expressed in terms of exponentials). The differential Galois group of (1.1) gives information about the existence of closed form solutions.

3. The Connection with Algebraic Groups

The differential Galois group $G := G_{\text{dg}}(L/K)$ of (1.1) is generally regarded as a matrix group. Specifically, any $g \in G$ defines a matrix $M_g = (m_{ij}(g)) \in \text{GL}(n, \mathbb{C})$ by

$$(3.1) \quad g \cdot y_j := \sum_{i=1}^n m_{ij}(g)y_i, \quad j = 1, \dots, n,$$

and the mapping $\rho : g \in G \mapsto M_g \in \text{GL}(n, \mathbb{C})$ is a faithful matrix representation; one therefore identifies G with $\rho(G) \subset \text{GL}(n, \mathbb{C})$. It is a fact⁷ that latter is actually an *algebraic group*, i.e., there is a finite collection $\{p_k(x_{ij})\}$ of complex polynomials in n^2 variables such that $g \in G \simeq \rho(G)$ if and only if $p_k(m_{ij}(g)) = 0$ for all k .

To make the algebraic group concept a bit more transparent two simple examples are offered. (i) The subgroup $G \subset \text{GL}(2, \mathbb{C})$ consisting of 2×2 complex matrices of the form

$$(3.2) \quad \begin{pmatrix} \lambda & 0 \\ \delta & \lambda^{-1} \end{pmatrix}, \quad \lambda, \delta \in \mathbb{C}, \quad \lambda \neq 0,$$

is algebraic: a matrix $m = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in \text{GL}(2, \mathbb{C})$ is in G if and only if for $p_1(x_{11}, x_{12}, x_{21}, x_{22}) = x_{11}x_{22} - x_{21}x_{12} - 1 = \det((x_{ij})) - 1$ and $p_2(x_{11}, x_{12}, x_{21}, x_{22}) = x_{12}$ we have $p_1(m_{11}, m_{12}, m_{21}, m_{22}) = 0$ and $p_2(m_{11}, m_{12}, m_{21}, m_{22}) = 0$. (ii) The subgroup $\text{SL}(n, \mathbb{C})$ of unimodular (i.e., determinant 1) matrices of $\text{GL}(n, \mathbb{C})$ is algebraic. Here we need only one polynomial, i.e., $p(x_{ij}) = \det((x_{ij})) - 1$.

Algebraic groups have a very rich structure which proves quite useful in calculations. Specifically, any algebraic subgroup $H \subset \text{GL}(n, \mathbb{C})$ can be viewed as a topological space which is a finite union of disjoint closed connected components, and the *component of the identity*, i.e., that component H^0 containing the identity matrix, is always a normal subgroup of finite index⁸. Example: The group $\text{SL}(n, \mathbb{C})$ is connected⁹, hence $\text{SL}(n, \mathbb{C})^0 = \text{SL}(n, \mathbb{C})$.

Theorem 3.3 : *The Picard-Vessiot extension $L \supset K \simeq \mathbb{C}(z)$ of (1.1) is a Liouvillean extension if and only if the component of the identity of the differential Galois group is solvable.*

⁷See, e.g., [Kap, Chapter 5, §21, Theorem 5.5, p. 36].

⁸See, e.g., [Kap, Chapter IV, Lemma 4.5, p. 28].

⁹See, e.g., [Spr, Exercise 2.2.2, p. 37].

Proof : See, e.g., [vdP-S, Chapter I, §1.5, Theorem 1.43, p. 33].

q.e.d.

When the component of the identity is solvable it is conjugate to a subgroup of the group of lower triangular matrices; this is the *Lie-Kolchin Theorem*¹⁰. Consequence: $\mathrm{SL}(2, \mathbb{C})$ is not solvable.

In these notes we will be mainly concerned with algebraic subgroups of $\mathrm{SL}(2, \mathbb{C})$.

Theorem 3.4 : *For any algebraic subgroup $G \subset \mathrm{SL}(2, \mathbb{C})$ one of the following possibilities holds:*

(a) G is “reducible”, i.e., conjugate to a subgroup of the group

$$\{m \in \mathrm{SL}(2, \mathbb{C}) : m = \begin{pmatrix} \lambda & 0 \\ \delta & \lambda^{-1} \end{pmatrix}, \lambda, \delta \in \mathbb{C}, \lambda \neq 0\}.$$

(b) G is “imprimitive”, i.e., conjugate to a subgroup of $D \cup \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} D$, where D is the group of diagonal matrices in $\mathrm{SL}(2, \mathbb{C})$, i.e.,

$$D := \{m \in \mathrm{SL}(2, \mathbb{C}) : m = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \lambda \in \mathbb{C} \setminus \{0\}\}.$$

(c) G is finite, contains the negative $-I$ of the identity matrix I , and the factor group $G/\{I, -I\}$ is isomorphic to either

- (i) the alternating group A_4 (the “projectively tetrahedral case”),
- (ii) the symmetric group S_4 (the “projectively octahedral case”), or
- (iii) the alternating group A_5 (the “projectively icosahedral case”).

(d) $G = \mathrm{SL}(2, \mathbb{C})$.

The possibilities are not mutually exclusive, e.g., any algebraic subgroup of D is both reducible and imprimitive. Moreover, (a) and (b) include finite groups, i.e., cyclic, dihedral and octahedral, although not those given in (c).

Proof : See [Kov, pp. 7 and 27].

q.e.d.

¹⁰See, e.g., [Kap, Chapter IV, §18, Theorem 4.11, p. 30].

4. Equations of Second-Order

In this section we specialize to the case $n = 2$ in (1.1), i.e., to

$$(4.1) \quad y'' + a_1(z)y' + a_2(z)y = 0.$$

The associated equation

$$(4.2) \quad y'' + (a_2(z) - \frac{1}{4}a_1^2(z) - \frac{1}{2}a_1'(z))y = 0$$

is called the *normal form* of (4.1) and (4.1) is the *standard form*¹¹ of (4.2). One checks easily that $y = y(z)$ is a solution of (4.1) if and only if $w = w(z) := e^{\frac{1}{2} \int^x a_1(t) dt} y(z)$ is a solution of (4.2), and since our concern is with the nature of solutions there is no loss of generality if we replace (4.1) with (4.2).

Examples 4.3 :

- (a) The normal form of the hypergeometric equation

$$y'' + \frac{\gamma - (\alpha + \beta + 1)z}{z(1-z)} y' - \frac{\alpha\beta}{z(1-z)} y = 0$$

is

$$y'' + \frac{1}{4} \left\{ \frac{1 - \lambda^2}{z^2} + \frac{1 - \nu^2}{(z-1)^2} - \frac{\lambda^2 - \nu^2 + \mu^2 - 1}{z} + \frac{\lambda^2 - \nu^2 + \mu^2 - 1}{z-1} \right\} y = 0,$$

where

$$\begin{aligned} \lambda &:= 1 - \gamma \\ \nu &:= \gamma - (\alpha + \beta) \\ \mu &:= \pm(\alpha - \beta). \end{aligned}$$

- (b) Equation (4.1) is known as *Riemann's equation* when

$$\begin{aligned} a_1(z) &= \frac{1 - \eta_1 - \mu_1}{z} + \frac{1 - \eta_2 - \mu_2}{z-1} \quad \text{and} \\ a_2(z) &= \frac{\eta_1 - \mu_1}{z^2} + \frac{\eta_2 - \mu_2}{(z-1)^2} + \frac{\eta_3\mu_3 - \eta_1\mu_1 - \eta_2\mu_2}{z(z-1)}, \end{aligned}$$

¹¹I have introduced the “standard form” terminology for convenience.

