DIFFERENTIAL GALOIS THEORY

SARAH FUJIMORI

1. Introduction

Classical Galois theory gives us the machinery to characterize the solutions of polynomial equations (for example, the Abel-Ruffini Theorem states that there is no formula for arbitrary polynomials of degree 5 or higher in terms of radicals). In this paper, we will introduce differential Galois theory, which will allow us to characterize solutions of differential equations. We will define differential fields and Picard-Vessiot extensions, and construct the differential Galois group. We will also prove an analogue of the Galois correspondence for Picard-Vessiot extensions, and a theorem that allows us to identify which functions are not elementary integrable. This paper assumes knowledge of group theory, basic calculus, linear algebra, and Galois theory.

2. Differential Fields

We begin by introducing a differential field, which is a field where we can take derivatives of elements:

Definition 2.1. A **differential field** is a field K with $\mathrm{char}(K) = 0$, endowed with a derivation $D : K \to K$ such that

(1) D is additive, i.e. $D(x + y) = D(x) + D(y)$.
(2) D satisfies the product rule, i.e. $D(xy) = xD(y) + yD(x)$.

We will sometimes denote $D(x)$ as x'.

Example. The trivial derivation is $D(x) = 0$ for all $x \in K$. The field $\mathbb{C}(x)$ with the trivial derivation would be an example of a differential field.

Example. The field of rational functions $\mathbb{R}(x)$, using the derivative we are familiar with, is also an example of a differential field.

An important subfield of a differential field to consider is the kernel of the derivation:

Definition 2.2. Let $C_K = \{x \in K : Dx = 0\}$. We call C_K the **field of constants**.

Example. The field of constants of $\mathbb{R}(x)$ (with the usual derivation) would be $\mathbb{R}$.

Now that we have a derivative, it is natural to consider linear differential equations:

Definition 2.3. Let K be a differential field. A **linear differential equation** over K is an equation of the form $a_nD^n(x) + \cdots + a_1D(x) + a_0 = 0$ for $a_0, a_1, \ldots, a_n \in K$, where $D^i(x)$ denotes the ith derivative of x. The roots of this equation are called the **solutions**. The **order** of the equation is n.

Example. An example of a differential equation over $\mathbb{Q}$ is $x' - 3x = 0$, which has order 1. An example of a solution of this equation is e^{3x}.

Nonexample. The equation $x'' + (x')^2 + 2 = 0$ over $\mathbb{R}(x)$ would not be an example of a linear differential equation, because it is not in the form $a_n D^n(x) + \cdots + a_1 D(x) + a_0$ for $a_0, a_1, \ldots, a_n \in K$.

Definition 2.4. Let $y_1, y_2, \ldots, y_n$ be elements of a differential field K. Define the **Wronskian** $W(y_1, y_2, \ldots, y_n)$ as the determinant of the matrix

$$\begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix}$$

Example. We take K to be $\mathbb{Q}(x)$. Then, $W(1, 2y^2) = \det \begin{bmatrix} 1 & 2y^2 \\ 0 & 4y \end{bmatrix} = 4y$.

Example. We can also come up with an example where the Wronskian is zero. Let $K = \mathbb{Q}(x)$ again; we calculate $W(y, 2y^2, y^2)$:

$$\det \begin{bmatrix} y & 2y^2 & y^2 \\ 1 & 4y & 2y \\ 0 & 4 & 2 \end{bmatrix} = y(8y - 8y) - 2y^2(2 - 0) + y^2(4 - 0) = 0.$$

Notice that in the first example, the elements are linearly independent and the Wronskian is nonzero, whereas in the second example, the elements are linearly dependent and the Wronskian is zero. The reason we care about this determinant is because of this property:

Proposition 2.5. *$W(y_1, y_2, \ldots, y_n) = 0$ if and only if $y_1, y_2, \ldots y_n$ are linearly dependent over C_K.*

Proof. ($\Longleftarrow$) Suppose the y_i's are linearly independent; then, there exist constants that are not all 0 such that $\sum_{i=1}^n c_i y_i = 0$. Differentiating this equality gives us

$$\sum_{i=1}^n c_i y_i^{(k)} = 0, 0 \le k \le n-1$$

This means that the columns of the matrix are linearly dependent, so the determinant $W(y_1, y_2, \ldots, y_n) = 0$.

