Exposition of the Fundamental Theorem of Differential Galois Theory

Contents

EXPOSITION OF THE FUNDAMENTAL THEOREM OF DIFFERENTIAL GALOIS THEORY

H.R.LAW

Abstract. This paper introduced the fundamental theorem of Galois theory and the background of differential Galois theory. This paper followed [Kaplansky] to make an elementary exposition of the fundamental theorem of differential Galois theory. I streamlined and make a briefer narration based on Kaplansky's narration. The proofs and statements are exactly from [Kaplansky]. I read and prepare examples as well as the proofs in [Kaplansky]. I added more geometric considerations in this paper like its connections with arithmetic algebraic geometry and Diophantine geometry. And I explained why this seemingly powerful tool has not come in a central place in the study of differential geometry in R^n and C^n as one may wonder. Also, some concrete examples and backgrounds are also provided in the text.

1. Introduction and Backgrounds

The differential Galois theory is a relatively young part of our long old river of mathematics. It originated in a historical problem of deciding the form of solutions to a given linear differential equation. Given an algebraic equation, some core questions could be inquired. Does this equation have some unique solution? If so, what is the form of its solution? The pursuit of answers to these questions about algebraic equations leads to the peak of classic algebra, algebraic Galois theory. Some great mathematicians wanted to answer the same questions for differential equations, and even partial differential equations. And that leads to the differential Galois theory. This origin is pointed out by R.F.Ritt and I.Kaplansky.

When the order of ODE is low, we can use analytic arguments to yield solutions in closed forms. As an analyst, Ritt naturally concerned the analytic aspect of what we call differential Galois theory nowadays. He wrote in his book [Ritt] using examples of linear equations of different types basically in a way of analysis that concerns the approximation theorems[1]. But later E.R.Kolchin developed this theory in a purely algebraic manner which is closed to the way we deployed algebraic Galois theory since E.Artin [Artin]. In that way, we figure out the classical correspondence between algebraic Galois groups and intermediate fields. And this algebraic aspect of differential Galois theory came into power

Date: 2015-04-19.

as soon as it came into existence. Kolchin introduced a set of algebraic language which allows us to describe and apply differential Galois theory other settings like $\mathcal{D}$-modules and algebraic geometry [Will Sawin]. Later researchers even find out the geometry of differential equations can lead to applications in discrete geometry, coding theory and so on.

I am not going to frighten my readers with big words and insightful backgrounds. On the contrast, we are not going to discuss these two thriving developments in this paper but focus on the fundamental theorem of Galois theory. These two developments are presented in conclusion section to illustrate recent progress in differential Galois theory.

In our deployment, we will see how analysis and algebra weaving together in a beautiful manner. Unlike Lie theory which has analysis as its underlying back color, differential Galois theory is an algebraic theory in its nature.[Will Sawin]

2. Derivations and Differential Algebraic Structures

2.1. **Existence and uniqueness of derivations.**

Definition 1. (Derivation) A derivation of a ring R is a mapping $\varphi : R \to R$ satisfying:

(i)(Additivity)$\varphi(a+b) = \varphi(a) + \varphi(b), \forall a, b \in R$

(ii)(Leibniz Rule)$\varphi(a \cdot b) = \varphi(a) \cdot b + a \cdot \varphi(b), \forall a, b \in R$

For iterative derivations, we also follow the classical notations $a', a'', \ldots, a^{(n)}$ for $\varphi(a), \varphi(\varphi(a)), \ldots, \varphi(\varphi(\ldots\varphi(a)))$.

For a ring equipped with a derivation mapping, we call it a *differential ring*, denoted by (R, φ) or simply ring R when the derivation is clear. Obviously, every ring is a differential ring if we assign the constant mapping sending everything to additive unity as a derivation on it. Similarly we can consider other algebraic structure which admits a ring structure along with a derivation on it. For example $(K, \mathit{\Delta})$ where K is a field and $\mathit{\Delta}$ is a derivation on its ring structure is called a *differential field*, and a *differential algebra* is also defined like-wisely concerning derivation on its ring structure.

Claim. In this article, we assume that every ring under discussion is a commutative ring with unity unless otherwise is stated.

Proposition 2. *The ring $E(\mathbb{C}^1)$ of entire functions on $\mathbb{C}^1$(Gaussian plane) is a differential ring along with the usual complex derivation.*

Remark. For those readers who are not familiar with complex function theory, the complex derivation is defined like this. If a complex function can be written as $f(z) = \alpha x + \beta y + \eta(z) \cdot z$,$z = x + iy \in \mathbb{C}$ and $\eta(z)$ is a higher order infinitesimal than the linear terms, then we can write this derivation by $\partial := \frac{1}{2}\left(\frac{\partial}{\partial x} - i\frac{\partial}{\partial y}\right) = \left(\frac{\partial}{\partial z}\right)$.

In fact, it's also natural to consider the ring of entire functions when we replace the Gauss plane with another simply connected domain in it. In that case we use holomorphic function ring instead of entire function ring because the domain and the whole complex plane are not the same due to the Riemann mapping theorem.

Proposition 3. *The ring of entire function of $E(\mathbb{C}^1)$ is an integral domain and its quotient field is a differential field*

Proof. For the commutative ring with unity $R = E(\mathbb{C}^1)$, there is no zero divisors in such rings due to the result of Cauchy integration formula $(f \circ g)(z_0) = \frac{1}{2\pi}\int_C f \circ g(z)dz$. So we have an integral domain. Therefore we can consider its quotient field $\widetilde{R}$. Define $\widetilde{\varphi} : \widetilde{R} \to \widetilde{R}, \frac{r}{s} \mapsto \frac{\varphi(r)s - r\varphi(s)}{s^2}$, let's check it's well-defined.

$\widetilde{\varphi}\left(\frac{rt}{st}\right) = \frac{\varphi(rt)\cdot st - rt\cdot\varphi(st)}{(st)^2} = \frac{r\varphi(t)\cdot st + \varphi(r)t\cdot st - rt\cdot s\varphi(t) - rt\cdot\varphi(s)t}{s^2t^2} = \frac{\varphi(r)s - r\varphi(s)}{s^2} = \widetilde{\varphi}\left(\frac{r}{s}\right)$. Then it's easily verified by definition that this is a derivation on $\widetilde{R}$, therefore the field $\left(\widetilde{R}, \widetilde{\varphi}\right)$ has a differential structure. With the natural extension of a derivation into a quotient field, we may regard the quotient field of a differential ring as a differential field. The quotient field of $E(\mathbb{C}^1)$ is the meromorphic functions with finite poles, denoted by $M(\mathbb{C}^1)$. $\square$

Thus we can also put the quotient field $E(\mathbb{C}^1)$ into our scope, which is the field $\mathrm{M}(\mathbb{C}^1)$ of the meromorphic functions on $\mathbb{C}^1$. As we can see now, derivation does exists for every ring, at least we have the trivial one. But another question concerning derivation of the ring arise naturally. Is the derivation unique? This question, to a large extent, is dependent on the nature of the elements of the ring. We can see this point in the following proposition.

Proposition 4. *The ring $C^\infty_{\mathbb{R}}(M)$ of smooth real functions on a smooth manifold M is a differential ring.*

Proof. As usual, the addition and the multiplication is point-wise. First of all, it's a ring because $\mathbb{R}$ is a field and the constant mapping $p \mapsto 0$ and $p \mapsto 1$ are the additive and multiplicative unities. There are more than one deviation $\varphi : C^\infty_{\mathbb{R}}(M) \to C^\infty_{\mathbb{R}}(M)$, $f \mapsto Xf$ where X is any smooth vector field. If the manifold is embedded into $\mathbb{R}^n$, with the usual frame $\left\{\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2}, \ldots, \frac{\partial}{\partial x_n}\right\}$ in $\mathbb{R}^n$, we have the representation in coordinates $X = \sum_i X_i(p) \cdot \frac{\partial}{\partial x_i}$,$X_i \in C^\infty_{\mathbb{R}}(M)$, $\varphi(f)(p) = X_i(p) \cdot \frac{\partial f}{\partial x_i}(p)$ $\square$

We can have more than one derivations on a ring by the choice of $X_i's$, which are abundant. So the derivation needs not to be unique for a differential ring. However, there are also some cases where the derivation is unique.