where the complex parameters η_j, μ_j are subject to the single constraint $\sum_j (\eta_j - \mu_j) = 1$. The normal form is

$$y'' + \frac{1}{4} \left\{ \frac{1 - (\eta_1 - \mu_1)^2}{z^2} + \frac{1 - (\eta_2 - \mu_2)^2}{(z-1)^2} + \frac{\nu}{z} - \frac{\nu}{z-1} \right\} y = 0,$$

where

$$\nu := 1 - (\eta_1 - \mu_1)^2 - (\eta_2 - \mu_2)^2 + (\eta_3 - \mu_3)^2.$$

- (c) Examples (a) and (b) are special cases of second-order ‘‘Fuchsian equations,’’ which in our setting can be defined as second-order equations of the form

$$y'' + \left(\sum_{j=1}^m \frac{A_j}{z - a_j} \right) y' + \left(\sum_{j=1}^m \frac{B_j}{(z - a_j)^2} + \sum_{j=1}^m \frac{C_j}{z - a_j} \right) y = 0.$$

Here the ‘‘singularities’’ $a_1, \dots, a_m \in \mathbf{C}$ are assumed distinct and the sole restriction on the the complex constants A_j, B_j and C_j is $\sum_j C_j = 0$. The normal form is

$$y'' + \frac{1}{4} \left(\sum_{j=1}^m \frac{\hat{B}_j}{(z - a_j)^2} + \sum_{j=1}^m \frac{\hat{C}_j}{z - a_j} \right) y = 0,$$

where

$$\begin{aligned} \hat{B}_j &:= \frac{1}{4}(1 + 4B_j - (1 - A_j)^2), \\ \hat{C}_j &:= C_j - \frac{1}{2}A_j \left(\sum_{i \neq j} \frac{A_i}{a_j - a_i} \right). \end{aligned}$$

The normal form is again Fuchsian.

- (d) The normal form of Bessel’s equation

$$y'' + \frac{1}{z}y' + \left(1 - \frac{\nu^2}{z^2} \right) y = 0$$

(‘‘of order ν ’’) ¹² is

$$y'' + \frac{1}{4} \left(\frac{1 - 4(\nu^2 - z^2)}{z^2} \right) y = 0.$$

Neither equation is Fuchsian.

¹²Bessel’s equation is commonly written as

$$z^2 y'' + z y' + (z^2 - \nu^2) y = 0;$$

we are simply adopting the format (4.1).

(e) Airy's equation

$$y'' - zy = 0$$

is already in normal form. (The standard form is exactly the same equation.) This is again a non-Fuchsian example.

To ease notation we rewrite (4.2) as

$$(4.4) \quad y'' = r(z)y, \quad r(z) \in \mathbb{C}(z).$$

The benefit of the normal form is given by the following result.

Proposition 4.5 : *The differential Galois group of (4.4) is an algebraic subgroup of $\mathrm{SL}(2, \mathbb{C})$.*

Proof : The proof is a simple exercise involving Wronskians, e.g., see [Kap, Chapter VI, §24, the Corollary on p. 41]. **q.e.d.**

Recall that when $y = y(z)$ is a non-zero solution a solution of (4.4) a linearly independent over \mathbb{C} is provided by

$$(4.6) \quad w = w(z) = y(z) \int \frac{1}{(y(t))^2} dt$$

(“reduction of order”), and so to understand the nature of the solutions of (4.4) we really need only understand the nature of a particular non-zero solution. This is where the differential Galois group can be quite helpful. In the following result we place the emphasis on the reducible case for illustrative purposes.

Theorem 4.7 : *Let $G \subset \text{SL}(2, \mathbb{C})$ denote the differential Galois group of (4.4).*

(a) (The Reducible Case) *The following statements are equivalent:*

- (i) *G is reducible;*
- (ii) *equation (4.4) has a solution of the form $y = e^{\int^z \theta(t) dt}$ with $\theta(z) \in K \simeq \mathbb{C}(z)$;*
- (iii) *the Riccati equation $w' + w^2 = r$ has a solution $\theta \in K$; and*
- (iv) *the linear operator $\mathcal{L} = \frac{d^2}{dz^2} - r$ factors in the non-commutative polynomial ring $K[\frac{d}{dz}]$, and when expressed as a product of monic polynomials that factorization must be*

$$\frac{d^2}{dz^2} - r = \left(\frac{d}{dz} + \theta\right)\left(\frac{d}{dz} - \theta\right),$$

where θ is as in (iii).

(b) (The Imprimitve Case) *When G is not reducible the following statements are equivalent:*

- (i) *G is imprimitive; and*
- (ii) *equation (4.4) has a solution of the form $y = e^{\int^z \theta(t) dt}$ with θ algebraic of degree 2 over K .*

(c) (The Remaining Finite Cases) *When G is not reducible and not imprimitive the following statements are equivalent:*

- (i) *G is finite; and*
- (ii) *all solutions of (4.4) are algebraic over K .*

(d) *When none of (a)-(c) hold $G = \text{SL}(2, \mathbb{C})$.*

Proof :

(a)

(i) \Rightarrow (ii) : By assumption there is a solution $y = y(z)$ of (4.4) such that for each $g \in G$ there is a $\lambda_g \in \mathbb{C}$ such that $g \cdot y = \lambda_g y$. (This can be seen by writing λ^{-1} in (3.2) as λ_g and using $y = y(z)$ as the second basis element.) Since g commutes with d/dz it follows that $g \cdot y' = (\lambda_g y)' = \lambda_g y'$. For $\theta := y'/y$, which we note implies $y = e^{\int \theta}$, we then have

$$g \cdot \theta = g \cdot (y'/y) = (g \cdot y') / (g \cdot y) = \lambda_g y' / \lambda_g y = y'/y = \theta,$$

and since K is the fixed field of G we conclude that $\theta \in K$.

(ii) \Rightarrow (i) : We have

$$\begin{aligned} \left(\frac{g \cdot y}{y}\right)' &= \frac{y g \cdot y' - y' g \cdot y}{y^2} \\ &= \frac{y g \cdot \theta y - \theta y g \cdot y}{y^2} \\ &= \frac{\theta(y g \cdot y - y g \cdot y)}{y^2} \\ &= 0, \end{aligned}$$

hence $\lambda_g := g \cdot y/y \in \mathbb{C}$. (In other words: when y is used as the second element of a basis the matrix of g is lower triangular.) Since $g \in G$ is arbitrary this gives reducibility.

(ii) \Leftrightarrow (iii) : For $y = e^{\int \theta}$ we have $y' = \theta y$ and $y'' = (\theta' + \theta^2)y$, hence $y'' = r y \Leftrightarrow \theta' + \theta^2 = r$.

(iii) \Leftrightarrow (iv) : From the chain-rule we have¹³ $\frac{d}{dz}t = t \frac{d}{dz} + t'$ for any $y \in K$, and when $s \in K$ also holds it follows that

$$\begin{aligned} \left(\frac{d}{dz} - s\right)\left(\frac{d}{dz} - t\right) &= \frac{d^2}{dz^2} - \frac{d}{dz}t - s \frac{d}{dz} + st \\ &= \frac{d^2}{dz^2} - \left(t \frac{d}{dz} + t'\right) - s \frac{d}{dz} + st \\ &= \frac{d^2}{dz^2} - (s + t) \frac{d}{dz} - t' + st, \end{aligned}$$

whereupon picking $t = -s := \theta$ we obtain

$$\left(\frac{d}{dz} + \theta\right)\left(\frac{d}{dz} - \theta\right) = \frac{d^2}{dz^2} - (\theta' + \theta^2).$$

The equivalence follows easily.

