# Some Differential Galois Theory



DEFINITION: Let $R$ be a (commutative) differential integral domain with 1. Use the usual abbreviation for our derivation: $\partial(a) = a'$. Let $R\{Y\} = R[Y, Y', Y'', \dots]$ (polynomials in variables $Y, Y', Y'', \dots$ and coefficients in $R$). We adopt the usual derivative notation: $Y^{(0)} = Y, Y^{(1)} = Y', Y^{(2)} = Y''$ etc. Extend the derivation on $R$ to a derivation on $R\{Y\}$ as follows: $\partial(Y^{(i)}) = Y^{(i+1)}$. This makes $R\{Y\}$ into a differential integral domain. This is the ring of polynomials in a **differential indeterminate** $Y$. Likewise, one can define $R\{Y_1, Y_2, \dots\}$ (differential polynomials in several or even infinitely many differential indeterminates).

Since $R$ is an integral domain, then so is any ring of polynomials with coefficients in $R$. Therefore, $R\{Y\}$ is an integral domain. We denote its field of fractions as $R\langle Y\rangle$. As discussed in our other handout, the derivation on a differential ring can be extended to its field of fractions in a unique way (using the quotient rule). Thus $R\langle Y\rangle$ is a differential field called **differential rational functions** in $Y$.

If $\mathbb{E}/\mathbb{K}$ is a differential field extension and $y_1, \dots, y_n \in \mathbb{E}$, we write $\mathbb{K}\{y_1, \dots, y_n\}$ for the differential subalgebra of $\mathbb{E}$ generated by $\mathbb{K}$ and $\{y_1, \dots, y_n\}$. Likewise, $\mathbb{K}\langle y_1, \dots, y_n\rangle$ is the differential subfield generated by $\mathbb{K}$ and $\{y_1, \dots, y_n\}$.

DEFINITION: Let $R$ be a differential ring and $y_1, \dots, y_n \in R$. We define the **Wronskian** of these elements as follows:

$$W(y_1, y_2, \dots, y_n) = \det\left(\begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix}\right)$$

Recall that when studying linear differential equations, one uses the Wronskian to determine whether a set of solutions is linearly independent or not.

DEFINITION: Let $\mathbb{E}$ be a differential field extension of a differential field $\mathbb{K}$. We say that $\mathbb{E}/\mathbb{K}$ is a **Picard-Vessiot** (read "Picard Vess-e-o") extension if $\mathbb{E}$ has no new constants (i.e. the constants of $\mathbb{E}$ and $\mathbb{K}$ are the same) and there exists some

$$\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y \in \mathbb{K}\langle Y\rangle$$

and $y_1, \dots, y_n \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{K}\langle y_1, \dots, y_n\rangle$, $\mathcal{L}(y_i) = 0$ for $i = 1, \dots, n$, and $W(y_1, \dots, y_n) \neq 0$.

This means that $\mathcal{L}(Y) = 0$ is an $n$-th order homogenous linear differential equation. We demand that $y_1, \dots, y_n$ is a fundamental solution set: $\mathcal{L}(y_i) = 0$ says that $y_i$ is a solution, $W(y_1, \dots, y_n) \neq 0$ says that these solutions are linearly independent. One can show that the solution set of $\mathcal{L}(Y) = 0$ is an $n$-dimensional (over the constants of $\mathbb{K}$) vector space. This means that if $\mathbb{C}$ is the field of constants of $\mathbb{K}$ (and $\mathbb{E}$) then the solution set of $\mathcal{L}(Y) = 0$ is $\text{span}_{\mathbb{C}}\{y_1, \dots, y_n\}$. Finally, $\mathbb{E} = \mathbb{K}\langle y_1, \dots, y_n\rangle$ says that $\mathbb{E}$ is generated by this solution set.