($\Longrightarrow$) We want to show that if $W(y_1, y_2, \ldots, y_n) = 0$, then $(y_1, y_2, \ldots, y_n)$ are linearly dependent. If $\det(A) = 0$, then there exist $c_i \in L$ which are not all 0, such that $\sum_{i=1}^n c_i y_i^{(k)} = 0$ for all $0 \le k \le n-1$.

We can assume that $c_1 = 1$ and $W(y_2, \ldots, y_n) \neq 0$. If we differentiate the equality $\sum_{i=1}^n c_i y_i^{(k)} = 0$, we get

$$\sum_{i=1}^n c_i y_i^{(k+1)} + \sum_{i=1}^n c_i' y_i^{(k)} = 0.$$

We know that $\sum_{i=1}^n c_i y_i^{(k+1)} = 0$, so $\sum_{i=1}^n c_i' y_i^{(k)} = 0$. But since $W(y_2, \ldots, y_n) \neq 0$, by the other direction of Proposition 2.5, we know that $c_i' = 0$, i.e. the c_i's are constants. Taking $k = 0$ gives us the relation $\sum_{i=1}^n c_i y_i = 0$, so the y_i's are linearly dependent.

□

3. Picard-Vessiot Theory and the Differential Galois Group

Recall that in classic Galois theory, we have splitting fields, where we adjoin all roots of a polynomial to the base field F. In differential Galois theory, we have the following analogue of the splitting field, where instead of adjoining all roots to a polynomial, we adjoin all solutions of a differential equation:

Definition 3.1. Let $\mathcal{L}(y)$ be a differential equation of order n, over a differential field K. A field extension L/K is a **Picard-Vessiot extension** if

(i) $L = K(y_1, y_2, \ldots y_n)$, where $y_1, y_2, \ldots y_n$ are solutions to $\mathcal{L}(y) = 0$.
(ii) $C_L = C_K$, i.e. L has no constants that are not in K.

Definition 3.2. Let L be a Picard-Vessiot extension L/K. The **differential Galois group** is the group of automorphisms σ of L that commute with the derivation, i.e. $\sigma(x') = (\sigma(x))'$. We denote this group by $G(L/K)$ or $\mathrm{Gal}(L/K)$.

Example. We can construct a Picard-Vessiot extension from the solutions to a differential equation. Let $K = \mathbb{C}(z)$, and consider the equation $zy'' + y' = 0$. The solutions to this equation are $k_1 \ln(z) + k_2$, where $k_1, k_2 \in \mathbb{C}$. Then, the resulting extension $E = \mathbb{C}(z, \ln z)$ is Picard-Vessiot.

Recall that we define automorphisms of a field extension by where they map the generators. An automorphism in the differential Galois group clearly needs to map $z \mapsto z$, and it needs to map a solution $k_1 \ln(z) + k_2$ to another solution in the form $k_1' \ln(z) + k_2$. Thus, any σ would be in the form of $\sigma(\ln(z)) = a \ln(z) + b$. Since the automorphism must commute with the derivation, we compute $\sigma(x')$ and $(\sigma(x))'$:

$$\sigma\left(\frac{d}{dz}\ln(z)\right) = \sigma\left(\frac{1}{z}\right) = \frac{1}{z}$$

(Note that $\sigma\left(\frac{1}{z}\right) = \frac{1}{z}$ because $\frac{1}{z}$ lies in the base field $\mathbb{C}(z)$). We set this equal to

$$\frac{d}{dz}\sigma(\ln z) = \frac{d}{dz}(a \ln z + b) = \frac{a}{z}$$

so we can see that all automorphisms map $\ln z \mapsto \ln(z) + b$, where b is a constant. This means that the Galois group of E/K is the group of complex numbers under addition.

