1

Introduction to the Galois Theory of Linear Differential Equations

Michael F. Singer

Department of Mathematics
North Carolina State University
Raleigh, NC 27695-8205
singer@math.ncsu.edu

1.1 Introduction

This paper is an expanded version of the 10 lectures I gave as the 2006 London Mathematical Society Invited Lecture Series at the Heriot-Watt University, 31 July - 4 August 2006†. My goal was to give the audience an introduction to the algebraic, analytic and algorithmic aspects of the Galois theory of linear differential equations by focusing on some of the main ideas and philosophies and on examples. There are several texts ([1, 2, 3, 4, 5] to name a few) that give detailed expositions and I hope that the taste offered here will encourage the reader to dine more fully with one of these.

The rest of the paper is organized as follows. In Section 1.2, *What is a Linear Differential Equation?*, I discuss three ways to think about linear differential equations: scalar equations, linear systems and differential modules. Just as it is useful to think of linear maps in terms of linear equations, matrices and associated modules, it will be helpful in future sections to go back and forth between the different ways of presenting linear differential equations.

In Section 1.3, *Basic Galois Theory and Applications*, I will give the basic definitions and describe the Galois correspondence. In addition I will describe the notion of monodromy and its relation to the Galois

† I would like to thank the London Mathematical Society for inviting me to present these lectures, the Heriot-Watt University for hosting them and the International Centre for the Mathematical Sciences for sponsoring a mini-programme on the Algebraic Theory of Differential Equations to complement these talks. Thanks also go to the Edinburgh Mathematical Society and the Royal Society of Edinburgh, who provided support for some of the participants and to Chris Eilbeck, Malcolm MacCallum, and Alexandre Mikhailov for organizing these events. This material is based upon work supported by the National Science Foundation under Grant No. 0096842 and 0634123

theory. I will end by giving several applications and ramifications, one of which will be to answer the question *Although* $y = \cos x$ *satisfies* $y'' + y = 0$*, why doesn't* $\sec x$ *satisfy a linear differential equation?*

In Section 1.4, *Local Galois Theory*, I will discuss the formal solution of a linear differential equation at a singular point and describe the asymptotics which allow one to associate with it an analytic solution in a small enough sector at that point. This will involve a discussion of Gevrey asymptotics, the Stokes phenomenon and its relation to the Galois theory. A motivating question (which we will answer in this section) is *In what sense does the function*

$$f(x) = \int_0^\infty \frac{1}{1+\zeta} e^{-\frac{\zeta}{x}} d\zeta$$

represent the divergent series

$$\sum_{n\geq 0} (-1)^n n! x^{n+1} \ ?$$

In Section 1.5, *Algorithms*, I turn to a discussion of algorithms that allow us to determine properties of a linear differential equation and its Galois group. I will show how category theory, and in particular the tannakian formalism, points us in a direction that naturally leads to algorithms. I will also discuss algorithms to find "closed form solutions" of linear differential equations.

In Section 1.6, *Inverse Problems*, I will consider the problem of which groups can appear as Galois groups of linear differential equations. I will show how monodromy and the ideas in Section 1.4 play a role as well as ideas from Lie theory.

In Section 1.7, *Families of Linear Differential Equations*, I will look at linear differential equations that contain parameters and ask *How does the Galois group change as we vary the parameters?*. This will lead to a discussion of a a generalization of the above theory to a Galois theory of parameterized linear differential equations.

1.2 What is a Linear Differential Equation?

I will develop an algebraic setting for the study of linear differential equations. Although there are many interesting questions concerning differential equations in characteristic p [6, 7, 8, 9], we will restrict ourselves throughout this paper, without further mention, to fields of characteristic 0. I begin with some basic definitions.

Definition 1.2.1 *1) A* differential ring (R, Δ) *is a ring* R *with a set* $\Delta = \{\partial_1, \ldots, \partial_m\}$ *of maps (*derivations*)* $\partial_i : R \to R$*, such that*

(i) $\partial_i(a+b) = \partial_i(a)+\partial_i(b)$, $\partial_i(ab) = \partial_i(a)b+a\partial_i(b)$ *for all* $a, b \in R$*, and*

(ii) $\partial_i\partial_j = \partial_j\partial_i$ *for all* i, j*.*

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

When $m = 1$, we say R is an *ordinary differential ring* (R, ∂). We frequently use the notation a' to denote $\partial(a)$ for $a \in R$. A differential ring that is also a field is called a *differential field*. If k is a differential field, then C_k is also a field.

