Differential Galois Theory

by

Ahmet Berkay Kebeci

A Dissertation Submitted to the
Graduate School of Sciences and Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in

Mathematics

KOÇ
UNIVERSITY

December 2018

Differential Galois Theory

Koç University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by

Ahmet Berkay Kebeci

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:

_____

Assoc. Prof. Sinan Ünver

_____

Prof. Burak Özbağcı

_____

Asst. Prof. Altan Erdoğan

Date: _____

To my family

ABSTRACT

Galois Theory is a powerful tool to study the roots of polynomials. In this sense, the differential Galois theory is the analogue of Galois theory for linear differential equations. In this thesis, we will construct the notion of a differential field and Picard-Vessiot extension of a linear differential equation as the analogue of a field and the splitting field of a polynomial, respectively. Then we define the differential Galois group and we see that it has a linear algebraic group structure. Using those, we have a Galois correspondence for algebraic subgroups of the differential Galois group similar to the correspondence in the Galois theory. Moreover, we find a characterization for Liouvillian functions corresponding to the solvability of G^0 , the identity component of differential Galois group G. This is the analogue of the characterization of solvability by radicals of a polynomial equation in Galois theory. As a corollary we find that identity component of the differential Galois group of an elementary function is abelian. Using this tool we can prove that $\int e^{-x^2}$ cannot be expressed as an elementary function. Besides, there is a connection between differential Galois theory and Tannakian categories. We also present this approach.

ÖZETÇE

Galois teorisi, polinomların köklerini çalışmak için güzel bir araç. Bu bağlamda diferansiyel Galois teorisi, Galois teorisinin lineer diferansiyel denklemler üzerine analoğu olarak görülebilir. Bu tezde diferansiyel cisimleri ve lineer diferansiyel denklemlerlerin Picard-Vessiot genişlemelerini, cisimlerin ve parçalanış cisimlerinin benzeşimi olacak şekilde kuracağız. Ardından diferansiyel Galois grubu tanımlayacağız ve üzerinde lineer cebirsel grup yapısı olduğunu göstereceğiz. Bunu kullanarak, Galois teorisindeki denkliğin benzerinin, diferansiyel Galois grubun cebirsel altgrupları için olduğunu söyleyeceğiz. Ayrıca, diferansiyel Galois grubun birim bileşeninin çözünür olmasının Liouvillian fonksiyonların bir tavsifi olduğunu bulacağız. Bu Galois teorisindeki polinomların radikal olarak çözümünü inceleyen duruma benzerlik göstermekte. Bunun sonucu olarak, elementer fonksiyonların diferansiyel Galois gruplarının birim bileşenlerinin abelyen olduğunu göstereceğiz. Böylelikle $\int e^{-x^2}$ fonksiyonunun elementer olamayacağının sonucunu çıkartacağız. Son olarak, diferansiyel Galois grubu ile Tannakacı kategoriler arasındaki bağlantıdan söz edeceğiz.

ACKNOWLEDGMENTS

I would like to thank my advisor *Prof. Sinan Ünver* for his motivation and patience during this research. His guidance and deep knowledge helped me in all the time of research and writing of this thesis.

I am grateful to *Prof. Burak Özbağcı* and *Prof. Altan Erdoğan* for accepting to be in the thesis committee. My sincere thanks also goes to *Prof. Ergün Yalçın* for his guidance in my undergraduate education. I would also like to thank my colleagues in Koç University Graduate School of Sciences and Engineering (GSSE) for their encouragement and support.

I am grateful to my parents *Birgül Kebeci*, *Faik Kebeci* and my brother *Ayberk Kebeci* for their love and continuous support.

Finally, I thank Technological Research Council of Turkey (TÜBİTAK) for their financial support.

TABLE OF CONTENTS

Chapter 0

INTRODUCTION

Differential Galois theory (or more precisely Galois theory of linear differential equations) studies the solutions of differential equations, by looking their symmetries, over a base differential field. It is in analogy with the Galois theory that studies the solutions of polynomials. A significant difference is that differential Galois groups have additional variety structures. In this thesis, we will only deal with linear homogeneous differential equations.

The branch that studies the linear differential equations is known as Picard-Vessiot theory, due to its founders C. Picard (1856-1941) and E. Vessiot (1865-1952). Fundamental papers are appeared in 1883 and 1892, respectively. The differential algebra and differential Galois theory starts with J. F. Ritt (1893-1951) and his publication in 1948. It continuous with E.R. Kolchin (1954-1961). This historical notes are due to the preface of [5] and more can be found there.

The main motivation of this thesis is to prove that $\int e^{-x^2}$ is not an elementary function. We emphasize that this is a similar concept with the solvability of polynomials like $x^5 - 4x^2 - 2 = 0$. The analogy between Galois theory and differential Galois theory can be seen as follows:

Polynomials	$\longrightarrow$	Linear differential equations
Rings	$\longrightarrow$	Differential rings
Splitting fields	$\longrightarrow$	Picard-Vessiot extensions
Galois group	$\longrightarrow$	Differential Galois group
Finite groups	$\longrightarrow$	Linear algebraic groups
Galois correspondence		Galois correspondence
for subgroups	$\longrightarrow$	for algebraic subgroups
Radical extensions	$\longrightarrow$	Liouvillian extensions
Profinite groups	$\longrightarrow$	Affine group schemes
Galois categories	$\longrightarrow$	Tannakian categories

Summary of Main Part

Throughout this thesis, all the rings considered are supposed to be commutative, to have 1 and to contain $\mathbb{Q}$. In the construction of a *differential ring*, we basically add a differential structure to a ring by attaching a linear map ∂ (or just $'$) that satisfies the Leibniz's rule. This map is called a *derivation*. We define *differential morphism* as a ring homomorphism which commutes with derivation. Let F be a differential field with algebraically closed field of constants $C = C_F := \partial^{-1}(0)$. We define a *(homogeneous) linear differential equation* over F in a traditional way:

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1y' + a_0y$$

where $a_i \in F$. A *differential field extension* means a field extension preserving the differentiation. We define its *Picard-Vessiot extension*, in analogy with splitting fields, as a smallest differential field extension that contains a full set of solutions i.e., set of solutions with zero wronskian, of $L(y) = 0$. Formal definition is as follows:

> A differential field extension $E \supseteq F$ is called a *Picard-Vessiot extension* for L if:
>
> (i) $E = F\langle y_1, ..., y_n\rangle$, where $y_1, ..., y_n$ is a full set of solutions of $L(y) = 0$.

(ii) Every constant of E lies in F.

$F\langle y_1, ..., y_n\rangle$ stands for the smallest differential field containing F and the elements $y_1, ..., y_n$. Second condition is to guarantee the minimality. First condition is saying that $y_1, ..., y_n$ are linearly independent over C. Therefore the solution space $V = L^{-1}(0)$ in E is an n-dimensional C-vector space.

Next, we construct the Picard-Vessiot extensions in a similar way to the construction of splitting fields. We consider the differential ring $F\{x_1, ..., x_n\}$ in n differential indeterminates. This is the smallest differential ring that contains $F, x_1, ..., x_n$. We take the quotient by the differential ideal generated by the elements

$$x_j^{(n)} + a_{n-1}x_j^{(n-1)} + ... + a_1x_j' + a_0x_j \ , \quad 1 \leq j \leq n$$

which is the ideal generated by these elements and their derivatives. We call this quotient R. Let P be a maximal differential ideal of R. Here, a differential ideal is an ideal containing derivatives of its elements. Then R/P is an integral domain whose field of fractions is a Picard-Vessiot extension over F. Taking quotient with P is for minimality. This shows the existence of Picard-Vessiot extensions given a linear differential equation L and a differential field F. It is also unique up to differential isomorphisms. This existence and uniqueness are proven in Theorem 3.2.9 and Theorem 3.2.11.

Fix a Picard-Vessiot extension $F \subseteq E$ having algebraically closed field of constants C. The *differential Galois group* of this extension is defined as a group of differential F-algebra automorphisms of E and denoted by $G(E/F)$. Note that any finite Galois extension is Picard-Vessiot and its Galois group corresponds with its differential Galois group.[1] Hence this notation does not lead any confusion. Let $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1y' + a_0y$ be the linear differential equation that makes the extension $F \subseteq E$ Picard-Vessiot. If t is a solution from E and $\sigma \in G(E/F)$, then $0 = \sigma(0) = \sigma(L(t)) = L(\sigma(t))$. Then $\sigma(t)$ is also a solution. If V is the solution space of L in E, then $\sigma(V) = V$. Hence there is a group injection $G(E/F) \to GL(V)$. We also show that

[1] See [5, Example 1.14. and Proposition 3.20.] for details.

image of this map is closed. Hence $G(E/F)$ is a linear algebraic group. This result is proven in Theorem 4.1.2.

Call $G = G(E/F)$. An important result to be used in the (differential) Galois correspondence is Lemma 4.2.1:

> If $x \in E \backslash F$, then there exists $\sigma \in G(E/F)$ such that $\sigma(x) \neq x$.

Since G has a variety structure, we can talk about its coordinate ring $C[G]$. Recall R/P defined above and denote it by T. Recall that field of fractions of T is isomorphic to E as differential fields. Theorem 4.2.3 states that there is a $\overline{F}[G]$-module isomorphism

$$\overline{F} \otimes_F T \xrightarrow{\sim} \overline{F} \otimes_C C[G].$$

This will also be useful in the proof of the (differential) Galois correspondence. It has a nice corollary:

$$dim G(E/F) = trdeg[E : F].$$

As in classical Galois theory, there is a Galois correspondence for differential Galois theory. The intermediate differential extensions of $F \subseteq E$ corresponds to closed subgroups of $G(E/F)$. This correspondence is given as:

> Let $\mathscr{F}$ be the category whose objects are the elements of the set
>
> $$Ob(\mathscr{F}) = \{E \supseteq K \supseteq F : K \text{ is an intermediate differential field}\}$$
>
> and morphisms are the inclusion homomorphisms. Let $\mathscr{G}$ be the category whose objects are the elements of the set
>
> $$Ob(\mathscr{G}) = \{H \leqslant G(E/F) : H \text{ is a Zariski closed subgroup}\}$$
>
> and morphisms are the inclusion homomorphisms. The Galois correspondence for differential equations indicates a contravariant isomorphism of categories $\mathscr{F}$ and $\mathscr{G}$ which is given by the functors
>
> $$\phi : K \mapsto G(E/K) \text{ and } \psi : H \mapsto E^H$$
>
> such that
>
> $$\phi\psi = 1_{\mathscr{G}} \text{ and } \psi\phi = 1_{\mathscr{F}}.$$

There is more. Picard-Vessiot subextensions corresponds to closed normal subgroups. If $K \supseteq F$ is one of them we have

$$G(K/F) = G(E/F)/G(E/K).$$

Identity component of $G(E/F)$ corresponds to the algebraic closure of F in E. If we take any subgroup (not necessarily Zariski closed) $H \leqslant G(E/F)$, then $G(E/E^H)$ is the Zariski closure of H. Let $M \supseteq E$ be a differential field extension with no new constants and let $M \supseteq K \supseteq F$ be an intermediate differential field. Then $EK \supseteq K$ is a Picard-Vessiot extension, where EK is the field compositum in M. In this case, the homomorphism

$$G(EK/K) \to G(E/F)$$

is an injection whose image has Zariski closure $G(E/E \cap K)$. These results are presented in Theorem 4.3.2, Theorem 4.3.3 and Proposition 4.3.4.

We can back to our motivating question about elementary functions. An *elementary function* is a finite composition of algebraic operations, exponentials and logarithms. We first study a more general concept called Liouvillian functions. We define a *Liouvillian function* as recursively, it is an elementary function or the integral of a Liouvillian function. Equivalently, a Liouvillian function is a finite composition of algebraic operations, exponentials and integrals.

We want to see Liouvillian functions in the language of Picard-Vessiot theory. For this, we will define Picard-Vessiot extensions contain nothing but Liouvillian functions. Algebraic operations occur in algebraic extensions. Therefore we can assume the rest of the extension purely transcendental. We represent an exponential by a differential field extension $F \subseteq F(a)$ where $a'/a \in F$. Such a purely transcendental extension is called an *adjunction of an exponential*. Similarly we represent an integral by an extension $F \subseteq F(a)$ where $a' \in F$. If this extension is purely transcendental then it is called an *adjunction of an integral*. Lemma 5.1.3 characterizes such extensions:

> Let $E \supseteq F$ be a Picard-Vessiot extension with algebraically closed field of constants C and let $G := G(E/F)$. Then,

(i) $G \simeq \mathbb{G}_a(C)$ if and only if $E \supseteq F$ is an adjunction of an integral.

(ii) $G \simeq \mathbb{G}_m(C)$ if and only if $E \supseteq F$ is an adjunction of an exponential.

With this fashion, we define a *Liouvillian extension* as a Picard-Vessiot extension of the form

$$F = F_0 \subseteq F_1 \subseteq ... \subseteq F_n = E$$

where

$$F_i = F_{i-1}(a_i)$$

and for all i either

(i) a_i is algebraic over F_{i-1}, or

(ii) $a_i \neq 0$ and $a_i'/a_i \in F_{i-1}$, or

(iii) $a_i' \in F_{i-1}$.

Fix a Picard-Vessiot extension $F \subseteq E$ and call $G = G(E/F)$. Assume this extension is Liouvillian. Since the transcendental part of this extension is given by adjunction of an integrals and exponentials, one can deduce that the identity component G^0 has a subnormal chain with quotients $\mathbb{G}_a$ or $\mathbb{G}_m$. But these groups are abelian, hence G^0 is solvable. Conversely, assume that G^0 is solvable. Using the results from Section 1.4., we know that G^0 has a subnormal chain of closed connected subgroups and each subquotient is isomorphic to either $\mathbb{G}_a$ or $\mathbb{G}_m$. Then $F \subseteq E$ is Liouvillian. This gives the first main theorem (Theorem 5.1.4):

> Let $E \supseteq F$ be a Picard-Vessiot extension with algebraically closed field of constants C and let $G := G(E/F)$. Following are equivalent.
>
> (i) G^0 is solvable.
>
> (ii) $E \supseteq F$ is liouvillian.
>
> (iii) E is contained in a liouvillian extension of F.

Let C be an algebraically closed field with trivial derivation, and let $F = C(x)$ be the field of rational functions with derivation $x' = 1$. Define a *field of elementary functions* as an extension in the form

$$F(a_1, a_2, ..., a_n, b_1, b_2, ..., b_m) \supseteq F$$

where

(i) $a_i' \in F$, for all i and

(ii) for all j, either $b_j'/b_j \in F(b_1, b_2, ..., b_{j-1})$ or b_j is algebraic over $F(b_1, b_2, ..., b_{j-1})$.

An *elementary function* is an element of a field of elementary functions. In this definition, the first part represents the logarithms, since it adds an integral from $C(x)$. The second part represents the algebraic elements and exponentials. The second main theorem (Theorem 5.2.2) states:

> Let
>
> $$\mathscr{C} = F(a_1, a_2, ..., a_n, b_1, b_2, ..., b_m) \supseteq F$$
>
> be a field of elementary functions. Suppose $E \supseteq F$ is a Picard-Vessiot subextension contained in $\mathscr{C}$ and let $G := G(E/F)$. Then G^0 is abelian.

Consider $t := \int e^{-x^2}$ over the differential field $\mathbb{C}(x)$ with derivation $x' = 1$. It can be seen as a solution of $y'' + 2xy' = 0$. Example 4.1.1 finds that the Picard-Vessiot field for this equation is $\mathbb{C}\langle x, t\rangle = \mathbb{C}(x, t, t')$. Moreover,

$$G(\mathbb{C}\langle x, t\rangle/\mathbb{C}(x)) = \{ \begin{bmatrix} 1 & 0 \\ a & b \end{bmatrix} : a, b \in \mathbb{C}, b \neq 0\}.$$

This is a connected non-abelian group. Hence $\int e^{-x^2}$ is not an elementary function.

Summary of Tannakian Approach

There is a categorical generalization for Galois group. This is done by Galois categories. First we examine the question: "When is a category can be seen as a category of

representations of a profinite group G and how do we recover G from this category?" The answer is given by lemma 2.1.1 and proposition 2.1.3:

> If $\mathcal{C} = \mathrm{Perm}_G$ for a profinite group G and $\omega : \mathcal{C} \to \mathrm{Fsets}$ is the forgetful functor, then
>
> $$G \xrightarrow{\sim} Aut^{\sqcup}(\omega)$$
>
> is an isomorphism of profinite groups. If $\mathcal{C}$ is a Galois category with the fibre functor ω and $G = Aut^{\sqcup}(\omega)$, then the categories
>
> $$\mathcal{C} \text{ and } \mathrm{Perm}_G$$
>
> are equivalent.

Then we ask the same question for the case that G is an affine group scheme. This time the answer is Tannakian categories and given by theorem 2.3.1 and theorem 2.3.3:

> If $\mathcal{C} = \mathrm{Repr}_G$ for an affine group scheme G over a field k and $\omega : \mathcal{C} \to \mathrm{Vect}_k$ is the forgetful functor, then
>
> $$G \xrightarrow{\sim} Aut^{\otimes}(\omega)$$
>
> is an isomorphism of affine group schemes. If $\mathcal{C}$ is a (neutral) Tannakian category with the fibre functor ω and $G = Aut^{\otimes}(\omega)$, then the categories
>
> $$\mathcal{C} \text{ and } \mathrm{Repr}_G$$
>
> are equivalent.

One example of a Galois categories is a category of finite field extensions of a fixed field. In this case, the corresponding profinite group is Galois group itself. This is explained in example 2.1.4. A profinite group is defined as a projective limits of finite groups. Analogously, an affine group scheme can be seen as a projective limit of linear algebraic groups[1]. In differential Galois theory, we have linear algebraic groups instead

[1]See [8, Corollary B.17.] for the proof of this statement.

of finite groups. In this sense, the Tannakian categories are analogous with the Galois categories. An example of a Tannakian category is given by using differential modules which we introduce in Section 3.3. Then, the corresponding affine group scheme is the differential Galois group. This is explained in Section 4.4.

Chapter-by-chapter Summary

Chapter 1 introduces the linear algebraic groups. We mostly follow [4] and sometimes pass to [1] and [7] in this chapter. First two sections give basic definitions and results. Section 1.3. presents a characterization for linear algebraic groups over k, namely closed subgroups of $GL_n(k)$, where k is an algebraically closed field of characteristic 0. Results on section 1.4. are crucial for chapter 4 and 5.

Chapter 2 investigates the Tannakian categories. References for this chapter are [3], [8], [9] and [10]. Section 2.1. aims to give a motivation for Tannakian categories by presenting the Galois categories. Section 2.2. introduces the tools for Section 2.3. which presents the Tannakian categories.

Chapter 3 prepares the playground for differential Galois theory. In this chapter, we introduce the basics of Picard-Vessiot theory. We follow [1], [5] and [8]. Section 3.1. introduces the differential rings and fields which are the main ingredients for Picard-Vessiot theory. Section 3.2. defines the Picard-Vessiot extensions and gives the basic properties of them including existence and uniqueness. Section 3.3. presents differential modules as another presentation of linear differential equations to be used in section 4.4.