Recall that in classical Galois theory, we want the automorphisms in the Galois group to fix the base field. We can show that this holds for Picard-Vessiot extensions with the following proposition:

Proposition 3.3. *Let K be a differential field with the field of constants C_K algebraically closed. Then the following hold:*

(i) *If L/K is a Picard–Vessiot extension, then there is $\sigma \in \mathrm{Aut}(L/K)$ such that $\sigma(x) \neq x$.*
(ii) *Let $M/L/K$ be a tower of field extensions such that L/K and M/K are Picard–Vessiot. Then any $\sigma \in \mathrm{Aut}(L/K)$ can be extended to an automorphism of M.*

Proof. We refer the reader to [CH11] Proposition 6.1.2 for a proof. □

This proposition has the following useful corollary:

Corollary 3.4. *If L/K is a Picard-Vessiot extension, then $L^{G(L/K)} = K$.*

4. The Zariski Topology

In this section, we define and discuss the Zariski topology, which is an important structure used in the Galois correspondence. See [Mic19] for more detail, or for background on ideals of rings.

Let F be a differential field with field of constants C_K, and let K/F be a Picard-Vessiot extension corresponding to an equation L. Any automorphism σ in the differential Galois group $G(K/F)$ fixes elements of F, so it sends solutions of L to other solutions. This means that we can think of $G(K/F)$ as a linear transformation of the solution space V represented as a matrix M.

The advantage of thinking of $G(K/F)$ as a group of matrices is the following:

Proposition 4.1. *The Galois group is isomorphic to a subgroup of* $\mathrm{GL}(n, C_K)$.

Example. Consider our previous example, with equation $zy'' + y' = 0$ and Picard-Vessiot extension $E(z, \ln(z))$ over $\mathbb{C}(z)$. Recall that the automorphisms were in the form of $\ln z \mapsto \ln z + a$ for $a \in \mathbb{C}$. If we view the solution space, which is the set of all expressions in the form $k_1 \ln(z) + k_2$ for $k_1, k_1 \in \mathbb{C}$, as a vector space over $\mathbb{C}$, we can write down the automorphism as the matrix

$$M_a = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$$

Suppose we have two such matrices, for $a_1, a_2 \in \mathbb{C}$. If we multiply them, we get

$$M_{a_1} M_{a_2} = \begin{bmatrix} 1 & a_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_1 + a_2 \\ 0 & 1 \end{bmatrix}$$

Notice that this aligns with our definitions of the automorphisms: if we compose the map $\ln(z) \mapsto \ln(z) + a_1$ with the map $\ln(z) + a_2$, then we get the map $\ln(z) \mapsto \ln(z) + a_1 + a_2$, which corresponds to the matrix above. In the case, the Galois group is isomorphic to the group

$$\left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{C} \right\} \leq \mathrm{GL}(2, \mathbb{C})$$

This allows us to endow the Galois group with the Zariski topology, which is an important and useful structure on $G(K/F)$. We begin by defining a topological space.

Definition 4.2. A **topological space** is a set X together with a set τ of subsets of X satisfying the following:

(i) The empty set and X are in τ.
(ii) Any arbitrary intersection (finite or infinite) of sets in τ is an element of τ.
(iii) Any finite union of sets in τ is an element of τ.

The subsets in τ are called the **closed sets**.

To define the Zariski topology, we need to define which sets are closed:

Definition 4.3. Let C be a field. A set is closed in the **Zariski topology** if it is of the form $\mathcal{V}(S) = \{x \in C^n : f(x) = 0 \forall f \in S\}$ for some set $S \subseteq C[x_1, x_2, \ldots, x_n]$.

It can be easily shown that the Zariski topology satisfies the properties above, i.e.:

Proposition 4.4. *The Zariski topology satisfies the following:*

(i) $C^n = \mathcal{V}(0), \varnothing = \mathcal{V}(C[x_1, x_2, \ldots, x_n])$.

(ii) *If I and J are ideals of $C[x_1, x_2, \ldots, x_n]$, then $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ)$.*
(iii) *If $\{I_\alpha\}$ is a set of ideals in $C[x_1, x_2, \ldots, x_n]$, then $\cap_\alpha \mathcal{V}(I_\alpha) = \mathcal{V}(\sum_\alpha I_\alpha)$.*

Because the differential Galois group is isomorphic to a subgroup of $\mathrm{GL}_n(C)$, it is endowed with the Zariski topology.