Examples 1.2.2 1) $(C^\infty(\mathbb{R}^m), \Delta = \{\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_m}\})$ = infinitely differentiable functions on $\mathbb{R}^m$.

2) $(\mathbb{C}(x_1, \ldots, x_m), \Delta = \{\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_m}\})$ = field of rational functions

3) $(\mathbb{C}[[x]], \frac{\partial}{\partial x})$ = ring of formal power series

$\mathbb{C}((x)) =$ quotient field of $\mathbb{C}[[x]] = \mathbb{C}[[x]][\frac{1}{x}]$

4) $(\mathbb{C}\{\{x\}\}, \frac{\partial}{\partial x})$ = ring of germs of convergent series

$\mathbb{C}(\{x\}) =$ quotient field of $\mathbb{C}\{\{x\}\} = \mathbb{C}\{\{x\}\}[\frac{1}{x}]$

5) $(\mathcal{M}_{\mathcal{O}}, \Delta = \{\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_m}\})$ = field of functions meromorphic on $\mathcal{O}^{\text{open,connected}} \subset \mathbb{C}^m$

The following result of Seidenberg [10, 11] shows that many examples reduce to Example 5) above:

Theorem 1.2.3 *Any differential field* k*, finitely generated over* $\mathbb{Q}$*, is isomorphic to a differential subfield of some* $\mathcal{M}_{\mathcal{O}}$*.*

We wish to consider and compare three different versions of the notion of a linear differential equation.

Definition 1.2.4 *Let* (k, ∂) *be a differential field.*

(i) *A* scalar linear differential equation *is an equation of the form*

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

(ii) *A* matrix linear differential equation *is an equation of the form*

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

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

(iii) *A* differential module *of dimension* n *is an* n*-dimensional* k*-vector space* M *with a map* $\partial : M \to M$ *satisfying*

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

We shall show that these three notions are equivalent and give some further properties.

From scalar to matrix equations: Let $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0 y = 0$. If we let $y_1 = y, y_2 = y', \ldots y_n = y^{(n-1)}$, then we have

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

We shall write this last equation as $Y' = A_L Y$ and refer to A_L as the companion matrix of the scalar equation and the matrix equation as the companion equation. Clearly any solution of the scalar equation yields a solution of the companion equation and *vice versa*.

From matrix equations to differential modules (and back):

Given $Y' = AY,\ A \in \mathrm{gl}_n(k)$, we construct a differential module in the following way: Let $M = k^n$, $e_1, \ldots, e_n$ the usual basis. Define $\partial e_i = -\sum_j a_{j,i} e_j$, *i.e.*, $\partial e = -A^t e$. Note that if $m = \sum_i f_i e_i$ then $\partial m = \sum_i (f_i' - \sum_j a_{i,j} f_j) e_i$. In particular, we have that $\partial m = 0$ if and only if

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

It is this latter fact that motivates the seemingly strange definition of this differential module, which we denote by (M_A, ∂).

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

matrix equation $Y' = AY$. If $\bar{e} = (\bar{e}_1, \ldots, \bar{e}_n)$ is another basis, we get another equation $Y' = \bar{A}Y$. If f and $\bar{f}$ are vectors with respect to these two bases and $f = B\bar{f},\ B \in \mathrm{GL}_n(k)$, then

$$\bar{A} = B^{-1}AB - B^{-1}B' \ .$$

Definition 1.2.5 *Let (M_1, ∂_1) and (M_2, ∂_2) be differential modules.*
1) A differential module homomorphism *$\phi : M_1 \to M_2$ is a k-linear map ϕ such that $\phi(\partial_1(m)) = \partial_2(\phi(m))$ for all $m \in M_1$.*
2) The differential modules (M_1, ∂_1) and (M_2, ∂_1) are isomorphic *if there exists a bijective differential homomorphism $\phi : M_1 \to M_2$.*
3) Two differential equations $Y' = A_1Y$ and $Y' = A_2Y$ are equivalent *if the differential modules M_{A_1} and M_{A_2} are isomorphic*

Instead of equivalent, some authors use the term "gauge equivalent" or "of the same type".