Chapter 4 starts with the definition of differential Galois group which is the main object of this thesis. In the first 3 sections of this chapter, we mostly follow [1], [5] and [8]. In the last section of this chapter we follow [2], [6], [8] and [9]. In Section 4.1., we define differential Galois group and show that it has a linear algebraic group structure. This is done by finding a closed injection to a general linear group over constants. Section 4.2. provides a formulation for the coordinate ring of the differential Galois group using "the solution algebra" of the corresponding Picard-Vessiot extension.

This helps to prove the Galois correspondence that is subject to Section 4.3. This is a correspondence between the closed subgroups and intermediate differential extensions. In Section 4.4., we present a different approach using Tannakian categories. In this section, the extra results from Chapter 2 and Section 3.3. are used.

Chapter 5 contains the main results of this thesis. The main references are [5] and [8]. First of the main results is that a Picard-Vessiot extension is Liouvillian if and only if it is virtually solvable i.e. its differential Galois group has solvable identity component. We state and prove this theorem in Section 5.1. The motivation of the thesis was to show that $\int e^{-x^2}$ is not an elementary function. This brings us to Section 5.2. where we present the other main theorem. It states that the differential Galois group of an extension of elementary functions has abelian identity component. This shows that $\int e^{-x^2}$ is not an elementary function.

The reader who wants to go directly the main theorems, by skipping Tannakian approach, can skip Chapter 2, Section 3.3. and Section 4.4. In this case, this order of sections seems to be intuitive:

3.1 - 3.2 - 4.1 - 1.1 - 1.2 - 1.3 - 4.2 - 4.3 - 1.4 - 5.1 - 5.2.

The reader who wants to go the Tannakian categorical definition of differential Galois group in the shortest way, can follow this way:

3.1 - 3.2 - 4.1 - 2.1 - 2.2 - 2.3 - 3.3 - 4.4.

Chapter 1

LINEAR ALGEBRAIC GROUPS

1.1 Basic Definitions and Examples

Throughout this section k will denote an algebraically closed field of characteristic 0 and all affine varieties, unless otherwise stated, will be defined over k.

Definition 1.1.1. A *linear algebraic group* G is a group object in the category of affine varieties (over k), i.e. G is an affine variety together with morphisms of affine varieties $\mu : G \times G \to G$, $\iota : G \to G$ and $\nu : \mathrm{Spec}(k) \to G$, such that the following diagrams commute

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mu \times \mathrm{id}} & G \times G \\ \downarrow{\scriptstyle \mathrm{id} \times \mu} & & \downarrow{\scriptstyle \mu} \\ G \times G & \xrightarrow{\mu} & G \end{array}$$

$$\begin{array}{ccc} G & \xrightarrow{(p,\mathrm{id})} & G \times G \\ \downarrow{\scriptstyle (\mathrm{id},p)} & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle \mu} \\ G \times G & \xrightarrow{\mu} & G \end{array}$$

$$\begin{array}{ccc} G & \xrightarrow{(\iota,\mathrm{id})} & G \times G \\ \downarrow{\scriptstyle (\mathrm{id},\iota)} & \searrow^{p} & \downarrow{\scriptstyle \mu} \\ G \times G & \xrightarrow{\mu} & G \end{array}$$

where $p : G \xrightarrow{\kappa} \mathrm{Spec}(k) \xrightarrow{\nu} G$ and κ is induced by the natural inclusion $k \to k[G]$ (where $k[G]$ is the coordinate ring of G), i.e. G is a group with multiplication μ, inverse ι and the identity element e as the single point in the image of ν.

Consider the coordinate ring $k[G]$ of G. The morphisms μ, ι and ν correspond to k-algebra homomorphisms $m^* : k[G] \to k[G] \otimes_k k[G]$, $\iota^* : k[G] \to k[G]$ and $\nu^* : k[G] \to k$.

Any closed subgroup of a linear algebraic group is again a linear algebraic group. A *morphism* $\varphi : G_1 \to G_2$ of linear algebraic groups is a morphism of affine varieties that is also a group homomorphism. Since φ is continuous $\ker\varphi$, being the inverse image of the closed set $\{1\}$, is a closed subgroup of G_1. Therefore $\ker\varphi$ is a linear algebraic group.

Example 1.1.2. Some basic examples of linear algebraic groups are as follows.

(i) The additive group $\mathbb{G}_a(k)$ (or simply $\mathbb{G}_a$) is the affine line $\mathbb{A}^1$ with $\mu(x, y) = x+y$, $\iota(x) = -x$ and $e = 0$. Its coordinate ring is $k[x]$ and $\mu^*(x) = x \otimes 1 + 1 \otimes x$, $\iota^*(x) = -x$.

(ii) The multiplicative group $\mathbb{G}_m(k)$ (or simply $\mathbb{G}_m$) is the affine variety $k^* \subset \mathbb{A}^1$ with $\mu(x, y) = xy$, $\iota(x) = x^{-1}$ and $e = 1$.

(iii) The direct product of two (or more) linear algebraic groups, i.e., the usual direct product of groups endowed with the Zariski topology, is again a linear algebraic group. For example, a torus of dimension n which is defined by the direct product of n copies of $\mathbb{G}_m(k)$ is a linear algebraic group.

(iv) $GL_n(k)$ is a linear algebraic group with matrix multiplication as it is an affine subset of $M_n(k)$ which can be identified with $\mathbb{A}^{n^2}$. Its coordinate ring is

$$k[x_{11}, x_{12}, ..., x_{nn}, y]/(det(x_{ij}) \cdot y - 1).$$

(v) $SL_n(k)$ is a linear algebraic group since it is the kernel of the determinant map $GL_n(k) \to \mathbb{G}_m(k)$.

(vi) $T_n(k)$, upper triangular group, consist of all the upper triangular matrices in $GL_n(k)$. It is a closed subgroup of $GL_n(k)$.

(vii) $D_n(k)$, diagonal group, consists of all the diagonal matrices in $GL_n(k)$. It is a closed subgroup of $T_n(k)$. $D_n(k)$ is also isomorphic (as a linear algebraic group) to a torus of dimension n.

(viii) $U_n(k)$, the upper triangular unipotent group, consists of all the matrices whose all diagonal entries 1 in $T_n(k)$. It is the kernel of the projection $T_n(k) \to D_n(k)$.

(ix) Any finite group is a linear algebraic group. Any symmetric group S_n is isomorphic to a subgroup of GL_n, in the form of permutation matrices, and any finite group is isomorphic to a subgroup of some symmetric group. Since all finite sets are closed, any finite group is isomorphic to a closed subgroup of GL_n, for some n.

1.2 Subgroups and Morphisms

1.2.1 Image of a Morphism

We want to show that image of a morphism of linear algebraic groups is closed and therefore it is a linear algebraic group. First we need a tool from topology.

Definition 1.2.1. A topological space is called *locally closed* if it is an intersection of an open set with a closed set. A finite union of locally closed sets is called a *constructible* set.

Proposition 1.2.2. *Let X be a topological space. If a subspace Y is constructible then it contains an open dense subset of its closure.*

Now we state a theorem from algebraic geometry. This result is due to Chevalley

Theorem 1.2.3. *[4, Theorem 4.4.] Let $\varphi : X \to Y$ be a morphism of varieties. Then φ maps constructible sets to constructible sets. In particular,* $\operatorname{Im}\varphi$ *is constructible in Y.*

Lemma 1.2.4. *Let U and V be two dense open subsets of a linear algebraic group G. Then $G = U \cdot V$.*

Proof. Let $x \in G$ be arbitrary. By the definition of a linear algebraic group, the inversion map $\iota : G \to G$ is continuous and its inverse is itself. Therefore ι is a homeomorphism and $\iota(V) = V^{-1}$ is again a dense open subset. Similarly, the translation

map by x, namely $G \to G$, $g \mapsto xg$, is a homeomorphism and therefore xV^{-1} is a dense open subset. Then U must meet xV^{-1} because otherwise $G \backslash U$ would be the smallest closed set containing xV^{-1} i.e. $G = G \backslash U$ and U would be empty. Hence there is an element $a \in U$ such that $a \in xV^{-1}$ i.e. $a^{-1}x \in V$. Thus $x = a \cdot a^{-1}x \in U \cdot V$. □

Proposition 1.2.5. *Let H be a subgroup of a linear algebraic group G, $\overline{H}$ its closure.*

(i) $\overline{H}$ is a subgroup of G.

(ii) If H is constructible, then H is closed.

Proof. (i) Let $x, y \in \overline{H}$. Being the composition of two homeomorphisms, inversion and translation by x, the following map

$$\begin{aligned} \varphi : G &\to G \\ g &\mapsto xg^{-1} \end{aligned}$$

is also a homeomorphism. Since inversion is a homeomorphism $\overline{H}^{-1} = \overline{H^{-1}} = \overline{H}$, therefore $\varphi(\overline{H}) = x\overline{H}^{-1} = x\overline{H^{-1}} = x\overline{H} = \overline{H}$. Hence $xy^{-1} = \varphi(y) \in \varphi(\overline{H}) = \overline{H}$.

(ii) If H is constructible, then by proposition 1.2.2, it contains an open dense subset U of $\overline{H}$. But $\overline{H}$ is a group by part (i), then by lemma 1.2.4, $\overline{H} = U \cdot U \subset H \cdot H = H$.

□

Corollary 1.2.6. *Let A, B be closed subgroups of a linear algebraic group G. If B normalizes A, then AB is a closed subgroup of G.*

Proof. Since B normalizes A, AB is a subgroup of G. Considering the product morphism $\mu : G \times G \to G$, we have that $\mu(A \times B) = AB$ is constructible by theorem 1.2.3. Hence AB is closed by proposition 1.2.5(ii). □

Now we are ready to prove that the image of a morphism is a linear algebraic group.

Proposition 1.2.7. *Let $\varphi : G \to H$ be a morphism of linear algebraic groups. Then,* $\operatorname{Im}\varphi$ *is a closed subgroup of H.*

Proof. $\varphi(G)$ is a subgroup of H. By theorem 1.2.3 it is a constructible subset of H and by proposition 1.2.5(ii), it is a closed subgroup of H. □

1.2.2 Quotients

Let N be a closed normal subgroup of a linear algebraic group G. Cosets of N form a group, by normality. We want to see G/N as a variety. Using closeness we define *Chevalley quotient* of G by N as a variety X together with a surjective morphism $\pi : G \to X$ such that the fibers of π are exactly the cosets of N. There is a categorical definition that is coincide with this one as follows. $\pi : G \to X$ is an epimorphism that is constant on all cosets of N and for any morphism $G \to Y$ that is constant on all cosets of N, there is a unique morphism $X \to Y$ such that the following diagram commutes.

$$\begin{array}{ccc} G & \xrightarrow{\pi} & X \\ \downarrow & \swarrow_{\exists!} & \\ Y & & \end{array}$$

Therefore G/N has both group and affine variety structure. Moreover, two structures coincide. Hence G/N is a linear algebraic group. Its coordinate ring is

$$k[G/N] \simeq k[G]^N$$

where $k[G]^N = \{f \in k[G] : n \cdot f = f, \text{ for any } n \in N\}$. Here the action is given by

$$\begin{aligned} G \times k[G] &\to k[G] \\ (g, f) &\mapsto \lambda_g(f) : x \mapsto f(g^{-1}x). \end{aligned}$$

As in the classical group theory, given a morphism of linear algebraic groups $\varphi : G \to H$, it induces an isomorphism of linear algebraic groups $G/\ker\varphi \to \varphi(G)$. Other isomorphism theorems also holds for closed subgroups.

1.2.3 Identity Component

Let G be a linear algebraic group with identity 1. Let

$$X_1, X_2, ..., X_m$$

be all distinct irreducible components containing 1. Then $X_1 \times X_2 \times ... \times X_m$ is irreducible and its image under the continuous map

$$G \times G \times ... \times G \to G$$

which is $X_1X_2...X_m$ is irreducible. But $1 \in X_1X_2...X_m$ so $X_1X_2...X_m$ is included in one of X_i's. Say $X_1X_2...X_m \subseteq X_i$. Hence $X_1, X_2, ..., X_m \subseteq X_1X_2...X_m \subseteq X_i$. Thus $X_1 = X_2 = ... = X_m$ and $m = 1$. Similarly, one can show that irreducible components of G are pairwise disjoint. Therefore irreducible components are the connected components of G. We denote by G^0 the unique irreducible component of 1, and call it the *identity component* of G. We call G is *connected* if $G = G^0$.

Example 1.2.8. Recall that an affine algebraic variety is irreducible if and only if its coordinate ring is an integral domain.

(i) $\mathbb{G}_a$ and $\mathbb{G}_m$ are connected since $k[\mathbb{G}_a] = k[x]$ and $k[\mathbb{G}_m] = k[x, x^{-1}]$ are integral domains.

(ii) $GL_n(k)$ is connected.

We present some basic properties of the identity component.

Proposition 1.2.9. *Let G be a linear algebraic group.*

(i) G^0 is a closed characteristic (therefore normal) subgroup of finite index in G, whose cosets are the connected as well as irreducible components of G.

(ii) Each closed subgroup of finite index in G contains G^0.

(iii) If S is a (Zariski) connected subset of G containing 1, then the subgroup of G generated by S is also connected.

(iv) Let H, K be subgroups of G where K is closed and connected. Then $[H, K]$ is closed and connected.

(v) If G is connected, then so is $G' = [G, G]$.

Proof. (i) Let φ be a continuous automorphism of G. Then φ is a homeomorphism. Hence $\varphi(G^0)$ is an irreducible component. But it contains 1, so $G^0 = \varphi(G^0)$ and G^0 is characteristic.

Since G^0 is irreducible so is its closure $\overline{G^0}$. But $1 \in \overline{G^0}$ hence $G^0 = \overline{G^0}$.

Since translation by an element is an homeomorphism, all cosets of G^0 are also irreducible components of G. But since G is Noetherian, it can only have finitely many irreducible components.

(ii) Let $H \leqslant G$ be a closed subgroup of finite index. Being an homeomorphic image of H, all of its left cosets in G, say $H, x_2H, x_3H, ..., x_kH$, are also closed. Then $G^0 \cap H, G^0 \cap x_2H, G^0 \cap x_3H, ..., G^0 \cap x_kH$ are closed subsets of G^0 and their union is G^0. But this contradicts with G^0 being irreducible unless $k = 1$. Hence $G^0 \cap H = G^0$.

(iii) If S is connected, then $S \cup S^{-1}$ is also connected (since inversion is continuous), so we may assume that S contains inverses. Since μ, the multiplication map of G, is continuous, $S_i := \{s_1 \cdot s_2 \cdot ... \cdot s_i : s_1, ..., s_i \in S\}$ is connected for each i. Taking the union of the nested connected family $S_1 \subset S_2 \subset S_3...$, we end up with another connected set $\bigcup S_i = \langle S \rangle$.

(iv) For $h \in H$, define $\varphi_h : K \to G$ as $k \mapsto [h, k]$. Being a composition of multiplication and inversion, φ_h is continuous and therefore each $\varphi_h(K)$ is connected. $[H, K]$ is generated by those elements, so by part (iii) it is also connected.

(v) Follows from part (iv).

□

Corollary 1.2.10. *Let G be a linear algebraic group and N a closed normal subgroup of G. If G/N is abelian and N^0 is solvable then G^0 is solvable.*

Proof. Since G/N is abelian, we have $(G^0)' \leqslant G' \leqslant N$. By proposition 1.2.9(v), $(G^0)'$ is connected and therefore $(G^0)' \leqslant N^0$. But N^0 is solvable, then $(G^0)'$ is solvable and so is G^0. □

Theorem 1.2.11. *Let G be a linear algebraic group and let N be a closed normal subgroup of G. Then, N^0 is normal in G^0 and $(G/N)^0 \simeq G^0/N^0$.*

Proof. It is easy to see that $N^0 = N \cap G^0 \trianglelefteq G^0$. Therefore, $G^0N/N \simeq G^0/N^0$ is connected and contained in $(G/N)^0$. Since $G^0N \geqslant G^0$, we have $[G : G^0N] = [G/N : G^0N/N]$ is finite. Then G^0N/N contains $(G/N)^0$. Hence $G^0/N^0 \simeq G^0N/N = (G/N)^0$. □

1.2.4 Some Other Properties

Here we present some additional properties of linear algebraic groups to be used in next chapters.

Proposition 1.2.12. *Let G be a linear algebraic group, S and T subgroups with $S \geqslant T$. If T contains the commutator subgroup S' of S, then the closure $\overline{T}$ of T contains the commutator subgroup of the closure $(\overline{S})'$ of S.*

Proof. This directly follows from the fact that $x \mapsto [x, y]$ is continuous for any y. □

Corollary 1.2.13. *Let G be a linear algebraic group and H be an abelian subgroup of G. If $\overline{H}$ is the closure of H in G, then $\overline{H}$ is also an abelian subgroup of G.*

Proof. Take $S = H$ and $T = 1$ in proposition 1.2.12. □

Corollary 1.2.14. *Let G be a linear algebraic group and H be a solvable subgroup of G. If $\overline{H}$ is the closure of H in G, then $\overline{H}$ is also a solvable subgroup of G.*

Proof. Since H is solvable, its derived series collapses i.e. $H^{(n)} = 1$ for some n. By proposition 1.2.12, $\overline{H^{(i+1)}} \geqslant (\overline{H^{(i)}})'$, taking $T = H^{(i+1)}$ and $S = H^{(i)}$. Then $\overline{H^{(i)}}/\overline{H^{(i+1)}}$ is abelian and $\overline{H}$ is solvable. □

Proposition 1.2.15. *Let $K \leqslant H$ be two subgroups of a linear algebraic group G and suppose that $[K : H]$ is finite. Then $[\overline{K} : \overline{H}]$ is also finite.*

Proof. Let $h_1K, ..., h_nK$ be cosets of K in H. Then $\bigcup h_i\overline{K} \supseteq \bigcup h_iK = H$. Since multiplication map in G is a homeomorphism, each $H_i\overline{K}$ is closed. Therefore we have $\bigcup h_i\overline{K} \supseteq \overline{H}$. Hence $[\overline{K} : \overline{H}]$ is finite. □

1.3 Linearization of Affine Algebraic Groups

In this section, we will show that a linear algebraic group over k is isomorphic to a closed subgroup of some $GL_n(k)$. By example 1.1.2(ix), we know that the converse is also true. Consequently, this may be seen as an equivalent definition of a linear algebraic group. For the proof of this, we first introduce the G-varieties.

Let G be a linear algebraic group and V be an affine variety. V is called a *G-variety* if G acts on V that is given by a morphism of affine varieties

$$\begin{aligned} G \times V &\to V \\ (g, v) &\mapsto g \cdot v \end{aligned}$$

such that $g_1 \cdot (g_2 \cdot v) = (g_1g_2) \cdot v$ and $1 \cdot v = v$ for any $g_1, g_2 \in G$ and $v \in V$. Using this action we define a G-action on the coordinate ring $k[V]$ by

$$\begin{aligned} G \times k[V] &\to k[V] \\ (g, f) &\mapsto g \cdot f : v \mapsto f(g^{-1} \cdot v). \end{aligned}$$

A morphism of G-varieties is a morphism of affine varieties $\varphi : V \to W$ such that the diagram

$$\begin{array}{ccc} G \times V & \longrightarrow & V \\ \downarrow{\scriptstyle (\mathrm{id}\,,\varphi)} & & \downarrow{\scriptstyle \varphi} \\ G \times W & \longrightarrow & W \end{array}$$

commutes.