Proposition 5. *For the ring of integers $\mathbb{Z}$, the only possible derivation is the trivial one.*

Proof. Assume the contrary, there is a nontrivial derivation $\varphi : \mathbb{Z} \to \mathbb{Z}$. $\varphi(0) = \varphi(0 \cdot 0) = 0 \cdot \varphi(0) = 0$ is clear. Then there exists $z_0 \in \mathbb{Z}\backslash\{0\}$ such that $\varphi(z_0) \neq 0$. By the additivity, $\varphi(z_0) = z_0 \cdot \varphi(1) \neq 0$. $\mathbb{Z}$ is an integral domain, so $\varphi(1) \neq 0$. But 1 is the multiplicative unity in $\mathbb{Z}$, and it must be true that $\varphi(u) = \varphi(u^n) = nu^{n-1}\varphi(u) = n\varphi(u)$ where $u = 1$. This leads to $\varphi(u) = 0$. Contradiction. $\square$

A similar proof may indicate that the only derivation on the rational field must also be the trivial one if it's compatible with the one in Proposition 5. And it's clear that if a field F admits only one derivation, then all of its subfields can only admit a trivial derivation. So we know that differential ring is a broad notion, every ring is a differential ring, some have unique derivations and others have more than one derivations.

2.2. **Clarification of terminologies.**

Definition 6. (Differential ideals) The differential ideal in a differential ring (R, φ) is an ideal $I \subset R$ such that $\varphi(I) \subset I$.

In the setting of differential forms on a differentiable manifold M, a differential ideal I is a graded ideal in the the exterior algebra $\mathcal{A}^*(M)$ which is closed under *exterior differentiation*. In the setting of differential algebras, a differential ideal I in a differential ring (R, φ) is an ideal closed under chosen derivation.

But the exterior derivation is not a derivation according to our definition.

Although we have presented an example $C^{\infty}_{\mathbb{R}}(M)$ above, the differential forms, as one may expect, do not make up a differential structure under the usual exterior derivative. The alternating differential forms on the manifold may not consist of a differential ring if we adopt the exterior product on it. This is almost obvious because the differential algebra follows the graded commutativity instead of the Leibniz rule. But we have an alternative definition below which causes confusion sometimes.

Although vector fields are natural derivations on the ring $C^{\infty}_{\mathbb{R}}(M)$, the connection ∇_Z does not provide a derivation on $Vect(M)$. This is a fundamental matter about the non-triviality caused by curvature and torsion of the space. If we use the Lie bracket as the multiplication in the ring $Vect(M)$, then $0 = \nabla_Z\{\nabla_X Y - \nabla_Y X - [X, Y]\}$ which breaks the Leibniz rules in the definition of derivation. You can obtain this under Levi-Civita connection and even more by differentiating Bianchi identity. So it is not possible to make the exterior algebra along with the exterior differentiation as an example of differential algebra. The first factor that preventing us from applying the differential Galois theory directly on manifolds is the curved nature of the space.

While our exposition insists that a differential ideal is just an ideal closed under the derivation of the ring. We should be careful about the settings because of the existence of such a difference in terminologies.

3. Basic Assumptions and Picard-Vessiot Extensions

3.1. **The constant field.** The observation of two examples above leads us to make our two fundamental assumptions in this article:

First we introduce a subfield of the differential field.

Lemma 7. (The constant field) *The subset $K_0 = \{x \in K : \varphi(x) = 0_K\}$, where (K, φ) is a differential field, is a differential subfield of K called the* constant field *of this differential field .*

Proof. $\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0. \forall a, b \in K_0$

$\varphi(-a) = -\varphi(a) = 0, \forall a \in K_0$

$\varphi(1) = \varphi(1 \cdot 1^{-1}) = \varphi(1) \cdot 1 + 1 \cdot \varphi(1)$, this argument also holds for the zero element. In fact, all units in K have derivation 0 due to the above argument.

Therefore $\varphi(1) = \varphi(0) = 0$ and $1, 0 \in K_0$. So the subset is a group under addition.

$\varphi(a \cdot b) = \varphi(a) \cdot b + a \cdot \varphi(b) = 0 \cdot b + a \cdot 0 = 0. \forall a, b \in K_0$

$\varphi(a \cdot (b+c)) = \varphi(a \cdot b) + \varphi(a \cdot c) = a \cdot \varphi(b) + \varphi(a) \cdot b + a \cdot \varphi(c) + \varphi(a) \cdot c = 0 \cdot b + a \cdot 0 + 0 \cdot c + a \cdot 0 = 0. \forall a, b \in K_0$

$\varphi(aa^{-1}) = \varphi(a)a^{-1} + a\varphi(a^{-1}) = \varphi(1) = 0$, $\varphi(a^{-1}) = -a^{-1} \cdot \varphi(a) \cdot a^{-1} = -a^{-1} \cdot 0 \cdot a^{-1} = 0$

So the subset is a differential subfield of K. □

An easy observation is that if we use trivial derivation, then the whole field will become its own constant field. And by the leibniz rule of the derivation we always have $(\sum_i c_i y_i)' = \sum c_i y_i'$.

Proposition 8. *The quotient field $\widetilde{C^\infty_{\mathbb{R}}(M)}$of the ring $C^\infty_{\mathbb{R}}(M)$is a differential field.*

We can abuse the terminology and use the characteristic of the constant field of a differential field F as the definition of the *characteristic of the differential field F* . The differential fields $M(\mathbb{C}^1)$ and $\widetilde{C^\infty_{\mathbb{R}}(M)}$ are of characteristic zero since both of them include a constant subfield $\mathbb{C}$ which is of characteristic zero.

Claim. (Assumption I) We consider only those differential fields with characteristic zero.

A special type of differential algebraic structure which is of central importance in differential Galois theory is the *Ritt algebra*, a differential ring containing the rational number field $\mathbb{Q}$ in it. Basically, we shall only consider Ritt algebra in our following examples.

Remark. One of the reasons why we introduced Ritt algebra is that the radicals of differential ideals are still differential ideals in the same Ritt algebra. [2] But we will not use this fact in the following discussion. What we need to know is that Ritt algebra is a common setting in differential algebra.

Both $M(\mathbb{C}^1)$ and $\widetilde{C^{\infty}_{\mathbb{R}}(M)}$ include the complex number field as their constant fields under their own common derivations. Another implication of this is that the usual fields which we are familiar with can be realized as differential fields. And it's also reasonable to have:

Claim. (Assumption II) We consider only those differential fields with an algebraically closed constant fields.

Before we move on, I construct two examples from analysis and point out their constant fields.

Example 9. $M = M(\mathbb{C}^1), L = \mathbb{C}(Z), K = \mathbb{C}$. The $\mathbb{C}(Z)$ is the quotient field of the integral domain of complex polynomials in one complex variable. These fields are equipped with differential structure by the complex differentiation of complex functions as we explained near Proposition 2. We can easily see that their constant fields are all $\mathbb{C}$. Moreover, we have $K \subset L \subset M$ as field extensions. $i_1 : K \to L, a \mapsto a$,$i_2 : L \to M, f \mapsto f$ are the embeddings. We may denote them as $(M(\mathbb{C}^1), \varphi, \mathbb{C}), (\mathbb{C}(Z), \varphi, \mathbb{C}), (\mathbb{C}, \varphi, \mathbb{C})$,appending their constant fields to the tuples. They are all Ritt algebras since $\mathbb{R} \subset \mathbb{C}$

Another example comes from the field of algebraic numbers. We call the algebraic elements over the quotient field $\mathbb{Q}$ algebraic numbers. This collection of algebraic numbers is an algebraically closed field, which can be proven by canceling the denominator of the rational polynomials they are satisfying. Let's denote this field by $\mathbb{A}$.

Example 10. $M = M(\mathbb{C}^1), L = \mathbb{C}, K = \mathbb{A}$. We may denote them as $(M(\mathbb{C}^1), \varphi, \mathbb{C})$,
$(\mathbb{C}, \varphi, \mathbb{C})$,$(\mathbb{A}, \varphi, \mathbb{A})$ and the embeddings are clear in this case. This case provides an example of field extension $K \subset L \subset M$ where the constant fields are altered.

Claim. In this paper, $K \subset L \subset M$ is a tower of differential field extension unless otherwise is stated.

Both of our examples above satisfy the two assumptions above. The second of our examples has nontrivial inclusion which is much more familiar, $\mathbb{A} \subsetneqq \mathbb{C}$.

3.2. **Linear independence in solutions to linear ODEs.** As one may observed,

> Perhaps the easiest description of differential Galois theory is that it is about algebraic dependence relations between solutions of linear differential equations.([Beukers])

With above two assumptions, we can introduce another notion of linear dependence over the constant field. Just like what we have done in the ordinary differential equation courses, there is no meaning if we multiply some scalar with a solution and claim that we have obtained a new solution since they're linear dependent on each other. However, when the coefficients of a differential equation (Or we consider only the differential polynomial) is chosen in a differential field, we need to clear up the ambiguity in the meaning of saying that two solutions are linear independent.

