AN INTRODUCTION TO DIFFERENTIAL GALOIS THEORY

BRUCE SIMON

San Francisco State University

Abstract. Differential Galois theory takes the approach of algebraic Galois theory and applies it to differential field extensions generated by appending solutions to differential equations. In doing so, it uncovers both the same relationship between the solutions to differential equations and the structure of the differential splitting field, and the same solubility conditions for differential equations, as the algebraic Galois theory found for polynomial equations.

This paper provides an informal exposition of the equivalence, through the presentation of simple, concrete examples of each differential analogue. Most of the literature is purely abstract and the algebraic theory employed is heavy. Hopefully, this introduction will be accessible to anyone with a basic knowledge of algebraic Galois theory and differential equations, helping them to more comfortably approach more rigorous treatments of the subject.

Contents

Date: December 17, 2015.

1. Introduction

In the early 19^{th} century, Evariste Galois discovered a relationship between the structure of the splitting field of an irreducible polynomial and the roots of the polynomial. In particular, he found that the subfields of the splitting field are in bijection with the subgroups of the group of automorphisms of the splitting field that fix the base field. This group is called the **Galois group** of the polynomial and the splitting field is said to be a **Galois extension** of the base field or, simply, **Galois**. This relationship between the Galois group and the Galois extension is given by the **Fundamental Theorem of Galois Theory**.

Theorem 1.1. *If L/K is Galois with Galois group G, $\mathcal{F} = \{F \text{ is a field} \mid K \subseteq F \subseteq L\}$, and $\mathcal{H} = \{H | H \leq G\}$ then*

(1) *There is a bijective map $\mathcal{H} \to \mathcal{F}$ defined by $H \to F \iff \sigma(x) = x \; \forall \sigma \in H, x \in F$.*

(2) *The map is order inverting. If $H_1 \to F_1$, $H_2 \to F_2$ then $F_1 \subset F_2 \iff H_2 < H_1$.*

(3) *$F \in \mathcal{F}$ is Galois over $K \iff F$ is the image of a normal subgroup of G*

Note that if $H \leq G$ then the set $L^H = \{x \in L | \sigma(x) = x \; \forall \sigma \in H\}$ is always a subfield of L and L^H is referred to as the fixed field of H.

Galois' work uncovered a solvability condition for polynomial equations: a polynomial is solvable by radicals if and only if its Galois group is solvable. By demonstrating that the Galois group of a general polynomial of degree 5 or higher was not solvable, Galois confirmed Abel's proof that a general polynomial of degree 5 or more not solvable by radicals.

Example 1.2. Consider $P(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$.

$P(x)$ has four real roots over $\mathbb{Q}$, $\pm\sqrt{2}$ and $\pm\sqrt{3}$, so $L = \mathbb{Q}\langle\sqrt{2}, \sqrt{3}\rangle$ is the splitting field for $P(x)$ over $\mathbb{Q}$. The extension $L/\mathbb{Q}$ is Galois with the intermediate fields $\mathbb{Q}\langle\sqrt{2}\rangle$, $\mathbb{Q}\langle\sqrt{3}\rangle$, and $\mathbb{Q}\langle\sqrt{6}\rangle$.

To identify the Galois group, $G = Gal(L/\mathbb{Q})$, note that since $\pm\sqrt{2}$ are the roots of $x^2 - 2$ and $\pm\sqrt{3}$ are the roots of $x^2 - 3$, any $\mathbb{Q}$-automorphism of L must map $\pm\sqrt{2} \to \pm\sqrt{2}$ and $\pm\sqrt{3} \to \pm\sqrt{3}$.

Thus, the Galois group is $G = \{1, \sigma, \tau, \sigma\tau\}$ where

$$\sigma : \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{cases} \qquad \sigma\tau : \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{cases}$$

The subgroups of G are $H_1 = 1, H_2 = \{1, \tau\}, H_3 = \{1, \sigma\}, H_4 = \{1, \sigma\tau\}$, and G.

As σ and τ are automorphisms $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = -\sqrt{6}$ and $\tau(\sqrt{6}) = \tau(\sqrt{2})\tau(\sqrt{3}) = -\sqrt{6}$. And, since the group operation in G is composition, $\sigma\tau(\sqrt{6}) = \tau\sigma(\sqrt{6}) = \sqrt{6}$. The bijection promised in (1.1) maps $G \to \mathbb{Q}$, $H_2 \to \mathbb{Q}\langle\sqrt{2}\rangle$, $H_3 \to \mathbb{Q}\langle\sqrt{3}\rangle$,$H_4 \to \mathbb{Q}\langle\sqrt{6}\rangle$, and $H_1 \to \mathbb{Q}\langle\sqrt{2}, \sqrt{3}\rangle$.