Lemma 1.3.1. *Let V be a finite dimensional k-vector subspace of $k[G]$. There is a finite dimensional G-stable subspace W with $V \subseteq W \subseteq k[G]$.*

Proof. Since every finite dimensional vector space is a finite sum of one-dimensional vector spaces, we can assume that V is one-dimensional. Suppose V is generated by $f \in k[G]$. Consider the action of G on itself

$$\begin{aligned} \varphi : G \times G &\to G \\ (g, h) &\mapsto gh \end{aligned}$$

which also corresponds to the action

$$\begin{aligned} G \times k[G] &\to k[G] \\ (g, f) &\mapsto \lambda_g(f) : x \mapsto f(g^{-1}x). \end{aligned}$$

Since φ is a morphism of varieties we have another map

$$\begin{aligned} \varphi^* : k[G] &\to k[G] \otimes k[G] \\ f &\mapsto f \circ \varphi \end{aligned}$$

induced by φ. Write $\varphi^*(f) = \sum_i m_i \otimes f_i$ for some $m_i, f_i \in k[G]$. Note that here only finitely many terms appear. Therefore

$$\begin{aligned} (\lambda_g(f))(x) &= f(g^{-1}x) \\ &= f(\varphi(g^{-1}, x)) \\ &= \varphi^*(f)(g^{-1}, x) \\ &= \sum_i (m_i \otimes f_i)(g^{-1}, x) \\ &= \sum_i m_i(g^{-1}) f_i(x) \end{aligned}$$

and $\lambda_g(f) = \sum_i m_i(g^{-1})f_i$ is in the span of f_i's. Hence, letting W be the span of

$$\{\lambda_g(f) : g \in G\}$$

we conclude that W is a G-stable subspace and it lies in the span of f_i's which is finite dimensional. □

Theorem 1.3.2. *Let G be a linear algebraic group. Then G is isomorphic to a closed subgroup of some $GL_n(k)$.*

Proof. Take generators $\hat{f}_1, \hat{f}_2, ..., \hat{f}_m$ for the coordinate algebra $k[G]$. They generate a finite dimensional k-vector subspace of $k[G]$, call V. By lemma 1.3.1, there is a finite dimensional G-stable subspace W of $k[G]$ containing V. Let $f_1, f_2, ..., f_n$ be a k-basis for W, notice that they also generate $k[G]$ as a k-algebra. We are going to find an embedding $G \to GL_n(k)$. For that purpose we will construct a surjection $k[GL_n(k)] = k[x_{ij}]_{det} \to k[G]$.

Consider the action

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto hg^{-1} \end{aligned}$$

and the action it corresponds to

$$\begin{aligned} G \times k[G] &\to k[G] \\ (g, f) &\mapsto \rho_g(f) : x \mapsto f(xg). \end{aligned}$$

Moreover, consider another action of G on itself

$$\begin{aligned} \phi : G \times G &\to G \\ (g, h) &\mapsto hg. \end{aligned}$$

We have also a C-algebra morphism

$$\begin{aligned} \phi^* : k[G] &\to k[G] \otimes k[G] \\ f &\mapsto f \circ \phi \end{aligned}$$

induced by ϕ. As in the proof of lemma 1.3.1, write $\phi^*(f_i) = \sum_j m_{ij} \otimes f_j$ with $m_{ij} \in k[G]$ for each i and therefore we have

$$\begin{aligned}(\rho_g(f_i))(x) &= f_i(xg) \\ &= f_i(\phi(g,x)) \\ &= \phi^*(f_i)(g,x) \\ &= \sum_j (m_{ij} \otimes f_j)(g,x) \\ &= \sum_j m_{ij}(g) f_j(x).\end{aligned}$$

Hence $\rho_g(f_i) = \sum_j m_{ij}(g) f_j$. Define the map

$$\begin{aligned}\varrho : k[x_{ij}]_{det} &\to k[G] \\ x_{ij} &\mapsto m_{ij}.\end{aligned}$$

Since

$$\begin{aligned}f_i(g) &= f_i(g1) \\ &= \sum_j m_{ij}(g) f_j(1)\end{aligned}$$

we have $f_i = \sum_j f_j(1) m_{ij}$. Therefore m_{ij} also generate $k[G]$ and we conclude that ϱ is surjective. Hence it correspond to a closed embedding of varieties,

$$G = \mathrm{Spec}(k[G]) \to \mathrm{Spec}(k[x_{ij}]_{det}) = GL_n(k).$$

□

1.4 Connected Solvable Linear Algebraic Groups

In this section, we will demonstrate that a connected solvable linear algebraic group G is isomorphic to $G_u \rtimes T$, where T is a maximal torus and G_u is the unipotent part of G. For this, we need to introduce what the uipotent part means. This definition comes from the Jordan decomposition.

1.4.1 Jordan Decomposition in Algebraic Groups

Let V be a finite dimensional vector space over k. Recall the additive Jordan decomposition.

Proposition 1.4.1. *Let $x \in End(V)$ be an endomorphism. Then there exist unique $s, n \in End(V)$ such that s is semisimple, i.e. diognalizible, n is nilpotent, $x = s + n$ and $sn = ns$.*

Using it, we can derive a multiplicative version of this.

Proposition 1.4.2. *Let $g \in GL(V)$. Then there exist unique $s, u \in GL(V)$ such that $g = su = us$, where s is semisimple and u is unipotent.*

Proof. Take unique s, v, with $g = s + n$ and $sn = ns$ as in proposition 1.4.1. Notice that $gn = sn + n^2 = ns + n^2 = ng$. Since g is invertible, $s = g - n$ is invertible since

$$(g - n)(g^{-1} + g^{-2}n + g^{-3}n^2 + ... + g^{-k}n^{k-1}) = 1$$

taking $n^k = 0$ such that k is minimal. Let $u := 1 + s^{-1}n$. Then $u - 1 = s^{-1}n$ is nilpotent and u is unipotent. Finally, $su = s + n = g$ and $us = s + s^{-1}ns = s + n = g$.

If $g = su = us$ is any such decomposition, then $u = 1 + n$ with n is nilpotent and $g = s + sn$, $g = s + ns$. Therefore $ns = sn$ and sn is nilpotent. Applying the uniqueness in proposition 1.4.1 to $g = s + sn$, we conclude that s and sn are unique. Hence u is also unique. □

Since given any linear algebraic group G can be embedded in some $GL(V)$, we can transfer this decomposition to an arbitrary linear algebraic groups.

Theorem 1.4.3. *[4, Theorem 15.3.] Let G be a linear algebraic group.*

(i) For any embedding $\rho : G \to GL(V)$ and for any $g \in G$, there exist unique $g_s, g_u \in G$ such that $g = g_s g_u = g_u g_s$, where $\rho(g_s)$ is semisimple and $\rho(g_u)$ is unipotent.

(ii) The decomposition $g = g_s g_u = g_u g_s$ is independent of the chosen embedding.

(iii) *Let $\varphi : G \to H$ be a morphism of linear algebraic groups. Then $\varphi(g_s) = \varphi(g)_s$ and $\varphi(g_u) = \varphi(g)_u$*

Now we can define G_u, G_s and unipotent groups.

Definition 1.4.4. Let G be a linear algebraic group. The decomposition $g = g_s g_u = g_u g_s$ is called *the Jordan decomposition* of $g \in G$, and g is called *semisimple*, respectively *unipotent*, if $g = g_s$, respectively $g = g_u$. We denote the subset consisting of all unipotent elements of G by G_u and the subset consisting of all semisimple elements of G by G_s. If $G = G_u$ then we call G a *unipotent group.*

1.4.2 Unipotent Groups

The next proposition indicates a classification for unipotent groups. This will be useful later.

Proposition 1.4.5. *[4, Corollary 17.5.] Let G be a unipotent subgroup of $GL_n(k)$. Then there exsists $g \in GL_n(k)$ such that $g^{-1}Gg \leqslant U_n(k)$.*

$U_n(k)$ has a chain of closed connected subgroups, each normal in $U_n(k)$ and of codimension 1 in the preceding one (see [4, Exercise 17.7.]). Using proposition 1.4.5, we can find such a chain for any unipotent group U. Therefore, to examine the unipotent groups we have to look at the connected groups of dimension 1. The following theorem gives the complete list.

Theorem 1.4.6. *[4, Theorem 20.5.] Let G be a connected linear algebraic group of dimension 1 over an algebraically closed field. G is isomorphic to either $\mathbb{G}_a$ or $\mathbb{G}_m$.*

Continuing the discussion above, by theorem 1.4.6, each quotient is isomorphic to $\mathbb{G}_a$. Hence we derive the following result.

Proposition 1.4.7. *Let U be a unipotent linear algebraic group. U has a chain of closed connected subgroups,*

$$1 = U_0 \leqslant U_1 \leqslant U_2 \leqslant ... \leqslant U_{n-1} \leqslant U_n = U$$

each normal in U, and therefore normal in each other, and have quotients

$$U_i/U_{i-1} \simeq \mathbb{G}_a.$$

1.4.3 Commutative Linear Algebraic Groups

Next theorem states that if G is an Abelian linear algebraic group then $G \simeq G_s \times G_u$. This gives a classification for Abelian linear algebraic groups.

Theorem 1.4.8. *[4, Theorem 15.5.] Let G be a commutative linear algebraic group.*

(i) G_s and G_u are closed subgroups of G.

(ii) The product map

$$\pi : G_s \times G_u \to G$$
$$(s, u) \mapsto su$$

is an isomorphism of linear algebraic groups.

(iii) If G is connected then so are G_s and G_u.

We finish this section with stating a property for tori that will be useful later.

Proposition 1.4.9. *[4, Theorem 16.2.] Any closed connected subgroup of $D_n(k)$ is a torus.*

1.4.4 Lie-Kolchin Theorem

Let V be a vector space over an algebraically closed field K and let G be a solvable connected closed subgroup of $GL(V)$. Lie-Kolchin theorem states that one can choose a basis for V in which the elements of G are represented by upper triangular matrices. In other words, if $\rho : G \to GL(V)$ is a representation then $\rho(G)$ is conjugate to a subgroup of $T_n(k)$. Aim of this subsection is to prove this theorem.

Definition 1.4.10. A variety X is called *complete* if for any variety Y, the projection map $\pi : X \times Y \to Y$ is closed.

There are immediate properties of complete varieties.

Proposition 1.4.11. *(i) A closed subvariety of a complete variety is complete.*

(ii) If $X \to Y$ is a morphism of varieties, with X complete, then the image is closed in Y, and complete.

(iii) A complete affine variety has dimension 0.

(iv) Projective varieties are complete.

(v) The flag variety $\mathfrak{F}(V)$ of a finite dimensional vector space V is projective, hence complete.

See [4, Chapter 6, Section 1.6, Section 1.8] for the proofs of the above statements.

Lemma 1.4.12. *[4, Lemma 21.1.] Let G be a linear algebraic group, and let X and Y be non-empty G-varieties with transitive actions and let $\varphi : X \to Y$ be a bijective morphism of G-varieties. If Y is complete then X is complete.*

Proposition 1.4.13. *[4, Proposition 3.2.] If Y is a proper closed subset of an irreducible variety X, then* $\dim(Y) < \dim(X)$.

The next theorem, it is sometimes called the fixed point theorem, will imply the Lie-Kolchin Theorem.

Theorem 1.4.14. *Let G be a connected solvable algebraic group, and let X be a non-empty complete G-variety. Then G has a fixed point in X.*

Proof. Obviously $G' := [G, G]$ is solvable and by proposition 1.2.9, G' is connected. Since G is solvable, it cannot be a perfect group, so $G \neq G'$. By proposition 1.4.13, we have $\dim G' < \dim G$. Hence by induction on $\dim G$ (it is trivial when $\dim G = 0$), G' has a fixed point in X i.e. $Y := X^{G'} = \{x \in X : h \cdot x = x, \text{ for any } h \in G'\}$ is non-empty. Let G-action on X be given by

$$\varphi : G \times X \to X$$

$$(g, x) \mapsto g \cdot x$$

and then the map

$$\varphi_h : X \to X$$
$$x \mapsto h \cdot x$$

where $h \in G'$, is also continuous. Therefore $X^h = \{x \in X : h \cdot x = x\} = \varphi^{-1}(x)$ is closed. Then $Y = \bigcap_{h \in G'} X^h$ is also closed. By proposition 1.4.11(i), Y is complete.

Claim 1.4.15. *G keeps Y stable.*

Proof. Let $y \in Y$. We have $hy = y$, for any $h \in G'$. Let $g \in G$ and $h \in G'$ be arbitrary, then $gh' = hg$ for some $h' \in G'$ since $G' \trianglelefteq G$. Hence $gy = gh'y = hgy$, therefore $gy \in Y$. □

Using claim, we may assume that $X = Y$. Then $G' \leqslant G_x = \{g \in G : g \cdot x = x\}$, for any $x \in X$. But G/G' is abelian so each G_x is normal in G. Moreover, $G_x = \varphi^{-1}(x) \cap (G \times \{x\})$ is closed, so G/G_x is a linear algebraic group for any $x \in X$. Chose $x \in X$ with $G \cdot x = \{g \cdot x : g \in G\}$ is closed. (For the proof of existence of closed orbits, see [4, Proposition 8.3.].) Then by proposition 1.4.11(i), $G \cdot x$ is complete. by orbit-stabilizer theorem, we have a bijection

$$G/G_x \to G \cdot x$$

such that $G \cdot x$ is complete. Applying lemma 1.4.12, we deduce that G/G_x is complete and is of dimension 0 by proposition 1.4.11(iii). Using proposition 1.4.13, we conclude that $G = G_x$. Thus $x \in X$ is a fixed point under the action of G. □

Finally, we can give a proof of the Lie-Kolchin Theorem.

Theorem 1.4.16. *Let V be a finite dimensional non-zero vector space and G be a connected solvable subgroup of $GL(V)$. Then G has a common eigenvector on V i.e. there exists a one-dimensiinal subspace of V stabilized by G.*

Proof. Since G acts on V, it also acts on the flag variety $\mathfrak{F}(V)$. But $\mathfrak{F}(V)$ is complete by proposition 1.4.11(v). So by theorem 1.4.14, G fixes a full flag, say $0 \subset V_1 \subset V_2 \subset ... \subset V_{n-1} \subset V$. Hence G keeps V_1 stable and $\dim V_1 = 1$. □

Corollary 1.4.17. *Let G be a connected solvable subgroup of $GL_n(k)$. Then, G is conjugate to a subgroup of $T_n(k)$.*

1.4.5 Connected Solvable Linear Algebraic Groups

Let G be a connected solvable linear algebraic group. Lie-Kolchin theorem allows us to regard G as a subgroup of some $T_n(k)$. Now consider the (split) exact sequence

$$1 \to U_n(k) \to T_n(k) \xrightarrow{\pi} D_n(k) \to 1$$

Being a subgroup of $T_n(k)$, all unipotent elements of G come from $U_n(k)$ and therefore the unipotent subgroup of G is $G_u = U_n(k) \cap G$. Hence we have an exact sequence

$$1 \to G_u \to G \xrightarrow{\pi} \pi(G) \to 1$$

$\pi(G)$ is a closed connected subgroup of $D_n(k)$. By proposition 1.4.9, $\pi(G)$ is a torus. Since any torus is abelian, $[G, G] \leqslant G_u$. One can show that this exact sequence is split and that if T is a maximal torus of G, then the dimension of G is equal to the dimension of $\pi(G)$.

We know from theorem 1.4.8 when G is abelian, $G \simeq G_s \times G_u$. Furthermore, G is nilpotent if and only if $G \simeq T \times G_u$ ([4, Proposition 19.2.]). In that case, G has a uniue maximal torus. For the general (solvable) case, we state the following theorem.

Theorem 1.4.18. *[4, Theorem 19.3.] Let G be a connected solvable algebraic group. Then,*

(i) G_u is a closed connected normal subgroup of G including $[G, G]$, and G_u has a chain of closed connected subgroups, each normal in G and of codimension 1 in the preceding one.

(ii) The maximal tori of G are conjugate and if T is one of those, then $G \simeq G_u \rtimes T$.

Chapter 2

TANNAKIAN CATEGORIES

2.1 Galois Categories

Let G be a finite group. We define the category Perm_G as follows. An object is of the form (F, ρ) where F is a finite G-set and $\rho : G \to Perm(F)$ is a group homomorphism determining the action of G on F. A morphism is a map $m : (F_1, \rho_1) \to (F_2, \rho_2)$ such that $m : F_1 \to F_2$ is a morphism of sets and the diagram

$$\begin{array}{ccc} F_1 & \xrightarrow{m} & F_2 \\ \downarrow{\scriptstyle \rho_1(g)} & & \downarrow{\scriptstyle \rho_2(g)} \\ F_1 & \xrightarrow{m} & F_2 \end{array}$$

commutes, for any $g \in G$. We can extend this definition to the case when G is a profinite group, with only one difference that is $\rho : G \to Perm(F)$ is a homomorphism such that the kernel is an open subgroup of G.

For two finite G-sets X_1 and X_2, consider the disjoint union (catogarical sum (or coproduct) in the category of sets) $X_1 \sqcup X_2$. There is a natural G-action on $X_1 \sqcup X_2$. Indeed letting $\rho_1 : G \to Perm(X_1)$ and $\rho_2 : G \to Perm(X_2)$ to be G-actions on X_1 and X_2, for an arbitrary element $g \in G$, one can see that $\rho_1(g) : X_1 \to X_1$ and $\rho_2(g) : X_2 \to X_2$ are morphisms of sets. If $\phi_1 : X_1 \to X_1 \sqcup X_2$ and $\phi_2 : X_2 \to X_1 \sqcup X_2$ are natural inclusions then $\phi_1 \circ \rho_1(g) : X_1 \to X_1 \sqcup X_2$ and $\phi_2 \circ \rho_2(g) : X_2 \to X_1 \sqcup X_2$ are also morphisms. Hence by definition of catogarical sum there is a unique morphism $\xi : X_1 \sqcup X_2 \to X_1 \sqcup X_2$ with $\phi_1 \circ \rho_1(g) = \xi \circ \phi_1$ and $\phi_2 \circ \rho_2(g) = \xi \circ \phi_2$. This morphism exists for any $g \in G$, hence it induces the G-action on $X_1 \sqcup X_2$.

Let Fsets denote the category of finite sets and consider the functor

$$\omega : \mathrm{Perm}_G \to \mathrm{Fsets}$$
$$(F, \rho) \rightsquigarrow F.$$

An *automorphism* σ of ω is defined as a map from Perm_G, such that for any $X \in \mathrm{Perm}_G$ it gives an element $\sigma(X) \in Perm(\omega(X))$, and for any morphism $m : X_1 = (F_1, \rho_1) \to X_2 = (F_2, \rho_2)$ the diagram

$$\begin{array}{ccc} F_1 & \xrightarrow{\omega(m)} & F_2 \\ \downarrow{\scriptstyle \sigma(X_1)} & & \downarrow{\scriptstyle \sigma(X_2)} \\ F_1 & \xrightarrow{\omega(m)} & F_2 \end{array}$$

commutes. Take two automorphism σ_1, σ_2 and an element $X \in \mathrm{Perm}_G$, then $\sigma_2(X) \circ \sigma_1(X)$ is another permutation of $\omega(X)$. Hence automorphisms of ω forms a group. We call an automorphism σ *respects* $\sqcup$ if for any $X_1, X_2 \in \mathrm{Perm}_G$, the restriction of $\sigma(X_1 \sqcup X_2)$ to $\omega(X_i)$ is the same as $\sigma(X_i)$ for $i = 1, 2$. We denote the set of such automorphisms with $Aut^{\sqcup}(\omega)$. It is actually a subgroup of the group of automorphisms of ω.