Definition 11. (Wronskian) The Wronskian of n elements $y_1, y_2, \dots, y_n$ in a differential ring (R, φ) is defined as:

$$\det \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1^{'} & y_2^{'} & \cdots & y_n^{'} \\ y_1^{''} & y_2^{''} & \cdots & y_n^{''} \\ \vdots & \vdots & & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{pmatrix}.$$

For example, the Wronskian of the two functions$\left\{\frac{1}{(z-1)} + z, \frac{1}{(z-1)^2} + \frac{1}{z-i}\right\}$in the M($\mathbb{C}^1$) can be calculated as $det \begin{pmatrix} \frac{1}{(z-1)} + z & \frac{1}{(z-1)^2} + \frac{1}{z-i} \\ \frac{-1}{(z-1)^2} + 1 & \frac{-2}{(z-1)^3} + \frac{-1}{(z-i)^2} \end{pmatrix}$.

On a surface S embedded in $\mathbb{R}^3, S : F(x, y, z) = z - x^2 - y^2 = 0$, let$f\,(x, y, z) = xy + z^2; g(x, y, z) = x^2 + z^2$ and a vector field $X = y\frac{\partial}{\partial x} + x\frac{\partial}{\partial y} + \frac{\partial}{\partial z}$.

Then as we shown in the previous part, we can calculate for $\{f, g\}$their Wronskian as $det \begin{pmatrix} xy + z^2 & x^2 + z^2 \\ y^2 + x^2 + 2z & 2xy + 2z \end{pmatrix}$.

Lemma 12. *Let K be a differential field with a constant field C. Then n elements of K are linear dependent over C if and only if their Wronskian vanishes.*

Proof. Suppose that $\sum_i c_i y_i = 0, c_i \in C, y_i \in K$, apply the derivation onto both sides for (n-1) terms and since c_i's are in the constant field $(\sum_i c_i y_i)' = \sum c_i y_i'$. We got a size n homogeneous linear system in $\{c_1, c_2, \dots, c_n\}$whose coefficient matrix determinant coincide with the Wronskian. Therefore, from the knowledge of linear algebra over general coefficient field, the linear combination of c_i is nontrivial if and only if the Wronskian vanishes. □

Hereafter when we're discussing the linear independence of differential indeterminate like $y_1, y_2, \dots, y_n$ shown above, we mean they're linearly independent over its constant field. So there exists no ambiguity when we say $y_1, y_2, \dots, y_n$ are independent in some extended differential field of K, as long as their constant fields are the same one. This seems quite natural for extension fields over K. However, not all extensions of differential fields preserve a common constant field. There is such a possibility that we may alter the constant field through extensions like Example 9. The following notion put some restrictions on the extensions of a differential field.

Lemma 13. *There're at most n linear independent (over constant field C)solutions to the differential equation with coefficients in a differential field K:*$L(y) := y^{(n)} + a_1 y^{(n-1)} + \ldots + a_{n-1}y' + a_n y, a_i \in K$ *Here y is some differentiable indeterminate over K.*

Proof. Suppose there are (n+1) linear independent solutions over C to $L(y) = 0$, say $\{u_1, u_2, \ldots, u_n\}$ .Then we may yield:

$u_1^{(n)} + a_1 u_1^{(n-1)} + \ldots + a_{n-1}u_1' + a_n u_1 = 0,$
$u_2^{(n)} + a_1 u_2^{(n-1)} + \ldots + a_{n-1}u_2' + a_n u_2 = 0,$
$\ldots$
$u_{n+1}^{(n)} + a_1 u_{n+1}^{(n-1)} + \ldots + a_{n-1}u_{n+1}' + a_n u_{n+1} = 0.$

Look vertically and treat it as an linear system in the column vectors $\left(u_1^{(n)} \ldots u_{n+1}^{(n)}\right), \ldots, (u_1 \ldots u_{n+1})$we instantly know the Wronskian of $\{u_1, u_2, \ldots, u_n\}$ is zero, since if a nontrivial solution exists for such a homogeneous system. And that contradicts the previous lemma. $\square$

3.3. **Picard-Vessiot extensions.**

Definition 14. (Picard-Vessiot extension) As above we consider a differential equation $L(y) = 0$ whose coefficients lie in some differential field K. We say that a differential field extension M/K, where M and K are both differential fields, is Picard-Vessiot extension with underlying equation $L(y) = 0$ if:

(i)(Solution space)$M = K < u_1, u_2, \ldots, u_n >$, where $\{u_1, u_2, \ldots, u_n\}$ are those linear independent solutions to $L(y) = 0$ over C. The *angled bracket* implies that this extension is a field extension while the *brace bracket* implies a ring adjunction.

(ii)(Constant preservation) M has the same constant field as K.

Careful readers may note above and in the following discussions that the differential equation $L(y) = 0$ play the role of the irreducible minimal polynomial over the smaller field in the common field extensions. In the conclusion section we will see that the differential Galois group mentioned by Katz is actually a Picard-Vessiot extension for a certain ODE using $\int exp(f(x))dx$ as its solution. However, our field extension here are almost always transcendental except the linear case $L(y) := y'$. For example, we know for $L(y) = y' \cdot sin^2 z + 1 = 0$ has the transcendental meromorphic function $cot\,(z)$ which has an essential singularity at the origin, as one of the solutions. $cot\,(z)$ is not in $M(\mathbb{C}^1)$ because those elements in $M(\mathbb{C}^1)$ have only poles while $cot\,(z)$ has $\{z = \pm k\pi : k \in \mathbb{Z}\}$. And thus $cot\,(z)$ cannot be a root of any equation whose coefficients are in $M(\mathbb{C}^1)$, since in that way we resort to *Hadamard Factorization* and find only *finitely many* poles occur. So we may use this transcendental meromorphic function $cot(z)$ to extend the differential field $M(\mathbb{C}^1)$.

We now know that a Picard-Vessiot extension exists for *some* differential equations as above. However, till now we do not know that whether there exist a Picard-Vessiot extension for an *arbitrarily chosen* $L(y)$. The answer to this question is affirmative due to:

Proposition 15. [3] *With the assumptions that differential field extension M/K and the characteristic of K is zero and the constant field of K is algebraically closed, we always have a Picard-Vessiot extension for any differential equation $L(y) = 0$ as the underlying equation whose coefficients lying in K.*

For an example, a general first-order linear equation of complex variable y, $y' = P(x)y+Q(x), P \in M^1_{n\times n}(x), Q \in M^1_{n\times 1}(x)$. The coefficients $P(x), Q(x)$ are matrix of fixed size whose entries are C^1continuous *complex* functions in *real* variable x on *real* parametric interval I. The ODE can be regarded as $L(y) = y' - P(x)y - Q(x) = 0$. Thus the differential field can be chosen as $K = M(\mathbb{C}^1)$. Then its Picard-Vessiot extension, using the classical analytic technique of variation of coefficients, is $K < exp(tP)\int_\tau^t exp^{-1}(sP) \cdot Q(s)ds >$. Here the solution $\varphi(t) = exp(tP)\int_\tau^t exp^{-1}(sP) \cdot Q(s)ds$ must satisfy $\varphi(\tau) = 0$. The term $exp(tP)\int_\tau^t exp^{-1}(sP) \cdot Q(s)ds$ is an element which is not in $K = M(\mathbb{C}^1)$ and such an extension is called *Liouville extension*[4], we will admit Proposition 15 and not go into details[5]. As soon as the notion of Picard-Vessiot field extension is introduced, a natural problem in Galois theory is to figure out all those automorphisms of the larger field that fix the smaller field. So we have following parallel notion of Galois group.[6]

4. Differential Homomorphisms and Galois Connections

4.1. Differential Galois groups.

Definition 16. (Differential homomorphisms) A differential homomorphism is a ring homomorphism defined on differential rings $\phi : (R, \varphi) \to (R', \varphi')$ such that $\phi(\varphi(a)) = \varphi'(\phi(a)), \forall a \in R$.

The differential isomorphisms and automorphisms are defined similarly. It's easily verified that the kernel of such an homomorphism is a differential ideal.

Definition 17. (Differential Galois group) Let M/K be a differential field extension, we define the differential Galois group $G = DGal\,(M/K)$ to be the group of all differential automorphisms of M leaving K fixed.

This definition is a well-defined one. The group operation is homomorphism compositions. The group has identity isomorphism on M as an identity. $\forall k \in K, \eta, \zeta \in G$, we have $\eta \circ \zeta(k) = \eta(k) = k \in K$. So its operation is closed. The inverse of an automorphism ζ is still in G because the elements shall not be moved by inverse of $\zeta \in G$ since $\zeta \circ \zeta^{-1}(k) = k \in K, \zeta^{-1}(k) \in G$. i.e. $\forall \sigma \in G, \sigma|_K = id_K$

Maybe it's the high time that we revisit our examples mentioned earlier. Pick $M = M(\mathbb{C}^1), K = \mathbb{C}$ and we will see that $\tau_\alpha : z \mapsto \alpha z \in DGal(M/K)$ if $\alpha \in \mathbb{C}$. We just use this as an example illustrating the notion of differential Galois group.