¹³The definition of $\frac{d}{dz}t : K \rightarrow K$ as an operator is $\frac{d}{dz}t : k \mapsto \frac{d}{dz}(tk)$. Since the chain-rule gives

$$\frac{d}{dz}(tk) = t \frac{d}{dz}k + \left(\frac{d}{dz}t\right) \cdot k = t \frac{d}{dz}k + t' \cdot k$$

we see that

$$\frac{d}{dz}t = t \frac{d}{dz} + t'.$$

- (b) See [Kov, §1.2 and 1.4].
- (c) By Theorems 3.4 and 1.2.
- (d) By Theorem 3.4.

q.e.d.

Write $r \in \mathbb{C}(z)$ as s/t , where $s, t \in \mathbb{C}[z]$ are relatively prime. The poles of r in the complex plane then coincide with the zeros of t , and the order of such a pole is the multiplicity of the corresponding zero. In the sequel “pole” will always mean “pole in the complex plane”. The *order of r at ∞* is defined to be $\deg(t) - \deg(s)$.

Theorem 4.8 (Kovacic) : *Necessary conditions in the first three respectively cases of Theorem 4.7 are as follows.*

Case I: *Any pole of r has order 1 or even order, and the order of r at ∞ must be even or else be greater than 2.*

Case II: *The rational function r must have at least one pole which is of order 2 or of odd order greater than 2.*

Case III: *The order of each pole of r cannot exceed 2 and the order of r at ∞ must be at least 2. Moreover, if the partial fraction expansion of r is*

$$r = \sum_i \frac{\alpha_i}{(z - c_i)^2} + \frac{\beta_j}{z - d_j},$$

and if $\gamma := \sum_i \alpha_i + \sum_j \beta_j d_j$, then each $\sqrt{1 + 4\alpha_i}$ must be a rational number, $\sum_j \beta_j = 0$ must hold, and $\sqrt{1 + 4\gamma}$ must also be a rational number.

A sketch of the argument for Case I should convey the spirit of the proof. First recall from Theorem 4.7(a) that $e^{\int \theta}$ is a solution of (4.4) if and only if $\theta' + \theta^2 = r$. One obtains the necessary conditions of Case I by substituting pole (i.e., Laurent) expansions of r and θ (in the second case with undetermined coefficients) into this equation and comparing exponents.

For the full proof see [Kov, §2.1, pp. 8-10].

Examples 4.9 :

- (a) *Airy's equation has no elementary solutions. More generally, equation (4.4) has no elementary solutions when r is a polynomial of odd degree.* (Airy's equation is introduced in Example 4.3(e).) The function r has no poles (in the complex plane), and the order at ∞ is an odd negative number. The necessary conditions of Cases I-III are therefore violated.
- (b) *Bessel's equation has elementary solutions if and only if ν is one-half of an odd integer.* Here the necessary conditions for Case III fail, but not those for Cases I and II. However, with a bit more work (which is carried out in [Kov, pages 14-15 and 19-20]) one can eliminate Case II and prove that Case I holds if and only if n has the stated form.

5. Examples of Differential Galois Group Calculations

In this section we specialize Example 4.3(c) to the case $m = 2$ (i.e., two finite singularities). Specifically, we consider the normal form

$$(5.1) \quad y'' + \frac{1}{4} \left(\sum_{j=1}^2 \frac{\hat{B}_j}{(z - a_j)^2} + \sum_{j=1}^2 \frac{\hat{C}_j}{z - a_j} \right) y = 0$$

of

$$w'' + \left(\sum_{j=1}^2 \frac{A_j}{z - a_j} \right) w' + \left(\sum_{j=1}^2 \frac{B_j}{(z - a_j)^2} + \sum_{j=1}^2 \frac{C_j}{z - a_j} \right) w = 0.$$

The hypergeometric and Riemann equations are particular cases.

The nature of the associated differential Galois group in this context is easily determined. (The results of this section are taken from [Ch].) To indicate how this is done define

$$A_3 := 2 - (A_1 + A_2), \quad B_3 := \sum_{j=1}^2 (B_j + C_j a_j),$$

and

$$t_j := -2 \cos \pi \sqrt{(A_j - 1)^2 - 4B_j}, \quad j = 1, 2, 3.$$

Examples 5.2 :

(a) For the hypergeometric equation one has

$$\begin{aligned} t_1 &= -2 \cos \pi(\gamma - 1) \\ t_2 &= -2 \cos \pi(\gamma - (\alpha + \beta)) \\ t_3 &= -2 \cos \pi(\alpha - \beta). \end{aligned}$$

(b) For Riemann's equation one has

$$t_j = -2 \cos \pi(\eta_j - \mu_j) \quad j = 1, 2, 3.$$

Now let

$$\sigma := t_1^2 + t_2^2 + t_3^2 - t_1 t_2 t_3.$$

Theorem 5.3 : *The differential Galois group of (5.1) is:*

- (a) *reducible if and only if $\sigma = 4$;*
- (b) *imprimitive but not reducible if and only if $\sigma \neq 4$ and at least two of t_1, t_2 and t_3 are zero;*
- (c_i) *projectively tetrahedral if and only if $\sigma = 2$ and $t_1, t_2, t_3 \in \{0, \pm 1\}$;*
- (c_{ii}) *projectively octahedral if and only if $\sigma = 3$ and $t_1, t_2, t_3 \in \{0, \pm 1, \pm\sqrt{2}\}$;*
- (c_{iii}) *projectively icosahedral if and only if $\sigma \in \{2 - \mu_2, 3, 2 + \mu_1\}$ and $t_1, t_2, t_3 \in \{0, \pm\mu_2, \pm 1, \pm\mu_1\}$, where $\mu_1 := \frac{1}{2}(1 + \sqrt{5})$ and $\mu_2 = -\frac{1}{2}(1 - \sqrt{5}) = \mu_1^{-1}$; and*
- (d) *otherwise is $\text{SL}(2, \mathbf{C})$.*

For a proof¹⁴ see [Ch], and for a generalization of assertions (c_i)-(c_{iii}) see [McCull].

Examples 5.4 :

- (a) For the hypergeometric equation one can use Theorem 5.3 to conclude that the reducible case holds for the normal form if and only if at least one of $\alpha, \beta, \gamma - \alpha$ and $\gamma - \beta$ is an integer¹⁵. (The argument is not quite straightforward.) Of course with additional work one can say much more. In particular, using the theorem one can reproduce the result of Schwarz on algebraic solutions discussed in §1.
- (b) For Riemann's equation the reducible case holds for the normal form if and only if at least one of the four quantities $\eta_1 + \eta_2 + \eta_3, \eta_1 + \eta_2 + \mu_3, \eta_1 + \mu_2 + \eta_3$ and $\mu_1 + \eta_2 + \eta_3$ is an integer¹⁶.
- (c) Legendre's equation is

$$w'' - \frac{2z}{1-z^2}w' + \frac{\lambda}{1-z^2}w = 0,$$

where $\lambda \in \mathbb{R}$. The normal form is

$$y'' + \frac{1}{4} \left(\frac{1}{(z-1)^2} + \frac{1}{(z+1)^2} - \frac{2\lambda+1}{z-1} + \frac{2\lambda+1}{z+1} \right) y = 0.$$

¹⁴A proof of (a) can also be found in [B-C, Proposition 2.22, pgs 1647-8].

¹⁵See, e.g., [B-C, Theorem 2.24 and Corollary 2.27, p. 1648]. For a classical perspective on this condition see [Poole, Chapter VI, §23, p. 90].

¹⁶See, e.g., [B-C, Corollary 2.27, p. 1648].

Here one computes that

$$t_1 = t_2 = -2, \quad t_3 = -2 \cos \pi \sqrt{1 + 4\lambda}$$

and

$$\sigma = 4 \left(\cos(\pi \sqrt{1 + 4\lambda}) + 1 \right)^2 + 4.$$

Using Theorem 5.3 one sees that the differential Galois group of the normal form is reducible if and only if $\lambda = k(k+1)$, where k is an integer, and otherwise is $\mathrm{SL}(2, \mathbb{C})$.