The equivalence of the structures of the Galois extension and the Galois group can be seen in the diagrams:

$$
\begin{tikzcd}[arrows=dash]
 & G \arrow[dl] \arrow[d] \arrow[dr] & \\
H_2 \arrow[dr] & H_3 \arrow[d] & H_4 \arrow[dl] \\
 & H_1 &
\end{tikzcd}
\qquad
\begin{tikzcd}[arrows=dash]
 & \mathbb{Q}\langle\sqrt{2},\sqrt{3}\rangle \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathbb{Q}\langle\sqrt{2}\rangle \arrow[dr] & \mathbb{Q}\langle\sqrt{3}\rangle \arrow[d] & \mathbb{Q}\langle\sqrt{6}\rangle \arrow[dl] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[arrows=dash]
 & L^{H_1} \arrow[dl] \arrow[d] \arrow[dr] & \\
L^{H_2} \arrow[dr] & L^{H_3} \arrow[d] & L^{H_4} \arrow[dl] \\
 & L^G &
\end{tikzcd}
$$

Clearly $\mathbb{Q}\langle\sqrt{2}\rangle$, $\mathbb{Q}\langle\sqrt{3}\rangle$, and $\mathbb{Q}\langle\sqrt{6}\rangle$ are all Galois over $\mathbb{Q}$ and it is easy to verify that H_2, H_3, and H_4 are all normal subgroups of G.

The idea of developing an analogue to algebraic Galois theory for differential equations originated with Sophus Lie in the early 1870's. Lie found that if a group of transformations under composition permutes the integral curves of a differential equation of the form $Xdy - Ydx = 0$, the group may be used to find an integrating factor for the equation. Additionally, he discovered necessary and sufficient conditions for the existence of the transformation group. [Ref5]

In the late 19$^{\text{th}}$ Emile Picard and Ernst Vessiot applied the theory of Lie groups to uncover a solvability condition for first order linear, homogeneous differential equations almost exactly equivalent to Galois' solvability condition for polynomials. Analyzing the relationship between the differential field extensions obtained by appending solutions to differential equations over a base field, and the group of symmetries of those roots they found that an ordinary, linear, homogeneous differential equation is solvable by quadratures if and only if its differential Galois group is solvable.

In a striking parallel to the development of algebraic Galois theory Ellis Kolchin, believing Picard-Vessiot theory was limited by the lack of a formal theory of linear algebraic groups, extended the work of Joseph Ritt in differential algebra to develop this theory. Using his new theory of algebraic matrix groups, Kolchin was able to formalize and extend the work of Picard and Vessiot. The Fundamental Theorem of Picard-Vessiot Theory stated below is due to Kolchin and it is his work that is generally referred to as Picard-Vessiot theory, or differential Galois theory, today. [Ref9]

Theorem 1.3. *If L/K is a Picard-Vessiot extension with differential Galois group G then*

(1) *There is an inclusion reversing bijective map between the set of Zariski closed subgroups H of G and the set of differential fields F with $K \subset F \subset L$ given by $H \to L^H$*

(2) *An intermediate differential field $F = L^H$ is a Picard-Vessiot extension $\iff$ $H \trianglelefteq G$.*

In this paper, we will informally explore the Picard-Vessiot theory. Each object in the Picard-Vessiot theory will be introduced and developed as an analogue to its algebraic counterpart.

Algebraic Galois Theory	**Picard-Vessiot Theory**
Polynomial	Linear Differential Operator
Root of polynomial	Solution to differential equation
Splitting field	Picard-Vessiot extension
Galois group	Differential Galois Group
Solvable Galois Group	Solvable Galois Group

As each object is introduced, it will be illustrated by example. Wherever possible, the same examples will be carried through the introduction of multiple objects.

2. Differential Rings and Fields

Before we can discuss the differential Galois theory, we need a few definitions.

Definition 2.1. Here are the basic definitions of differential rings and fields we will need:

(1) A **derivation** of a ring R is a map $d : R \to R$ such that $\forall r, s \in R$
  (a) $d(r + s) = d(r) + d(s)$
  (b) $d(rs) = d(r)s + rd(s)$
(2) A **differential ring** is a commutative ring with identity and a defined derivation.
(3) A **differential field** is a field with a defined derivation. Of course, every differential field is also a differential ring.
(4) An element in a differential ring or field is **constant** $\iff$ its derivation is 0.
(5) An ideal $I \subseteq R$ is a **differential ideal** if it is closed under the derivation.
(6) A **differential automorphism** is an automorphism, σ, that respects the derivation: $\sigma(r') = [\sigma(r)]' \;\; \forall r \in R$

Proposition 2.2. *Here are some basic facts of differential rings and fields we will need:*