4.2. Galois connections and prime notations.

Definition 18. (Prime notation)We let $G = DGal(M/K)$.

For those intermediate differential field L, define $L' := DGal(M/L)$ to be the subgroup H of G consisting of differential automorphisms leaving the subfield L fixed. So there is a correspondence between G's subgroups and those intermediate field of M/K.

For a subgroup of G, we define H' to be the set of elements in M left fixed by all elements lying in H. Easily we can verify that:

Proposition 19. *H' is an intermediate differential field of M/K.*

Proof. $H' \subset M$ is easy by definition. $H' \supset K$ is due to the fact that H is a subgroup of G. So all of its elements fix K.

H' is also a field. For the multiplicative unity and additive identity, they are in H' because they're always fixed by homomorphisms.

$\forall a, b \in H', \forall h \in H, h(a+b) = h(a) + h(b) = a + b$.

$\forall a \in H', \forall h \in H, h(-a) = -h(a) = -a$.

$\forall a, b \in H', \forall h \in H, h(a \cdot b) = h(a) \cdot h(b) = a \cdot b$

$\forall a \in H', \forall h \in H, h(a^{-1}) = h(a)^{-1} = a^{-1}$.

$\forall a, b, c \in H', \forall h \in H, h(a \cdot (b+c)) = h(a \cdot b + a \cdot c) = h(a \cdot b) + h(a \cdot c) = h(a) \cdot h(b) + h(a) \cdot h(c) = a \cdot b + a \cdot c$.

$\forall a \in H', \forall h \in H, h(\varphi(a)) = \varphi(h(a)) = \varphi(a)$

The first equality of the last line is due to the definition of differential automorphism. So the set is closed under derivation of the ring. $\square$

Proposition 20. *For an intermediate differential field L of M/K we have $L'' \supset L$; for a subgroup H of G we have $H'' \supset H$. So $L''' = L', H''' = H'$*

Definition 21. (Galois closed fields and groups[7]) We define those intermediate fields L and subgroups H such that $L'' = L, H'' = H$ to be (Galois) closed fields and subgroups.

Now we're fully-prepare to establish a correspondence between the differential Galois (sub)groups and the (intermediate) Picard-Vessiot extension fields. The main theorem we are to introduce in this paper is the following one pointing out a Galois connection which lies between differential Galois subgroups and intermediate fields.

5. The Fundamental Theorem of Differential Galois Theory

5.1. **The main result.**

Theorem 22. *(The fundamental theorem of differential Galois theory)*

(Assumption I)K is a differential field of characteristic zero.

(Assumption II)K has an algebraically closed constant field.

(Theorem Assumption) M/K is a Picard-Vessiot extension.

Under all these assumptions we have:

(i)There is a bijective correspondence between the intermediate differential fields and the algebraic subgroups of the differential Galois group $G = DGal(M/K)$.

(ii)There is a bijective correspondence between the normal *extensions L/K and the* closed normal *algebraic subgroups of the differential Galois group $G = DGal(M/K)$. In this case we know in addition that $G/H = DGal(L/K)$ where $H = L'$.*

$$
\begin{array}{ccccc}
K & \subset & L & \subset & M \\
\vdots & & \vdots & & \vdots \\
G = K' = DGal(M/K) & \supset & L' = DGal(M/L) & \supset & M' = DGal(M/M) = \{e\}
\end{array}
$$

We may want to compare this theorem with the fundamental theorem of algebraic Galois theory:

Theorem. *(The fundamental theorem of algebraic Galois theory)*

E/F is a finite field extension.

(i)For any subgroup H of $Gal(E/F)$, the corresponding fixed field, denoted H', is the set of those elements of E which are fixed by H.

$$
\begin{array}{ccccc}
F & \subset & H' & \subset & E \\
\vdots & & \vdots & & \vdots \\
Gal(E/F) & \supset & H & \supset & DGal(E/E) = \{e\}
\end{array}
$$

(ii)For any intermediate field K of E/F, the corresponding subgroup is K', the set of those automorphisms in $Gal(E/F)$ which fix every element of K.

This correspondence is a one-to-one correspondence if (and only if) E/F is a Galois extension.

$$
\begin{array}{ccccc}
F & \subset & K & \subset & E \\
\vdots & & \vdots & & \vdots \\
F' = Gal(E/F) & \supset & K' = Gal(E/K) & \supset & E' = DGal(E/E) = \{e\}
\end{array}
$$

5.2. **Algebraic matrix groups.** Now we may explain a little bit of the terminology. In most cases, we are concerned about algebraic matrix groups(Lie groups), so we may only give the word-by-word definition of algebraic matrix group instead of algebraic groups. For those who are interested in its historical motivation, [Kolchin3],[Singer] and [Ritt]are good reads.

Definition 23. (Algebraic matrix groups (over field K)) A (multiplicative) group G of matrices of degree n is called algebraic matrix group if there exists an algebraic variety V in n^2-dimensional space such that:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in G \leftrightarrow (1,2,3,4) \in V$$

(i)(variety side)Every matrix $\sigma \in G$ is a point on V, if it's considered as a point in n^2-dimensional space by expanding by rows.

(ii)(group side)Every point $p \in V$, contracting by rows, which is not a singular matrix is in G. Moreover, if the algebraic variety does not have an irreducible component consisting solely of singular matrices, then the variety is unique and called the *underlying manifold* of G.

We shall explain a bit here. We saw that the the theorem requires algebraic subgroups of the differential Galois group, this requirement is based on the fact that $DGal(M/K) \cong$a subgroup of $GL_n(K)$. This isomorphism is easily seen by definition. Let some $g : M \to M$ and for $g \in DGal(M/K)$ and $u_i's$ are the solutions to some given ODE $u^{(n)} + \ldots + a_1 u^{(1)} + a_0 = 0, a_i \in K$. Then we can see that if $u^{(n)} + \ldots + a_1 u^{(1)} + a_0 = 0$, then $(g\,(u))^{(n)} + \ldots + a_1(g(u))^{(1)} + a_0 = g(u^{(n)}) + \ldots + g(a_1 u^{(1)}) + g(a_0) = g(u^{(n)} + \ldots + a_1 u^{(1)} + a_0) = 0$. So for such element $g \in DGal(M/K)$ we may assume that $g(u) = \Sigma_{i=1}^{n} k_i u_i, k_i \in K, u_i \in K$, being expressed by linear combination of linearly independent solutions. Therefore any algebraic subgroup of $DGal(M/K)$ can be identified with some subgroup of $GL_n(K)$ using a basis consisting of $u_i's$. So we can use its matrix representation and the definition above makes sense in the theorem.

This definition is actually a mild geometric restriction on the differential Galois group which furtherly restrict the scope of the objects which we might study using the theory. And the second factor why the theory is more close to the algebraic varieties instead of differential manifolds is clear by this requirement of algebraic subgroups of the fundamental theorem.

We may finally prove this theorem, before that you may wonder why this seemingly powerful theorem is not so frequently encountered in applications. Well, you see that the assumptions are too strong to include the fundamental theorem of *algebraic* Galois theory as a special case since it requires algebraically closed. And now we come to its lengthy proof. Not all the technical details are included here, for those who are interested, see [Kaplansky].

6. Results Concerning Homomorphisms

6.1. **Some lemmas.** First we observe that Assumption II is needed because this is a direct consequence of Hilbert's Nullstellensatz. We omit its proof here.

Lemma 24. [8] *Let K be a differential field with algebraically closed constant field C. Let L be a differential field extension of K with constant field D. Let f_α, g be polynomials in a finite number of differential indeterminates over K, α ranging over a possibly infinite index set. If the equations $\{f_\alpha = 0, g \neq 0\}$ have a solution in D they have a solution in C.*

The $\{f_\alpha = 0, g \neq 0\}$ requires an inequality term in order to the ideal generated by the equations is a proper one. In the improper case we cannot use Hilbert's Nullstellensatz.