6. A Brief Digression on Derivations

In §7 we will indicate how a linear differential equation as in (1.1) can be viewed as a coordinate-description of an entity known as a “differential structure”, and in §8 and §9 we will show that associated differential Galois group is intrinsically associated with that structure, not simply with the equation. Our treatment will be purely algebraic, in the spirit of differential algebra¹⁷. A few preliminaries are required.

Let R be a (not necessarily commutative) ring with identity. An additive group endomorphism $\delta : r \in R \mapsto r' \in R$ is a *derivation* if the *Leibniz rule*

$$(6.1) \quad (rs)' = rs' + r's$$

holds for all $r, s \in R$. One also writes r' as $r^{(1)}$ and defines $r^{(n)} := (r^{(n-1)})'$ for $n \geq 2$. The notation $r^{(0)} := r$ also proves convenient.

The usual derivative $\frac{d}{dz}$ on the field $\mathbb{C}(z)$ of rational functions on the Riemann sphere \mathbb{P}^1 is the basic example of a derivation. The same derivation is described in terms of the usual coordinate $t = 1/z$ at ∞ by $-t^2 \frac{d}{dt}$, i.e., both operators can be viewed as coordinate descriptions of the same derivation on the field $\mathcal{M}(\mathbb{P}^1)$ of meromorphic functions on \mathbb{P}^1 . For a second example of a derivation note that the zero mapping $r \in R \mapsto 0 \in R$ satisfies the required properties; this is the *trivial derivation*.

For a non-commutative example choose an integer $n > 1$, let R be the collection of $n \times n$ matrices with entries in a commutative ring A with a derivation $a \mapsto a'$, and for $r = (a_{ij}) \in R$ define $r' := (a'_{ij})$.

When $r \mapsto r'$ is a derivation on R one sees from (6.1) that $1' = (1 \cdot 1)' = 1 \cdot 1' + 1' \cdot 1$ and as a result that

$$(6.2) \quad 1' = 0.$$

When $r \in R$ is a unit it then follows from $1 = rr^{-1}$ and (6.1) that

$$0 = (rr^{-1})' = r \cdot (r^{-1})' + r' \cdot r^{-1},$$

whence

$$(6.3) \quad (r^{-1})' = -r^{-1} \cdot r' \cdot r^{-1}.$$

This formula is particularly useful in the matrix example given above. When R is commutative it assumes the more familiar form

$$(6.4) \quad (r^{-1})' = -r'/r^2.$$

¹⁷Although now a bit out-dated, [Kol] remains the basic reference for the subject.

The ring assumption suggests the generality of the concept of a derivation, but our main interest will be in derivations on fields. In this regard we note that any derivation on an integral domain extends uniquely via the quotient rule to the quotient field.

Henceforth K denotes a *differential field* (of characteristic 0), i.e., a field K equipped with a non-trivial derivation $k \mapsto k'$. By a *constant* we mean an element $k \in K$ satisfying $k' = 0$, e.g., we see from (6.2) that $1 \in R$ has this property. Indeed, the collection $K_C \subset K$ of constants is easily seen to be a subfield containing \mathbb{Q} ; this is the *field of constants* (of $K = (K, \delta)$).

When $K = \mathbb{C}(z)$ with derivation $\frac{d}{dz}$ we have $K_C = \mathbb{C}$.

The determinant

$$(6.5) \quad W := W(k_1, \dots, k_n) := \det \begin{pmatrix} k_1 & k_2 & \cdots & & k_n \\ k_1' & k_2' & & \vdots & k_n' \\ k_1^{(2)} & k_2^{(2)} & & & \vdots \\ \vdots & & & & \vdots \\ k_1^{(n-1)} & k_2^{(n-1)} & \cdots & \cdots & k_n^{(n-1)} \end{pmatrix}$$

is the *Wronskian* of the elements $k_1, \dots, k_n \in K$. This entity is useful for determining linear (in)dependence over K_C .

Proposition 6.6 : *Elements k_1, \dots, k_n of a differential field K are linearly dependent over the field of constants K_C if and only if their Wronskian is 0.*

Proof :

\Rightarrow For any $c_1, \dots, c_n \in K_C$ and any $0 \leq m \leq n$ we have $(\sum_j c_j k_j)^{(m)} = \sum_j c_j k_j^{(m)}$. In particular, when $\sum_j c_j k_j = 0$ the same equality holds when k_j is replaced by the j^{th} column of the Wronskian and 0 is replaced by a column of zeros. The forward assertion follows.

\Leftarrow The vanishing of the Wronskian implies a dependence relation (over K) among columns, and as a result there must be elements $c_1, \dots, c_n \in K$, not all 0, such that

$$(i) \quad \sum_{j=1}^n c_j k_j^{(m)} = 0 \quad \text{for} \quad m = 0, \dots, n-1.$$

What requires proof is that the c_j may be chosen in K_C , and this we establish by induction on n . As the case $n = 1$ is trivial we assume $n > 1$ and that the result holds for any subset of K with at most $n - 1$ elements.

If there is also a dependence relation (over K) among the columns of the Wronskian of y_2, \dots, y_n , e.g., if $c_1 = 0$, then by the induction hypothesis the elements $y_2, \dots, y_n \in K$ must be linearly dependent over K_C . But the same then holds for y_1, \dots, y_n , which is precisely what we want to prove. We therefore assume (w.l.o.g.) that $c_1 = 1$ and that the columns of the Wronskian of y_2, \dots, y_k are linearly independent over K . From (i) we then have

$$0 = \left(\sum_{j=1}^n c_j k_j^{(m)} \right)' = \sum_{j=1}^n c_j k_j^{(m+1)} + \sum_{j=2}^n c_j' k_j^{(m)} = 0 + \sum_{j=2}^n c_j' k_j^{(m)} = \sum_{j=2}^n c_j' k_j^{(m)}$$

for $m = 0, \dots, n - 2$, thereby forcing $c_2' = \dots = c_n' = 0$. But this means $c_j \in K_C$ for $j = 1, \dots, n$, and the proof is complete. **q.e.d.**

7. Differential Structures

In this section K denotes a differential field with derivation $k \mapsto k'$ and V is a K -space (i.e., a vector space over K). We view the elements of K^n , for any integer $n \geq 1$, as column vectors, i.e., as $n \times 1$ matrices. The collection of $n \times n$ matrices with entries in K is denoted $\mathfrak{gl}(n, K)$.

A *differential structure* on V is an additive group homomorphism $D : V \rightarrow V$ satisfying

$$(7.1) \quad D(kv) = k'v + kDv, \quad k \in K, \quad v \in V,$$

where Dv abbreviates $D(v)$. The *Leibniz rule* terminology is also used with (7.1). Vectors $v \in V$ satisfying $Dv = 0$ are said to be *horizontal*. The zero vector $0 \in V$ is always has this property; other such vectors need not exist.

When $D : V \rightarrow V$ is a differential structure the pair (V, D) is called a *differential module*.

As an example of a differential structure take $V := K^n$, regard the elements of V as column vectors, and define

$$(7.2) \quad D \begin{pmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{pmatrix} := \begin{pmatrix} k'_1 \\ k'_2 \\ \vdots \\ k'_n \end{pmatrix}.$$

Further examples will be evident from Proposition 7.10.

Since K_C is a subfield of K we can regard V as a vector space over K_C by restricting scalar multiplication to $K_C \times V$.