(1) *If R is an integral domain with derivation d, d extends uniquely to the quotient field with the usual quotient rule: $d(\frac{r}{s}) = \frac{d(r)s - rd(s)}{s^2}$.*
(2) *If R is a commutative differential ring and A is a multiplicative system of R the derivation of R extends to the ring $A^{-1}R$ uniquely in the same way.*
(3) *If R is a differential ring then the derivation of R can be extended to the polynomial ring $R[X_1, X_2, \ldots, X_n]$ such that $(\Sigma a_i X^i)' = \Sigma(a_i' X^i + a_i i X^{i-1} X')$*
(4) *If K is a differential field and L/K is a separable algebraic extension, the derivation of K extend uniquely to L and every K-automorphism of L is a differential automorphism.*
(5) *If K is a differential field and $R \supset K$ is a differential ring then any maximal ideal, $I \subset R$, is a prime ideal.*

Examples:

(1) Any commutative ring, R, with identity may be given a differential structure by defining $d(r) = 0 \; \forall r \in R$. Thus, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all differential fields in which every element is constant.

(2) The polynomial rings $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$ with the usual derivation $d(x) = 1$ are all differential rings. Likewise, the polynomial rings in n indeterminates $\mathbb{Q}[x_1, \ldots, x_n]$, $\mathbb{R}[x, \ldots, x_n]$, and $\mathbb{C}[x, \ldots, x_n]$ with $d(x_i) = 1 \; \forall i$ are all differential rings.

(3) The fields of rational functions, $\mathbb{Q}(x)$, $\mathbb{R}(x)$, and $\mathbb{C}(x)$ are all differential fields with the usual derivative.

(4) The ring of infinitely differentiable real valued functions with their usual derivatives is a differential ring and the field of meromorphic functions with their usual derivatives is a differential field.

(5) If R is a differential ring then the ring $R[x_1, \ldots, x_n]$ with the derivation extended by defining $d(x_i) = x_{i+1}$ for $i \leq n-1$ and $d(x_n)$ to be a member of $R[x_1, \ldots, x_n]$ is a differential ring.

In this construction, each x_i is a **differential indeterminate** and the elements of $R[x_1, \ldots, x_n]$ are **differential polynomials** in the indeterminate x_1.
If R was a field, this derivation extends uniquely to the quotient field $R\langle x_1, \ldots, x_n \rangle$

All of the above propositions and examples were taken from chapter 5 of [Ref1]. Some proofs are available there.

The original Picard-Vessiot theory was established in the case where the base field is of characteristic 0 and the field of constants is algebraically closed. Kolchin was able to prove his results for fields of arbitrary characteristic. Recently, the results have been shown to obtain for any closed real field of constants. [Ref10]

3. Linear Differential Operators

The **ring of differential operators** over a differential field K is simply a polynomial ring in one indeterminate, the derivation d, and is analogous to the usual polynomial ring $K[x]$ over a field.

Definition 3.1. The **ring of differential operators** over a differential field K is the noncommutative ring of all polynomials in d with coefficients in K .

$$K[d] = \{\mathcal{L} = a_n d^n + a_{n-1} d^{n-1} + \ldots + a_1 d + a_0 \mid a_i \in K \; \forall i\}$$

The product $d \cdot a$ in the ring of differential operators is defined by $d \cdot a = a' + ad$.

Powers of d act on members of K and its differential extensions as repeated applications of the derivation. Every $\mathcal{L} \in K[d]$ acts on any differential extension of K to create a degree n differential polynomial in one differential indeterminate, giving rise to a **linear homogeneous differential equation** of order n.

$$\mathcal{L}(Y) = a_n Y^{(n)} + a_{n-1} Y^{(n-1)} + \ldots + a_1 Y' + a_0 Y = 0.$$

A differential equation written in the form of a differential polynomial is called a **scalar** equation.

Every order n ordinary linear homogeneous differential equation may also be represented as the 1^{st} order matrix differential equation $Y' = AY$, $A \in GL_n(K)$. The derivation of $M = (m_{ij}) \in gl_n(K)$ is given by $M' = (m_{ij})'$.

Letting $b_i = \frac{a_i}{a_n}$, it is clear that y is a solution of $\mathcal{L}(Y) = a_n Y^{(n)} + a_{n-1} Y^{(n-1)} + \ldots +$

$a_1Y' + a_0Y = 0$ if and only if $\begin{pmatrix} y, & y', & \dots & y^{n-1}, & y^n \end{pmatrix}^T$ satisfies the matrix equation

$$\begin{pmatrix} y \\ y' \\ \vdots \\ y^{n-1} \\ y^n \end{pmatrix}' = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -b_0 & -b_1 & -b_2 & \dots & -b_{n-1} \end{pmatrix} \begin{pmatrix} y \\ y' \\ \vdots \\ y^{n-1} \\ y^n \end{pmatrix}$$

As all the differential equations we consider in this paper will be linear homogenous ordinary equations, we will not continue to qualify each equation as such.