By the same philosophy, we may have following two lemmas, our proofs are exactly those of Kaplansky's except for minor modifications:

Lemma 25. [9] *Let K be a differential field with constant field C. Let $k_1, k_2, \ldots, k_r$ be constants in some differential field extension of K. Then if $k_1, k_2, \ldots, k_r$ are algebraically dependent over K, then they are also algebraically dependent over C.*

Proof. Assume that $k_1, k_2, \ldots, k_r$ are dependent over C, there exists a polynomial relation $f(k_1, \ldots, k_r) = 0$ with coefficients in K. Find a basis of K over C and write $f = \sum_i h_i u_i, h_i \in C$. $h_i(k_1, \ldots, k_r) = 0$ because of the linear independence of basis over C. Then this relation is what we need. $\square$

Next, we prove the strict transcendental degree descendence on the integral domain:

Lemma 26. [10] *Let F be any field, I is an integral domain over F with finite transcendental degree over F. Let P be a nontrivial proper prime ideal in I. Then the transcendental degree of I/P over F is strictly less than that of I over F.*

Proof. Choose a nonzero element $u \in P$. It's impossible for u to be an algebraic element over F, otherwise P will contain some constant term. The minimal irreducible polynomial must contain a nonzero constant term or it can be shortened. So P is not a proper ideal in that case. Take some transcendental basis $\{u_1, u_2, \ldots, u_r\}$ containing u_1 such that $u_1 \in P$. So $\{u_1, u_2, \ldots, u_r\}$ is mapped to $\{\bar{u_2}, \ldots, \bar{u_r}\}$ under the canonical projection $\pi_P : u \mapsto u + P$. Now we claim that I/P has a transcendental basis$\{\bar{u_2}, \ldots, \bar{u_r}\}$ over F . Pick any $x \in I/P$ and find $y \in I$ such that $\pi(y) = \bar{y} = x$, then $\sum h_k y^k = 0, h_k \in F[u_1, \ldots, u_r]$. Let $f(y) = \sum_k \bar{h_k} x^k$ be of such polynomials of the least degree. We see x is dependent on $\{\bar{u_2}, \ldots, \bar{u_r}\}$ only. Possible exception is the case where all $h_k \in P$. But then $\overline{(h_k y^{k-1} + \ldots + h_1)y} = \bar{0}$ which means $\overline{h_k y^{k-1} + \ldots + h_1} = \bar{0}$, contradicting the least degree choice. $\square$

6.2. **Admissible homomorphisms.** Now we have to consider the other side of the story. While all elements in $DGal\,(M/K)$, where $K \subset M$ are differential fields extensions, cannot be simply viewed as elements in $DGal\,(L/K)$ by restriction of the domain to L since for some $\tau \in DGal(M/K), \tau(L) \nsubseteq L$. But can every element in $DGal\,(L/K)$be extended to an element in $DGal\,(M/K)$ by some sort of extension? When the extension is normal, the answer is affirmative in algebraic field theory. It's natural to have faith in such existence result. But don't be so positive, there exists some homomorphisms which cannot be extended (although we cannot give an example here). So we feel it natural to consider:

Definition 27. (Admissible isomorphisms) A (differential) isomorphisms between two (differential) fields K and L will be called admissible if there exists a (differential) field M containing both K and L.

In algebraic field theory, such extension exists trivially by adding those fixed elements in larger fields. This notion is an intermediate notion like the diagrams below indicates:

differential isomorphisms $\overset{Thm28,29}{\Rightarrow}$

admissible differential isomorphisms $\overset{Lemma32}{\Rightarrow}$

differential automorphisms $\in DGal(M/K)$,

i.e.

$$K \overset{\varphi}{\to} L \quad \overset{Thm28,29}{\Rightarrow} \quad \begin{array}{ccc} K & \overset{\varphi}{\to} & L \\ i_1 \downarrow & & \downarrow i_2 \\ M & \dashrightarrow & M \end{array} \quad \overset{Lemma32}{\Rightarrow} \quad M \overset{\hat{\varphi}}{\to} M$$

As the story goes on, we will grasp the full meaning of this diagram. We will conclude the result we want in Theorem 35.

Theorem 28. [11 12] *Let M be a differential field of characteristic zero, K, L are its subfields. And let there be given a differential isomorphisms $s : K \to L$. Then s can be extended to an admissible differential isomorphism defined on M.*

We omit the proof and provide a synopsis instead. When we extend for one adjunction, we may proceed to infinite ring adjunctions by Hausdorff maximality and take its quotient field.

But the core of the argument is that we find some prime ideal Q which intersects $L\{y\}$, the ring adjunction of y to L, to be P. (In fact, to prove that this choice is possible requires much work.) P is the prime differential ideal being the image of $Ker(e_u)$ under s. $Ker(e_u)$ is the kernel of the evaluation homomorphism e_u from $K\{y\}$ to $K\{u\}$ where $u \in M \setminus K$.

We can regard P as the irreducible polynomials in usual algebraic extensions. We put the solutions to P into $L\{y\}$ and project it to $L\{y\}/Q$ via the canonical projection $\pi_Q : M\{y\} \to M\{y\}/Q$ defined on $M\{y\}$. So the composition mapping $\pi_Q \circ s$ has a kernel equals to $Q \cap L\{y\} = P$. The rest of our work is to extend the homomorphism. Define the extended homomorphism $\hat{s} : K\{y\} \subset M\{y\} \to L\{\pi_Q(y)\} \subset M\{y\}/Q, y \mapsto \pi_Q(y)$. This is the first adjunction and we may do this procedure repetitively.

$$\begin{array}{ccc} Q \cap L\{y\} = P \subset L\{y\} & \overset{\pi_Q}{\to} & L\{y\}/Q \\ \uparrow \hat{s}, s & & \vdots \\ Ker(e_u) \subset K\{y\} & \overset{e_u}{\to} & K\{u\} \end{array}$$

Maybe it is more perceivable to do manipulations on our example $M = M(\mathbb{C}^1), L = \mathbb{C}(Z), K = \mathbb{C}$. Specifically we pick $u = exp(z) \in M \setminus K$. Consider the evaluation homomorphism at u $e_u : K\{y\} \to K\{u\}$, we may calculate the kernel by letting $e_u\left(a_n y^{(n)} + a_{n-1}y^{(n-1)} \ldots + a_1 y' + a_0 y\right) = 0$, then we calculate $a_n exp(z) + a_{n-1} exp(z) \ldots + a_1 exp(z) + a_0 exp(z) = 0$, and that leads to $a_n + \ldots + a_1 + a_0 = 0$. So

$Ker(e_u) = \left\{f \in K\{y\}, f = \sum_k a_k y^{(k)}, \sum a_k = 0\right\}$

$P = \hat{s}(Ker(e_u))$ where $s : K \to L, z \mapsto z, \hat{s} : K\{y\} \to L\{y\}, \sum_k a_k y^{(n)} \mapsto \sum_k a_k y^{(n)}$. In this case we may now know Q is the ideal spanned by $\{a_k, \sum a_k = 0\}$. Reverse the process and we may see how the idea above works. In many other cases, if the u is not so good, we cannot obtain an explicit expression of the ideal Q.

Similarly we have the following theorem whose proof is omitted but is intuitively clear from the diagram below. A hint is we can send $u \in L \setminus K$ into $\pi_Q(y)$ instead.

$$\begin{array}{ccc} s^{\#}(Ker(e_u))K < u > \subset K < u > \{y\} & \overset{\pi_Q}{\to} & K < u > \{y\}/Q \\ \uparrow s^{\#} & & \vdots \\ Ker(e_u) \subset K\{y\} & \overset{e_u}{\to} & K\{u\} \end{array}$$

Theorem 29. [13,14]*Let K be a differential field of characteristic zero. Let $u \in L \setminus K$. Then there exists an admissible differential isomorphism on L which actually moves u and is identity on K.*

Again, review our example $M = M(\mathbb{C}^1), L = \mathbb{C}(Z), K = \mathbb{C}$ and pick $u = exp(z) \in M \setminus K$. The admissible isomorphisms $d_c : z \mapsto c \cdot z - z'$ are admissible isomorphisms separating those additional elements (The reader can check this easily). Then we can reach our first step towards the fundamental theorem.

Theorem 30. [15]*Let K be a differential field with constant field C, $M := K < u_1, u_2, \ldots, u_n >$ a Picard-Vessiot extension of K.*

i.e. We have a tower of differential fields: $C \subset K \subset M := K < u_1, u_2, \ldots, u_n >$

There exists a set S of polynomials in n^2 ordinary indeterminates with coefficients in C such that:

(i) Every admissible differential isomorphisms of M over K gives rise to a matrix of constants satisfying S.[16]

(ii)Every differential field extension N/M, along with a non-singular matrix $(k_{ij})_{n\times n}$ of constants of N satisfying S, there exists an admissible differential isomorphism of M/K into N sending u_i into $\sum k_{ij}u_j$.[17]

Remark. The term 'satisfying S' means that the transformation represented by the matrix $(c_{ij})_{n\times n}$ permutes the zeros of the collection of polynomials in S, understand this using the isomorphism between ring of matrix polynomials and ring of matrices using polynomials as entries.

Proof. Let $y_1, y_2, \ldots, y_n$ be differential indeterminates over K. Define a differential homomorphism of

$\varphi : K\{y_1, \ldots, y_n\} \to M = K < u_1, \ldots, u_n >, f(y_1, \ldots, y_n) \mapsto f(\frac{u_1}{1}, \ldots, \frac{u_n}{1}), \Gamma := Ker\varphi$ where f_i are differential polynomials of y_i with coefficients in K.