Proposition 7.3 :

- (a) Any differential structure $D : V \rightarrow V$ is K_C -linear.
- (b) The collection of horizontal vectors of a differential structure $D : V \rightarrow V$ coincides with the kernel $\ker D$ of D when D is considered as a K_C -linear mapping¹⁸.
- (c) The horizontal vectors of a differential structure $D : V \rightarrow V$ constitute a K_C -subspace of (the K_C -space) V .

¹⁸When D is not linear the “kernel” terminology is generally replaced by “zero set” or “vanishing set”, or is indicated by means of the notation $D^{-1}(\{0\})$.

Proof :

- (a) Immediate from (7.1).
- (b) Obvious from the definition of horizontal.
- (c) Immediate from (b).

q.e.d.

A differential structure can be viewed as a coordinate-free formulation of a first-order system of linear ordinary differential equations. Specifically, suppose V is finite-dimensional, $\mathbf{e} = (e_j)_{j=1}^n \subset V^n$ is a(n ordered) basis, and $B = (b_{ij}) \in \mathfrak{gl}(n, K)$ is defined by

$$(7.4) \quad De_j := \sum_{i=1}^n b_{ij}e_i, \quad j = 1, \dots, n.$$

(Example: For D as in (7.2) and¹⁹ $e_j = (0, \dots, 0, 1, 0, \dots, 1)^\tau$ [1 in slot j] for $j = 1, \dots, n$ we have $B = (0)$ [the zero matrix].) We refer to B as the *defining (e)-matrix* of D , or as the *defining matrix of D relative to the basis \mathbf{e}* . Note that for any $v = \sum_{j=1}^n v_j e_j \in V$ the Leibniz rule (7.1) gives

$$(7.5) \quad Dv = \sum_{i=1}^n (v'_i + \sum_{j=1}^n b_{ij}v_j)e_i.$$

If for any $w = \sum_{j=1}^n w_j e_j \in V$ we write $w_{\mathbf{e}}$ (resp. $w'_{\mathbf{e}}$) for the column vector with j^{th} -entry w_j (resp. w'_j) this last equality can be expressed in the matrix form

$$(7.6) \quad (Dv)_{\mathbf{e}} = v'_{\mathbf{e}} + Bv_{\mathbf{e}},$$

and we conclude that $v \in V$ is horizontal if and only if $v_{\mathbf{e}}$ is a solution of the first-order linear system

$$(7.7) \quad x' + Bx = 0,$$

wherein $x = (x_1, \dots, x_n)^\tau$. This is the *defining (e)-equation* of D .

Linear systems of ordinary differential equations of the form (7.7) are called *homogeneous*. One can also ask for solutions of *inhomogeneous* systems, i.e., systems of the form

$$(7.8) \quad x' + Bx = b,$$

¹⁹The superscript τ (“tau”) denotes transposition.

wherein $0 \neq b \in K^n$ is given. For $b = w_e$ this is equivalent to the search for a vector $v \in V$ satisfying

$$(7.9) \quad Dv = w.$$

Equation (7.7) is the *homogeneous equation corresponding to (7.8)*.

Proposition 7.10 : *When $\dim_K V < \infty$ and e is a basis the correspondence between differential structures $D : V \rightarrow V$ and $n \times n$ matrices B defined by (7.4) is bijective; the inverse assigns to a matrix $B \in \mathfrak{gl}(n, K)$ the differential structure $D : V \rightarrow V$ defined by (7.6).*

Proof : The proof is by routine verification.

q.e.d.

Since the correspondence between matrices $B \in \mathfrak{gl}(n, K)$ and linear systems $x' + Bx$ is also bijective, the statement opening the paragraph surrounding (7.4) should now be clear.

Proposition 7.11 :

- (a) *The solutions of (7.7) within K^n form a vector space over K_C .*
- (b) *When $\dim_K V = n < \infty$ and e is a basis of v the K -linear isomorphism $v \in V \mapsto v_e \in K^n$ restricts to a K_C -linear isomorphism between the K_C -subspace of V consisting of horizontal vectors and the K_C -subspace of K^n consisting of solutions of (7.7).*

Proof :

- (a) When $y_1, y_2 \in K^n$ are solutions and $c_1, c_2 \in K_C$ we have

$$\begin{aligned} (c_1 y_1 + c_2 y_2)' &= (c_1 y_1)' + (c_2 y_2)' \\ &= c_1' y_1 + c_1 y_1' + c_2' y_2 + c_2 y_2' \\ &= 0 \cdot y_1 + c_1(-B y_1) + 0 \cdot y_2 + c_2(-B y_2) \\ &= -B c_1 y_1 - B c_2 y_2 \\ &= -B(c_1 y_1 + c_2 y_2). \end{aligned}$$

- (b) That the mapping restricts to a bijection between horizontal vectors and solutions was already noted immediately before (7.7), and since the correspondence $v \mapsto v_e$ is K -linear and K_C is a subfield of K any restriction to a K_C -subspace must be K_C -linear.

q.e.d.

Suppose $\hat{\mathbf{e}} = (\hat{e}_j)_{j=1}^n \subset V^n$ is a second basis and $P = (p_{ij})$ is the transition matrix, i.e., $e_j = \sum_{i=1}^n p_{ij} \hat{e}_i$. Then the defining \mathbf{e} and $\hat{\mathbf{e}}$ -matrices B and A of D are easily seen to be related by

$$(7.12) \quad A := P^{-1}BP + P^{-1}P',$$

where $P' := (p'_{ij})$. The transition from B to A is viewed classically as a change of variables: substitute $x = Pw$ in (7.7); then note from

$$0 = (Pw)' + BPw = Pw' + P'w + BPw$$

that

$$w' + (P^{-1}BP + P^{-1}P')w = 0.$$

The modern viewpoint is to regard $(B, P) \mapsto P^{-1}BP + P^{-1}P'$ as defining a right action of $GL(n, K)$ on $\mathfrak{gl}(n, K)$; this is the action by *gauge transformations*.

The concept of an n^{th} -order linear homogeneous equation in the context of a differential field K is formulated in the obvious way: an element $k \in K$ is a solution of

$$(7.13) \quad y^{(n)} + \ell_1 y^{(n-1)} + \cdots + \ell_{n-1} y' + \ell_n y = 0,$$

where $\ell_1, \dots, \ell_n \in K$, if and only if

$$(7.14) \quad k^{(n)} + \ell_1 k^{(n-1)} + \cdots + \ell_{n-1} k' + \ell_n k = 0,$$

where $k^{(2)} := k'' := (k')'$ and $k^{(j)} := (k^{(j-1)})'$ for $j > 2$. Using a Wronskian argument one can easily prove that (7.13) has at most n solutions (in K) linearly independent over K_C .

As in the classical case $k \in K$ is a solution of (7.13) if and only if the column vector $(k, k', \dots, k^{(n-1)})^\tau$ is a solution of

$$(7.15) \quad x' + Bx = 0, \quad B = \begin{pmatrix} 0 & -1 & 0 & \cdots & 0 \\ \vdots & 0 & -1 & & \vdots \\ & & 0 & \ddots & \\ & & & \ddots & -1 & 0 \\ & & & & 0 & -1 \\ \ell_n & \ell_{n-1} & \cdots & \cdots & \ell_2 & \ell_1 \end{pmatrix}.$$

Indeed, one has the following analogue of Proposition 7.11.

Proposition 7.16 :

- (a) *The solutions of (7.13) within K form a vector space over K_C .*
- (b) *The K_C -linear mapping $(y, y', \dots, y^{(n-1)})^\tau \in K^n \mapsto y \in K$ restricts to a K_C -linear isomorphism between the K_C -subspace of V consisting of horizontal vectors and the K_C -subspace of K described in (a).*

Proof : The proof is a routine verification.

q.e.d.