Some analogies: $\mathbb{K}\{Y\}$ is the differential analog of $\mathbb{K}[x]$ (polynomials). $\mathbb{K}\langle Y\rangle$ is the analog of $\mathbb{K}(x)$ (rational functions). Instead of a polynomial $f(x) \in \mathbb{K}[x]$, we have a differential operator $\mathcal{L}(Y)$. Instead of roots of $f(x)$, we have solutions of $\mathcal{L}$. Instead of a splitting field $\mathbb{E}$ being generated by the roots of $f(x)$, we have the Picard-Vessiot extension $\mathbb{E}$ generated by the solutions of $\mathcal{L}(Y) = 0$. Also, recall that $\mathbb{F}[x]/(p(x)) \cong \mathbb{F}[\alpha]$ if $p(x) \in \mathbb{F}[x]$ is irreducible and $p(\alpha) = 0$. Likewise, we can build $\mathbb{E} = \mathbb{K}\{Y\}/I$ where $I$ is the differential ideal generated by $\mathcal{L}(Y)$ and its dervatives. Then $\mathbb{E}$ extends $\mathbb{K}$ and has a solution "$Y + I$" for $\mathcal{L}(Y) = 0$.

At this point you might anticipate that *the* Picard-Vessiot extension of $\mathcal{L}(Y)$ over $\mathbb{K}$ is unique up to a differential isomorphism extending the identity on $\mathbb{K}$ (if we assume that we have an algebraically closed field of constants).

DEFINITION: Let $\mathbb{E}/\mathbb{K}$ be a differential field extension.

$$\text{Gal}(\mathbb{E}/\mathbb{K}) = \{\sigma : \mathbb{E} \to \mathbb{E} \mid \sigma \text{ is a differential field automorphism of } \mathbb{E} \text{ and } \sigma(x) = x \text{ for all } x \in \mathbb{K}\}$$

That is, $\text{Gal}(\mathbb{E}/\mathbb{F})$ is the automorphisms of $\mathbb{E}$ fixing $\mathbb{K}$ pointwise. We call this the **differential Galois group** of the differential field extension $\mathbb{E}/\mathbb{K}$.

Since every differential ring homomorphism is also a plain old ring homomorphism, we get that the differential Galois group is actually a subgroup of the regular Galois group of $\mathbb{E}/\mathbb{K}$ thought of as a plain old field extension.

As with regular Galois theory, if $\mathbb{E}/\mathbb{K}$ is the Picard-Vessiot extension of some linear differential equation $\mathcal{L}(Y) = 0$, we call $\text{Gal}(\mathbb{E}/\mathbb{K})$ the Galois group of $\mathcal{L}(Y)$.

Proposition 6.2.1 in [Crespo & Hajto] proves that for a Picard-Vessiot extension $\mathbb{E} = \mathbb{K}\langle y_1, \dots, y_n\rangle/\mathbb{K}$ where the constants $\mathbb{C}$ are algebraically closed, there exists a set of polynomials $S \subset \mathbb{C}[x_{11}, \dots, x_{1n}, x_{21}, \dots, x_{2n}, \dots, x_{n1}, \dots, x_{nn}]$

such that for all $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ and $\sigma(y_j) = \sum_i c_{ij} y_i$ (where $c_{ij} \in \mathbb{C}$) then $F(c_{11}, \ldots, c_{nn}) = 0$ for all $F \in S$. Also, given $C = (c_{ij}) \in \mathrm{GL}_n(\mathbb{C})$ such that $F(c_{11}, \ldots, c_{nn}) = 0$ for all $F \in S$, then $\sigma$ defined by $\sigma$ is the identity on $\mathbb{K}$ and $\sigma(y_j) = \sum_i c_{ij} y_i$ is always an element of $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$.

This Proposition tells us that the differential Galois group of a Picard-Vessiot extension is a closed subgroup of $\mathrm{GL}_n(\mathbb{C})$. In other words, these are **Linear Algebraic Groups**.

It turns out that $\dim(\mathrm{Gal}(\mathbb{E}/\mathbb{K}))$ equal to the transcendence degree of $\mathbb{E}/\mathbb{K}$.

$\boxed{\text{EXAMPLE:}}$ Notice $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$. The closed subgroups of this group are either the whole group itself (i.e. $\mathbb{C}^\times$) or finite (hence cyclic since finite subgroups of a group of units of a field must be cyclic). So the Galois group of any first order $\mathcal{L}(Y) = Y' + aY$, must be a subgroup of $\mathrm{GL}_1(\mathbb{C})$ and so it is either finite and cyclic or $\mathbb{C}^\times$.