Γ is a prime differential ideal because $\{y_1, \ldots, y_n\}$ are linearly independent over K (So when the element is in Γ, it must be a linear combination of all these y_i's). And we immediately got an induced homomorphism:

Let $c_{ij}, i, j = 1, \ldots n$ be a set of n^2 ordinary indeterminates over M. Define a differential homomorphism:

$\bar{\varphi} : K\{y_1, \ldots, y_n\}[c_{ij}] \to M[c_{ij}] = K < u_1, \ldots, u_n > [c_{ij}]$,

$\sum_{l,m} f_{lm}(y_1, \ldots, y_n)c_{lm} \mapsto \sum_{l,m} f_{lm}(\frac{u_1}{1}, \ldots, \frac{u_n}{1})c_{lm}$

$\psi : K\{y_1, \ldots, y_n\} \to M[c_{ij}]$,

$f(y_1, \ldots, y_n) \mapsto \sum_{l,m} f(\frac{u_1}{1}, \ldots, \frac{u_n}{1})c_{lm}, \Delta := \psi(\Gamma)$

where f are differential polynomials with coefficients in K. (when $c_{ij} = \delta_{ij}, \psi(\Gamma) = \Gamma$)

Since Γ is a prime differential ideal and ψ is a differential homomorphism, Δ is a differential ideal in $M[c_{ij}]$ consisting of polynomials of $c_{ij}$with coefficients in M.

$$\begin{array}{ccc} K\{y_1, \ldots, y_n\} & \xrightarrow{\varphi} & M \\ \downarrow \psi & & \nearrow \\ M[c_{ij}] & & e_{k_{ij}} \end{array}$$

Let w_α be a vector space basis of M over C. Write each polynomial in Δ as a linear combination of $w's$ with coefficients in the field C, denote this set of polynomials by S. The number of polynomials in this set may be very large.

(i) Let $\sigma : M/K \to M/K$ be an admissible differential isomorphism of M/K. ($\sigma \circ \varphi(\Gamma) = \sigma(0) = 0$, and check the above diagram commutes.)

Under the solution space basis of M, we have $\sigma : u_i \mapsto \sum_j k_{ij}u_j, k_{ij} \in K$ represented in a matrix form.

Let $e_{k_{ij}} : M[c_{ij}] \to M$ be the evaluation homomorphism at k_{ij}, $e_{k_{ij}}(S) = e_{k_{ij}} \circ \psi(Ker\varphi) = 0$,$S \subset Ker(e_{ij})$

(ii) Given N and a non-singular matrix $(k_{ij})_{ij}$ of constants in N satisfying S. We may define a homomorphism of $K\{y_1, \dots, y_n\} \to N$ using the following sequence.

$$K\{y_1, \dots, y_n\} \overset{\varphi}{\to} K\{u_1, \dots, u_n\} \overset{\iota}{\to} M := K < u_1, \dots, u_n > \overset{\sigma}{\to} M[c_{ij}] \overset{\gamma'}{\to} N$$

$$y_i \mapsto u_i \mapsto \frac{u_i}{1} \mapsto \sum_j c_{ij}u_j \mapsto \sum_j k_{ij}u_j$$

Then if we denote this mapping by ρ, then $Ker\rho \supset \Gamma$. So we have a homomorphism $\sigma : K\{y_1, \dots, y_n\} \to K\{\sigma(u_1), \dots, \sigma(u_n)\}$, where $\sigma(u_i) := \sum_j k_{ij}u_j$. If we can prove that this mapping is injective, then $K\{\sigma(u_1), \dots, \sigma(u_n)\}$ can be extended into a quotient field. And this is done by Lemma 26.

Assume the contrary, $\partial K < u_{1,\dots}, u_n > /K > \partial K < \sigma(u_1), \dots, \sigma(u_n) > /K$, where the partial denotes the transcendental degree. Both sides of the inequality cannot be infinite since these u_i's satisfy the definition of Picard-Vessiot extension and thus must be solutions to a differential polynomial of finite degree. And hence by Lemma 13 we can assert that both sides are finite and the inequality is never vacantly satisfied. From the additivity of transcendental degrees, the last equality follows from Lemma 25:

$\partial K < u_{1,\dots}, u_n, \sigma(u_1), \dots, \sigma(u_n) > /K < u_{1,\dots}, u_n >$
$= \partial K < u_{1,\dots}, u_n, k_1, \dots, k_n > /K < u_{1,\dots}, u_n >$
$= \partial C(k)/C$
$\partial K < u_{1,\dots}, u_n, \sigma(u_1), \dots, \sigma(u_n) > /K < \sigma(u_1), \dots, \sigma(u_n) >$
$= \partial K < u_{1,\dots}, u_n, k_1, \dots, k_n > /K < \sigma(u_1), \dots, \sigma(u_n) >$
$= \partial C'(k)/C'$

where C, C' are constant field corresponding to $K, K < \sigma(u_1), \dots, \sigma(u_n) >$ respectively.

$\partial C'(k)/C' < \partial C(k)/C$ is due to the Picard-Vessiot extension's definition of constant field preservation. Hence we have a contradiction against Lemma 24 which said $\partial C'(k)/C' \geq \partial C(k)/C$. □

Corollary 31. *The differential Galois group of a Picard-Vessiot extension is an algebraic matrix group over the constant field.*

Lemma 32. [18,19] *Let K be a differential field with an algebraically closed field of constants. Let M be a Picard-Vessiot extension of K.*

Suppose $\{x_\alpha\}$ and $\{y_\alpha\}$ are two collections of elements in M. $z \in M$. φ is an admissible differential isomorphism of M over K sending $\{x_\alpha\}$

into $\{y_\alpha\}$ and moving z. Then there exists a differential automorphism $\tilde{\varphi}$ of M over K sending $\{x_\alpha\}$ into $\{y_\alpha\}$ and moving z.

Proof. Let σ be the given admissible differential isomorphism. u_i's are the solutions to the underlying differential polynomials of Picard-Vessiot extension. Say, $\sigma(u_i) = \sum_j k_{ij}u_j, k \in D$, where D is the constant field of L. For $\forall x \in \{x_\alpha\}, y \in \{y_\alpha\}$, each is a ratio of two differential polynomial in u_i's , this is from the quotient field construction and the definition of Picard-Vessiot extension. Let $x = \frac{P(u_1,\ldots,u_n)}{Q(u_1,\ldots,u_n)}, y = \frac{R(u_1,\ldots,u_n)}{S(u_1,\ldots,u_n)}$. If $\sigma(x) = y$ in M, then $S(u_1, \ldots, u_n)P(\sigma(u_1), \ldots, \sigma(u_n))$ $= R(u_1, \ldots, u_n)Q(\sigma(u_1), \ldots, \sigma(u_n))$. And we have $\sigma(u_i) = \sum_j k_{ij}u_j$, which can be regarded as a polynomial equation in $k'_{ij}s$ with coefficients in M. Let the index set α vary, we have a system of differential equations, denoted S_1. And we yield from Theorem 30 another system of equations, denoted S_2. Additionally we must move the single element z, so $S_3 = \{\sigma(z) \neq z, |k_{ij}| \neq 0\}$. There exists constant solutions to the combined system $\{S_1, S_2, S_3\}$to k_{ij} because we have such an admissible differential isomorphism. Since the solution falls in K, we can find a corresponding solution in $C \subset K$ due to the Lemma 24. The solution in C uniquely gives out an automorphism satisfying the conditions. □

6.3. **Normality of Picard-Vessiot extensions.**

Definition 33. (Normal field extension) A (Picard-Vessiot) field extension L/K is said to be normal if for any $z \in L\backslash K$ there exists a (differential) automorphism φ of L/K moving z.

Theorem 34. *The Picard-Vessiot extensions L/K of any differential field K with characteristic zero and an algebraically closed constant field is normal.*

Proof. We need a differential automorphism of M/K which moves an arbitrarily chosen $z \in M \setminus K$. Theorem 28 and 29 give us the existence of such an admissible isomorphism. Then Lemma 30 told us that it could be extended into a differential automorphism. □

We can see the characteristic zero assumption as well as the algebraic closeness cannot be dropped here due to the usage of Theorem 28 and 29. Also, Theorem 28 and Lemma 32 gives the following consequence, which can be considered as another side of normality of the field extension.

Theorem 35. [20] *Let K be a differential field of characteristic zero and and algebraically closed constant field.*

Let M be a Picard-Vessiot extension of K.

Then any differential isomorphisms over K between two intermediate differential fields can be extended to a differential automorphism of M. In particular, any differential automorphisms over K of an intermediate differential field can be so extended.

We may want to review the following diagram:

differential isomorphisms $\overset{Thm28,29}{\Rightarrow}$

admissible differential isomorphisms $\overset{Lemma32}{\Rightarrow}$

differential automorphisms $\in DGal(M/K)$

Then we can go on to our second step towards the fundamental theorem.

Theorem 36. *Let M be a differential field, K a differential subfield of it. $G := DGal(M/K)$.*

(i) If H is a normal subgroup of G, then any differential automorphism of M/K sends H' onto itself.