A solution to a differential equation is the equivalent of a root of a polynomial in the algebraic Galois theory. Unlike the algebraic setting, there are three distinct types of solutions to a differential equation with coefficients in the differential field K.

(1) y is algebraic over K.
(2) y is the integral of a member of K.
(3) y is the exponential of an integral of a member of K

If C_K is the field of constants of K then all C_K-linear combinations of solutions to a differential equation with coefficients in K are also solutions of the differential equation.

Examples:

(1) Let $K = \mathbb{C}(x)$ with the standard derivation and consider the scalar differential equation $\mathcal{L}(Y) = Y'' + \frac{1}{x}Y' = 0$.
By inspection, $y_1 = 1$ and $y_2 = ln\, x$ are two solutions that are linearly independent over $\mathbb{C}$. $y_1 = 1$ is an algebraic element of K and $y_2 = ln\, x$ is the integral of $\frac{1}{x} \in K$. If $c_1, c_2 \in \mathbb{C}$, then the linear combination $c_1 + c_2 \cdot ln\, x$ is also a solution of $\mathcal{L}(Y) = 0$.
(2) The first order matrix equation for the differential equation in example 1 is $\begin{pmatrix} y \\ y' \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ 0 & -\frac{1}{x} \end{pmatrix} \begin{pmatrix} y \\ y' \end{pmatrix}$. The solution vectors are $(1, 0)^T$ and $(ln\, x, \frac{1}{x})^T$.
(3) Let $K = \mathbb{C}(x)$ with the standard derivation and consider the scalar equation $\mathcal{L}(Y) = Y'' + Y = 0$.
By inspection, $y_1 = sin\ x$ and $y_2 = cos\ x$ are two solutions of $\mathcal{L}(Y) = 0$ that are linearly independent over $\mathbb{C}$. Additionally, it's easy to see that $y_3 = e^{ix}$ and $y_4 = e^{-ix}$ are another pair of solutions that are linearly independent over $\mathbb{C}$.
Note that the set of solutions $\{y_1, y_2, y_3, y_4\}$ is not linearly independent over $\mathbb{C}$ as, for example, $y_1 = \frac{i}{2}(y_4 - y_3)$
(4) The matrix equation for the differential operator in example 3 is $\begin{pmatrix} y \\ y' \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} y \\ y' \end{pmatrix}$.
The solution vectors are $(sinx, cosx)^T$, $(cosx, -sinx)^T$ or $(e^{ix}, ie^{ix})^T$, $(e^{-ix}, -ie^{-ix})^T$

As a polynomial of degree n has at most n distinct roots, a differential equation of order n has at most n linearly independent solutions. It is a well known fact that an n^{th} order differential equation will always have a full set of n linearly independent solutions.

Definition 3.2. If K is a field of characteristic 0 and $\mathcal{L}(Y) = 0$ is an n^{th} order differential equation with coefficients in K, then

(1) $\{y_1, \ldots, y_n\}$ is a **fundamental set of solutions** if and only if $\mathcal{L}(y_i) = 0$ for $1 \leq i \leq n$ and the y_i are linearly independent over K.
(2) If $\{y_1, \ldots, y_n\}$ is a fundamental set of solutions to $\mathcal{L}(Y) = 0$ with the associated matrix equation $Y' = AY$ then the **fundamental solution matrix** for $Y' = AY$ is

$$M_A = \begin{pmatrix} y_1 & y_2 & \ldots & y_n \\ y_1' & y_2' & \ldots & y_n' \\ \vdots & \vdots & \ldots & \vdots \\ y_1^{n-1} & y_2^{n-1} & \ldots & y_n^{n-1} \end{pmatrix}$$

(3) The **Wronskian determinant** of any set $\{y_1, \ldots, y_n\}$ is

$$W(y_1, \ldots, y_n) = \begin{vmatrix} y_1 & y_2 & \ldots & y_n \\ y_1' & y_2' & \ldots & y_n' \\ \vdots & \vdots & \ldots & \vdots \\ y_1^{n-1} & y_2^{n-1} & \ldots & y_n^{n-1} \end{vmatrix} = det M_A$$

Since $W(y_1, \ldots, y_n)$ is the determinant of an n by n matrix, $W(y_1, \ldots, y_n) \neq 0$ if $\{y_1, \ldots, y_n\}$ is a fundamental set of solutions to the differential operator $\mathcal{L}(Y) = 0$.