Let $\mathbb{K} = \mathbb{C}(x)$. If $a = 0$, then $\mathcal{L}(Y) = Y'$. Here the solutions are just constants (i.e. $\mathbb{C}$). Thus $\mathbb{E} = \mathbb{K}\langle 1 \rangle = \mathbb{C}(x)$. Thus $\mathbb{E}/\mathbb{K}$ is trivial and so $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is trivial. On the other hand if $a \neq 0$, then $\mathcal{L}(Y) = Y' + aY = 0$ has solution $t = e^{-\int a}$. When $a \neq 0$, $t = e^{-\int a}$ is transcendental over $\mathbb{K} = \mathbb{C}(x)$. So $\mathbb{E} = \mathbb{C}(x, e^{-\int a})$ has transcendence degree 1 (over $\mathbb{K} = \mathbb{C}(x)$) and so the Galois group is 1 dimensional. Therefore, $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) = \mathbb{C}^\times$.

$\boxed{\text{THEOREM:}}$ (The fundamental theorem of differential Galois theory) Let $\mathbb{E}/\mathbb{K}$ be a Picard-Vessiot extension and $G = \mathrm{Gal}(\mathbb{E}/\mathbb{K})$. Assume that $\mathbb{C}$, the field of constants of $\mathbb{E}$ and $\mathbb{K}$, is algebraically closed. Then $H \mapsto \mathbb{E}^H$ and $\mathbb{F} \mapsto \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is an inclusion reversing bijection (and its inverse) from the collection of closed subgroups of $G$ to the set of intermediate differential fields of $\mathbb{E}/\mathbb{K}$.

Moreover, if $H$ is a closed normal subgroup of $G$, then $\mathbb{E}^H/\mathbb{K}$ is a Picard-Vessiot extension and $G/\mathrm{Gal}(\mathbb{E}/\mathbb{E}^H) \cong \mathrm{Gal}(\mathbb{E}^H/\mathbb{K})$. Also, if $\mathbb{F}/\mathbb{K}$ is Picard-Vessiot, then $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is a closed normal subgroup of $G$.

$\boxed{\text{DEFINITION:}}$ Let $\mathbb{E}/\mathbb{K}$ be a differential field extension. We say that $t \in \mathbb{E}$ is **integral** over $\mathbb{K}$ if $t' \in \mathbb{K}$ (i.e. $t = \int a$ for some $a \in \mathbb{K}$). We say that $t \in \mathbb{E}$ is **exponential integral** over $\mathbb{K}$ if $t \neq 0$ and $t'/t \in \mathbb{K}$ (i.e. $t' = at$ for some $a \in \mathbb{K}$ so that $t = \exp(\int a)$).

For example, $\mathbb{C}(x)/\mathbb{C}$ is an extension by an integral since $x = \int 1$. Whereas, $\mathbb{C}(x, e^{\mathrm{atan}(x)})/\mathbb{C}(x)$ is an extension by an exponential integral since $(e^{\mathrm{atan}(x)})'/e^{\mathrm{atan}(x)} = \dfrac{1}{x^2+1} \in \mathbb{C}(x)$ (i.e. $e^{\mathrm{atan}(x)} = e^{\int 1/(x^2+1)}$).

Adjunction of an integral yields a Galois group isomorphic to $\mathbb{C}$ (under addition). Adjunction of an exponential of an integral yields a Galois group isomorphic to $\mathbb{C}^\times$ (under multiplication). See [Crespo & Hajto] Example 6.1.4.

$\boxed{\text{DEFINITION:}}$ Let $\mathbb{K} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n = \mathbb{E}$ be a tower of differential fields and assume they all share the same algebraically closed field of constants (call this $\mathbb{C}$). Then $\mathbb{E}/\mathbb{K}$ is a **Liouville extension** if for $i = 1, \ldots, n$, $\mathbb{F}_i = \mathbb{F}_{i-1}(t)$ for some $t \in \mathbb{F}_i$ and $t$ is either algebraic, integral, or exponential integral over $\mathbb{F}_{i-1}$.