Differential modules offer us an opportunity to study linear differential equations in a basis-free environment. Besides being of theoretical interest, it is important in computations to know that a concept is independent of bases, since this allows one to then select a convenient basis in which to compute.

Before we show how one can recover a scalar equation from a differential module, we show that the standard constructions of linear algebra can be carried over to the context of differential modules. Let (M_1, ∂_1) and (M_2, ∂_2) be differential modules and assume that for certain bases these correspond to the equations $Y' = A_1Y$ and $Y' = A_2Y$.

In Table 1.1 we list some standard linear algebra constructions and how they generalize to differential modules. In this table, I_{n_i} represents the $n_i \times n_i$ identity matrix and for two matrices $A = (a_{i,j})$ and B, $A \otimes B$ is the matrix where the i,j-entry of A is replaced by $a_{i,j}B$. Also note that if $f \in \mathrm{Hom}_k(M_1, M_2)$ then $\partial(f) = 0$ if and only if $f(\partial m_1) = \partial_2(f(m_1))$, that is, if and only if f is a differential module homomorphism.

Referring to the table, it is not hard to show that $\mathrm{Hom}_k(M_1, M_2) \simeq M_1 \otimes M_2^*$ as differential modules. Furthermore, given (M, ∂) with $\dim_k(M) = n$, corresponding to a differential equation $Y' = AY$, we have that $M \simeq \oplus_{i=1}^n \mathbf{1}_k$if and only if there exist $y_1, \ldots, y_n$ in k^n, linearly independent over k such that $y_i' = Ay_i$.

Table 1.1.

Construction	∂	Matrix Equation
$(M_1 \oplus M_2, \partial)$	$\partial(m_1 \oplus m_2) = \partial_1 m_1 \oplus \partial_2 m_2$	$Y' = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} Y$
$(M_1 \otimes M_2, \partial)$	$\partial(m_1 \otimes m_2) = \partial_1 m_1 \otimes m_2 + m_1 \otimes \partial m_2$	$Y' = (A_1 \otimes I_{n_2} + I_{n_1} \otimes A_2)Y$
$(\mathrm{Hom}_k(M_1, M_2), \partial)$	$\partial(f)(m) = f(\partial_1 m) - \partial_2(f(m))$	$Y' = Y A_2^T - A_1^T Y$
$\mathbf{1}_k = (k, \partial) =$ trivial differential module	$\partial \equiv 0$	$Y' = 0$
$(M^*, \partial) = \mathrm{Hom}_k(M, \mathbf{1}_k)$	$\partial(f)(m) = f(\partial(m))$	$Y' = -A^T Y$

From matrix to scalar linear differential equations: Before I discuss the relationship between matrix and scalar linear differential equations, I need one more concept.

Definition 1.2.6 *Let k be a differential field. The* ring of differential operators over $k = k[\partial]$ *is the ring of noncommutative polynomials $\{a_n\partial^n + \ldots + a_1\partial + a_0 \mid a_i \in k\}$ with coefficients in k, where multiplication is determined by $\partial \cdot a = a' + a\partial$ for all $a \in k$.*

We shall refer to the degree of an element $L \in k[\partial]$ as its order $\operatorname{ord} L$. The following properties are not hard to check ([5], Chapter 2.1):

Lemma 1.2.7 *Let $L_1 \neq 0, L_2 \in k[\partial]$.*

1) There exist unique $Q, R \in k[\partial]$ with $\operatorname{ord} R < \operatorname{ord} L_1$ such that $L_2 = QL_1 + R$.

2) Every left ideal of $k[\partial]$ is of the form $k[\partial]L$ for some $L \in k[\partial]$.

We note that any differential module M can be considered a left $k[\partial]$-module and conversely, any left $k[\partial]$-module that is finite dimensional as a k-vector space is a differential module. In fact we have a stronger statement:

Theorem 1.2.8 *(Cyclic Vector Theorem) Assume there exists an $a \in k$ such that $a' \neq 0$. Every differential module is of the form $k[\partial]/k[\partial]L$ for some $L \in k[\partial]$.*

This result has many proofs ([12, 13, 14, 15, 16, 17] to name a few), two of which can be found in Chapter 2.1 of [5].