Lemma 2.1.1. *[8, Lemma B.5.] The natural map $G \to Aut^{\sqcup}(\omega)$ is an isomorphism of profinite groups.*

Next, we ask the question, which categories are equivalent to Perm_G for some profinite group G. The answer leads us to Galois categories.

Definition 2.1.2. Let $\mathcal{C}$ be a category. $\mathcal{C}$ is called a *Galois category* if the following conditions are satisfied.

1. There is a final object 1 and all fibre products $X_1 \times_{X_3} X_2$ exist.

2. Finite sums and quotient of any object by a finite group of autmorphism exists.

3. Every morphism $f : X \to Y$ can be written as a composition $X \xrightarrow{f_1} Y' \xrightarrow{f_2} Y$ where f_1 is a strict epimorphism and f_2 is a monomorphism that is an isomorphism onto a direct summond.

4. There exists a covariant functor $\omega : \mathcal{C} \to \text{Fsets}$ (called the *fibre functor*) that commutes with fibre products and transforms right units into right units.

5. ω commutes with finite direct sums, transforms strict epimorphisms to strict epimorphisms and commutes with forming the quotient by a finite group of automorphism.

6. Let m be a morphism in $\mathcal{C}$. If $\omega(m)$ is bijective, m is an isomorphism.

One can see that Perm_G is a Galois category with the forgetful functor ω.

Given a Galois category with the fibre functor ω, we can define an automorphism of ω and the group $Aut^{\sqcup}(\omega)$ in the same way above. Next proposition states that any Galois category, with the fibre functor ω, is equivalent to the category of permutations of $Aut^{\sqcup}(\omega)$.

Proposition 2.1.3. *[8, Proposition B.6.] Let $\mathcal{C}$ be a Galois category and let $G = Aut^{\sqcup}(\omega)$. Then $\mathcal{C}$ is equivalent to the category* Perm_G.

Example 2.1.4. Let k be a field of characteristic zero and $\overline{k}$ be a algebraic closure of k. Define the category $\mathcal{C}$ as follows. The objects are fields L containing k such that $L \supseteq k$ is a finite extension. A morphism $L_1 \to L_2$ is a k-algebra homomorphism $L_2 \to L_1$. In this category, the categorical sum $L_1 \sqcup L_2$ is the direct product $L_1 \times L_2$. Consider the functor

$$\begin{aligned} \omega : \mathcal{C} &\to \text{Fsets} \\ L &\rightsquigarrow \text{Spec}(\overline{k} \otimes_k L). \end{aligned}$$

Then $\mathcal{C}$ is a Galois category with the fibre functor ω. The profinite group $G = Aut^{\sqcup}(\omega)$ is isomorphic to the absolute Galois group $G(\overline{k}/k)$.

2.2 Affine Group Schemes

For the rest of the section we let k be an algebraically closed field of characteristic 0.

Let $X = \mathrm{Spec}(A)$ and $Y = \mathrm{Spec}(B)$ be affine schemes. We define the product of affine schemes as $X \times_k Y = \mathrm{Spec}(A \otimes_k B)$.

Definition 2.2.1. A *affine group scheme* over k is a group object G in the category of affine schemes over k, i.e. G is an affine scheme $\mathrm{Spec}(A)$ together with morphisms of affine schemes $m : G \times_k G \to G$, $i : G \to G$ and $e : \mathrm{Spec}(k) \to G$, such that the following diagrams commute

$$\begin{array}{ccc} G \times_k G \times_k G & \xrightarrow{m\times\mathrm{id}} & G \times_k G \\ \downarrow{\scriptstyle \mathrm{id}\times m} & & \downarrow{\scriptstyle m} \\ G \times_k G & \xrightarrow{m} & G \end{array}$$

$$\begin{array}{ccc} G & \xrightarrow{(p,\mathrm{id})} & G \times_k G \\ \downarrow{\scriptstyle (\mathrm{id},p)} & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle m} \\ G \times_k G & \xrightarrow{m} & G \end{array}$$

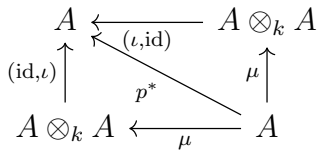
$$\begin{array}{ccc} G & \xrightarrow{(i,\mathrm{id})} & G \times_k G \\ \downarrow{\scriptstyle (\mathrm{id},i)} & \searrow^{p} & \downarrow{\scriptstyle m} \\ G \times_k G & \xrightarrow{m} & G \end{array}$$

where $p : G \xrightarrow{\kappa} \mathrm{Spec}(k) \xrightarrow{e} G$ and κ is induced by the natural inclusion $k \to A$, i.e. G is a group with multiplication m, inverse i and the identity element as the single point in the image of e.

The maps m, i and e above correspond to k-algebra morphisms $\mu : A \to A \otimes_k A$ (the comultiplication), $\iota : A \to A$ (the antipode or coinverse) and $\epsilon : A \to k$ (the counit). A *commutative Hopf algebra* over k is a k-algebra A equipped with k-algebra homomorphisms μ, ι, ϵ and the following diagrams commute

$$\begin{array}{ccc} A \otimes_k A \otimes_k A & \xleftarrow[\mu\times\mathrm{id}]{} & A \otimes_k A \\ \uparrow{\scriptstyle \mathrm{id}\times\mu} & & \uparrow{\scriptstyle \mu} \\ A \otimes_k A & \xleftarrow[\mu]{} & A \end{array}$$

$$\begin{array}{ccc} A & \xleftarrow{} & A \otimes_k A \\ \uparrow{\scriptstyle (\mathrm{id},p^*)} & \nwarrow^{(p^*,\mathrm{id})} & \uparrow{\scriptstyle \mu} \\ A \otimes_k A & \xleftarrow[\mu]{} & A \end{array}$$



where $p^* : A \xrightarrow{\epsilon} k \xrightarrow{\text{incl}} A$ and incl is the natural inclusion $k \to A$.

There is an equivalent definition of affine group schemes as follows. Let $\mathcal{F} : \text{Grp} \to \text{Set}$ be the fortegful functor. An *affine group scheme* over k is a functor $G : k\text{-Alg} \to \text{Grp}$ such that $\mathcal{F} \circ G$ is representable.

Example 2.2.2. Let us see some familiar examples.

(i) The functor $\mathbb{G}_a$: CRing $\to$ Grp maps a commutative ring to its underlying additive group. The functor $\mathcal{F} \circ \mathbb{G}_a$ is represented by $k[x]$.

(ii) Similarly $\mathbb{G}_m$: CRing $\to$ Grp maps a commutative ring to its group of units. It is represented by $k[x, x^{-1}]$.

(iii) For some k-vector space V, the functor GL_V : k-Alg $\to$ Grp maps R to $Aut_R(V \otimes_k R)$.

As in the groups, it is natural to define a representation as a morphism $G \to GL_n$. Here, considering schemes as functors, we will define a *representation of affine scheme* G as a natural transformation of functors $\varrho : G \to GL_V$. Consider $\text{id} \in G(A)$, which is the identity map $A \to A$, $a \mapsto a$. Then $\varrho(\text{id}) \in GL_V(A) = Aut_A(V \otimes A)$, and therefore $\varrho(\text{id}) : V \otimes A \to V \otimes A$ is an A-linear map. This map is determined by its restriction to $V \otimes k$, call ρ. To define a representation this way we need some additional properties. We state the following theorem.

Theorem 2.2.3. *[10, Theorem 3.2] Let $G = \text{Spec}(A)$ be an affine group scheme. Linear representations of G on a k-vector space V correspond to k-linear maps $\rho : V \to V \otimes A$ such that the diagrams*

$$\begin{array}{ccc} V & \xrightarrow{\rho} & V \otimes A \\ \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \text{id} \otimes \mu} \\ V \otimes A & \xrightarrow{\rho \otimes \text{id}} & V \otimes A \otimes A \end{array} \qquad \begin{array}{ccc} V & \xrightarrow{\rho} & V \otimes A \\ \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle \text{id} \otimes \epsilon} \\ V & \xrightarrow{\sim} & V \otimes k \end{array}$$

commute.

2.3 Tannakian Categories

For an affine group scheme G over k, the category of all finite dimensional representations of G is denoted by Repr_G. The objects are of the form (V, ρ) where V is a finite dimensional k-vector space and ρ is a k-linear map as in theorem 2.2.3. A morphism $f : (V_1, \rho_1) \to (V_2, \rho_2)$ is a k-linear map satisfying $\rho_2 \circ f = f \circ \rho_1$. Let

$$\omega : \mathrm{Repr}_G \to \mathrm{Vect}_k$$
$$(V, \rho) \rightsquigarrow V$$

be the forgetful functor, where Vect_k is the category of finite dimensional k-vector spaces.

Fix an affine group scheme $G : k\text{-Alg} \to \mathrm{Grp}$. We define $G' := Aut^{\otimes}(\omega)$ to be a functor from k-Alg to Grp as follows. Given a k-algebra R, the group $G'(R)$ consists of the families $\{\sigma(X)\}$, $X \in \mathrm{ob}(\mathrm{Repr}_G)$, where each $\sigma(X)$ is an R-linear automorphism of $R \otimes_k \omega(X)$ such that

(i) $\sigma(1)$ is the identity on $R \otimes_k \omega(1) = R$,

(ii) for every morphism $f : X \to Y$ in Repr_G, we have

$$(\mathrm{id}_R \otimes_k \omega(f)) \circ \sigma(X) = \sigma(Y) \circ (\mathrm{id}_R \otimes_k \omega(f)),$$

(iii) for every objects X, Y in Repr_G, we have $\sigma(X \otimes Y) = \sigma(X) \otimes \sigma(Y)$.

Then $G'(R)$ is a group and G' is an affine group scheme. In analogy with Galois categories, next theorem states that $G \simeq G'$.

Theorem 2.3.1. *[8, Theorem B.20.] Let G be an affine group scheme over k and let $\omega : \mathrm{Repr}_G \to \mathrm{Vect}_k$ be the forgetful functor. Then there is an isomorphism of functors*

$$G \to \mathrm{Aut}^{\otimes}(\omega).$$

Now, we ask when is a category $\mathcal{C}$ with a "fibre functor" $\omega : \mathcal{C} \to \mathrm{Vect}_k$ is equivalent to Repr_G for some affine group scheme G. This question leads us to the neutral Tannakian categories whose definition requires the tensor categories.

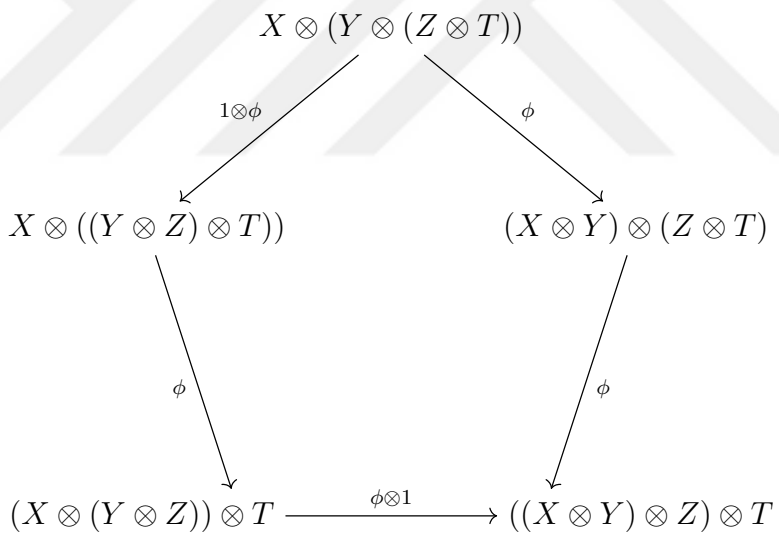
A *tensor category* is a category $\mathcal{C}$ together with a functor

$$\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$$
$$(X, Y) \rightsquigarrow X \otimes Y$$

that has compatible associativity and commutativity constrains. Here, an *associativity constrain* for $\otimes$ is a functorial isomorphism

$$\phi_{X,Y,Z} : X \otimes (Y \otimes Z) \to (X \otimes Y) \otimes Z$$

such that for all objects X, Y, Z, T of $\mathcal{C}$, the diagram



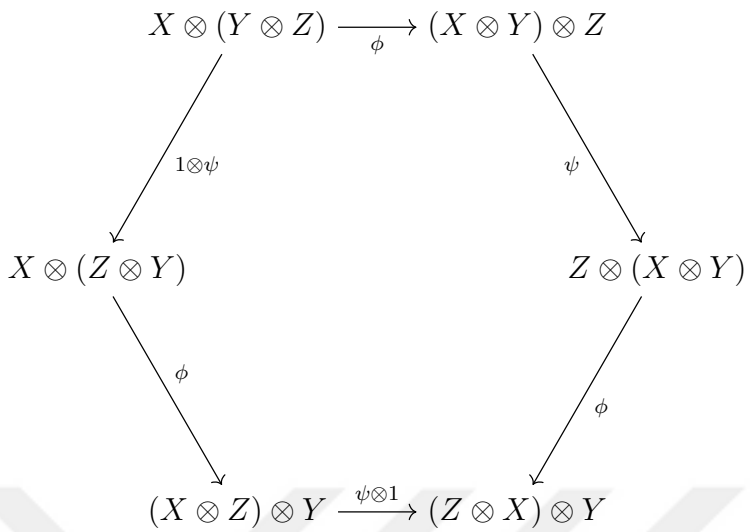
commutes. A *commutativity constrain* for $\otimes$ is a functorial isomorphism

$$\psi_{X,Y} : X \otimes Y \to Y \otimes X$$

such that for all objects X, Y of $\mathcal{C}$,

$$\psi_{Y,X} \circ \psi_{X,Y} : X \otimes Y \to X \otimes Y$$

is the identity morphism on $X \otimes Y$. An associativity constrain ϕ and a commutativity constrain ψ are called *compatible* if, for all objects X, Y, Z of $\mathcal{C}$, the diagram



commutes.

The *internal* Hom of two objects X and Y is a new object $\underline{\mathrm{Hom}}(X, Y)$ such that the functors

$$T \rightsquigarrow \mathrm{Hom}(T \otimes X, Y)$$

and

$$T \rightsquigarrow \mathrm{Hom}(T, \underline{\mathrm{Hom}}(X, Y))$$

are isomorphic. A tensor cateogry is called *rigid* if internal Hom's exist for each pair of objects and there are also canonical isomorphisms

$$X \to \underline{\mathrm{Hom}}(\underline{\mathrm{Hom}}(X, 1), 1)$$

and

$$\underline{\mathrm{Hom}}(X_1, Y_1) \otimes \underline{\mathrm{Hom}}(X_2, Y_2) \to \underline{\mathrm{Hom}}(X_1 \otimes X_2, Y_1 \otimes Y_2)$$

for every object X, X_1, X_2, Y_1, Y_2.

Definition 2.3.2. Let $\mathcal{C}$ be a category. $\mathcal{C}$ is called a *neutral Tannakian category* over k if the following conditions are satisfied.

1. $\mathcal{C}$ is a rigid tensor category.

2. $\mathcal{C}$ is an abelian category.

3. $\mathrm{End}(1) \simeq k$.

4. There is a fibre functor $\omega : \mathcal{C} \mapsto \mathrm{Vect}_k$ which means ω is an exact faithful k-linear functor that commutes with tensor products.

The main theorem of this chapter states that any neutral Tannakian category, with the fibre functor ω, is equivalent to the category of representations of $\mathrm{Aut}^{\otimes}(\omega)$.

Theorem 2.3.3. *[8, Theorem B.22.] Let $\mathcal{C}$ be a neutral Tannakian category over k with fibre functor $\omega : \mathcal{C} \mapsto \mathrm{Vect}_k$. Then, $\mathcal{C}$ is canonically isomorphic to Repr_G where G represents the functor $\mathrm{Aut}^{\otimes}(\omega)$.*

Chapter 3

INTRODUCTION TO PICARD-VESSIOT THEORY

In this chapter, we define some basic objects like differential rings and Picard-Vessiot extensions. All the rings considered are supposed to be commutative, to have 1 and to contain $\mathbb{Q}$.

3.1 Differential Rings

First we define a *derivation* over a ring R by the map $\partial : R \to R$ such that the following diagrams commute

$$\begin{array}{ccc} R \times R & \xrightarrow{+} & R \\ \downarrow{\scriptstyle (\partial,\partial)} & & \downarrow{\scriptstyle \partial} \\ R \times R & \xrightarrow{+} & R \end{array} \qquad\qquad \begin{array}{ccc} R \times R & \xrightarrow{\cdot} & R \\ & \searrow^{\mathcal{L}} & \downarrow{\scriptstyle \partial} \\ & & R \end{array}$$

where

$$\mathcal{L} : R \times R \to R \text{ such that } (a, b) \mapsto \partial(a)b + a\partial(b).$$

Mostly, we will write a' instead of $\partial(a)$. A ring R equipped with a derivation ∂ is called a *differential ring* and $C_R := \partial^{-1}(0)$ is called *the ring of constants* of R (it is easy to see that C_R forms a subring). A *differential field* F is a differential ring which is a field, in this case C_F is also a field an called *the field of constants* of F.

An ideal I of a differential ring R is called a *differential ideal* if $\partial(I) \subseteq I$. One can define a derivation on R/I by $\partial(a + I) = \partial(a) + I$. One can check that this definition does not depend on the choice of representatives.

A ring extension of differential rings $S \supset R$ with derivations ∂_S, ∂_R, respectively, is called a *differential extension* if the restriction of ∂_S to R is the same as ∂_R.

Let A and B be differential rings with derivations ∂_A and ∂_B, respectively. A ring homomorphism $f : A \to B$ is called a *differential morphism* if the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \partial_A} & & \downarrow{\scriptstyle \partial_B} \\ A & \xrightarrow{f} & B \end{array}$$

commutes. A bijective differential morphism is called a *differential isomorphism* and a differential isomorphism $A \to A$ is called a *differential automorphism*. Given a differential morphism $f : A \to B$, it is easy to see that $\ker f$ is a differential ideal of A and the natural map $A/\ker f \to \operatorname{Im} f$ is a differential isomorphism.

A derivation on a differential integral domain extends to the fraction field in a unique way. More generally, a derivation on a differential ring extends to any localization in a unique way. To show that we introduce an equivalent definition of derivation. Let R be a ring. Consider $R[\varepsilon]$ where $\varepsilon^2 = 0$. It is easy to see that $\partial : R \to R$ is a derivation if and only if the map

$$\begin{aligned} A_\partial : R &\to R[\varepsilon] \\ r &\mapsto r + \partial(r)\varepsilon \end{aligned}$$

is a ring homomorphism.