(ii)If L is an intermediate differential field with the property that any differential automorphism of M/K sends L onto itself, then L' is a normal subgroup of G.

Proof. Set g to be a differential automorphism of M/K, fix arbitrarily chosen $x \in H'$.

$g^{-1} \circ f \circ g \in H \Leftrightarrow g^{-1} \circ f \circ g(x) = x \Leftrightarrow f \circ g(x) = g(x), \forall f \in H \Leftrightarrow g(x) \in H'$. Interchange the places of g, g^{-1}, we have conclude that g sends H' onto itself. Meanwhile, this also proves (ii) if we read from right to left and replace H with L'. i.e. We pick up $\forall g \in L'$. Then $g|_L = id_L$, and for $\forall h \in G$ we have $h^{-1} \circ g \circ h(x) \subset h^{-1} \circ g(h(K)) \subset h^{-1} \circ h(K)$. □

By the repetitive usage of computation as Theorem 36[21], we have got:

Lemma 37. *Let L be a Galois closed subfield of M, L normal over K. Let H be a subgroup corresponding to L.(i.e. $H = L'$)*

Then the normalizer of H, denoted $N(H)$, consists of all $g \in G = DGal(M/K)$ that maps L onto L.

Proof. Let us prove $N(H) \subset \{g \in G | g(L) \subset L\}$ first.

Pick up any element $g \in N(H) = \{g \in G | g^{-1} \circ h \circ g \in H, \forall h \in H\}$, for $\forall l \in L, (g^{-1} \circ h \circ g)(l) = l$ by definition of H and the definition $g^{-1} \circ h \circ g \in H$. So $h \circ g(l) = g(l), \forall l \in L \Rightarrow g(L) \subset L$

Now we prove $N(H) \supset \{g \in G | g(L) \subset L\}$.

$\forall g \in G$, since L is normal over K[22] we have $h \circ g(l) = g(l), \forall h \in H, \forall l \in L$. So $g^{-1} \circ h \circ g(l) = l, g^{-1} \circ h \circ g \in H$ □

Using this lemma and Theorem 36 we can have:

Theorem 38. *Let L be a closed subfield of M, $H = L'$. L is normal as a field over K, which is a subfield of L.*

Assume that

(1)$N(H)$ is closed.

(2)Every differential automorphism of L/K can be extended to M.

Then

(i)H is normal.

(ii)$DGal(M/K)/H = DGal(L/K)$.

Proof. A natural observation shows that: $H \subset G$ is normal $\Leftrightarrow N(H) = G \overset{N(H)\ Galois\ closed}{\Leftrightarrow} N(H)' = K$. Lemma 37 tells us that $N(H) =$

$\{g \in G | g(L) = L\}$. Among these we find all the differential automorphisms of L/K. Check (2) to ensure that we can extend these differential automorphisms to M (We can have looser conditions if we notice the Theorem 35.). But we hypothesized that L is normal over K, no elements in $L \setminus K$ can be fixed by the normalizer $N(H) \Leftrightarrow N(H) = K$. So we invoke Theorem 36 (ii) to finish our proof. □

Definition 39. (C-groups) We say a group G is a C-group if:

(i)it's a matrix group $M_n(F)$ endowed with a Zariski topology taking all those algebraic varieties whose defining systems lies on $F[x_{11}, \dots, x_{1n}, \dots, x_{n1}, \dots, x_{nn}]$ as closed sets.

(ii)it's a T_1-space with respect to Zariski topology.

(iii)The following mappings are continuous with respect to this topology: $\alpha \mapsto \alpha^{-1}$,$(\alpha, \beta) \mapsto \alpha \cdot \beta$,$\alpha \mapsto \alpha \cdot x \cdot \alpha^{-1}, \forall x \in G$.

A rather obvious example of C-group is the compact Lie groups, symmetric spaces, etc. We admit following two results and leave their proofs for interested readers. For an answer, see [Kaplansky].

Proposition 40. *Matrix groups endowed with the Zariski topology in the above definition are C-groups.*

Lemma 41. *In a C-group the normalizers of a closed subgroup is closed.*

8. Things All Considered and the Proof of the Fundamental Theorem

Finally we can reach our third step towards the fundamental theorem. Let's review its statement:

Theorem. *(The fundamental theorem of differential Galois theory)* [23]

(Assumption I)K is a differential field of characteristic zero.

(Assumption II)K has an algebraically closed constant field.

(Theorem Assumption) M/K is a Picard-Vessiot extension.

Under all these assumptions we have:

(i)There is a bijective correspondence between the intermediate differential fields and the algebraic subgroups of the differential Galois group $G = DGal(M/K)$.

(ii)There is a bijective correspondence between the normal *extensions L/K and the* closed normal *algebraic subgroups of the differential Galois group $G = DGal(M/K)$. In this case we know in addition that $G/H = DGal(L/K)$ where $H = L'$.*

Remark. Readers may want to review the meaning of closedness of fields and groups in differential Galois theory by referrring to Definition 21.

Let M/K be a Picard-Vessiot extension. If we insert another intermediate field $K \subset L \subset M$ into the extension, then M/L is also a Picard-Vessiot extension.

By Theorem 34, M is normal over L, so all intermediate fields lying between these two fields are closed.

Let H be a normal subgroup of G, $L = H'$ be the corresponding closed subfield of differential field M.

In addition we assume that $H = H''$. Then by Theorem 35 we know that all the differential automorphisms of L/K are extendable to M. Theorem 36(ii) said that $G/H = DGal(L/K)$ .All of its subgroups are normal and closed, by Theorem 38 and Lemma 41 since L is closed and normal (By Therorem 34) over K due to the assumption that the algebraic subgroups in (ii) must be *normal*.

By Corollary 31, G is an algebraic matrix group.

So all of its subgroups correspond to the intermediate differential subfields by Theorem 38.

The rest of our jobs: prove that the algebraic subgroups of G is not only closed in Zariski topology but also in sense of Galois theory(i.e.$H = H''$). It's equivalent to show that the given subgroup $H \subset G$ is Zariski-dense in H''. If not dense, there exists a polynomial f in n^2 variables (c_{ij}) whose coefficients are in $C \subset K$. And this polynomial f vanishes on H yet not H'', due to Theorem 30.

Intuitively, this is impossible because we can apply some $\sigma \in H$ onto the variables (c_{ij}) ,and we can subtract and get a lower-degree polynomials by equalizing the lowest degree term. And we are done.

For details in $n = 2$, see [Kaplansky]. For a general argument for arbitrary n, see [Ritt] or [Kolchin2].

9. Conclusion

9.1. **Why differential Galois theory is not widely used in differential geometry?** Since differential Galois theory originated from the problem of deciding the form of solution to a linear ODE, one may wonder what can we say about the geometric consequence behind this ODE. To be more precisely, if we are given a set of equations (e.g. Frenet-Serret equations) what can we deduce from the restrictive form of its solutions. This problems involves at least two sub-problems.

The first is whether we can find a corresponding equation for complex surfaces. Due to our assumption II above, we have to consider at least some curve embedded in $\mathbb{C}^n$, the Riemannian surfaces. The differential Galois theory deals with only algebraically closed constant fields as we seen above, so we must discuss the complex geometry instead of the real one. The complex geometry is different from the real one. But then we lost the structural equation which we have in real Euclidean space. Although Riemannian surfaces can also be realized as real surfaces in $\mathbb{R}^n$, we cannot obtain satisfying differential structural equations from Gauss-Mainardi-Codazzi structural equations for real surfaces through clumsy calculations. For more general settings, like $\mathbb{F}^n$ where the based field is algebraically closed, we do not even have a analytic topology well-defined on it. (I shall thank S.Z.Lee for pointing out this to me.) And this possible application on finite fields is discussed by Prof. Nicholas Katz in details in [Nicholas Katz].