Corollary 1.2.9 *(Systems to Scalar equations) Let k be as above. Every system $Y' = AY$ is equivalent to a scalar equation $L(y) = 0$.*

Proof Let $A^* = -A^t$. Apply the Cyclic Vector Theorem to M_{A^*} to find an $L \in k[\partial]$ such that $M_{A^*} = k[\partial]/k[\partial]L$. If A_L is the companion matrix of L, a calculation shows that $M_A \simeq M_{A_L}$. □

We note that the hypothesis that k contain an element a with $a' \neq 0$ is necessary. If the derivation is trivial on k, then two matrix equations $Y' = A_1Y$ and $Y' = A_2Y$ are equivalent if and only if the matrices are similar. There exist many examples of matrices not similar to a companion matrix.

Before we leave (for now) our discussion of the ring $k[\partial]$, I wish to make two remarks.

First, we can define a map $i : k[\partial] \to k[\partial]$ by $i(\sum a_j\partial^j) = \sum(-1)^j\partial^j a_j$,. This map is is an involution ($i^2 = id$). Denoting $i(L) = L^*$, we have that $(L_1L_2)^* = L_2^*L_1^*$. The operator L^* is referred to as the *adjoint* of L. Using the adjoint one sees that there is right euclidean division as well and that every right ideal of $k[\partial]$ is also principal.

Second, Lemma 1.2.7.2 allows us to define

Definition 1.2.10 *Let $L_1, L_2 \in k[\partial]$.*

1) The least common left multiple $\mathrm{LCLM}(L_1, L_2)$ *of L_1 and L_2 is the monic generator of $k[\partial]L_1 \cap k[\partial]L_2$.*
2) The greatest common right divisor $\mathrm{GCRD}(L_1, L_2)$ *of L_1 and L_2 is the monic generator of $k[\partial]L_1 + k[\partial]L_2$.*

A simple modification of the usual euclidean algorithm allows one to find these objects. One can also define least common right multiples and greatest common left divisors using right ideals.

Solutions I will give properties of solutions of scalar and matrix linear differential equations and define the notion of the solutions of a differential module. Let (k, ∂) be a differential field with constants C_k (see Definition 1.2.1).

Lemma 1.2.11 *Let $v_1, \ldots v_r \in k^n$ satisfy $v_i' = Av_i$, $A \in \mathrm{gl}_n(k)$. If $v_1, \ldots, v_r$ are k-linearly dependent, then they are C_k-linearly dependent.*

Proof Assume, by induction, that $v_2, \dots, v_r$ are k-linearly independent and $v_1 = \sum_{i=2}^{r} a_i v_i, a_i \in k$. We then have

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

so by assumption, each $a_i' = 0$. □

Corollary 1.2.12 *Let (k, ∂) be a differential field with constants C_k, $A \in \mathrm{gl}_n(k)$ and $L \in k[\partial]$.*

1) The solution space $\mathrm{Soln}_k(Y' = AY)$ of $Y' = AY$ in k^n is a C_k-vector space of dimension at most n.

2) The elements $y_1, \dots, y_r \in k$ are linearly dependent over C_k if and only if the wronskian determinant

$$yr(y_1, \dots, y_r) = \det \begin{pmatrix} y_1 & \dots & y_r \\ \vdots & \vdots & \vdots \\ y_1^{(r-1)} & \dots & y_r^{(r-1)} \end{pmatrix}$$

is zero.

3) The solution space $\mathrm{Soln}_k(L(y) = 0) = \{y \in k \mid L(y) = 0\}$ of $L(y) = 0$ in k is a C_k-vector space of dimension at most n.

Proof 1) This follows immediately from Lemma 1.2.11.

2) If $\sum_{i=1}^{r} c_i y_i = 0$ for some $c_i \in C_k$, not all zero, then $\sum_{i=1}^{r} c_i y_i^{(j)} = 0$ for all j. Therefore, $wr(y_1, \dots, y_r) = 0$. Conversely if $wr(y_1, \dots, y_r) = 0$, then there exists a nonzero vector $(a_0, \dots, a_{r-1})$ such that

$$(a_0, \dots, a_{r-1}) \begin{pmatrix} y_1 & \dots & y_r \\ \vdots & \vdots & \vdots \\ y_1^{(r-1)} & \dots & y_r^{(r-1)} \end{pmatrix} = 0$$

Therefore each y_i satisfies the scalar linear differential equation $L(y) = a_{r-1} y^{(r-1)} + \ldots + a_0 y = 0$ so each vector $v_i = (y_i, y_i', \dots, y_i^{(r-1)})^t$ satisfies $Y' = A_L Y$, where A_L is the companion matrix. Lemma 1.2.11 implies that the v_i and therefore the y_i are linearly dependent over C_k.