Note that any fundamental set of solutions to an n^{th} order differential equation with coefficients in K forms a basis for an n-dimensional vector space over C_K. This is the **solution space** of $\mathcal{L}(Y) = 0$

Examples:

(1) $\{1, ln\, x\}$ is a fundamental solution set for $\mathcal{L}(Y) = Y'' + \frac{1}{x}Y' = 0$.
$M_A = \begin{pmatrix} 1 & ln\, x \\ 0 & \frac{1}{x} \end{pmatrix}$ is a fundamental solution matrix for $\begin{pmatrix} y \\ y' \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ 0 & -\frac{1}{x} \end{pmatrix} \begin{pmatrix} y \\ y' \end{pmatrix}$.
$W(1, ln\, x) = det M_A = \frac{1}{x} \neq 0$ for all x in the domain of $ln\, x$.

(2) $\{sin\, x, cos\, x\}$ and $\{e^{ix}, e^{-ix}\}$ are fundamental solution sets for $\mathcal{L}(Y) = Y'' + Y = 0$.
The matrices $\begin{pmatrix} sin\ x & cos\ x \\ cos\ x & -sin\ x \end{pmatrix}$ and $\begin{pmatrix} e^{ix} & e^{-ix} \\ ie^{ix} & -ie^{-ix} \end{pmatrix}$ are fundamental solution matrices for the first order matrix equation $\begin{pmatrix} y \\ y' \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} y \\ y' \end{pmatrix}$.
$W(sin\ x, cos\ x) = det \begin{pmatrix} sin\ x & cos\ x \\ cos\ x & -sin\ x \end{pmatrix} = -1$
$W(e^{ix}, e^{-ix}) = det \begin{pmatrix} e^{ix} & e^{-ix} \\ ie^{ix} & -ie^{-ix} \end{pmatrix} = -2i.$

4. Picard-Vessiot Extensions

The **Picard-Vessiot field** of $\mathcal{L}(Y) = 0$ with coefficients in a differential field K is analogous to the splitting field of the polynomial $P(x)$ over K. It is the smallest extension of K that contains a fundamental solution set for $\mathcal{L}(Y) = 0$.

Definition 4.1. If $\mathcal{L}(Y) = 0$ has order n with coefficients in the differential field K then a differential extension $L \supseteq K$ is a **Picard-Vessiot extension** if

(1) $L = K\langle y_1, \ldots, y_n\rangle$ where $\{y_1, \ldots, y_n\}$ is a fundamental set of solutions to $\mathcal{L}(Y) = 0$.

(2) L contains no constants that were not in K; $C_L = C_K$.

If L/K is a Picard-Vessiot extension then L is the Picard-Vessiot field of $\mathcal{L}(Y) = 0$.

The condition that $C_L = C_K$ insures that L is the minimal extension of K that contains a fundamental set of solutions to $\mathcal{L}(Y) = 0$.

Examples:

(1) If $K = \mathbb{C}(x)$ with standard derivation, the Picard-Vessiot field of $\mathcal{L}(Y) = Y'' + \frac{1}{x}Y' = 0$ is $L = K\langle ln\, x\rangle$.
(2) The Picard-Vessiot field of $\mathcal{L}(Y) = Y''+Y = 0$ over $K = \mathbb{C}(x)$ is $L = K\langle sinx, cosx\rangle$.

Theorem 4.2. *There exists a Picard-Vessiot extension for $\mathcal{L}(Y) = 0$ over K if*

(1) *K has characteristic 0 and the field of constants C_K is algebraically closed.*
(2) *If C_K is a closed real field.*
(3) *$\mathcal{L}(Y) = 0$ has an irreducible auxiliary polynomial $P(x) = 0$ with coefficients in C_K. In this case, the Picard-Vessiot extension of $\mathcal{L}(Y) = 0$ is isomorphic to the splitting field of $P(x) = 0$.*

The Picard-Vessiot field of a differential equation $\mathcal{L}(Y) = 0$ is unique up to isomorphism.

If C_K is algebraically closed, the Picard-Vessiot field L/K for $\mathcal{L}(Y) = 0$ may be constructed as follows:

(1) Adjoin a fundamental solution set $\{y_1, \ldots y_n\}$ and their first $n-1$ derivatives to obtain $K[y_{ij}]$, a differential ring in n^2 indeterminates.
These may be structured as the matrix (y_{ij}) where y_{0j} is the j^{th} solution and $y_{(i+1)j} = y'_{ij}$ for $0 \le i \le n-2$, $y_{nj} = -a_{n-1}y_{(n-1)j} - \ldots - a_1 y_{1j} - a_0 y_{0j}$.
(2) Localize by $W(y_1, \ldots, y_n)$ to obtain $R = K[y_{ij}][W^{-1}]$ the **full universal solution algebra** for $\mathcal{L}$.
(3) Any maximal ideal P of a full universal solution algebra is a prime ideal [Crespo] so the quotient R/P, the **Picard-Vessiot ring**, is an integral domain.
(4) The Picard-Vessiot field L is the field of quotients of the Picard-Vessiot ring.