Example 7.17 : Assume $K = \mathbb{C}(z)$ with derivation $\frac{d}{dz}$ and consider the first-order system

$$(i) \quad x' + \begin{pmatrix} \left(\frac{6z^4 + (1-2\nu^2)z^2 - 1}{z(2z^4 - 1)} \right) & \frac{4z^6 - 4\nu^2 z^4 - 8z^2 + 1}{z^4(2z^4 - 1)} \\ - \left(\frac{z^2(z^4 + z^2 - \nu^2)}{2z^4 - 1} \right) & \frac{(2\nu^2 - 1)z^2 + 3}{z(2z^4 - 1)} \end{pmatrix} x = 0,$$

i.e.,

$$\begin{aligned} x'_1 + \left(\frac{6z^4 + (1-2\nu^2)z^2 - 1}{z(2z^4 - 1)} \right) x_1 + \left(\frac{4z^6 - 4\nu^2 z^4 - 8z^2 + 1}{z^4(2z^4 - 1)} \right) x_2 &= 0 \\ x'_2 - \left(\frac{z^2(z^4 + z^2 - \nu^2)}{2z^4 - 1} \right) x_1 + \left(\frac{(2\nu^2 - 1)z^2 + 3}{z(2z^4 - 1)} \right) x_2 &= 0 \end{aligned} ,$$

wherein ν is a complex parameter. This has the form (7.7) with

$$B := \begin{pmatrix} \left(\frac{6z^4 + (1-2\nu^2)z^2 - 1}{z(2z^4 - 1)} \right) & \frac{4z^6 - 4\nu^2 z^4 - 8z^2 + 1}{z^4(2z^4 - 1)} \\ - \left(\frac{z^2(z^4 + z^2 - \nu^2)}{2z^4 - 1} \right) & \frac{(2\nu^2 - 1)z^2 + 3}{z(2z^4 - 1)} \end{pmatrix},$$

and with the choice

$$P := \begin{pmatrix} \frac{-1}{z^2(2z^4 - 1)} & \frac{2z}{2z^4 - 1} \\ \frac{z^3}{2z^4 - 1} & \frac{-z^2}{2z^4 - 1} \end{pmatrix}$$

one sees that the transformed system

$$(ii) \quad x' + Ax = 0, \quad \text{where} \quad A := P^{-1}BP + P^{-1}P' = \begin{pmatrix} 0 & -1 \\ 1 - \frac{\nu^2}{z^2} & -\frac{1}{z} \end{pmatrix},$$

assumes the form seen in (7.15). The system (i) is thereby reduced to

$$(iii) \quad y'' + \frac{1}{z}y' + \left(1 - \frac{\nu^2}{z^2} \right) y = 0,$$

i.e., to Bessel's equation (recall Example 4.3(d)).

We regard (i)-(ii) as distinct basis descriptions of the same differential structure, and (iii) and (iv) as additional ways of describing that structure.

Converting the n^{th} -order equation (7.13) to the first-order system (7.15) is standard practice. Less well-known is the fact that any first-order system of n equations can be converted to the form (7.15), and as a consequence can be expressed n^{th} -order form²⁰. For many purposes n^{th} -order form has distinct advantages, e.g., explicit solutions are often easily constructed with series expansions.

Proposition 7.18 : *When V is a K -space with differential structure $D : V \rightarrow V$ the following assertions hold.*

- (a) *A collection of horizontal vectors within V is linearly independent over K if and only if it is linearly independent over K_C .*
- (b) *The collection of horizontal vectors of V is a vector space over K_C of dimension at most $\dim_K(V)$.*

Proof :

(a) \Rightarrow Immediate from the inclusion $K_C \subset K$. (In this direction the horizontal assumption is unnecessary.)

\Leftarrow If the implication is false there is a collection of horizontal vectors in V which is K_C -(linearly) independent but K -dependent, and from this collection we can choose vectors v_1, \dots, v_m which are K -dependent with $m > 1$ minimal w.r.t. this property. We can then write $v_m = \sum_{j=1}^{m-1} k_j v_j$, with $k_j \in K$, whereupon applying D and the hypotheses $Dv_j = 0$ results in the identity $0 = \sum_{j=1}^{m-1} k'_j v_j$. By the minimality of m this forces $k'_j = 0$, $j = 1, \dots, m-1$, i.e., $k_j \in K_C$, and this contradicts linear independence over K_C .

(b) This is immediate from (a) and the fact that any K -linearly independent subset of V can be extended to a basis.

q.e.d.

Suppose $\dim_K V = n < \infty$, \mathbf{e} is a basis of V , and $x' + Ax = 0$ is the defining \mathbf{e} -equation of D . Then assertion (c) of the preceding result has the following standard formulation.

Corollary 7.19 : *For any matrix $B \in \mathfrak{gl}(n, K)$ a collection of solutions of*

$$(i) \quad x' + Bx = 0$$

within K^n is linearly independent over K if and only if the collection is linearly independent over K_C . In particular, the K_C -subspace of K^n consisting of solutions of (i) has dimension at most $\dim_K V$.

²⁰See, e.g., [C-K].

Proof : By Proposition 7.11.

q.e.d.

Equation (i) of Corollary 7.19 is always satisfied by the column vector $x = (0, 0, \dots, 0)^\tau$; this is the *trivial solution*, and any other is *non-trivial*. Unfortunately, non-trivial solutions (with entries in K) need not exist. For example, the linear differential equation $y' - y = 0$ admits only the trivial solution in the field $\mathbb{C}(z)$: for non-trivial solutions one must recast the problem so as to include the extension field $(\mathbb{C}(z))(\exp(z))$.

Corollary 7.20 : For any elements $\ell_1, \dots, \ell_{n-1} \in K$ a collection of solutions $\{y_j\}_{j=1}^m \subset K$ of

$$(i) \quad y^{(n)} + \ell_1 y^{(n-1)} + \dots + \ell_{n-1} y' + \ell_n y = 0$$

is linearly independent over K_C if and only if the collection $\{(y_j, y_j', \dots, y_j^{(n-1)})\}_{j=1}^m$ is linearly independent over K . In particular, the K_C -subspace of K consisting of solutions of (i) has dimension at most n .

Proof : Use Proposition 7.16(b) and Corollary 7.19.

q.e.d.

A non-singular matrix $M \in \mathfrak{gl}(n, K)$ is a *fundamental matrix solution* of

$$(7.21) \quad x' + Ax = 0, \quad A \in \mathfrak{gl}(n, K),$$

if M satisfies this equation, i.e., if

$$(7.22) \quad M' + AM = 0,$$

wherein $0 \in \mathfrak{gl}(n, K)$ represents the zero matrix.

Proposition 7.23 : A matrix $M \in \mathfrak{gl}(n, K)$ is a *fundamental matrix solution* of (4.4) if and only if the columns of M constitute n solutions of that equation linearly independent over K_C .

Of course linear independence over K is equivalent to the non-vanishing of the Wronskian $W(y_1, \dots, y_n)$.

Proof : First note that (7.22) holds if and only if the columns of M are solutions of (4.4). Next observe that M is non-singular if and only if these columns are linearly independent over K . Finally, note from Propositions 7.11(b) and 7.18(a) that this will be the case if and only if these columns are linearly independent over K_C . **q.e.d.**

Proposition 7.24 : *Suppose $M, N \in \mathfrak{gl}(n, K)$ and M is a fundamental matrix solution of (4.4). Then N is a fundamental matrix solution if and only if $N = MC$ for some matrix $C \in \mathfrak{gl}(n, K_C)$.*

Proof : B

\Rightarrow : By (6.3) we have

$$\begin{aligned}
 (M^{-1}N)' &= M^{-1} \cdot N' = (M^{-1})' \cdot N \\
 &= M^{-1} \cdot (-AN) + (-M^{-1}M'M^{-1}) \cdot N \\
 &= -M^{-1}AN + (-M^{-1})(-AM)(-M^{-1})N \\
 &= -M^{-1}AN + M^{-1}AN \\
 &= 0.
 \end{aligned}$$

\Leftarrow : We have $N' = (MC)' = M'C = -AM \cdot C = -A \cdot MC = -AN$.

q.e.d.