3) Apply Lemma 1.2.11 to $Y' = A_L Y$. □

In general, the dimension of the solution space of a linear differential equation in a field is less than n. In the next section we will construct a

field such that over this field the solution space has dimension n. It will be useful to have the following definition:

Definition 1.2.13 *Let (k, ∂) be a differential field, $A \in \mathrm{gl}_n(k)$ and R a differential ring containing k. A matrix $Z \in \mathrm{GL}_n(R)$ such that $Z' = AZ$ is called a* fundamental solution matrix *of $Y' = AY$.*

Note that if R is a field and Z is a fundamental solution matrix, then the columns of Z form a C_R-basis of the solution space of $Y' = AY$ in R and that this solution space has dimension n.

Let (M, ∂) be a differential module over k. We define the solution space $\mathrm{Soln}_k(M)$ of (M, ∂) to be the kernel $\ker_M \partial$ of ∂ on M. As we have noted above, if $\{e_i\}$ is a basis of M and $Y' = AY$ is the associated matrix differential equation in this basis, then $\sum_i v_i e_i \in \ker \partial$ if and only if $v' = Av$ where $v = (v_1, \ldots, v_n)^t$. If $K \supset k$ is a differential extension of k, then $K \otimes_k M$ can be given the structure of a K-differential module, where $\partial(a \otimes m) = a' \otimes m + a \otimes \partial m$. We then define $\mathrm{Soln}_K(M)$ to be the kernel $\ker(\partial, K \otimes_k M)$ of ∂ on $K \otimes_k M$.

1.3 Basic Galois Theory and Applications

Galois theory of polynomials The idea behind the Galois theory of polynomials is to associate to a polynomial a group (the group of symmetries of the roots that preserve all the algebraic relations among these roots) and deduce properties of the roots from properties of this group (for example, a solvable group implies that the roots can be expressed in terms of radicals). This idea can be formalized in the following way.

Let k be a field (of characteristic 0 as usual) and let $P(X) \in k[X]$ be a polynomial of degree n without repeated roots (i.e., $\mathrm{GCD}(P, P') = 1$).Let

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

(the reason for the term $\frac{1}{\prod (X_i - X_j)}$ will be explained below) and let $I = (P(X_1), \ldots, P(X_n)) \triangleleft S$ be the ideal generated by the $P(X_i)$. The ring S/I is generated by n distinct roots of P but does not yet reflect the possible algebraic relations among these roots. We therefore consider any maximal ideal M in S containing I. This ideal can be thought of as a maximally consistent set of algebraic relations among the roots. We define

Definition 1.3.1 *1) The* splitting ring *of the polynomial P over k is the ring*

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

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

Note that since M is a maximal ideal, R is actually a field. Furthermore, since S contains $\frac{1}{\prod(X_i - X_j)}$, the images of the X_i in R are *distinct* roots of P. So, in fact, R coincides with the usual notion of a splitting field (a field generated over k by the distinct roots of P) and as such, is unique up to k-isomorphism. Therefore, R is independent of the choice of maximal ideal M containing I. We will follow a similar approach with linear differential equations.

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

Let

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

where $Y = (Y_{i,j})$ is an $n \times n$ matrix of indeterminates. We define a derivation on S by setting $Y' = AY$. The columns of Y form n independent solutions of the matrix linear differential equation $Y' = AY$ but we have not yet taken into account other possible algebraic and differential relations. To do this, let M be any maximal *differential* ideal and let $R = S/M$. We have now constructed a ring that satisfies the following definition

Definition 1.3.2 *Let (k, ∂) be a differential field and $Y' = AY, A \in \mathrm{gl}_n(k)$ a matrix differential equation over k. A* Picard-Vessiot ring (PV-ring) *for $Y' = AY$ is a differential ring R over k such that*

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