5. The Galois Correspondence

Recall that in classical Galois theory, for a Galois extension K/F, we have a bijective correspondence between intermediate fields and subgroups of the Galois group $\mathrm{Gal}(K/F)$; and that the normality of a subgroup of $\mathrm{Gal}(K/F)$ gives us information about the corresponding intermediate field. In differential Galois theory, we have the following analogue of the Galois correspondence:

Theorem 5.1 (Picard–Vessiot)**.** *Let L/K be a Picard-Vessiot extension of degree n, and let $G(L/K)$ be the differential Galois group. Then the following hold:*
(i) *There is a bijective correspondence between Zariski closed subgroups H of $G(L/K)$ and intermediate fields F given by $\phi(F) = G(F/K)$ with inverse $\psi(H) = L^H$.*
(ii) *An intermediate field F satisfying $K \subset F \subset L$ is a Picard-Vessiot extension of K iff $G(L/F)$ is normal in $G(L/K)$. Then, $G(L/K)/G(L/F) \cong G(F/K)$.*

Before we prove this theorem, we give a simple example of how this correspondence works:

Example. Take $K = \mathbb{C}(z)$, and consider the differential equation $y' - y = 0$. The solutions to this differential equation are in the form ke^z, where $k \in \mathbb{C}$, so the extension $L = \mathbb{C}(z, e^z)$ is a Picard-Vessiot extension. We can easily see that the automorphisms for L/K map $e^z \mapsto ae^z$, where $a \in \mathbb{C}$. Note that since the order is 1, the differential Galois group is just the entire group $GL(1, \mathbb{C})$. We can consider the subgroup of the roots of unity, which we denote as μ_n. An automorphism $\sigma(e^z) = \zeta e^z$ sends e^{kz} to $\sigma(e^z)^k = \zeta^k e^{kz}$, so $L^{\mu_n} = \mathbb{C}(z, e^{nz})$.

We also have $\mu_n \lhd G(L/K)$, and indeed, the intermediate field $\mathbb{C}(z, e^{nz})$ is the Picard-Vessiot extension corresponding to the differential equation $y' = ny$.

Proof of Theorem 5.1, part (i). We follow the proof from [CH11].

We show that the maps $\phi \circ \psi$ and $\psi \circ \phi$ are the identity maps on the set of Zariski closed subgroups of $G(L/K)$ and the set of intermediate field between L and K, respectively. For $\psi \circ \phi$, we have

$$\psi \circ \phi(F) = \psi(G(F/K)) = L^{G(F/K)}$$

which is just F by Corollary 3.4.

For $\phi \circ \psi$, we need to prove that $L^{G(L/F)} = F$ for an intermediate field F. For $H \leq G(L/K)$, let $H' = G(L/L^H)$. We show that H' is the Zariski closure of H in G, i.e. H' is the smallest Zariski closed set containing H. Assume for contradiction that this is false, i.e. if $L = K\langle y_1, y_2, \ldots y_n\rangle$, there exists f on $\mathrm{GL}(n, C_K)$ such that $f = 0$ on H but not on H' (remember that H and H' can be represented as subgroups of $\mathrm{GL}(n, C_K)$.)

Let $u_1, u_2, \ldots u_n$ be variables. Consider the two matrices

$$A = \begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix}, B = \begin{bmatrix} u_1 & u_2 & \cdots & u_n \\ u_1' & u_2' & \cdots & u_n' \\ \vdots & \vdots & \ddots & \vdots \\ u_1^{(n-1)} & u_2^{(n-1)} & \cdots & u_n^{(n-1)} \end{bmatrix}$$

where $x^{(k)}$ denotes the kth derivative of x. Recall from Proposition 2.5 that $\det(A) \neq 0$, since the y_i's are linearly independent. This means that A is invertible.