This procedure is described in more detail, with proof of (3), in [Ref1].

Examples:

(1) Let $K = \mathbb{C}(x)$ with the usual derivative, $a \in \mathbb{C}$ and consider the differential equation $\mathcal{L}(Y) = Y' - \frac{a}{x}Y = 0$. If y is a solution to $\mathcal{L}(Y) = 0$ and $W = y$. If $a \notin \mathbb{Z}$ then $y \notin K$. [Ref2]

 (a) If $a = \frac{n}{m} \in \mathbb{Q}$ then adjoining y to create the full universal solution algebra $K[y, \frac{1}{y}]$ introduces the relationship $y^m - x^n = 0$. Note that $(y^m - x^n)$ is a maximal differential ideal so is a prime ideal. The Picard-Vessiot field is the field of fractions of the quotient $K[y, \frac{1}{y}]/(y^m - x^n), K\langle x^{\frac{n}{m}}\rangle$.

(b) If $a \notin \mathbb{Q}$ then there is no non-trivial proper differential ideal so the Picard-Vessiot extension is the field of fractions of $K[y, \frac{1}{y}]$.

(2) Let $K = \mathbb{C}(x)$ with the usual derivative and consider $Y^{(3)} - 2Y = 0$ which has the auxiliary polynomial $P(x) = x^3 - 2$. The roots of P are $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, and $\rho^2\sqrt[3]{2}$ where $\rho = e^{\frac{2\pi i}{3}}$ so $\{e^{\sqrt[3]{2}x}, e^{\rho\sqrt[3]{2}x}, e^{\rho^2\sqrt[3]{2}x}\}$ form a fundamental set of solutions. Thus, the Picard-Vessiot extension is $\mathbb{C}\langle e^{\sqrt[3]{2}x}, e^{\rho\sqrt[3]{2}x}, e^{\rho^2\sqrt[3]{2}x}\rangle$.

5. The Differential Galois Group

Definition 5.1. If L/K is a Picard-Vessiot extension for $\mathcal{L}(Y) = 0$, the **differential Galois group** of $L \supset K$ is $G(L/K) = G_K(\mathcal{L})$, the group of all differential K-automorphisms of L.

As the members of the algebraic Galois group are exactly those transformations under which the polynomial is invariant, the members of $G_K(\mathcal{L})$ are the automorphisms under which the differential operator is invariant. If $\sigma \in G_K(\mathcal{L})$ and y is a solution of $\mathcal{L}(Y) = 0$, $\sigma(y)$ is also a solution. Thus, σ maps each y_i in the fundamental solution set to a C_K-linear combination of the y_i: $\sigma(y_i) = \Sigma c_j y_i$ where $c_j \in C_K$ for $j = 1, \ldots, n$. Like the algebraic Galois group, the members of the differential Galois group are completely determined by their action on the generators of L/K.

Definition 5.2. A **linear algebraic group** is a subgroup $G \subseteq GL_n(C_K)$ that is the set of zeros of of a system of polynomials in n^2 variables with coefficients in C_K.

While algebraic Galois groups are subgroups of S_n, differential Galois groups are linear algebraic groups. In particular, if $\mathcal{L}(Y) = 0$ has order n, $G_K(\mathcal{L})$ is a Lie subgroup of $GL_n(C_K)$.

Examples:

(1) Let $K = \mathbb{C}(x)$, $L = K\langle ln\, x\rangle$ be the Picard-Vessiot field for $\mathcal{L}(Y) = Y'' + \frac{1}{x}Y' = 0$. Any differential K-automorphism in $G_K(\mathcal{L})$ must fix the solution $y = 1 \in C_K$ and map $ln\, x$ to $c_1 + c_2 ln\, x$.

Further, $\sigma \in G_K(\mathcal{L}) \implies \sigma(d(ln\, x)) = d(\sigma(ln\, x)) \implies \frac{c_2}{x} = \frac{1}{x} \implies c_2 = 1$.

Thus $\sigma \in G_K(\mathcal{L})$ maps $ln\, x \to ln\, x + c$ where $c \in \mathbb{C}$ and $G_K(\mathcal{L})$ is isomorphic to $\mathbb{C}$. $G_K(\mathcal{L})$ is the subgroup of $GL_2(\mathbb{C})$ generated by $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ for $c \in \mathbb{C}$.