Let $\mathbb{E}/\mathbb{K}$ be a Picard-Vessiot extension associated with some $\mathcal{L}(Y)$. We say $\mathcal{L}(Y) = 0$ is **solvable** (by a finite number of integrations) if there exists some Liousville extension $\mathbb{L}/\mathbb{K}$ with $\mathbb{E}$ a differential subfield of $\mathbb{L}$.

So $\mathcal{L}(Y) = 0$ is solvable if its solutions can be obtained after a finite number of integrations, exponentiations, and algebraic operations.

*Note:* Liouville extensions can be arranged so that $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$ where $\mathbb{F}/\mathbb{K}$ is a Galois extension (in the standard Galois theory sense) and $\mathbb{E}/\mathbb{K}$ is the result of adjoining integrals and exponentials of integrals (i.e. you can arrange your tower so that all of the algebraic stuff is attached first). This is why [Crespo & Hajto] don't allow for adjoining algebraic stuff in their Liouville extensions (they assume your base field already includes all that stuff).

Algebraic groups are a good deal more complicated than finite groups. There is a way to define "connectedness" in such groups. It turns out that, given an algebraic group $G$, the connected component at the identity $G_0$ (this is the connected piece of the algebraic group $G$ which contains the identity) is in fact a subgroup of $G$. An algebraic group is called **virtually solvable** if $G_0$ is solvable.

$\boxed{\text{THEOREM:}}$ Liouville extensions have virtually solvable differential Galois groups. Moreover, $\mathcal{L}(Y) = 0$ is solvable if and only if its differential Galois group is virtually solvable.

$\boxed{\text{EXAMPLE:}}$ $\mathbb{C}(x)$ is a Picard-Vessiot (and Liouville) extension of $\mathbb{C}$. It is Picard-Vessiot with respect to $\mathcal{L}(Y) = Y''$. Notice that $\{1, x\}$ form a solution set for $Y'' = 0$ also $W(1, x) = \det \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = 1 \neq 0$. Clearly, $\mathbb{C}(x) = \mathbb{C}(x, 1)$. It is Liouville since $x = \int 1$ is integral over $\mathbb{C}$.

$$\mathrm{Gal}(\mathbb{C}(x)/\mathbb{C}) \cong \mathbb{C} \text{ (under addition) } \cong \left\{ \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \;\middle|\; c \in \mathbb{C} \right\} \text{ (a closed subgroup of } \mathrm{GL}_2(\mathbb{C}))$$

$\boxed{\text{EXAMPLE:}}$ Let $\mathcal{L}(Y) = Y'' + 2xY' \in \mathbb{C}(x)\{Y\}$. Let $\mathbb{E}/\mathbb{K} = \mathbb{C}(x)$ be the Picard-Vessiot extension for $\mathcal{L}(Y) = 0$. We have that $\mathbb{E} = \mathbb{C}(x)\langle 1, y\rangle$ for some solutions $\{1, y\}$. We must have $W(1, y) = \det \begin{bmatrix} 1 & y \\ 0 & y' \end{bmatrix} = y' \neq 0$. In fact, [Magid] in Example 6.10 shows that $y' \notin \mathbb{C}(x)$. Moreover, he also shows that $y \notin \mathbb{C}(x, y')$. We get the following tower:

$$\mathbb{K} = \mathbb{C}(x) \subsetneq \mathbb{L} = \mathbb{K}(y') \subsetneq \mathbb{E} = \mathbb{K}(y)$$

Consider some $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ then $\sigma(y)$ must be some solution of $\mathcal{L}(Y) = 0$ since $\sigma$ must send solutions to solutions (like old school Galois theory sent roots to roots). Thus $\sigma(y) = c1 + dy$ for some $c, d \in \mathbb{C}$. Notice that $\sigma(y') = \sigma(y)' = (c + dy)' = dy'$. Because $\sigma$ is a bijection, $d \neq 0$. This gives us that

$$\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \cong \left\{ \begin{bmatrix} 1 & c \\ 0 & d \end{bmatrix} \;\middle|\; c, d \in \mathbb{C} \text{ and } d \neq 0 \right\} \text{ (a closed subgroup of } \mathrm{GL}_2(\mathbb{C}))$$