Let R be a differential ring equipped with a derivation ∂, and Q be a multiplicatively closed subset of R containing 1 and not containing 0. We have the homomorphism $A_\partial : R \to R[\varepsilon]$ as above. Consider its composition φ with the natural injection $R[\varepsilon] \to Q^{-1}R[\varepsilon]$. Then for any $q \in Q$, we have $\varphi(q) = q/1 + \partial(q)/1\varepsilon$ which is a unit of $Q^{-1}R[\varepsilon]$ if and only if $q/1$ is a unit of $Q^{-1}R$, since ε is nilpotent. But $1/q$ is the inverse of $q/1$ in $Q^{-1}R$, so $\varphi(Q)$ is included in the set of units of $Q^{-1}R[\varepsilon]$. Hence by the universal property of $Q^{-1}R$, there is a unique map $\psi : Q^{-1}R \to Q^{-1}R[\varepsilon]$ such that the diagram

$$\begin{array}{ccccc} R & \xrightarrow{A_\partial} & R[\varepsilon] & \hookrightarrow & Q^{-1}R[\varepsilon] \\ \downarrow & & & \overset{\psi}{\nearrow} & \\ Q^{-1}R & & & & \end{array}$$

commutes and for $r \in R$, $q \in Q$,

$$\begin{aligned}\psi(\frac{r}{q}) &= \varphi(r)\varphi(q)^{-1} \\ &= (\frac{r}{1} + \frac{\partial(r)}{1}\varepsilon)(\frac{q}{1} + \frac{\partial(q)}{1}\varepsilon)^{-1} \\ &= (\frac{r}{1} + \frac{\partial(r)}{1}\varepsilon)(\frac{1}{q} - \frac{\partial(q)}{q^2}\varepsilon) \\ &= \frac{r}{q} + \frac{\partial(r)q - r\partial(q)}{q^2}\varepsilon.\end{aligned}$$

Hence the derivation on $Q^{-1}R$ is defined by

$$\partial(\frac{r}{q}) = \frac{\partial(r)q - r\partial(q)}{q^2}.$$

Given a differential ring R, a *differential R-algebra* is an R-algebra that is a differential extension of R. Let S and T be differential R-algebras, with derivations ∂_S and ∂_T, respectively. We claim that the map

$$\begin{aligned}S \otimes_R T &\to S \otimes_R T \\ s \otimes t &\mapsto s' \otimes t + s \otimes t'\end{aligned}$$

where $s' = \partial_S(s)$ and $t' = \partial_T(t)$, gives a derivation over $S \otimes_R T$. To verify this, first we will show that the same construction is a well-defined derivation over $S \otimes_C T$. It is easy to check that

$$((s_1 \otimes t_1)(s_2 \otimes t_2))' = (s_1 \otimes t_1)'(s_2 \otimes t_2) + (s_1 \otimes t_1)(s_2 \otimes t_2)'$$

for any $s_1, s_2 \in S$, $t_1, t_2 \in T$. Since ∂_T and ∂_S are C-linear, we have that

$$\partial_S \otimes_C \mathrm{id}_T + \mathrm{id}_S \otimes_C \partial_T$$

is linear. Finally, $I = \langle r \otimes 1 - 1 \otimes r : r \in R \rangle$ is a differential ideal and the derivation can be transferred to the quotient $(S \otimes_C T)/I \simeq S \otimes_R T$.

Let R be a differential ring. The *ring of differential polynomials* over R in the variable y is defined as the polynomial ring

$$R\{y\} := R[\{y^{(i)} : i = 0, 1, 2, ...\}] = R[y, y', y'', ..., y^{(i)}, ...]$$

in the countable number of indeterminates $y^{(i)}$ with extending to derviation on R by $(y^{(i)})' = y^{(i+1)}$. One can extend the number of variables by $R\{y_1, y_2\} = R\{y_1\}\{y_2\}$ as in the polynomial rings. If R is an integral domain, so is $R\{y\}$. In this case we denote the field of fractions of $R\{y\}$ by $R\langle y\rangle$.

If $R \subseteq S$ is a differential extension of rings and X is a subset of S, then the R-subalgebra of S generated by X is denoted by $R\{X\}$. If R and S are fields, then $R\langle X\rangle$ denotes the differential subfield of S generated by R and X.

3.1.1 Differential Ideals

A *simple differential ring* is a differential ring whose only differential ideals are 0 and itself.

Proposition 3.1.1. *Any simple differential ring is an integral domain.*

Proof. Let a, b be non-zero elements of R such that $ab = 0$. We claim that $a^{(k)}b^{k+1} = 0$ for all $k \geq 0$. For $k = 0$, we already have $ab = 0$. Assume $a^{(n-1)}b^n = 0$ for some natural number n. Then $0 = (a^{(n-1)}b^n)' = a^{(n)}b^n + na^{(n-1)}b^{n-1}$, and multiplying with b we have $0 = a^{(n)}b^{n+1} + na^{(n-1)}b^n = a^{(n)}b^{n+1}$. Hence we showed the claim by induction.

Assume b is not nilpotent and let J be the differential ideal generated by a. Let $j = r_0a + r_1a' + ... + r_na^{(n)}$ be an arbitrary element of J, then by claim, $b^{n+1}j = 0$. Since $b^{n+1} \neq 0$, we established that j is a zero divisor. Therefore $1 \notin J$. Since $a \in J$, J is a proper differential ideal of R, contradiction. Therefore b is nilpotent. Since b was arbitrary, we conclude that every zero divisor of R is nilpotent. Therefore a is nilpotent.

Let $a^m = 0$, and choose m minimal. Taking the derivative, we have $ma^{m-1}a' = 0$. Hence a' is a zero divisor, and by induction $a^{(l)}$ is a zero divisor for all l. Hence J consists of only zero divisors and therefore $1 \notin J$. Thus J is a proper differential ideal, contradiction. □

Corollary 3.1.2. *Let R be a differential ring and let I be a maximal differential ideal of R such that R/I is of characteristic zero. Then I is prime.*

3.2 Picard-Vessiot Extensions

3.2.1 Linear Differential Equations

Let us take a differential field F with the field of constants C.

$$L(y) = \partial^n(y) + a_{n-1}\partial^{(n-1)}(y) + ... + a_1\partial(y) + a_0 y$$

where all $a_i \in F$, is called a *linear differential equation* of degree n over F.

Definition 3.2.1. Let $y_1, ..., y_n$ be elements in a differential field F. The determinant

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

is called the *wronskian* of $y_1, ..., y_n$.

Proposition 3.2.2. *Let $y_1, ..., y_n$ be elements in a differential field F whose field of constants is C. $y_1, ..., y_n$ are linearly independent over C if and only if $w(y_1, ..., y_n) \neq 0$.*

Proof. This is trivial. □

Proposition 3.2.3. *Let $L(y)$ be a linear differential equation of degree n over a differential field F. If $y_1, ..., y_{n+1}$ are solutions of $L(y) = 0$ in a differential extension E of F, then $w(y_1, ..., y_{n+1}) = 0$. In particular, $L(y) = 0$ has at most n solutions in E linearly independent over C_E.*

Proof. The last column of wronskian matrix is $(y_1^{(n)}, ..., y_{n+1}^{(n)})$. Since $L(y)$ is of degree n, this column is a linear combination of the preceding ones. □

3.2.2 Definition of a Picard-Vessiot Extension

Let F be a differential field with algebraically closed field of constants C. Consider the linear differential equation

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1y' + a_0y$$

over F. If $K \supseteq F$ is a differential extension, the solutions of $L(y) = 0$ in K is a vector space of dimension at most n over C_K. We will show that we can always find an extension field E' of F in which $L(y) = 0$ has a full set of solutions. We also want the field of constants of E' to be C. We call the minimal extension, $E \supseteq F$, with these properties, a *Picard-Vessiot extension* of F for L. We will show that E is unique up to differential field isomorphism and call E, the *Picard-Vessiot field* of L over F.

Consider the differential equation $y' + ay = 0$, $a \in F$. We want to define Picard-Vessiot field as an analogus to the splitting field. A good choice for this field would be $E = F\langle t\rangle$ for some t satisfying $t' + at = 0$. Assume z is another solution i.e. $z' + az = 0$ and $K = E\langle z\rangle$. But $(z/t)' = 0$, so K contains a constant not in E. More generally, take a linear differential equation $L(y)$ over F of degree n. Suppose $y_1, ..., y_n$ is a full set of solutions i.e. $L(y_i) = 0$ and $w(y_1, ..., y_n) \neq 0$. Let $E = F\langle y_1, ..., y_n\rangle$, then $V = \{y \in E : L(y) = 0\}$ is a vector space of dimension n over the field of constants of E, say C. Consider another full set of solutions $z_1, ..., z_n$ and field $K = F\langle z_1, ..., z_n\rangle$ whose field of constants is C_K. Again $V_K = \{y \in K : L(y) = 0\}$ is a vector space of dimension n over C_K. Assume $E = F\langle V\rangle$ properly contains $K = F\langle V_K\rangle$. In this case V_K is a proper subset of V and C contains C_K. If $C = C_K$, then both of V and V_K's are of dimension n over the same field, which is a contradiction. Hence K contains a constant not in E. To sum up, allowing no new constants guarantees the minimality of the extension containing full set of solutions.

Proposition 3.2.4. *Let $L(y)$ be a linear differential equation over the differential field F, and let $E \supseteq F$ and $K \supseteq F$ be differential extensions in which E and K have full set of solutions. If $K \supset E \supseteq F$ with $E \neq K$, then K contains a constant not in E.*

This will motivate our definition of Picard-Vessiot field.

Definition 3.2.5. Let $L(y)$ be a linear differential equation of order n over the differential field F. A differential field E is called a *Picard-Vessiot field* of L over F (or $E \supseteq F$ is called a *Picard-Vessiot extension* for L) if:

(i) $E = F\langle y_1, ..., y_n \rangle$, where $y_1, ..., y_n$ is a full set of solutions of $L(y) = 0$.

(ii) Every constant of E lies in F.

There is an immediate consequence of proposition 3.2.4 and part (ii) of definition 3.2.5.

Lemma 3.2.6. *Let $E \supseteq F$ be a Picard-Vessiot extension for $L(y)$. If $E \supseteq K \supseteq F$ is a subextension such that K contains a full set of solutions of $L(y) = 0$, then $E = K$.*

3.2.3 Existence and Uniquness

Next we want to show the existence and uniquness of the Picard-Vessiot extension, given a linear differential equation. To show the existence we will construct the Picard-vessiot field for a linear differential equation

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1y' + a_0y$$

over a differential field F. Consider the differential ring $F\{x_1, ..., x_n\}$ in n differential indeterminates and take the quotient by the differential ideal generated by the elements

$$x_j^{(n)} + a_{n-1}x_j^{(n-1)} + ... + a_1x_j' + a_0x_j \ , \quad 1 \leq j \leq n$$

which is the ideal generated by these elements and their derivatives. We will write a differential isomorphism from this quotient to the ring $F[y_{ij}, 0 \leq i \leq n-1, 1 \leq j \leq n]$ as

$$x_j^{(i)} \mapsto y_{ij}.$$

For this to be a differential isomorphism we define the derivation of $F[y_{ij}]$ from extending the derivation of F as follows

$$y'_{ij} = y_{i+1,j}, \quad 0 \leq i \leq n-2$$
$$y'_{n-1,j} = -a_{n-1}y_{n-1,j} - ... - a_1 y_{1j} - a_0 y_{0j}.$$

Let $R := F[y_{ij}][w^{-1}]$ where $w = det(y_{ij})$. As we have shown before, the derivation of $F[y_{ij}]$ uniquely extends to R since R is the localization of $F[y_{ij}]$ at w. R is called the *full universal solution algebra* for L.

Let P be a maximal differential ideal of R. By corollary 3.1.2, R/P is an integral domain. Denote E for the field of fractions of R/P. We will show that E is a Picard-Vessiot extension of F for $L(y)$.

First we will show that E has the same field of constants as F. For later use, we state a more general proposition.

Proposition 3.2.7. *Let F be a differential field with algebraically closed field of constants. Let $F \subseteq R$ be an extension of differential rings, such that R is a simple differential ring, generated as an F-algebra. Let E be the field of fractions of R. Then E has the same field of constants as F.*

Proof. It is trivial that $C_E \supseteq C_F$. We will show the other inclusion. Let $a \in C_E \backslash C_F$. Assume a is algebraic over F. Then

$$a^m + c_{m-1}a^{m-1} + ... + c_1 a + c_0 = 0$$

for some $c_i \in F$ and $m \in \mathbb{N}$. We can assume that m is minimal. Taking the derivative, we have

$$c'_{m-1}a^{m-1} + ... + c'_1 a + c'_0 = 0.$$

Since $c'_i \in F$, this contradicts with minimality of m, so all $c'_i = 0$. Therefore $c_i \in C_F$, for each i, and a is algebraic over C_F. But C_F was algebraically closed so, $a \in C_F$, contradiction. Therefore, a is not algebraic over F.
Since $a \in C_E \subseteq E$, we have $a = f/g$ for some $f, g \in R$. Consider the ideal

$$J = \{h \in R : ha \in R\}.$$

Since $g \in R$, it contains nonzero elements. If $h \in J$, then $ha \in R$ and $h'a \in R$ since R is a differential ring. This implies that $h' \in J$, then J is a differential ideal. Since R is a simple differential ring, $J = R$, hence $1 \in J$ and $a \in R$.

Claim 3.2.8. *There exists an element $c \in C_F$ such that $a - c$ is not invertible in R.*

Proof. See [5, Lemma 1.16]. □

Consider element c in claim 3.2.8. Let I be the ideal generated by $a - c$ in R. By claim 3.2.8, we have $I \neq R$. Since $a - c$ is constant in R, I is a differential ideal. Hence $I = (0)$ and $a = c \in C_F$. □

Back to construction above, by proposition 3.2.7, E has the same field of constants as F.

We claim that E is a Picard-Vessiot extension of F for $L(y)$. Recall that $y_{01}, y_{02}, ..., y_{0n}$ in the construction of E is a set of solutions of L. Notice that $w = det(y_{ij}) = w(y_{01}, y_{02}, ..., y_{0n})$. Since w is an invertible element, it is non-zero. Therefore E is differentially generated by a fundamental set of solutions of $L(y) = 0$. Hence using proposition 3.2.7, we are done.

We collect our results in the following theorem.

Theorem 3.2.9. *Let $L(y)$ be a linear differential equation over a differential field F. Let R be the full universal solution algebra for L and P be a maximal differential ideal of R. Then R/P is an integral domain whose field of fractions is a Picard-Vessiot extension of F for $L(y)$.*

Now we prove the uniqueness of the Picard-Vessiot extension, up to differential isomorphisms.

Lemma 3.2.10. *Let $E_1 \supseteq F$ and $E_2 \supseteq F$ be Picard-Vessiot extensions for $L(y)$. Let $E \supseteq F$ be a differential field extension with $C_E = C_F =: C$. Let $\sigma_i : E_i \to E$ be differential F-morphisms, $i = 1, 2$. Then $\sigma_1(E_1) = \sigma_2(E_2)$.*

Proof. Let $V_1 = \{y \in E_1 : L(y) = 0\}$, $V_2 = \{y \in E_2 : L(y) = 0\}$ and $V = \{y \in E : L(y) = 0\}$. Since E_1 and E_2 are Picard-Vessiot fields for $L(y)$, we have $dim_C V_1 = dim_C V_2 = n$. Also, we know that $dim_C V \leq n$. Since σ_1 and σ_2 are differential morphisms, we have $\sigma_1(V_1), \sigma_2(V_2) \subseteq V$. Using dimensions, we have $\sigma_1(V_1) = V = \sigma_2(V_2)$. But $E_1 = F\langle V_1 \rangle$ and $E_2 = F\langle V_2 \rangle$, so $\sigma_1(E_1) = \sigma_1(F\langle V_1 \rangle) = \sigma_2(F\langle V_2 \rangle) = \sigma_2(E_2)$. □

Theorem 3.2.11. *Let $E_1 \supseteq F$ and $E_2 \supseteq F$ be Picard-Vessiot extensions for $L(y)$. Assume that F has algebraically closed field of constans C. Then there is an F-differential isomorphism $E_1 \to E_2$.*

Proof. Take E_1 to be the field of fractions of R/P where R is the full universal solution algebra for $L(y)$, and P is a maximal differential ideal of R.

Let $A := R/P \otimes_F E_2$. We can define a derivation on A, extending the derivation on E_2, as $(x \otimes y)' = x' \otimes y + x \otimes y'$. Let Q be a maximal differential ideal of A. Consider the injection

$$\begin{aligned} \varphi : R/P &\to A \\ a &\mapsto a \otimes 1 \end{aligned}$$

then $\varphi^{-1}(Q) = \{a \in R/P : a \otimes 1 \in Q\}$ is a differential ideal of R/P since $a' \otimes 1 = (a \otimes 1)' \in Q$, for any $a \in \varphi^{-1}(Q)$. But R/P is a simple differential ring, so either $\varphi^{-1}(Q) = 0$ or $\varphi^{-1}(Q) = P/Q$. If $\varphi^{-1}(Q) = P/Q$, for any $a \in R/P$ we have $a \otimes 1 \in Q$, therefore $a \otimes b \in Q$, for any $a \in R/P$, $b \in E_2$, so $A = Q$, contradiction. Hence, $\varphi^{-1}(Q) = 0$ and we can extend φ to another injection

$$\begin{aligned} \overline{\varphi} : R/P &\to A/Q \\ a &\mapsto \overline{a \otimes 1}. \end{aligned}$$

Let E be the field of fractions of A/Q, then $\overline{\varphi}$ expends to the injection $\sigma_1 : E_1 \to E$. Similarly E_2 injects into A/Q by $b \mapsto \overline{1 \otimes b}$. This leads to an injecton $\sigma_2 : E_2 \to A/Q \to E$. By proposition 3.2.7, we have $C_E = C$. By lemma 3.2.10, $\sigma_1(E_1) = \sigma_2(E_2)$. Hence $E_1 \simeq \sigma_1(E_1) = \sigma_2(E_2) \simeq E_2$. □

3.3 Differential Modules

Let k be a differential field with field of constants C.

3.3.1 Matrix Differential Equations

There are other ways to express linear differential equations. One of them is using matrices. The derivation on k extends to vectors in k^n and matrices in $M_n(k)$ componentwise. Denote $y = (y_1, ..., y_n)^T \in k^n$ and $A = (a_{i,j}) \in M_n(k)$. Derivation extends as $y' = (y_1', ..., y_n')^T$ and $A' = (a_{i,j}')$. One can show that $(AB)' = A'B + AB'$, $(A^{-1})' = -A^{-1}A'A^{-1}$ and $(Ay)' = A'y + Ay'$ where $A, B \in M_n(k)$, $y \in k^n$.

Definition 3.3.1. A *matrix differential equation* over k of dimenion n is $y' = Ay$ where $A \in M_n(k)$, $y \in k^n$.

A linear differential equation over k, namely $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1y' + a_0y = 0$ can be seen as a matrix differential equation $Y' = A_LY$ where

$$A_L = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{bmatrix}, \qquad Y = \begin{bmatrix} y \\ y' \\ y'' \\ \vdots \\ y^{(n-1)} \end{bmatrix}.$$

Therefore, linear differential equations can be seen as a special case of matrix linear equations.

As an analog of linear differential equations, *the solution space* V of $y' = Ay$ over k is defined as $\{v \in k^n : v' = Av\}$. Suppose V has dimension n over C and has a C-basis $\{v_1, ..., v_n\}$. Let $F \in GL_n(k)$ be the matrix with columns $v_1, ..., v_n$. Then we have $F' = AF$. Let $R \supseteq k$ be a differential extension. We want to express the soluions of $y' = Ay$ in R, namely $\{v \in R^n : v' = Av\}$. This motivates the following definition.