To verify this is a subgroup of $GL_2(\mathbb{C})$ we compute $\begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & c_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c_1 + c_2 \\ 0 & 1 \end{pmatrix}$

(2) Let $K = \mathbb{C}(x)$ and $L = K\langle sin\, x, cos\, x\rangle$ be the Picard-Vessiot field for $\mathcal{L}(Y) = Y'' + Y = 0$.

Any K-automorphism of L, must map $sinx \to asinx + bcosx$, $cosx \to csinx + dcosx$ and satisfy:

$$\sigma(d(sin\,x)) = d(\sigma(sin\,x)) \qquad \sigma(d(cos\,x)) = d(\sigma(cos\,x))$$
$$\sigma(cos\,x) = d(asin\,x + bcos\,x) \qquad \sigma(-sin\,x) = d(csin\,x + dcos\,x)$$
$$csin\,x + dcos\,x = acos\,x - bsin\,x \qquad -asin\,x - bcos\,x = ccos\,x - dsin\,x$$

From which it immediately follows that $a = d$ and $b = -c$.

$G_K(\mathcal{L})$ is the subgroup of $GL_2(\mathbb{C})$ generated by $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ $a, b \in \mathbb{C}$ not both zero.

As $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$, $G_K(\mathcal{L})$ is a subgroup of $GL_2(\mathbb{C})$.

(3) Let $K = \mathbb{C}(x)$, $L = K\langle x^a \rangle$ be the Picard-Vessiot field for $\mathcal{L}(Y) = Y' - \frac{a}{x}Y = 0$. If y is a solution of $\mathcal{L}(Y) = 0$ then $\sigma \in G_K(\mathcal{L})$ must be defined by $\sigma(y) = cy$.

   (a) If $a = \frac{n}{m}$, then y is algebraic over K with minimal polynomial of degree m so $\sigma \in G_K(\mathcal{L})$ must map $y \to cy$ where $c \in \mathbb{C}$ is an m^{th} root of unity. Thus $G_K(\mathcal{L})$ is cyclic of order m.

   (b) If $a \notin \mathbb{Q}$ then y is not algebraic over K then $\sigma(y) = cy$ is a differential K-automorphism $\forall c \in \mathbb{C}$ and $G_K(\mathcal{L}) = GL_1(\mathbb{C})$.

(4) If $K = \mathbb{C}(x)$ and $L = \mathbb{C}\langle e^{\sqrt[3]{2}x}, e^{\rho\sqrt[3]{2}x}, e^{\rho^2\sqrt[3]{2}x} \rangle$ is the Picard-Vessiot field for $\mathcal{L}(Y) = Y^{(3)} - 2Y = 0$.
Suppose $\sigma y_i = c_1y_1 + c_2y_2 + c_3y_3$. Computing $d\sigma(y_i)$ and $\sigma(dy_i)$ as in example (2) above shows that any K-automorphism of L must be of the form $\sigma : \begin{cases} y_1 \to c_1y_1 \\ y_2 \to c_2y_2 \\ y_3 \to c_3y_3 \end{cases}$
Thus $G_K(\mathcal{L}) = (\mathbb{C}^*)^3$, the group of invertible, diagonal matrices in $GL_3(\mathbb{C})$.

6. The Galois Correspondence

The correspondence between the subgroups of the differential Galois group and the intermediate fields in the Picard-Vessiot extension is exactly analogous to the Galois correspondence in algebraic Galois Theory.

Theorem 6.1. *If L/K is a Picard-Vessiot extension with differential Galois group G then*

(1) *There is an inclusion reversing bijective map between the set of Zariski closed subgroups H of G and the set of differential fields F with $K \subset F \subset L$ given by $H \to L^H$*

(2) *An intermediate differential field $F = L^H$ is itself a Picard-Vessiot extension $\iff$ $H \trianglelefteq G$.*

A proof of this theorem is section 6.3 in [Ref1].

Definition 6.2. A subgroup $H \subseteq G$ is **Zariski closed** if H is a linear algebraic group.

Example:

(1) Let $K = \mathbb{C}(x)$ and consider the linear differential operator $\mathcal{L}(Y) = Y' - Y = 0$. $y = e^x$ is a solution to $\mathcal{L}(Y) = 0$ and $L = K\langle e^x\rangle$ is the Picard-Vessiot extension. The differential Galois group is $G_K(\mathcal{L}) = C^*$.

The Zariski closed proper subgroups of C^* are the groups of units of order n: $\mu_n = (e^{\frac{2\pi i}{n}}), n \geq 2$. μ_n is the set of simultaneous solutions to $x^n - 1 = 0$.