> While differential Galois theory may seem analytic it is actually much more algebraic, For instance, in analysis and differential geometry you tend to care how large things are, while in algebra you don't, and differential Galois theory says nothing about size. In algebra you hope for exact solutions, while in analysis approximate solutions are usually good enough, and differential Galois theory good for describing exact solutions. In differential geometry you often have great freedom in gluing together local pieces to get a global structure, where in algebra local pieces are rigid and hard to glue together, and differential Galois theory describes rigid structures where one tiny piece controls everything.([Will Sawin])

The second is to what extent the form of solution decides the properties of the surfaces. We can decide the solution of a differential equation (i.e. after reduction to the Ricatti equation) lies in a Picard-Vessiot extension. But re-examine our arguments in the proof of the fundamental theorem, we see that the connection between Galois groups and equations is established using underlying algebraic varieties (algebraic matrix group) instead of differential manifolds defined by the differential polynomials provided by the Picard-Vessiot extension using differential Galois theory. This makes our guess over-optimistic. And Prof. Antoine Chambert-Loir pointed out that[Antoine]:

> A reason why differential Galois theory does not explicitly appears in differential geometry is that DGT(Differential Galois theory) works in the framework of differential fields, and smooth functions on a connected open subset of $\mathbb{R}^n$ do not form a field (unless $n = 0$)
>
> However, as explained in the book of Thomas Hawkins (*Emergence of the theory of Lie groups*), the works of Lie were explicitly motivated by generalizing Galois theory to differential equations.([Antonie])

9.2. **Applications and developments of differential Galois theory.** Altough its algebraic nature prohibits its usage in the differential geometry, differential Galois theory is by no means a dead branch. On the contrary, it has at least two thriving applications and developments in other branches in recent years. The first application is:

> This book [Nicholas Katz] is concerned with two areas of mathematics, at first sight disjoint, and with some of the analogies and interactions between them. These areas are the theory of linear differential equations in one complex variable with polynomial coefficients and the theory of one-parameter families of exponential sums over finite fields.[24]

The exponential sum $\sum_{x\in\mathbb{F}_p} exp(\frac{2\pi i\cdot f(x)}{p}), f(x) \in \{f_t(x) : f_t(x) \in \mathbb{Z}[x,t]\}$ is a natural tool used to make a common ground for linear ODEs and algebra. We observed a formal analogy between exponential sum and $\int exp(f(x))dx, f(x) \in \{f_t(x) : f_t(x) \in \mathbb{Z}[x,t]\}$ via the correspondence $\sum_{x\in\mathbb{F}_p} exp(\frac{2\pi i\cdot f(x)}{p}) \longleftrightarrow \int exp(f_t(x))dx$. This correspondence is just like the one between Riemannian sum and Riemannian integral except that our analysis now is done on a finite field. And Katz discussed following important questions about this connection:

(1) For a given p, how do the exponential sums vary as the parameter t varies?

(2) What is the differential Galois group $DGal(M/K)$ of the the differential equation satisfied by the integral $\int exp(f(x))dx$?

(3) How the geometric monodromy group of character p varies while the parameter t varies?

(4) Can we prove that for $p \gg 0$ the geometry monodromy groups are all equal to differential Galois groups?

The first and second question are attempt to figure out the correspondence between the differential Galois groups and the intermediate differential fields we mentioned earlier. The technique involves deep results in representation theory and number theory. And the third and fourth question are attempt to apply this on geometry. This book immediately laid the ground for introducing of differential Galois theory into arithmetic algebraic geometry.

This is one of the later development of differential Galois theory. Another development is led by A.Buium [Buium] who introduce differential Galois theory into Diophantine geometry. This is much more complicated than a few questions and it's still thriving. It does not refer to Galois representation so often as Katz did a decade ago.

As pointed out as above, there are two obstacles, the loss of analytic topology in $\mathbb{R}^n$ and the underlying algebraic variety for those algebraic matrix subgroups. These two are the major reasons why the applications of differential Galois theory are dominant only in discrete settings like Diophantine geometry (See [Buium]) and coding theory via difference equation (See [Franke]). It has an algebraic nature. Besides this paper, there are many other recent introductions to the differential Galois theory like [Beukers] [Singer] and [Marius & Singer]

For more knowledge of this direction from differential equation towards geometry, [Bryant, Griffiths and Hsu] is a good starting point, although it finally falls into the discussion of equations. But with the fundamental theorem of differential Galois theory, we can know the shape of solutions to many differential equations, one of which is the ODE of Fuchs type(See [V.B.Alekseev]).

Thanks: My parents J.Law and W.X.Yau, who support me during these years. My tutor Prof. X.L.Jiang, who gives me a lot of advice and teachings during the writing. My friend Dr.S.Z.Lee, who provide inspiring discussions with me.

Notes

[1][Ritt]pp.81-83
[2][Kaplansky]pp.1-10
[3][Kolchin1]pp.2
[4][Kaplansky]pp.38-39
[5][N.Levinson & E.A.Coddington]pp.70-78
[6]For a simpler example, see[Singer]
[7][Kolchin3]
[8][Kaplansky] Lemma 5.1
[9][Kaplansky] Lemma 5.2
[10][Kaplansky] Lemma 5.7
[11]Differential isomorphisms between subfields can be extended to admissible isomorphisms
[12][Kaplansky] Theorem 2.5
[13]Admissible isomorphisms can separate those additional elements
[14][Kaplansky] Theorem 2.6
[15][Kaplansky] Lemma 5.4
[16]Any element in $DGal(M/K)$ can be represented by some C-matrix satisfying C-polynomials S
[17]Any C_N-matrix satisfying C-polynomials S can be extended into an admissible isomorphism
[18]Admissible differential isomorphisms can be extended into differential automorphisms
[19][Kaplansky] Lemma 5.6
[20]Differential isomorphisms can be extended into differential automorphisms
[21]I shall thank Prof. Jiang for helping me work out the proof here.
[22]So we can preserve those elements in L
[23][Kaplansky] Theorem 5.9
[24][Nicholas Katz] pp.1

References

[Antoine] [1]Prof. Antoine Chambert-Loir's answer to my question on mathoverflow.net. Antoine Chambert-Loir is a Professor at Université Paris-Sud, Orsay, France. http://mathoverflow.net/questions/201853/Why-differenlial-galois-theory-is-not-widely-used, 2015-04-04. BJT.

[Artin] [2]Emil Artin. Galois theory. Dover Publications, 1998.

[Bass&Buium] [3]Hyman Bass and Alexandru Buium et.al. Selected Works of Ellis Kolchin with Commentary. American Mathematical Society, 1999.

[Beukers] [4]Frits Beukers, Differential Galois Theory, Chapter 8, edited by M. Waldschmidt, P. Moussa,

J. M. Luck et.al, From Number Theory to Physics. Springer-Verlag, 1995: pp.413-439.

[Bryant, Griffiths and Hsu] [5]Robert Bryant, Phillip Griffiths and Lucas Hsu. Toward a geometry of differential equations, edited by S.-T. Yau, Geometry, Topology and Physics, Conf. Proc. Lecture Notes Geom. Topology. vol. IV, 1995: pp. 1-76.

[Buium] [6]Alexandru Buium. Differential Algebra and Diophantine Geometry. Hermann Paris, 1994.

[Franke] [7]Charles H. Franke, Picard-Vessiot theory of linear homogeneous difference equations, Trans. Amer. Math. Soc. 108, 1963: pp.491-515.

[Kaplansky] [8]Irving Kaplansky, Introduction to differential algebra, Hermann Paris,1957.

[Kolchin1] [9]Ellis R. Kolchin, Existence theorems connected with the Picard-Vessiot theory of homogeneous linear ordinary differential equations. Bull. Amer. Math. Soc. 54. AMS, 1948: pp.927-932.

[Kolchin2] [10]E. R. Kolchin. Galois Theory of Differential Fields. American Journal of Mathematics, Vol. 75, No. 4, 1953: pp. 753-824.

[Kolchin3] [11]E. R. Kolchin. Algebraic Matric Groups and the Picard-Vessiot Theory of Homogeneous Linear Ordinary Differential Equations. Annals of Mathematics, Second Series, Vol. 49, No.1, 1948: pp.1-42.

[Marius & Singer] [12]Marius van der Put & Michael F. Singer. Galois Theory of Linear Differential Equations. Springer:2003.

[Morita] [13]Morita Shigeyuki. Geometry of Differential Forms, American Mathematical Society, 2001.

[Nicholas Katz] [14]Nicholas M. Katz. Exponential sums and differential equations. Princeton University Press, 1990.

[N.Levinson & E.A.Coddington] [15][N.Levinson & E.A.Coddington]N.Levinson & E.A.Coddington. Theory of Ordinary Differential Equations. McGraw-Hill Publishing, 1955.

[Ritt] [16]Joseph Fels Ritt. Differential Algebra, American Mathematical Society Colloquium Publications, vol. 33. American Mathematical Society, 1950.

[Singer] [17]M.F.Singer. Introduction to the Galois Theory of Linear Differential Equations Algebraic Theory of Differential Equations. M.A.H. MacCallum and A.V. Mikhalov, eds., London Mathematical Society Lecture Note Series (no. 357), Cambridge University Press, 2009:pp.1-82.

[V.B.Alekseev] [18]V. B. Alekseev. Abel's Theorem in Problems and Solutions. Springer, 2004.

[Weyl] [19]Hermann Weyl. The Classical Groups. Princeton University Press, 1997.

[Will Sawin] [20]Will Sawin's answer to my question on mathoverflow.net. Will Sawin is a PhD student whose advisor is Nicholas M. Katz at Princeton University. http://mathoverflow.net/questions/201853/Why-differenlial-galois-theory-is-not-widely-used, 2015-04-03. BJT.