Now that this is done, we'll let the out our secret: $y = \int e^{-x^2}\,dx$ $\quad [y' = e^{-x^2}$ and $y'' = -2xe^{-x^2}$ so that $y'' + 2xy' = 0.]$

$\boxed{\text{THEOREM:}}$ Let $\mathbb{C}$ be algebraically closed and $\mathbb{F} = \mathbb{C}(x)$ with $x' = 1$. Let $\mathcal{E}/\mathbb{F}$ be an elementary extension and $\mathbb{E}/\mathbb{F}$ a Picard-Vessiot extension with $\mathbb{E} \subseteq \mathcal{E}$. Then the connected component of the identity of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is abelian.

This is Proposition 6.12 in [Magid]. Notice that in the above example, $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is not an abelian group. This means that $\mathbb{E}/\mathbb{K}$ is not contained in an elementary extension. Thus $y = \int e^{-x^2}\,dx$ is not elementary! On the other hand, $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is virtually solvable, so $y = \int e^{-x^2}\,dx$ does lie in a Liouville extension (this is kind of a silly observation – $y$ is obviously an integral of an exponential of an integral).

$\boxed{\text{EXAMPLE:}}$ Let $\mathcal{L}(Y) = Y'' - xY$ and let $\mathbb{E}$ be the Picard-Vessiot extension of $\mathbb{C}(x)$ associated with $\mathcal{L}(Y) = 0$. In [Magid] Example 6.21, it is shown that $\mathrm{Gal}(\mathbb{E}/\mathbb{C}(x)) \cong \mathrm{SL}_2(\mathbb{C}) = \{A \in \mathbb{C}^{2\times 2} \mid \det(A) = 1\}$. Now $\mathrm{SL}_2(\mathbb{C})$ is not a virtually solvable group. This means that $\mathbb{E}/\mathbb{C}(x)$ is not embeddable in a Liouville extension. This means that $Y'' - xY = 0$ has a solution $y = f(x)$ such that $f(x)$ is not obtainable from $\mathbb{C}(x)$ by a finite number of steps of algebra, integration, and exponentiation. This makes $f(x)$ *way* beyond being elementary.

The equation $y'' - xy = 0$ is called the **Airy equation**. One of it solutions (one that you can't get to by integration and algebra) is called the **Airy function**.

My main references for this are [Crespo & Hajto] and [Magid]. Both books are well written and modern. [Crespo & Hajto] is a bit easier to read and includes a careful development of algebraic groups. [Magid] has some interesting examples and results that are lacking in the other text. The books [Ritt] and [Kaplansky] are interesting as well, but a bit dated. The large text [Put & Singer 2003] is much more in depth than these other books, but it is written at level which makes it much less accessible.

We have seen Galois theory (for polynomials) and differential Galois theory (for linear differential equations). It is interesting to note that one can develop a Galois theory for linear difference equations (kind of like a discrete version of differential equations). This is done in [Put & Singer 1997] and it looks a lot like the theories we've explored.

# References


[Crespo & Hajto] T. Crespo and Z. Hajto, *Algebraic Groups and Differential Galois Theory*, AMS Graduate Studies in Mathematics **Vol. 122** (2011).

[Kaplansky] I. Kaplansky, *An Introduction to Differential Algebra*, Publications of De L'Institut De Mathematique De L'Universite De Nancago (1957).
Available free online at: http://mmrc.iss.ac.cn/∼weili/DifferentialAlgebra/References/Kaplansky.pdf

[Magid] A. Magid, *Lectures on Differential Galois Theory*, AMS University Lecture Series **Vol. 7** (1994).

[Put & Singer 1997] M. van der Put, M. Singer, *Galois Theory of Difference Equations*, Lecture Notes in Mathematics, Spring-Verlag (1997).

[Put & Singer 2003] M. van der Put, M. Singer, *Galois Theory of Linear Differential Equations*, Springer (2003).
Available free online at: https://singer.math.ncsu.edu/papers/dbook.ps

[Ritt] J. Ritt, *Differential Algebra*, Dover Publications (1950).