Let $F(u_1, u_2, \dots u_n) = f(A^{-1}B)$. We claim that

$$F(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_n)) = 0$$

for all $\sigma \in H$, but not all $\sigma \in H'$. Let M_σ be a matrix representation of σ, i.e.

$$(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_n)) = (y_1, y_2, \dots, y_n)M_\sigma$$

. Then, we compute B for $(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_n))$ (remember that σ commutes with the derivation):

$$B = \begin{bmatrix} \sigma(y_1) & \sigma(y_2) & \cdots & \sigma(y_n) \\ \sigma(y_1)' & \sigma(y_2)' & \cdots & \sigma(y_n)' \\ \vdots & \vdots & \ddots & \vdots \\ \sigma(y_1)^{(n-1)} & \sigma(y_2)^{(n-1)} & \cdots & \sigma(y_n)^{(n-1)} \end{bmatrix} = \begin{bmatrix} \sigma(y_1) & \sigma(y_2) & \cdots & \sigma(y_n) \\ \sigma(y_1') & \sigma(y_2') & \cdots & \sigma(y_n') \\ \vdots & \vdots & \ddots & \vdots \\ \sigma(y_1^{(n-1)}) & \sigma(y_2^{(n-1)}) & \cdots & \sigma(y_n^{(n-1)}) \end{bmatrix}$$

Since each row is now in the form of $(\sigma(x_1), \sigma(x_2), \dots, \sigma(x_n))$, we can express this in terms of M_σ:

$$= \begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix} M_\sigma = AM_\sigma$$

We conclude that

$$F(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_n)) = f(A^{-1}AM_\sigma) = f(M_\sigma)$$

So by the definition of f, $f(M_\sigma) = 0$ for $\sigma \in H$, but not always for $\sigma \in H'$.

We have now shown that there exists a polynomial F such that $F(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_n))$ is 0 for $\sigma \in H$, but not always for $\sigma \in H'$. We can then take F to be the shortest such polynomial (i.e., has the smallest number of terms) that satisfies this property. We will use a minimality argument to show that F is 0 for all $\sigma \in H'$, which will be our contradiction.

Let $\tau \in H$, and let τF be the polynomial we get when we apply τ to the coefficients of F. Then,

$$(\tau F)(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_n)) = \tau(F(\tau^{-1}\sigma(y_1), \tau^{-1}\sigma(y_2), \dots, \tau^{-1}\sigma(y_n)))$$

This is equal to 0 for all $\sigma \in H$ because $\tau^{-1}\sigma \in H$. We can see that this quantity should also be 0 for all $\sigma \in H'$, or else we can find some $a \in L$ such that $G = F - a(F - \tau F)$ is shorter than F, but still shares the property that $G(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_n))$ is 0 for all $\sigma \in H$. Since $F - \tau F = 0$ for all $\tau \in H$, we know the coefficients of F are invariant under H.

Notice now that F has coefficients in L^H. We defined H' to be $G(L/L^H)$, so

$$L^{H'} = L^{G(L/L^H)} = L^H$$

Thus, the coefficients of F are also invariant under H', and we have for $\sigma \in H'$:

$$F(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_n)) = (\sigma F)(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_n))$$

$$= \sigma(F(\sigma^{-1}\sigma(y_1), \sigma^{-1}\sigma(y_2), \ldots, \sigma^{-1}\sigma(y_n))) = \sigma(F(y_1, y_2, \ldots y_n)) = 0$$

which is a contradiction to our statement that $F(\sigma(y_1), \sigma(y_2), \ldots, \sigma(y_n))$ is not 0 for all $\sigma \in H'$. This completes the proof of part (i). □

To prove the second part of the theorem, we first need the following lemmas:

Lemma 5.2. *Let $L/F/K$ be a tower of field extensions, and let $G = \mathrm{Gal}(L/K)$. Then, F is G-stable, i.e. for $\sigma \in G$ and $a \in F$, we have $\sigma a \in F$.*

Proof. See [CH11]Proposition 5.6.6 for a proof. □

Lemma 5.3. *Suppose for some tower of field extensions $L/F/K$, F is $G(L/K)$-stable. Then, $G(L/F) \triangleleft G(L/K)$.*

Proof. Let $\sigma \in G(L/K)$ and $\tau \in G(L/F)$. We want to show that $\sigma^{-1}\tau\sigma \in G(L/F)$, i.e. for $a \in F$, we have $\sigma^{-1}\tau\sigma a = a$. This is equivalent to $\tau\sigma a = \sigma a$. Since F is $G(L/K)$-stable, $\sigma a \in F$, and since $\tau \in G(L/F)$, it fixes all elements in F. We conclude that $\sigma^{-1}\tau\sigma a = a$, so $G(L/F) \triangleleft G(L/K)$. □

Proof of Theorem 5.1, part (ii). ($\Longrightarrow$) Let F be an intermediate field with $L/F/K$, and suppose F is a Picard-Vessiot extension of K. Then, we show that $G(L/F) \triangleleft G(L/K)$ and $G(L/K)/G(L/F) \cong G(F/K)$.