The intermediate differential fields of L/K are $L \supset E_n \supset K$ where $E_n = K\langle e^{nx}\rangle$, $n \geq 2$. If m divides n, the Galois correspondence is given by:

$$\begin{array}{ccc}
\text{Differential Fields} & & \text{Zariski Closed Subgroups} \\
 & & \\
K\langle e^x\rangle = L & \Longleftrightarrow & 1 \\
| & & | \\
K\langle e^{mx}\rangle & \Longleftrightarrow & (e^{\frac{2\pi i}{m}}) \\
| & & | \\
K\langle e^{nx}\rangle & \Longleftrightarrow & (e^{\frac{2\pi i}{n}}) \\
| & & | \\
\mathbb{C}(x) = K & \Longleftrightarrow & G_K(\mathcal{L}) = C^*
\end{array}$$

Since C^* is commutative, $H = \mu_n \trianglelefteq C^*$ for all n. $L^H = K\langle e^{nx}\rangle$ is the Picard-Vessiot extension for $\mathcal{L}(Y) = Y' - nY = 0$.

7. Solvability

The algebraic Galois' theory established a solvability condition for polynomials given by the following theorem.

Theorem 7.1. *A polynomial over a field of characteristic 0 is solvable by radicals* $\Longleftrightarrow$ *it has a solvable Galois group.*

Definition 7.2. G is **solvable** if there is a chain of subgroups $1 = G_0 \subset G_1 \ldots \subset G_n = G$ such that $G_{i+1} \trianglelefteq G_i$ and G_{i+1}/G_i is abelian.

Definition 7.3. Let K be a differential field, $\mathcal{L}(Y) = 0$ a differential equation over K. A solution $y \notin K$ is **Liouvillian** if

(1) y is algebraic over K
(2) y is the integral of an element in K
(3) y is the exponential of an element in K

Picard and Vessiot stated an almost identical condition for a linear differential equation to be solvable in terms of Liouvillian functions. Their statement was "given a formal modern proof" by Kolchin. [Ref2]

Theorem 7.4. *Let K be a differential field, L the Picard-Vessiot field for $\mathcal{L}(Y) = 0$ over K. $\mathcal{L}(Y) = 0$ is solvable by Liouvillian functions* $\Longleftrightarrow$ *the identity component of $G_K(L)$ is solvable.*

Singer provides several equivalent and stronger statements, with proofs, as well as examples in section 1.5 of [Ref2].

8. Concluding Thoughts

We have confined ourselves here to the basics of the direct question of differential Galois theory: given an easily solved differential equation, what is the Picard-Vessiot extension, the differential Galois group and the Galois correspondence. There was a great deal of interest in developing algorithms for finding differential Galois groups in the late 1990's and early 2000's. The article by van der Put referenced below provides a summary of those activities and some applications. More recently, work seems to be focused on algorithms for parameterized differential Galois theory.

The inverse question, "given a differential field K with field of constants C and a linear algebraic group G defined over C find a linear differential equation defined over$K$ whose differential Galois group is G" is also being studied. Crespo and Hajto give several suggested references in the last chapter of their book (Pg. 213). The preliminary paper by Harbater, Hartmann, and Maier referenced below claims a positive solution to the problem over Laurent series fields of characteristic 0, namely that every algebraic group over such a field is the Galois group of a differential equation.

Singer discusses several applications of differential Galois theory in mathematics in section 1.3 of his lectures beginning on page 18.

9. References

(1) Teresa Crespo and Zbigniew Hajto. Algebraic Groups and Differential Galois Theory. American Mathematical Society. 2010.

(2) Michael Singer. Introduction to the Galois Theory of Linear Differential Equations. Lectures to the London Mathematical Society at Heriot-Watt University. www4.ncsu.edu/ Singer/papers/LMSlectures.

(3) Andy Magid. Differential Galois Theory. Notices of the AMS. October 1999.

(4) Moshe Kamensky. Differential Galois Theory.
www.math.bg.ac.il/ Kamensky/lectures/DiffGalois.pdf.

(5) Sigurdur Helgason. Sophus Lie and the Role of Lie Groups in Mathematics. ocw.mit.edu/courses/mathematics/18-755-introduction-to-lie-groups-fall-2004/readings /helga_sophusl1_1.pdf

(6) T. Dykerhoff. Tutorial on Differential Galois Theory 1. University of Pennsylvania, Department of Mathematics. http://users.math.yale.edu/ td276/lecture1.pdf.

(7) Marius van der Put. Galois Theory and Algorithms for Differential Equations. Journal of Symbolic Computation (39). 2005

(8) David Harbater, Julia Hartmann, Annette Maier. Differential Galois Groups over Laurent Series Fields. University of Pennsylvania. Preliminary, updated December 2014.

(9) //math.berkeley.edu/ reb/courses/261/12.pdf. No author or source attribution.

(10) Elzbieta Sowa. Picard-Vessiot Extensions for Real Fields. Proceedings of the American Mathematical Society. Volume 139, Number 7, July 2011.