Definition 3.3.2. Let $R \supseteq k$ be a differential extension of rings such that $C_R = C_k$. Let $A \in M_n(k)$. A matrix $F \in GL_n(R)$ is called a *fundamental matrix* for the equation

$y' = Ay$ if $F' = AF$.

Let $F, \tilde{F}$ be both fundamental matrices for $y' = Ay$. Let $M = F^{-1}\tilde{F}$. Then,

$$A\tilde{F} = \tilde{F}' = (FM)' = F'M + FM' = AFM + FM' = A\tilde{F} + FM'$$

and therefore $FM' = 0$. Since F is invertible, we have $M' = 0$. Hence $M \in GL_n(C)$. In short, the set of all fundamental matrices is $F \cdot GL_n(C)$.

In the case of linear differential equations $Y' = A_L Y$, a fundamental matrix is

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

where $y_1, ..., y_n \in R$ is a fundamental set of solutions of $L(y) = 0$.

We can define the Picard-Vessiot extensions for matrix differential equations which coincides with the one in linear differential equations.

Definition 3.3.3. A Picard-Vessiot ring for the matrix differential equation $y' = Ay$ over k is a differential ring R satisfying

(i) R is a simple differential ring.

(ii) There exists a fundamental matrix $F \in GL_n(R)$ for $y' = Ay$.

(iii) R is generated as a ring by k, the entries of a fundamental matrix F and the inverse of the determinant F.

By proposition 3.1.1, Picard-Vessiot ring defined above is an integral domain.

Definition 3.3.4. A *Picard-Vessiot field* for $y' = Ay$ over k is the field of fractions of a Picard-Vessiot ring for this equation.

Notice from the F_L above, a Picard-Vessiot ring for a linear differential equation $Y' = A_L Y$ is R/P where R is the full universal solution algebra for L and P is a

maximal differential ideal. By theorem 3.2.9, its field of fractions is a Picard-Vessiot field. Hence the definition above coincides with the definition in linear differential equations.

As in the linear differential equations, a Picard Vessiot ring of a matrix differential equation exists and unique up to differential isomorphism. (See [8, Proposition 1.20].) Same applies to the Picard Vessiot fields. As a final note of the section, we state an equivalent definition for a Picard-Vessiot field for matrix linear equations.

Proposition 3.3.5. *[8, Proposition 1.22] Let $y' = Ay$ be a matrix differential equation over k and $L \supseteq k$ be an extenion of differential fields. L is a Picard-Vessiot field for $y' = Ay$ if and only if the following are satisfied*

(i) $C_L = C_k$.

(ii) There exists a fundamental matrix $F \in GL_n(L)$ for $y' = Ay$.

(iii) L is generated as a field over k by the entries of F.

3.3.2 Differential Modules

Definition 3.3.6. A *differential module* (M, ∂) of dimension n is an n-dimensional k-vector space equipped with the map $\partial : M \to M$ such that $\partial(fm) = f'm + f\partial(m)$ for all $f \in k$ and $m \in M$.

A differential module of dimension one has the form $M = ke$. We have $\partial(e) = -ae$ for some $a \in k$ and $\partial(m) = \partial(fe) = (f' - fa)e$, for an arbitrary $m = fe \in M$. Then $\partial(m) = 0$ is equivalent with $f' = fa$.

Let M be a differential module of dimension n over k with a basis $\{e_1, ..., e_n\}$. There are elements $a_{j,i} \in k$ such that $\partial(e_i) = -\sum_j a_{j,i}e_j$. Then for an arbitrary element $m = \sum_i f_i e_i \in M$, one has $\partial(m) = \sum_i f_i' e_i - \sum_i \sum_j a_{j,i} f_i e_j$. Now $\partial(m) = 0$

means $f_i' = \sum_j a_{i,j} f_j$ for all i i.e.

$$\begin{bmatrix} f_1' \\ f_2' \\ \vdots \\ f_n' \end{bmatrix} = A \cdot \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix}$$

where $A = (a_{i,j}) \in M_n(k)$.

Therefore a choice of a basis for a differential module M produces a matrix differential equation $y' = Ay$ for some $A \in M_n(k)$. Then a different choice would produce another matrix differential equation $f' = \tilde{A}f$. Here $y = Bf$ where $B \in GL_n(k)$ represents the change of basis. Then we have

$$B'f + B\tilde{A}f = B'f + Bf' = (Bf)' = A(Bf)$$

and therefore

$$\tilde{A}f = (B^{-1}AB - B^{-1}B')f.$$

With this motivation, two matrix differential equations given by matrices A and $\tilde{A}$ is called *equivalent* if there exists $B \in GL_n(k)$ such that $\tilde{A} = B^{-1}AB - B^{-1}B'$. Thus two matrix differential equations are equivalent if they are induced from the same differential module. Furthermore, any matrix differential equation $y' = (a_{ij})y$ is induced from the differential module $M = k^n$ by choosing the standard basis $\{e_1, ..., e_n\}$ with derivation $\partial(e_i) = -\sum_j a_{j,i} e_j$.

Proposition 3.3.7. *Let $y' = Ay$ and $f' = \tilde{A}f$ be two equivalent matrix differential equations over k. A differential ring R is a Picard-Vessiot ring for $y' = Ay$ if and only if R is a Picard-Vessiot ring for $f' = \tilde{A}f$.*

Proof. By equivalence of equations, there exists $B \in GL_n(k)$ such that $\tilde{A} = B^{-1}AB - B^{-1}B'$ i.e. $B\tilde{A}B^{-1} + B'B^{-1} = A$. If $F \in GL_n(R)$ is the fundamental matrix for $y' = Ay$, then we have $F' = AF = B\tilde{A}B^{-1}F + B'B^{-1}F$ and therefore $(B^{-1}F)' = B^{-1}F' - B^{-1}B'B^{-1}F = \tilde{A}B^{-1}F$. So $B^{-1}F$ is a fundamental matrix for $f' = \tilde{A}f$. Since $B^{-1} \in GL_n(k)$, the entries and determinant of B are contained in k and the result follows. □

Corollary 3.3.8. *Two matrix differential equations over k have the same Picard-Vessiot ring (and therefore the same Picard-Vessiot field) up to isomorphism if they are induced from the same differential module.*

This proposition means that in sense of Picard-Vessiot theory, differential modules and matrix differential equations are equivalent. It also justifies the next definition.

Definition 3.3.9. A *Picard Vessiot ring* for a differential module M over k is defined as the Picard-Vessiot ring of a matrix differential equation $y' = Ay$ associated to M. The field of fractions of a Picard Vessiot ring for M is called a *Picard-Vessiot field*.

Recall the construction of a matrix differential equation $y' = Ay$ over k from a differential k-module M. The solution space of $y' = Ay$ corresponds to elements $m \in M$ such that $\partial(m) = 0$ that is the set $\ker \partial$. Given a Picard-Vessiot extension $L \supseteq k$, the linearly independent solutions in L produces a fundamental matrix F in $GL_n(L)$. Passing to the differential module M, these solutions in L corresponds to the kernel of the derivation

$$\partial_L : L \otimes_k M \to L \otimes_k M.$$

Let $V := \ker(\partial_L)$. Hence existence of a fundamental matrix is equivalent with $\dim_C V = n$. Let $e_1, ..., e_n$ be a k-basis of M and $\overline{e}_1, ..., \overline{e}_n$ be the corresponding L-basis for $L \otimes_k M$. Then the entries of F and the coefficients of all $v \in V$ w.r.t. $\overline{e}_1, ..., \overline{e}_n$ generates the same field over k. Hence we proved the following.

Proposition 3.3.10. *Let M be a differential module of dimension n over k. Then L is a Picard-Vessiot field for M if and only if the following are satisfied*

(i) $C_L = C$.

(ii) $V := \ker(\partial, L \otimes_k M)$ *has dimension n over C.*

(iii) L *is generated as a field over k by the coefficients of all $v \in V$ w.r.t. any L-basis of $L \otimes_k M$ coming from a k-basis of M.*

Remark 3.3.11. Assume $k \neq C$. Then any differential module M of dimension n over k contains an element e such that M is generated over k by $e, \partial e, \partial^2 e, ...$ (Such an element is called a *cyclic vector*. For the existence, see [8, Proof of Proposition 2.9.].) Since M is of dimension n, the elements $e, \partial e, ..., \partial^{n-1} e$ forms a basis for M and $e, \partial e, ..., \partial^n e$ are linearly dependent over k. Hence there exist unique $b_i \in k$ such that $\partial^n e + b_{n-1}\partial^{n-1} e + ... + b_1 \partial e + b_0 e = 0$. Hence any differential module corresponds to a unique linear differential equation. This means that any matrix differential equation is equivalent to a matrix differential equation $y' = A_L y$ for some linear differential equation L. As a result, all three ways to formulate linear differential equations are equivalent in Picard-Vessiot theory.

Chapter 4

THE DIFFERENTIAL GALOIS GROUP

4.1 The Differential Galois Group

Given $E \supseteq F$, a Picard-Vessiot extension for a linear differential equation $L(y)$, *the differential Galois group* of L over F is defined to be the group of differential F-algebra automorphisms of E and denoted by $G(E/F)$. If V is the solution space of $L(y) = 0$, one can find a natural injective group homomorphism

$$G(E/F) \to GL(V)$$

hence, $G(E/F)$ can be considered as a subgroup of $GL_n(C)$ where n is the degree of $L(y)$ and C is the field of constants of both F and E. Moreover we will show that $G(E/F)$ is a linear algebraic group.

Example 4.1.1. Consider $t := \int e^{-x^2}$ over the differential field $\mathbb{C}(x)$ with derivation $x' = 1$. t is in the solution space of $y'' + 2xy' = 0$. The Picard-Vessiot field for this equation is $\mathbb{C}\langle x, t\rangle = \mathbb{C}(x, t, t')$ and the solution space is $\{a + bt : a, b \in \mathbb{C}\}$. For every $\varphi \in G(\mathbb{C}\langle x, t\rangle / \mathbb{C}(x))$,

$$\varphi : 1 \mapsto 1 \text{ and } \varphi : t \mapsto a + bt$$

for some $a, b \in \mathbb{C}$. Then,

$$\varphi : e^{-x^2} \mapsto be^{-x^2}$$

and

$$\varphi : -2xe^{-x^2} \mapsto -2xbe^{-x^2}$$

which is no problem if b is nonzero. Hence φ sends $\begin{bmatrix} 1 \\ t \end{bmatrix}$ to $\begin{bmatrix} 1 \\ a+bt \end{bmatrix}$ where $a \in \mathbb{C}$ and $b \in \mathbb{C}^{\times}$. Thus,

$$G(\mathbb{C}\langle x,t\rangle/\mathbb{C}(x)) = \{ \begin{bmatrix} 1 & 0 \\ a & b \end{bmatrix} : a, b \in \mathbb{C}, b \neq 0\}.$$

Theorem 4.1.2. *Let $E \supseteq F$ be a Picard-Vessiot extension for a linear differential equation $L(y)$. The differential Galois group $G = G(E/F)$ is a linear algebraic group.*

Intuition. Stating "the differential Galois group $G = G(E/F)$ is a linear algebraic group" is not fully tells what we will prove. What the reader should understand from this statement is that G is isomorphic to a subgroup $\varphi(G)$ of $GL_n(C)$ and $\varphi(G)$ is (Zariski) closed in $GL_n(c)$. The idea of the proof is as follows. Say $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1y' + a_0y$, for $a_i \in F$ and let $V = L^{-1}(0)$. For any $\sigma \in G$, we have

$$\begin{aligned} \sigma(L(y)) &= \sigma(y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1y' + a_0y) \\ &= (\sigma(y))^{(n)} + a_{n-1}(\sigma(y))^{(n-1)} + ... + a_1(\sigma(y))' + a_0\sigma(y)) \\ &= L(\sigma(y)). \end{aligned}$$

Hence $L(z) = 0$ if and only if $0 = \sigma(0) = L(\sigma(z))$. This means that z is a solution if and only if $\sigma(z)$ is a solution. So $V = \sigma(V)$. Since σ is an F-algebra automorphism of E, it is also a linear transformation from C-vector space V to itself. Hence $\sigma \in End(V)$. Clearly $\ker\sigma$ is trivial. So we get $\sigma \in Aut(V) = GL(V)$. This induces a natural injection $\varphi : G \to GL_n(C)$. We will show that image is a closed subgroup.

Here we give the formal proof.

Proof. Say $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1y' + a_0y$. Let

$$A_L := \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{bmatrix}, \qquad \tilde{y} := \begin{bmatrix} y \\ y' \\ y'' \\ \vdots \\ y^{(n-1)} \end{bmatrix}.$$

The linear equation $L(y) = 0$ corresponds to $\tilde{y}' = A_L\tilde{y}$. Letting

$$N := \begin{bmatrix} y_1 & y_2 & \dots & y_n \\ y_1' & y_2' & \dots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \dots & y_n^{(n-1)} \end{bmatrix},$$

where $y_1, ..., y_n \in E$ is a fundamental set of solutions of $L(y) = 0$, we have $N' = A_LN$. Take an arbitrary $\sigma \in G$. Since the entries of A_L are contained in F, we have $\sigma(N)' = A_L\sigma(N)$. We know that $\det N = w(y_1, ..., n_n) \neq 0$. Define $M_\sigma := N^{-1}\sigma(N) \in GL_n(E)$. Now,

$$A_L\sigma(N) = \sigma(N)' = (NM_\sigma)' = N'M_\sigma + NM_\sigma' = A_LNM_\sigma + NM_\sigma' = A_L\sigma(N) + NM_\sigma'$$

and $M_\sigma' = 0$, i.e. $M_\sigma \in GL_n(C)$. Define the map

$$\begin{aligned} \varphi : G &\to GL_n(C) \\ \sigma &\mapsto M_\sigma = N^{-1}\sigma(N). \end{aligned}$$

It is easy to check this is an injective group homomorphism. Indeed,

$$\sigma_1(\sigma_2(N)) = \sigma_1(NM_{\sigma_2}) = \sigma_1(N)\sigma_1(M_{\sigma_2}) = NM_{\sigma_1}\sigma_1(M_{\sigma_2}) = NM_{\sigma_1}M_{\sigma_2}$$

for any $\sigma_1, \sigma_2 \in G$. Injectivity follows from that $N^{-1}\sigma(N) = \mathrm{id}$ implies $\sigma(N) = N$ and this means σ fixes all of y_i and therefore all E. Then $\sigma = \mathrm{id}$ and $\ker\varphi$ is trivial.

From now on, we may treat G as a subgroup of $GL_n(C)$. Let $R = F[y_{ij}, \det^{-1}]$ be the full universal solution algebra for L and P be a maximal differential ideal of

R. By theorem 3.2.9 and theorem 3.2.11, E is isomorphic to the field of fractions of R/P. Due to the construction of this isomorphism, we can take $y_{ij} + P = y_j^{(i)}$ and $R/P \subseteq E$. With this notation G may be seen as

$$G = \{M_\sigma \in GL_n(C) : \sigma(P) = P\}$$

considering each σ as an automorphism of R. We want to show that this is a Zariski closed subset of $GL_n(C)$.

Fix some $\sigma : R \to R$ with $\sigma(P) = P$. Let $q_1, ..., q_r$ be generators of the ideal P and $\{e_1, ..., e_l\}$ be a C-basis for R/P. Then $\sigma(q_j) + P \in R/P$ can be written as $\sum_i c_{ij}e_i$ where each $c_{ij} \in C$. Then $\sigma(P) = P$ if and only if $c_{ij} = 0$ for any i, j. We will show that each c_{ij} can be written as a polynomial in the entries of M_σ and $\frac{1}{\det M_\sigma}$ over C.

Let $\alpha : R \to R/P$ be the quotient map. Let $R/P[x_{ij}]$ be a polynomial ring with $x'_{ij} = 0$. Define $\phi : R \to R/P[x_{ij}]$ by $y_{0j} \mapsto \sum_i x_{ij}y_i$. Therefore $\phi : y_{kj} \mapsto \sum_i x_{ij}y_i^{(k)}$. Define $\beta : R/P[x_{ij}] \to R/P$ by $x_{ij} \mapsto (M_\sigma)_{ij}$. The diagram

$$\begin{array}{ccc} R & \xrightarrow{\alpha} & R/P \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \sigma} \\ R/P[x_{ij}] & \xrightarrow{\beta} & R/P \end{array}$$

commutes, since

$$\sigma(\alpha(y_{0j})) = \sigma(y_j) = \sum_i (M_\sigma)_{ij}y_i = \sum_i \beta(x_{ij})y_i = \beta(\sum_i x_{ij}y_i) = \beta(\phi(y_{0j})).$$

Since $\{e_1, ..., e_l\}$ is a C-basis for R/P, there exists $d_{ij} \in C[x_{ij}]$ such that $\phi(q_j) = \sum_i d_{ij}e_i$. Hence

$$\sum_i c_{ij}e_i = \sigma(q_j) + P = \sigma(q_j + P) = \sigma(\alpha(q_j)) = \beta(\phi(q_j)) = \beta(\sum_i d_{ij}e_i) = \sum_i \beta(d_{ij})e_i$$

and we have $c_{ij} = \beta(d_{ij}) \in \beta(C[x_{ij}]) = C[(M_\sigma)_{ij}]$. (Since there are different c_{ij}'s for each σ, write $c_{ij\sigma}$ instead of c_{ij}.) Thus

$$G = \{M_\sigma \in GL_n(C) : c_{ij\sigma} = 0\}$$

is closed in $GL_n(C)$. □

4.2 Structure of Picard-Vessiot Extensions

Throughout this section we let $E \supseteq F$ be a Picard-Vessiot extension with algebraically closed field of constants C for a linear differential equation $L(y)$, and let $G = G(E/F)$. We also let R be the full universal solution algebra for $L(y)$ and P be a maximal differential ideal of R. We will denote R/P by $T(E/F)$ or just T, when it is obvious.

First we present a lemma that will be useful in this section and the Galois correspondence.