By Lemma 5.2, we know that F is $G(L/K)$-stable, so by Lemma 5.3, $G(L/F) \triangleleft G(L/K)$. To show $G(L/K)/G(L/F) \cong G(F/K)$, let $\Phi : G(L/K) \to G(F/K)$ map σ to σ_F, the restriction of σ to F (we can do this because F is $G(L/K)$-stable).

Then, $\ker(\Phi)$ is the set of automorphisms of L which fix F, so $\ker(\Phi) = G(L/F)$. Furthermore, by Proposition 3.3 part (ii), $\mathrm{im}(\Phi) = G(F/K)$. Thus, $G(L/K)/\ker(\Phi) \cong \mathrm{im}(\Phi)$, so $G(L/K)/G(L/F) \cong G(F/K)$.

($\Longleftarrow$) See [CH11]Proposition 6.3.5 for a proof of the other direction, which is much more difficult. □

6. Solutions of Differential Equations

In this section, we discuss the application of the Galois correspondence to solutions to differential equations. To begin, we define Liouvillian extensions:

Definition 6.1. An extension of differential fields L/K is called **Liouvillian** if $C_L = C_K$ and there exist fields $K = F_1 \subset F_2 \subset \cdots \subset F_n = L$ such that for each i, $F_{i+1} = F_i(t_i)$ is one of the following:

(i) an **extension by integral**, i.e. $t_i' \in K_i$
(ii) an **extension by exponential**, i.e. $t_i'/t_i \in K_i$
(iii) an **algebraic extension**, i.e. t_i is algebraic over K_i

The notions of a Picard-Vessiot extension and a Liouvillian extension are actually quite different, in the sense that a Liouvillian extension is not necessarily a Picard-Vessiot extension. An example of this is the differential field extension $K(t, f)/K$, where t is transcendental over K and $\frac{t'}{t} \in K^{\times}$; and f is algebraic over $K(t)$ with $f^2 = 1 - t^2$. This field extension is clearly Liouvillian, but turns out to not be a Picard-Vessiot extension; see [Wu] for an explanation of this.

The connection between Picard-Vessiot extensions and Liouvillian extensions can be described by the differential Galois group. We first define the identity component of the differential Galois group:

Definition 6.2. An **irreducible component** is a subset of a topological group that cannot be written as the union of two proper closed subsets.

Definition 6.3. The **identity component** of a topological group G is the unique irreducible component containing the identity, as is denoted G^0.

Proposition 6.4. *G^0 is a normal subgroup of G.*

Proof. Note that for any $x \in G$, xG^0x^{-1} is an irreducible component which contains e. Since the identity component is the unique irreducible component containing the identity, we conclude that $xG^0x^{-1} = G^0$. This means that $G^0 \triangleleft G$. □

It turns out that if L/K is a Picard-Vessiot extension, then there exists an intermediate field F such that L/F is a Liouville extension, and F/K is a finite normal extension.

Theorem 6.5. *Let K be a differential field with C_K algebraically closed. Let L/K be a Picard-Vessiot extension, and suppose the identity component of the differential Galois group G^0 is solvable. Then, L can be obtained from K by a finite normal extension followed by a Liouville extension.*

Proof. The idea of the proof is that G^0 is a normal subgroup of $G(L/K)$ with finite index (by Proposition 6.4), so by the Galois correspondence, $F = L^{G^0}$ is a finite normal extension. We then have to show that L/F is a Liouville extension, which we can do using the Lie-Kolchin Theorem from representation theory. We refer the reader to [CH11]Theorem 6.5.2 for more details. □

We can actually prove something even stronger:

Theorem 6.6 (Liouville)**.** *Let L/K be a Picard-Vessiot extension, and let G be the differential Galois group. The following are equivalent:*

(1) *G^0 is a solvable group.*
(2) *L/K is Liouvillian.*
(3) *L is contained in a Liouvillian extension of K.*

Proof. We refer the reader to [Wu] for a proof. □

Liouville extensions are useful because we can use them to characterize which elements of a differentiable field are elementary integrable:

Theorem 6.7 (Liouville)**.** *Let K be a differential field, and let $\alpha \in K$. Suppose E/K is a Liouvillian extension, and there is $y \in E$ with $y' = \alpha$. Then, there exist $v, u_1, u_2, \dots u_m \in K$ with $u_i \neq 0$ for each i, and $c_1, c_2, \dots c_m \in C_K$ such that*

$$\alpha = D(v) + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}$$

Proof. The full proof is out of the scope of this paper; we will give a very brief outline.

Let $E = K(t_1, t_2, \ldots, t_N)$; we use induction on N. The case of $N = 0$ is easy, since then $y \in K$. Suppose the claim holds for some $N > 0$. Since E/K is a Liouvillian extension, we have the following chain of intermediate fields:

$$K \subset K(t_1) \subset K(t_1, t_2) \subset \cdots \subset K(t_1, t_2, \ldots, t_N)$$

We can now apply the induction hypothesis to the field extension $K(t_1, t_2, \ldots, t_N)/K(t_1)$. Then, we can express α as

$$\alpha = D(v) + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}$$

but with $v, u_1, u_2, \ldots, u_m \in K(t_1)$ instead of K. We know that t_1 is either an algebraic element, a logarithm, or an exponential, so the rest of the proof is to analyze each case and use the properties of t_1 to express α in the desired form. The casework is rather technical, so we skip it; see [Ros72] for the full proof. □

A special case of this theorem gives us the following result:

Theorem 6.8. *Let K be a differential field, and suppose that L/K is a field extension satisfying $C_L = C_K$ and $L = K(e^g)$ for some $g \in K$ such that e^g is transcendental over K. Then, for $f \in L$, fe^g is elementary integrable iff there exists $a \in E$ with $f = a' + ag'$.*

Proof. We refer the reader to [Con05] for a proof. □

Corollary 6.9. *e^{-t^2} has no elementary antiderivative.*

Proof. We take $K = \mathbb{C}(x)$, $f = 1$, and $g = -x^2$ in Theorem 6.8, so $a' + ag' = 1$ for some $a \in \mathbb{C}(x)$. If $a = \frac{p}{q}$ where $\gcd(p, q) = 1$ and p, q are polynomials, then

$$\frac{qp' - q'p}{q^2} + 2\frac{px}{q} = 1$$

Rearranging this, we get

$$q - 2px - p' = \frac{q'p}{q}$$

If we compare the left hand side and right hand side, we conclude that $q \mid q'p$. But we assumed that $\gcd(q, p) = 1$, so then we have $q \mid q'$. The only way this can happen is if q is constant, so without loss of generality we can now assume that $a = p$ for some polynomial p. Then, if we consider the equation $1 = a' + 2ax$, we know that the right side has degree ≥ 1 in x, while the left side clearly has degree 0 in x. This is a contradiction, so we are done. □

For a more thorough characterization of solutions to differential equations using representation theory, we refer the reader to [Kam]. Basic background on representation theory can be found in [EGH+11].

References

[CH11] Teresa Crespo and Zbigniew Hajto. *Algebraic groups and differential Galois theory*, volume 122. American Mathematical Soc., 2011.

[Con05] Brian Conrad. Impossibility theorems for elementary integration. 2005.

[EGH+11] Pavel I Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. *Introduction to representation theory*, volume 59. American Mathematical Soc., 2011.

[Kam] Moshe Kamensky. Differential galois theory.

[Mic19] Oscar Michel. An introduction to the zariski topology. 2019.
[Ros72] Maxwell Rosenlicht. Integration in finite terms. *The American Mathematical Monthly*, 79(9):963–972, 1972.
[Wu] Ju-Feng Wu. Galois correspondence and liouvillian extensions.