8. Extensions of Differential Structures

Here K is a differential field with derivation $k \mapsto k'$, V is a K -space (i.e., a vector space over K) of dimension n , and $D : V \rightarrow V$ is a differential structure. Primes ' will also be used to indicate the derivation on any differential extension field $L \supset K$.

Recall²¹ that when $L \supset K$ is an extension field of K (not necessarily differential) the tensor product $L \otimes_K V$ over K admits an L -space structure characterized by $\ell \cdot (m \otimes_K v) = (\ell m) \otimes_K v$, and this structure will always be assumed. By means of the K -embedding

$$(8.1) \quad v \in V \mapsto 1 \otimes v \in L \otimes_K V$$

one views V as a K -subspace of $L \otimes_K V$ when the latter is considered as a K -space. In particular, any (ordered) basis \mathbf{e} of V can be regarded as a subset of $L \otimes_K V$.

Proposition 8.2 (“Extension of the Base”) : *Assuming the notation of the previous paragraph any basis of the K -space V is also a basis of the L -space $L \otimes_K V$. In particular,*

$$(i) \quad \dim_K V = \dim_L(L \otimes_K V).$$

Proof : See, e.g., [Lang, Chapter XVI, §4, Proposition 4.1, p. 623]. **q.e.d.**

Proposition 8.3 : *Suppose W , \hat{V} and \hat{W} are finite-dimensional²² K -spaces and $T : V \rightarrow W$ and $\hat{T} : \hat{V} \rightarrow \hat{W}$ are K -linear mappings. Then there is a K -linear mapping $T \otimes_K \hat{T} : V \otimes_K \hat{V} \rightarrow W \otimes_K \hat{W}$ characterized by*

$$(i) \quad (T \otimes_K \hat{T})(v \otimes_K \hat{v}) = Tv \otimes_K \hat{T}\hat{v}, \quad v \otimes_K \hat{v} \in V \otimes_K \hat{V}.$$

Proof²³ : There is a standard characterization of the tensor product $V \otimes_K \hat{V}$ in terms of K -bilinear mappings of $V \times \hat{V}$ into K -spaces Y , e.g., see [Lang, Chapter XVI, §1, p. 602]. The proposition results from considering the K -bilinear mapping $(v, \hat{v}) \in V \times \hat{V} \mapsto Tv \otimes_K \hat{T}\hat{v} \in W \otimes_K \hat{W}$. **q.e.d.**

²¹As a general reference for the remarks in this paragraph see, e.g., [Lang, Chapter XVI, §4, pp. 623-4, particularly Example 2]. Except for references to bases, most of what we say does not require V to be finite-dimensional.

²²The finite-dimensional hypothesis is not needed; it is assumed only because this is a standing hypothesis for V .

²³We offer only a quick sketch. The result is more important for our purposes than a formal proof, and filling in all the details would lead us too far afield.

Proposition 8.4 : *To any differential field extension $L \supset K$ there corresponds a unique differential structure $D_L : L \otimes_K V \rightarrow L \otimes_K V$ extending $D : V \rightarrow V$, and this structure is characterized by the property*

$$(i) \quad D_L(\ell \otimes_K V) = \ell' \otimes_K v + \ell \otimes_K Dv, \quad \ell \otimes_K v \in L \otimes_K V.$$

Recall from (8.1) that we are viewing V as a K -subspace of $L \otimes_K V$ by identifying V with its image under the embedding $v \mapsto 1 \otimes_K v$. Assuming (i) we have $D_L(1 \otimes_K v) = 1 \otimes_K Dv \simeq Dv$ for any $v \in V$, and this is the meaning of D_L “extending” D .

In the proof we denote the derivation $\ell \mapsto \ell'$ by $\delta : L \rightarrow L$, and we also write the restriction $\delta|_K$ as δ .

One is tempted to prove the proposition by invoking Proposition 8.3 so as to define mappings $\delta \otimes_K \text{id}_V : L \otimes_K V \rightarrow L \otimes_K V$ and $\text{id}_L \otimes_K D : L \otimes_K V \rightarrow L \otimes_K V$ and to then set $D_L := \delta \otimes_K \text{id}_V + \text{id}_L \otimes_K D$. Unfortunately, Proposition 8.3 does not apply since D is not K -linear.

Proof²⁴ : The way around the problem is to first use the fact that D is K_C -linear; one can then conclude from Proposition 8.3 (with K replaced by K_C) that a K_C -linear mapping $\hat{D} : L \otimes_{K_C} V \rightarrow L \otimes_{K_C} V$ is defined by

$$(ii) \quad \hat{D} := \delta \otimes_{K_C} \text{id}_V + \text{id}_{K_C} \otimes_{K_C} D.$$

The next step is to define $Y \subset L \otimes_{K_C} V$ to be the K_C -subspace generated by all vectors of the form $\ell k \otimes_{K_C} v - \ell \otimes_{K_C} kv$, where $\ell \in L$, $k \in K$ and $v \in V$. Then from the calculation

$$\begin{aligned} \hat{D}(\ell k \otimes_{K_C} v - \ell \otimes_{K_C} kv) &= \delta(\ell k) \otimes_{K_C} v + \ell k \otimes_{K_C} Dv \\ &\quad - \delta(\ell) \otimes_{K_C} kv - \ell \otimes_{K_C} D(kv) \\ &= \ell k' \otimes_{K_C} v + k \ell' \otimes_{K_C} v + \ell k \otimes_{K_C} Dv \\ &\quad - \ell' \otimes_{K_C} kv - \ell \otimes_{K_C} (k'v + kDv) \\ &= \ell k' \otimes_{K_C} v - \ell \otimes_{K_C} k'v \\ &\quad + \ell' k \otimes_{K_C} v - \ell \otimes_{K_C} k'v \\ &\quad + \ell k \otimes_{K_C} Dv - \ell \otimes_{K_C} kDv \end{aligned}$$

²⁴Footnote 23 applies here also.

we see that Y is \hat{D} -invariant, and \hat{D} therefore induces a K_C -linear mapping $\tilde{D} : (L \otimes_{K_C} V)/Y \rightarrow (L \otimes_{K_C} V)/Y$ which by (ii) satisfies

$$(iii) \quad \tilde{D}([\ell \otimes_{K_C} v]) = [\ell' \otimes_{K_C} v] + [\ell \otimes_{K_C} Dv],$$

where the bracket $[\]$ denotes the equivalence class (i.e., coset) of the accompanying element.

Now observe that when $L \otimes_{K_C} V$ is viewed as an L -space (*resp.* K -space), Y becomes an L -subspace (*resp.* a K -subspace), and it follows from (iii) that \tilde{D} is a differential structure when the L -space (*resp.* K -space) structure is assumed.

In view of the K -space structure on $(L \otimes_{K_C} V)/Y$ the K -bilinear mapping²⁵ $(\ell, v) \mapsto [\ell \otimes_{K_C} v]$ induces a K -linear mapping $T : L \otimes_K V \rightarrow (L \otimes_{K_C} V)/Y$ which one verifies to be K -isomorphism. It then follows from (iii) and (iv) that the mapping $D_L := T^{-1} \circ \tilde{D} \circ T : L \otimes_K V \rightarrow L \otimes_K V$ satisfies (i), and it follows that D_L is a differential structure on the L -space $L \otimes_K V$.