Lemma 4.2.1. *If $x \in E \backslash F$, then there exists $\sigma \in G(E/F)$ such that $\sigma(x) \neq x$.*

Proof. We may assume that E is the field of fractions of T. Write $x = \frac{a}{b}$ with $a, b \in T$. Then $x \in T[\frac{1}{b}] =: A \subseteq E$. Let $k := A \otimes_F A \subseteq E \otimes_F E \simeq E$ and $z := x \otimes 1 - 1 \otimes x \in k$. Since $x \neq 0$, we have $z \neq 0$. Since A has no nilpotents and F is of characteristic 0, we have $k = A \otimes_F A$ has also no nilpotents. Localize k at z and let Q be a maximal differential ideal of $k[\frac{1}{z}]$. Consider the integral domain $k[\frac{1}{z}]/Q$. Since z is a unit in $k[\frac{1}{z}]$, its image $\overline{z}$ in the quotient is non-zero. Consider F-differential morphisms

$$\tau_1 : A \to k[1/z]/Q$$
$$w \mapsto w \otimes 1$$
$$\tau_2 : A \to k[1/z]/Q$$
$$w \mapsto 1 \otimes w.$$

Since A is a simple differential ring, both τ_1 and τ_2 are injective. Therefore they extend to the field of fractions as

$$\tau_{1,2} : E \to S$$

where S is the field of fractions of $k[\frac{1}{z}]/Q$. Applying proposition 3.2.7 to the extension $F \subseteq k[\frac{1}{z}]/Q$, we have $C_S = C_F$. By lemma 3.2.10, we have $\tau_1(E) = \tau_2(E)$. But $\tau_1(x) - \tau_2(x) = x \otimes 1 - 1 \otimes x = \overline{z} \neq 0$, so $\tau := \tau_1^{-1}\tau_2 \in G(E/F)$ satisfies $\tau(x) \neq x$. $\square$

By construction T is a finitely generated G-stable differential F-algebra with fraction field E, and there is an isomorphism of $\overline{F}[G]$-modules

$$\overline{F} \otimes_F T \xrightarrow{\sim} \overline{F} \otimes_C C[G]$$

where $C[G]$ denotes the affine coordinate ring of G. In particular if F is algebraically closed, then there is an isomorphism

$$T \xrightarrow{\sim} F \otimes_C C[G]$$

As a corollary of Noether normalization lemma, $trdeg[E : F] = trdeg[T : F] = dimT - dimF = dimT$ and the latter is equal to $dimF \otimes_C C[G] = dimC[G] = dimG$ by the above isomorphism. Hence, we have

$$dimG(E/F) = trdeg[E : F].$$

We shall prove the isomorphism above. We can consider G as a closed subgroup of $GL_n(C)$. Then there is an ideal I of $C[GL_n(C)]$ such that $C[G] = C[GL_n(C)]/I$. One can show that I is G-stable with the action $g \cdot f = \lambda_g(f) : h \mapsto f(g^{-1}h)$. Hence we want to prove

$$\overline{F} \otimes_F R/P \xrightarrow{\sim} \overline{F} \otimes_C C[GL_n(C)]/I.$$

Next lemma will show that there is a bijection between the set of differential ideals of R and the G-stable ideals of $C[GL_n(C)]$.

Lemma 4.2.2. *Let $A = E[y_{ij}, 1/det]$, $B = C[y_{ij}, 1/det]$ and $D = F[y_{ij}, 1/det]$.*

(a) Consider A as a differential ring where derivation is extended from E with $y'_{ij} = 0$ and consider B as a subring of A. There is a bijection

$$\{\textit{set of ideals of } B\} \leftrightarrow \{\textit{set of differential ideals of } A\}$$
$$I \mapsto IA$$
$$J \cap B \hookleftarrow J$$

(b) Assume $G = G(E/F)$ acts trivially on y_{ij}'s. There is a bijection

$$\{\textit{set of ideals of } D\} \leftrightarrow \{\textit{set of } G\textit{-stable ideals of } A\}$$
$$I \mapsto IA$$
$$J \cap D \hookleftarrow J$$

Proof. (a) Let I be an ideal of B. Since every element of B and therefore of I is a constant, IA is a differential ideal of A. It is clear that given a differential ideal J of A, the intersection $J \cap B$ is an ideal of B. Now we will show that $IA \cap B = I$ and $(J \cap B)A = J$.

Let $\{v_s\}$ be a C-basis for E, including 1. Then it is also a free B-basis for A as a module. Then elements of IA are the fintie sums $\sum_s \lambda_s v_s$ where $\lambda_s \in I$. These sums are included in $IA \cap B$ only when $v_s = 1$. Hence $IA \cap B = I$.

Let $b \in J$. For the last equality it suffices to show that $b \in (J \cap B)A$. Let $\{w_s\}$ be a C-basis for B. Then $b = \sum_s \mu_s w_s$ for some unique elements $\mu_s \in E$. Denote the number of non-zero indices μ_s of b by $l(b)$. We will perform induction on $l(b)$. When $l(b) = 0$, we have $b = 0 \in (J \cap B)A$. When $l(b) = 1$, we have $b = \mu_1 w_1$ therefore $w_1 \in J$. Then, $\mu_1 \in E \subseteq A$ and $w_1 \in J \cap B$ implies $b \in (J \cap B)A$. Assume $l(b) > 1$. WLOG we may assume $\mu_1 = 1$. If $\mu_s \in C$ for all s, we have $b' = 0$ which implies that $b \in B$ and therefore $b \in J \cap B \subseteq (J \cap B)A$. So we may assume that $\mu_2 \in E \backslash C$. Since $\mu_1 = 1$, the derivative b' has 0 as the coefficient of μ_1. Then $l(b') < l(b)$ and by induction $b' \in (J \cap B)A$. Similarly $(\mu_2^{-1}b)' \in (J \cap B)A$. Hence $(\mu_2^{-1})'b = (\mu_2^{-1}b)' - \mu_2^{-1}b' \in (J \cap B)A$. But $\mu_2^{-1} \in E \backslash C$, so its derivative is nonzero. Thus $b \in (J \cap B)A$.

(b) Proof is similar with the above case. Let I be an ideal of D. Action of G on D and therefore on I is trivial, so IA is G-stable. Let J be a G-stable ideal of A. Then $J \cap D$ is an ideal of D. We are to show that $IA \cap D = I$ and $(J \cap D)A = J$. Same proof in part (a) applies to the former equality. We will show the latter. Let $\{w_s\}$ be a F-basis for D. Then $b = \sum_s \mu_s w_s$ for some unique elements $\mu_s \in E$. Let $l(b)$ be the number of non-zero indices of μ_s. We will make induction on $l(b)$. Similar to part (a), the result is clear when $l(b) \in \{0, 1\}$. Assume $l(b) > 1$. WLOG assume $\mu_1 = 1$. If $\mu_s \in F$ for any s, then b is fixed under G-action so $b \in D$ and therefore we have the result. Then we may assume that $\mu_2 \in E \backslash F$. Let $\sigma \in G$ be arbitrary. Since σ fixes all $w_s \in D$, the coefficient of w_1 in $\sigma(b)$ is 1.

Hence the coefficient of w_1 in $\sigma(b) - b$ is 0. Then $l(\sigma(b) - b) < l(b)$. By induction $\sigma(b) - b \in (J \cap D)A$. Similarly $\sigma(\mu_2^{-1}b) - \mu_2^{-1}b \in (J \cap D)A$. By lemma 4.2.1, there is an element $\sigma \in G$ such that $\sigma(\mu_2) \neq \mu_2$ since $\mu_2 \in E \backslash F$. Then $\sigma(\mu_2^{-1}) - \mu_2^{-1} \neq 0$. But $(\sigma(\mu_2^{-1}) - \mu_2^{-1})b = \sigma(\mu_2^{-1}b) - \mu_2^{-1}b - \sigma(\mu_2^{-1})(\sigma(b) - b) \in (J \cap D)A$, so $b \in (J \cap D)A$.

□

Theorem 4.2.3. *There is an isomorphism of $\overline{F}[G]$-modules*

$$\overline{F} \otimes_F T \xrightarrow{\sim} \overline{F} \otimes_C C[G].$$

Proof. In this proof, we will consider G as a closed subgroup of $GL_n(C)$. We consider the G-action on the variety $GL_n(C)$ as the left multiplication.

$$G \times GL_n(C) \to GL_n(C)$$
$$(g, h) \mapsto gh.$$

This action corresponds to a G-action on the coordinate ring as follows.

$$G \times C[GL_n(C)] \to C[GL_n(C)]$$
$$(g, f) \mapsto \lambda_g(f) : h \mapsto f(g^{-1}h).$$

We have $C[GL_n(C)] = C[x_{st}, 1/det]$ and recall that $R = F[y_{ij}, 1/det]$. Recall that the derivation on R is given by

$$y'_{ij} = y_{i+1,j}, \quad 0 \leq i \leq n-2$$
$$y'_{n-1,j} = -a_{n-1}y_{n-1,j} - ... - a_1y_{1j} - a_0y_{0j}.$$

We consider $C[x_{st}, 1/det]$ with the G-action above and the inclusion $C[x_{st}, 1/det] \subseteq E[x_{st}, 1/det]$. We define the relation between y_{ij}'s and $x'_{st}s$ with the matrix multiplication $(y_{ij}) = (r_{ab})(x_{st})$ where r_{ab} are the images of y_{ab} in the quotient map $R \to R/P = T$. Then r'_{ab} are the images of y'_{ab} in the same map and $(y_{ij})' = (r_{ab})'(x_{st})$. But $(y_{ij})' = (r_{ab})'(x_{st}) + (r_{ab})(x_{st})'$, so x'_{st} for all s, t. Moreover, if we take y_{ij} to be G-invariant then G-action on x_{st} is compatible with G-action on E. Hence we have

$$F[y_{ij}, 1/det] \subseteq E[y_{ij}, 1/det] = E[x_{st}, 1/det] \supseteq C[x_{st}, 1/det]$$

where each ring has a derivation and a G-action which are compatible with each other.

Since G is an algebraic subgroup of $GL_n(C)$, it corresponds to a radical ideal I of $C[GL_n(C)]$. If $f \in I$, then $g \cdot f(x) = f(g^{-1}x) = 0$ for any $g, x \in G$. So $g \cdot f \in I$ and I is G-stable. Let J be a maximal G-stable ideal containing I. One can see that the radical of J is also G-stable. Hence by maximality, J is radical and defines a subvariety W of $GL_n(C)$. Let $M \in W$. Then for any $f \in Q$, $f(M) = 0$ and since $g \cdot f \in Q$ for any $g \in G$, we have $f(g^{-1}M) = (g \cdot f)(M) = 0$. Hence $g^{-1}M \in W$ and $GW = W$. But $I \subseteq J$, so $G \supseteq W$. Then for any $M \in W$, we have $M, M^{-1} \in G$, so $1 = M^{-1}M \in GW = W$. Hence $G \subseteq GW = W$ and $G = W$. Thus $I = J$ and I is a maximal G-stable ideal.

By lemma 4.2.2, there is a bijection between the set of differential ideals of $R = F[y_{ij}, 1/det]$ and the G-stable ideals of $C[GL_n(C)] = C[x_{st}, 1/det]$. Then I corresponds to a differential ideal $Q = IA \cap R$ of R, where $A = E[y_{ij}, 1/det] = E[x_{st}, 1/det]$. Since I is a maximal G-stable ideal, Q is a maximal differential stable ideal. The construction of the Picard-Vessiot extension is independent from the choice of the maximal differential ideal P of R by theorem 3.2.11. So we can assume $Q = P$. Hence

$$\begin{aligned} E \otimes_C C[G] &= E \otimes_C C[GL_n(C)]/I \simeq A/AI \\ &\simeq E \otimes_F R/(AI \cap R) = E \otimes_F R/P \\ &= E \otimes_F T \end{aligned}$$

and therefore $\overline{E} \otimes_C C[G] \simeq \overline{E} \otimes_F T$. Using [1, Proposition 1.1.29.], we deduce $\overline{F} \otimes_C C[G] \simeq \overline{F} \otimes_F T$. □

Remark 4.2.4. There is a more technical proof in [5, Theorem 5.12.]. We will give a sketch of this proof.

Since T is G-stable, there is an action of G on T which can be seen as a morphism $\Delta : T \to T \otimes_C C[G]$, as in theorem 2.2.3. It extends to another action $\overline{\Delta} : \overline{F} \otimes_F T \to (\overline{F} \otimes_F T) \otimes_{\overline{F}} (\overline{F} \otimes_C C[G])$. Choose an F-algebra morphim $f : T \to \overline{F}$ and extend it to $\overline{f} : \overline{F} \otimes_F T \to \overline{F}$. Then $(\overline{f} \otimes 1) \circ \overline{\Delta} : \overline{F} \otimes_F T \to \overline{F} \otimes_C C[G]$ is a $\overline{G}$-equivariant $\overline{F}$-algebra morphism, where $\overline{G} = \mathrm{Spec}(\overline{F} \otimes_C C[G])$. Moreover, it is an injection.

Let $X = \mathrm{Spec}(\overline{F} \otimes_F T)$. Then $(\overline{f} \otimes 1) \circ \overline{\Delta}$ corresponds to the morphism $\overline{G} \to X$, $g \mapsto gx$, where $x \in X$ is the point corresponding to $\overline{f}$. One shows that $\overline{G} \to X$ is an isomorphism and therefore $\overline{F} \otimes_F T = \overline{F}[X] \to \overline{F}[\overline{G}] = \overline{F} \otimes_C C[G]$ is an isomorphism.

We proved the following corollary above.

Corollary 4.2.5. *$dim G(E/F) = trdeg[E : F]$.*

4.3 The Galois Correspondence

There is a Galois correspondence for differential equations similar to one that is for polynomials. In this section, we will prove this correspondence and some of its consequences.

Throughout this section we let $E \supseteq F$ be a Picard-Vessiot extension with algebraically closed field of constants C for a linear differential equation $L(y)$. We also let R be the full universal solution algebra for $L(y)$ and P be a maximal differential ideal of R. We will denote R/P by $T(E/F)$ or just T, when it is obvious.

Lemma 4.3.1. *Let N be a closed normal subgroup of $G(E/F)$. Then E^N is the field of fractions of T^N.*

Proof of lemma 4.3.1 is technical and uses the character theory which is beyond the scope of this thesis. For the proof, see [4, Proof of Proposition 6.3.5.(d)] or [5, Proof of Proposition 6.2.].

Theorem 4.3.2. *Let $\mathscr{F}$ be the category whose objects are the elements of the set*

$$Ob(\mathscr{F}) = \{E \supseteq K \supseteq F : K \text{ is an intermediate differential field}\}$$

and morphisms are the inclusion homomorphisms. Let $\mathscr{G}$ be the category whose objects are the elements of the set

$$Ob(\mathscr{G}) = \{H \leqslant G(E/F) : H \text{ is a Zariski closed subgroup}\}$$

and morphisms are the inclusion homomorphisms. The Galois correspondence for differential equations indicates a contravariant isomorphism of categories $\mathscr{F}$ and $\mathscr{G}$ which is given by the functors

$$\phi : K \mapsto G(E/K) \text{ and } \psi : H \mapsto E^H$$

such that

$$\phi\psi = 1_{\mathscr{G}} \text{ and } \psi\phi = 1_{\mathscr{F}}.$$

Moreover, $K \supseteq F$ is a Picard-Vessiot extension if and only if $G(E/K)$ is normal in $G(E/F)$. In this case, $G(K/F) = G(E/F)/G(E/K)$.

Note that, if $H \leqslant G(E/F)$ is any subgroup (not necessarily Zariski closed), then $G(E/E^H)$ is the Zariski closure of H.

Proof. We will show that

(i) ϕ is a contravariant functor,

(ii) ψ is a contravariant functor,

(iii) $\psi\phi = 1_{\mathscr{F}}$, i.e. $E^{G(E/K)} = K$ for any $K \in Ob(\mathscr{F})$,

(iv) $\phi\psi = 1_{\mathscr{G}}$, i.e. $G(E/E^H) = H$ for any $H \in Ob(\mathscr{G})$,

(v) $H \leqslant G(E/F)$ implies $G(E/E^H) = \overline{H}$,

(vi) if $K \supseteq F$ is a Picard-Vessiot extension, $G(E/K) \trianglelefteq G(E/F)$ and $G(K/F) = G(E/F)/G(E/K)$

(vii) if $G(E/K) \trianglelefteq G(E/F)$, $K \supseteq F$ is a Picard-Vessiot extension,

in this order.

(i) Let $K \in Ob(\mathscr{F})$. Since $E \supseteq F$ is a Picard-Vessiot extension, so is $E \supseteq K$. Then $G(E/K)$ is a closed subgroup by theorem 4.1.2 and $\phi(K) = G(E/K) \in Ob(\mathscr{G})$. The functorial property is obvious.

(ii) Let $H \in Ob(\mathscr{G})$. Clearly, $E^H \subseteq E$ is a differential subfield. Let $x \in F$ and $\sigma \in H$. Since $\sigma \in G$, $\sigma(x) = x$, so $F \subseteq E^H$. Hence $\psi(H) = E^H \in Ob(\mathscr{F})$.

(iii) $E^{G(E/K)} \supseteq K$ follows from the definition of $G(E/K)$. To show the other inclusion, let $x \in E^{G(E/K)}$. Then $x \in E$ and $\sigma(x) = x$ for any $\sigma \in G(E/K)$. By lemma 4.2.1, we have $x \in K$.

(iv) Let $k := E^H$, $G := G(E/k)$. Since $k \subseteq E$ is a Picard-Vessiot extension, we have $\overline{k} \otimes_k T(E/k) \simeq \overline{k} \otimes_C C[G]$. Taking the total rings of fractions, $\overline{k} \otimes_k E \simeq \overline{k} \otimes_C Qt(C[G])$ where $Qt(C[G])$ is the field of fractions of $C[G]$. Taking H-invariants, $\overline{k} \otimes_k E^H \simeq \overline{k} \otimes_C Qt(C[G])^H$. LHS is $\overline{k} \otimes_k E^H = \overline{k} \otimes_k k \simeq \overline{k}$. On the other hand, $Qt(C[G])^H$ is the ring of the H-invariant rational functions on G. Therefore it is the ring of rational functions on G/H since $C[G]^H \simeq C[G/H]$. Hence $G/H = 1$ and $G = H$.

(v) We will show that $E^H = E^{\overline{H}}$. Then from (iv), we will have $G(E/E^H) = G(E/E^{\overline{H}}) = \overline{H}$. The inclusion $E^H \supseteq E^{\overline{H}}$ is obvious. Now let $x \in E^H$, i.e. $\sigma \cdot x = x$ for any $\sigma \in H$. But $\sigma \cdot x - x$ is a polynomial over H and the result follows.

(vi) Consider the map

$$\varphi : G(E/F) \to G(K/F)$$
$$\sigma \mapsto \sigma_{|K}.$$

By lemma 3.2.10, $\sigma_{|K}(K) = K$, so φ is well-defined. We will show that this is a surjection of linear algebraic group with kernel $G(E/K)$. Let $E = F\langle V \rangle$, $K = F\langle W \rangle$, where V and W are solution spaces of linear equations corresponding to Picard-Vessiot extensions $E \supseteq F$ and $K \supseteq F$, respectively. We know that there is an injection of linear algebraic groups $G(E/F) \to GL(V)$. Since W is a submodule of V, there is a morphism of linear algebraic groups $GL(V) \to GL(W)$. Taking the composition, we have another morphism $G \to GL(W)$.

Since $K = F\langle W\rangle$, this map factors through φ. Hence φ is also a morphism. To show surjectivity, let $\tau \in G(K/F)$. Consider $\lambda : K \xrightarrow{\tau} K \xrightarrow{\text{incl}} E$. Call $L(y)$ for the linear differential equation making $E \supseteq K$ a Picard-Vessiot extension. Notice that $\lambda(L(y)) = L(y)$ and $E \supseteq \lambda(K)$ is a Picard-Vessiot extension. Then by uniqueness, λ extends to a differential F-algebra automorphism $E \to E$. Finally, $\ker\varphi = \{\sigma \in G(E/F) : \sigma(x) = x, \forall x \in K\} = G(E/K)$.

(vii) Call $G := G(E/F)$ and $N := G(E/K)$. Note that by part (iii), $K = E^N$. Now, T is G-stable, by construction. We will show that T^N is also G-stable. Let $t \in T^N$ and $\tau \in G$. If $\sigma \in N$, then $(\tau^{-1}\sigma\tau)(t) = t$ since $\tau^{-1}\sigma\tau \in N$, by normality of N. Then $\sigma(\tau(t)) = \tau(t)$ and $\sigma(t) \in T^N$. Therefore $\tau(T^N) = T^N$ for any $\tau \in G$, i.e. T^N is G-stable.