As for uniqueness, suppose $\check{D} : L \otimes_K V \rightarrow L \otimes_K V$ is any differential structure extending D , i.e., having the property

$$\check{D}(1 \otimes_K v) = 1 \otimes_K Dv, \quad v \in V.$$

Then for any $\ell \otimes_K v \in L \otimes_K V$ one has

$$\begin{aligned} \check{D}(\ell \otimes_K v) &= \check{D}(\ell \cdot (1 \otimes_K v)) \\ &= \ell' \cdot (1 \otimes_K v) + \ell \cdot \check{D}(1 \otimes_K v) \\ &= \ell' \otimes_K v + \ell \cdot (1 \otimes_K Dv) \\ &= \ell' \otimes_K v + \ell \otimes_K Dv \\ &= D_L(\ell \otimes_K v), \end{aligned}$$

hence $\check{D} = D_L$.

q.e.d.

When considered over the differential field $\mathbb{C}(z) = (\mathbb{C}(z), \frac{d}{dz})$ the linear differential equation $y'' = y$, has only the trivial solution, but if we “allow solutions” from the differential field extension $\mathbb{C}(z)(\exp(z)) = (\mathbb{C}(z)\exp(z), \frac{d}{dz})$ this is no longer the case. At the conceptual level, “allowing solutions from a differential field extension” simply means considering extensions of the given differential structure. However, at the computational level these extensions play no role, as one sees from the following result.

²⁵Which we note is not L -bilinear, since for $v \in V$ the product ℓv is only defined when $\ell \in K$.

Proposition 8.5 : *Suppose \mathbf{e} is a basis of V and*

$$(i) \quad x' + Bx = 0$$

is the defining \mathbf{e} -equation for D . Let $L \supset K$ be a differential field extension and consider \mathbf{e} as a basis for the L -space $L \otimes_K V$. Then the defining \mathbf{e} -equation for the extended differential structure $D_L : L \otimes_K V \rightarrow L \otimes_K V$ is also (i).

Proof : Since D_L extends D the \mathbf{e} matrices of these two differential structures are the same. **q.e.d.**

Proposition 8.6 : *Suppose \mathbf{e} and $\hat{\mathbf{e}}$ are two bases of V and*

$$x' + Bx = 0$$

and

$$x' + Ax = 0$$

are the defining \mathbf{e} and $\hat{\mathbf{e}}$ -equations of D respectively. Let $L \supset K$ be a differential field extension in which both equations have fundamental matrix solutions. Then the field extensions of K generated by the entries of the fundamental matrix solutions are the same.

Proof : For the transition matrix $P \in \text{GL}(n, K)$ between bases we have²⁶ $A = P^{-1}BP + P^{-1}P'$, and all the entries of P , P^{-1} and P' belong to K . **q.e.d.**

²⁶Recall the discussion surrounding (7.12).

9. An Intrinsic Definition of the Differential Galois Group

Here K is a differential field and (V, D) is a differential module. We assume $\dim_K V = n < \infty$.

When $L \supset K$ is a differential field extension one also has $L_C \supset K_C$ for the corresponding fields of constants. When $L_C = K_C$ one speaks of an extension with *no new constants*, or of a *no new constants* extension. This is automatically the case with the extensions of fields of germs of meromorphic functions considered in the early sections of the notes. In a purely algebraic setting it is often a crucial hypothesis.

A *Picard-Vessiot extension* of (V, D) is a differential field extension $L \supset K$ satisfying the following conditions:

- (a) the extension has no new constants;
- (b) the L -space $L \otimes_K V$ admits a basis consisting of horizontal vectors of D_L ;
- (c) when $M \supset K$ is any other differential extension satisfying (a) and (b) there is an field embedding $\varphi : L \rightarrow M$ over K which commutes with the derivations δ_K and δ_M on L and M respectively, i.e., which satisfies

$$(9.1) \quad \varphi \circ \delta_L = \delta_M \circ \varphi;$$

and

- (d) any field embedding $\eta : L \rightarrow L$ over K which commutes with δ_L is an automorphism.

The *differential Galois group* of (V, D) corresponding to an associated Picard-Vessiot extension is the group G_L of automorphisms of L over K which commute with the derivation δ_L on L . This group obviously depends on L , but only up to isomorphism. Indeed, when $M \supset K$ is any other Picard-Vessiot extension for (V, D) we have field embeddings $\varphi_{LM} : L \rightarrow M$ and $\varphi_{ML} : M \rightarrow L$ as in (c), and by (d) the composition $\eta := \varphi_{ML} \circ \varphi_{LM} : L \rightarrow L$ must be an automorphism. When $g \in G_M$ we see from (d) that the mapping $\ell \in L \mapsto \varphi_{ML}(g \cdot \varphi_{LM}(\ell))$ is in G_L , and one sees easily that this establishes an isomorphism between G_M and G_L . One therefore refers to G_L as “the” differential Galois group of (V, D) .

Two questions immediately arise.

- In the case $K = \mathbb{C}(z)$ with derivation $\frac{d}{dz}$ is the differential Galois group as defined above the same (up to isomorphism) as that defined earlier for a defining basis equation? The answer is yes, but the proof is not so simple, and will not be given here. However, a key ingredient is Proposition 8.6, which guarantees that the the field generated by a fundamental matrix solution with entries in L of an associated defining basis equation is independent of that defining equation.
- Does a Picard-Vessiot extension exist for any differential module (V, D) ? Here the answer is no; the standard existence proof requires characteristic zero and algebraically closed assumptions on K_C .

Proofs of all the assertions in this section can be constructed from arguments found in [vdP-S, Chapter I, §1.3, pp. 12-18].

Acknowledgment

On 14 August 2004 I lectured on this material at the Workshop on Linear Operators: Theory, Applications and Computation given at the Banff Research Station in Banff, Alberta (Canada). These notes represent a minor modification of notes I distributed there. It is a pleasure to thank Professors Binding and Lancaster of the University of Calgary for inviting me to give that lecture.

Bibliography

- [B-C] A. Baider and R.C. Churchill, On monodromy groups of second-order Fuchsian equations, *SIAM J. Math. Anal.*, **21**, No. 6, (1990), 1642-1652.
- [Ch] R.C. Churchill, Two generator subgroups of $SL(2, \mathbf{C})$ and the hypergeometric, Riemann and Lamé equations, *J. Symb. Comp.*, **28**, (1999), 521-546.
- [C-K] R.C. Churchill and J. Kovacic, Cyclic Vectors, in *Differential Algebra and Related Topics*, (Li Guo, P. Cassidy, W. Keigher and W. Sit, eds.), World Scientific, Singapore, 2002.
- [Kap] I. Kaplansky, *An Introduction to Differential Algebra*, Second Edition, Hermann, Paris, 1976.
- [Kol] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.
- [Kov] J.J. Kovacic, An Algorithm for Solving Second Order Linear Homogeneous Differential Equations, *J. Symbolic Computation*, **2**, (1986), 3-43.
- [Lang] S. Lang, *Algebra*, Revised Third Edition, Springer-Verlag, New York, 2002.
- [McCull] D. McCullough, Exceptional Subgroups of $SL(2, F)$, preprint, University of Oklahoma, June, 2005.
- [Poole] E.G.C. Poole, *Introduction to the Theory of Linear Differential Equations*, Dover Publications, New York, 1960,
- [Spr] T.A. Springer, *Linear Algebraic Groups*, Second Printing, Birkhäuser, Basel, 1983.

[vdP-S] M. van der Put and M.F. Singer, *Galois Theory of Linear Differential Equations*, Springer-Verlag, Berlin, 2003.

R.C. Churchill
Department of Mathematics
Hunter College and the Graduate Center, CUNY,
and the University of Calgary
e-mail rchurchi@math.hunter.cuny.edu