We have $\overline{F}\otimes_F T^N = (\overline{F}\otimes_F T)^N \simeq (\overline{F}\otimes_C C[G])^N = \overline{F}\otimes_C C[G]^N \simeq \overline{F}\otimes_C C[G/N]$. Since the coordinate ring $C[G/N]$ is a finitely generated C-algebra, T^N is a finitely generated F-algebra.

Let $a_1, ..., a_r$ be generators of T^N over F. Let V be the C-vector space generated by $a_1, ..., a_r$. Then V is G-stable and generates T^N as an F-algebra. By lemma 4.3.1, E^N is the field of fractions of T^N. Hence V generates $K = E^H$ as a (differential) F-algebra. Then K is generated by the solutions of the linear differential equation

$$\frac{w(y, a_1, ..., a_r)}{w(a_1, ..., a_r)} = 0$$

having coefficients over F. Since $C_K = C_F$, we deduce that $K \supseteq F$ is a Picard-Vessiot extension.

□

Theorem 4.3.3. *Let $E \supseteq F$ be a Picard-Vessiot extension and let $G := G(E/F)$. Then, $E^{G^0} \supseteq F$ is a finite Galois extension with Galois group G/G^0 and E^{G^0} is the algebraic closure of F in E.*

Proof. By theorem 4.3.2(vii), $G(E^{G^0}/F) = G/G^0$. Since $(E^{G^0})^{G/G^0} = E^G = F$, the extension $E^{G^0} \supseteq F$ is Galois with Galois group G/G^0. By proposition 1.2.9(i), G/G^0 is finite therefore the extension $E^{G^0} \supseteq F$ is finite. Let $u \in E$ be algebraic over F. Then $F(u) \supseteq F$ is a finite extension. Then $[G : Aut(F(u)/F)]$ is finite and by proposition 1.2.9(ii), $Aut(F(u)/F) \geqslant G^0$. Thus $F(u) \subseteq E^{G^0}$ and $u \in E^{G^0}$. □

Proposition 4.3.4. *Let F be a differential field with algebraically closed field of constants, and let $M \supseteq F$ be a differential field extension with no new constants. Suppose that $E \supseteq F$ is a Picard-Vessiot extension with $M \supseteq E \supseteq F$ and that $M \supseteq K \supseteq F$ is an intermediate differential field. Then the field compositum EK is a Picard-Vessiot extension of K and the homomorphism*

$$G(EK/K) \to G(E/F)$$

is an injection whose image has Zariski closure $G(E/E \cap K)$.

Proof. Consider the morphism of differential rings

$$E \otimes_C K \to M$$
$$e \otimes k \mapsto ek$$

and notice that EK is the field of fractions of the image. Then EK is a differential field. There is a linear differential equation $L(y)$ over F such that $E = F\langle V \rangle$ where $V = L^{-1}(0)$. Then $EK = K\langle V \rangle$. Since $C_M = C_F$, we have $C_{EK} = C_K$. Hence $K \subseteq EK$ is a Picard-Vessiot extension for $L(y)$.

Let $\sigma \in G(EK/K)$. Restricting σ to E, we have a map $\sigma_{|E} : E \to EK$. Applying lemma 3.2.10 to $\sigma_{|E}$ and id : $E \to EK$, we have $\sigma_{|E}(E) = E$. Since σ is a differential K-algebra morphism, it also fixes elements of F. Therefore we have a morphism

$$\varphi : G(EK/K) \to G(E/F)$$
$$\sigma \mapsto \sigma_{|E}.$$

Since $EK = K\langle V\rangle$, each $\sigma \in G(EK/K)$ is determined by their values on V, and therefore on E. So φ is an injection. Let $H := \operatorname{Im}\varphi$. Since each $\sigma_{|E} \in H$, fixes elements of K, we have $E^H \subseteq K$ and $E^H \subseteq E \cap K$. On the other hand, if $a \in E \cap K \subseteq K$, we have $\sigma(a) = a$, for any $\sigma \in G(EK/K)$. Then $\sigma_{|E}(a) = a$ and we have $a \in E^H$. Hence $E^H = E \cap K$. By theorem 4.3.2,

$$\overline{H} = G(E/E^H) = G(E/E \cap K)$$

is the Zariski closure of H. □

4.4 Tannakian Category Approach

Let k be a differential field with field of constants C. The category of all differential modules over k is denoted by Diff_k. A morphism $\phi : (M_1, \partial_1) \to (M_2, \partial_2)$ is a k-linear map $\phi : M_1 \to M_2$ such that $\phi \circ \partial_1 = \partial_2 \circ \phi$.

A *differential submodule* N of (M, ∂) is a k-vector space $N \subseteq M$ such that $\partial(N) \subseteq N$. In this case $(N, \partial|_N)$ is a differential module. M/N with the differentiation $\partial(m + N) = \partial(N) + m$ is also a differential module and it is called the *quotient differential module*. Hence Diff_k is an abelian category.

The tensor product $(M_1, \partial_1) \otimes (M_2, \partial_2)$ of two differential modules is $(M_1 \otimes_k M_2, \partial)$ where $\partial(m_1 \otimes m_2) = \partial_1(m_1) \otimes m_2 + m_1 \otimes \partial_2(m_2)$. The identity object 1 is the trivial differential module of dimension 1 over k. With this tensor product Diff_k is a tensor category.

The internal hom of two objects $\underline{\mathrm{Hom}}((M_1, \partial_1), (M_2, \partial_2))$ is $\mathrm{Hom}_k(M_1, M_2)$ since tensor product is left adjoint to Hom in modules. Differentiation on $\mathrm{Hom}_k(M_1, M_2)$ is given by $\partial(\phi) = \phi \circ \partial_1 - \partial_2 \circ \phi$.

So far, we obtained that Diff_k is a rigid abelian tensor category with $\mathrm{End}(1) \simeq k$.

Fix a differential module M over k. For non-negative integers m and n, define $M_n^m := M \otimes M \otimes ... \otimes M^* \otimes ... \otimes M^*$, i.e. the tensor product of n copies of M and m copies of its dual $M^* := \mathrm{Hom}_k(M, 1)$. We define the subcategory $\{\{M\}\}$ of Diff_k

as follows. The objects are subqoutients[1] of finite direct sums of M_n^m and morphisms are differential module morphisms as in Diff_k. Thus $\{\{M\}\}$ is a full subcategory of Diff_k.

$\{\{M\}\}$ is also a rigid abelian tensor category with $\mathrm{End}(1) \simeq k$. We will attach a fibre functor. Let L be a Picard-Vessiot field for M over k. Define the functor

$$\begin{aligned} \omega_L : \{\{M\}\} &\to \mathrm{Vect}_C \\ N &\rightsquigarrow \ker(\partial, L \otimes_k N). \end{aligned}$$

Denote $G(M, \partial) := \mathrm{Aut}^{\otimes}(\omega_L)$. Since every Picard-Vessiot field for M over k are isomorphic, $G(M, \partial)$ is independing of choosing L.

Theorem 4.4.1. *[8, Theorem 2.33][9, Proposition 6.6.8] Let M be a differential module over k with differential Galois group G. Then $\{\{M\}\}$ is a neutral Tannakian category and G is the corresponding affine group scheme i.e. the categories $\{\{M\}\}$ and Repr_G are equivalent. Consequently, the affine group schemes G and $G(M, \partial)$ are isomorphic.*

[1] A *subqoutient* of N is an object N_1/N_2 with $N_2 \subseteq N_1 \subseteq N$ subobjects.

Chapter 5

LIOUVILLIAN EXTENSIONS

5.1 Virtually Solvable Extensions

A group having a solvable subgroup of finite index is called a *virtually solvable group.* A Picard-Vessiot extension whose differential Galois group is virtually solvable is called a *virtually solvable extension.* In this section we will examine the virtually solvable extensions. Note that if G is a linear algebraic group then G is virtually solvable if and only if G^0, the identity component of G, is solvable.

Definition 5.1.1. Let $E \supseteq F$ be a Picard-Vessiot extension with algebraically closed field of constants C. If there is a chain of subfields

$$F = F_0 \subseteq F_1 \subseteq ... \subseteq F_n = E$$

where

$$F_i = F_{i-1}(a_i)$$

and for all i either

(i) a_i is algebraic over F_{i-1}, or

(ii) $a_i \neq 0$ and $a_i'/a_i \in F_{i-1}$, or

(iii) $a_i' \in F_{i-1}$

then $E \supseteq F$ is called a *liouvillian extension.*

Our first main theorem states that $E \supseteq F$ is liouvillian if and only if virtually solvable i.e. $G(E/F)^0$ is solvable.

Proposition 5.1.2. *Let $E \supseteq F$ be a Picard-Vessiot extension with algebraically closed field of constants C and let $G := G(E/F)$. Let G has dimension n and its unipotent radical has dimension m. If G^0 is solvable, then there is a chain of subfields*

$$F \subseteq F(a_0) \subseteq F(a_0, a_1) \subseteq ... \subseteq F(a_0, a_1, ..., a_n) = E$$

such that

(i) a_0 *is algebraic over* F,

(ii) a_i *is transcendental over* $F(a_0, a_1, ..., a_{i-1})$ *with* $a_i'/a_i \in F(a_0, a_1, ..., a_{i-1})$ *for* $1 \leq i \leq n - m$,

(iii) a_j *is transcendental over* $F(a_0, a_1, ..., a_{j-1})$ *with* $a_j' \in F(a_0, a_1, ..., a_{j-1})$ *for* $n - m + 1 \leq j \leq n$.

Our strategy of the proof will be as follows. Let $G = G(E/F)$ be a differential Galois group with solvable identity component. In chapter 4, we showed that fixed field of G^0 corresponds to the finite Galois part of $E \supseteq F$. In chapter 1, we showed that G^0 can be written as a semi-direct product of its unipotent part U and one of its maximal tori T. Thus we have a chain of characteristic subgroups

$$1 \leqslant U \leqslant G^0 \leqslant G$$

with quotients $U/1 = U$ unipotent, $G^0/U = T$ a torus and G/G^0 a finite group. Finite part will give us an algebraic element. Unipotent part, as we showed proposition 1.4.7, can be divided into finitely many $\mathbb{G}_a$'s and the torus part, by definition, can be divided into finitely many $\mathbb{G}_m$'s. In the next lemma we will show that each $\mathbb{G}_a$ represents the adjunction of an integral and each $\mathbb{G}_m$ represents the adjunction of an exponential.

Lemma 5.1.3. *Let $E \supseteq F$ be a Picard-Vessiot extension with algebraically closed field of constants C and let $G := G(E/F)$. Then,*

(i) $G \simeq \mathbb{G}_a(C)$ *if and only if* $E = F(a)$ *for some* a *such that* a *is transcendental over* F *with* $a' \in F$.

(ii) $G \simeq \mathbb{G}_m(C)$ *if and only if* $E = F(a)$ *for some* a *such that* a *is transcendental over* F *with* $a'/a \in F$.

Proof. (i) If $E = F(a)$ with $a' \in F$ and a is transcendental over F, then $F(a)$ is a Picard-Vessiot extension of F for the linear differential equation

$$L(y) = y'' - \frac{a''}{a'}y'$$

whose solution space has a basis $\{1, a\}$ over C. Then for any $\varphi \in G = G(E/F)$,

$$\varphi : 1 \mapsto 1 \text{ and } \varphi : a \mapsto c_1 a + c_2$$

for some $c_1, c_2 \in C$. Then, $a' = \varphi(a') = (\varphi(a))' = c_1 a'$ since $a' \in F$. Therefore $c_1 = 1$ and letting $c := c_2$ we have

$$\varphi : \begin{bmatrix} 1 \\ a \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ a + c \end{bmatrix}$$

where $c \in C$ is depending on φ. Hence G is isomorphic to a subgroup of

$$\{ \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} : c \in C\} \simeq \mathbb{G}_a(C).$$

Since the only algebraic subgroups of $\mathbb{G}_a(C)$ are itself and 1, we have $G \simeq \mathbb{G}_a(C)$.

On the other hand, let $E \supseteq F$ be a Picard-Vessiot extension for a linear differential equation

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1 y' + a_0 y$$

where $a_i \in F$ and let $G \simeq \mathbb{G}_a(C)$. Note that since $G \simeq \mathbb{G}_a(C)$ is connected, by theorem 4.3.3, E is purely transcendental over F. Since $G \simeq \mathbb{G}_a(C)$ is unipotent, by proposition 1.4.5, one can choose a basis $y_1, ..., y_n$ for the solution space of $L(y) = 0$

over C such that $G \leqslant GL_n(C)$ consists of matrices of the form

$$\begin{bmatrix} 1 & & & \\ & 1 & & * \\ & & 1 & \\ & 0 & & \ddots \\ & & & & 1 \end{bmatrix}$$

w.r.t. the basis $y_1, ..., y_n$. So for any $\varphi \in G$,

$$\varphi : y_1 \mapsto y_1$$

and therefore $y_1 \in F$. Then, if we let b_i's be such that

$$L(yy_1) = b_n y^{(n)} + b_{n-1} y^{(n-1)} + ... + b_1 y' + b_0 y$$

then $b_i \in F$, for all i. Moreover $0 = L(y_1) = b_0$ so

$$L(yy_1) = b_n y^{(n)} + b_{n-1} y^{(n-1)} + ... + b_1 y'.$$

Consider

$$M(f) = b_n f^{(n-1)} + b_{n-1} f^{(n-2)} + ... + b_1 f.$$

Its solution space lies in E and has a basis

$$\{(y_2/y_1)', (y_3/y_1)', ..., (y_n/y_1)'\}$$

over C. Hence the Picard-Vessiot extension of $M(f)$ over F, call K, lies in E. Moreover since $y_2, ..., y_n \in E$, we have $K(y_2, ..., y_n) \subseteq E$. But former contains all solutions of $L(y) = 0$, then by lemma 3.2.6, $E = K(y_2, ..., y_n) = K(\frac{y_2}{y_1}, ..., \frac{y_n}{y_1})$. Let $K_i := K(\frac{y_2}{y_1}, ..., \frac{y_i}{y_1})$, for $2 \leq i \leq n$, and $K_1 := K$. Hence we have a chain of subfields

$$F \subseteq K = K_1 \subseteq K_2 \subseteq K_3 \subseteq ... \subseteq K_n = E$$

and since $G \simeq \mathbb{G}_a(C)$ is abelian, each extension is a Picard-Vessiot extension by theorem 4.3.2. Since the only algebraic subgroups of $\mathbb{G}_a(C)$ are itself and the trivial

group, each $G(E/K_i)$, for $1 \leq i \leq n$, is either isomorphic to $\mathbb{G}_a(C)$ or 1. We will make induction on n. Since $GL_1(C)$ does not contain any subgroup isomorphic to $\mathbb{G}_a(C)$ we have $n \geq 2$. If $n = 2$, then the chain above is

$$F \subseteq K = K_1 \subseteq K_2 = E$$

with $G(E/K)$ is either isomorphic to $\mathbb{G}_a(C)$ or 1. If $G(E/K) = 1$, then $E = K$ and $E \supseteq F$ is a Picard-Vessiot extension for $M(f) = b_2 f' + b_1 f$, with one dimensional solution space i.e. G is isomorphic to a subgroup of $GL_1(C)$, but this contradicts with $G \simeq \mathbb{G}_a$. So $G(E/K) \simeq \mathbb{G}_a(C)$. Then $G(K/F)$ should be a finite group, but since G is connected only finite quotient of G is the trivial group 1, so $G(K/F) = 1$ and $K = F$. Hence $E = K_2 = K(\frac{y_2}{y_1}) = F(\frac{y_2}{y_1})$ with $(y_2/y_1)' \in K = F$ and we are done. Now assume that $n > 2$. If $G(E/K) = 1$, then $E = K$ and $E \supseteq F$ is a Picard-Vessiot extension for $M(f)$ which has degree $n - 1$, and by induction we are done. If $G(E/K) \simeq \mathbb{G}_a(C)$, then for some i we have $G(E/K_i) \simeq \mathbb{G}_a(C)$. Take maximal i with this property. Then $G(E/K_{i+1}) = 1$ and $K_{i+1} = E$. But $G/G(E/K_i) \simeq G(K_i/F)$. Then $G(K_i/F)$ is finite and by connectedness of G, we have $G(K_i/F) = 1$ i.e. $F = K_i$. Thus $E = K_{i+1} = K_i(\frac{y_{i+1}}{y_i}) = F(\frac{y_{i+1}}{y_i})$ with $(y_{i+1}/y_i)' \in K_i = F$ and we are done.

(*ii*) If $E = F(a)$ with $a'/a \in F$ and a is transcendental over F, then $F(a)$ is a Picard-Vessiot extension of F for the linear differential equation

$$L(y) = y' - \frac{a'}{a} y$$

whose solution space has a basis $\{a\}$ over C. Then for any $\varphi \in G = G(E/F)$,

$$\varphi : a \mapsto ca$$

for some $c \in C$ depending on φ. Hence G is isomorphic to a subgroup of

$$\{\left[c\right] : c \in C\} \simeq \mathbb{G}_m(C).$$

The algebraic subgroups of $\mathbb{G}_m(C)$ are either the entire group or finite cyclic group. Since $E \supseteq F$ is not algebraic, we have $G \simeq \mathbb{G}_m(C)$.

Let $E \supseteq F$ be a Picard-Vessiot extension for a linear differential equation

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1y' + a_0y$$

where $a_i \in F$ and let $G \simeq \mathbb{G}_m(C)$. Firstly, $G \simeq \mathbb{G}_m(C)$ is connected so by theorem 4.3.3, E is purely transcendental over F. Since $G \simeq \mathbb{G}_m(C)$ is a torus, we can choose a basis $y_1, ..., y_n$ for the solution space of $L(y) = 0$ over C such that $G \leqslant GL_n(C)$ consists of matrices of diagonal matrices w.r.t. the basis $y_1, ..., y_n$. Let $\varphi \in G$ be a non-identity element. Then φ can be represented as

$$\begin{bmatrix} * & & & \\ & * & & 0 \\ & & * & \\ & 0 & & \ddots \\ & & & & * \end{bmatrix}$$

with at least one of $*$'s are not 1. Let the first $*$ be $c \neq 1$. Then

$$\varphi : y_1 \mapsto cy_1$$

so $y_1 \notin G$. But φ was arbitrary so for any $\varphi \in G$, there is $c(\varphi) \in C$ such that

$$\varphi : y_1 \mapsto c(\varphi)y_1$$

and therefore

$$\varphi : y_1' \mapsto c(\varphi)y_1'$$

and combaning them

$$\varphi : \frac{y_1'}{y_1} \mapsto \frac{y_1'}{y_1}$$

Hence $\frac{y_1'}{y_1} \in F$. One can deduce that $y_1^{(k)} \in F(y_1)$ for any positive integer k. Then $F(y_1)$ is a differential field. Then $F(y_1) \supseteq F_1$ is a Picard-Vessiot extension by theorem 4.3.2 since G is abelian. In addition, $y_1 \in E$ is transcendental over F, so by above case, $G(F(y_1)/F) \simeq \mathbb{G}_m$. Let $y_i \neq y_1$. We can apply same argument to y_i, so either $y_i \in F$ or y_i is transcendental over F with $\frac{y_i'}{y_i} \in F$. Similarly, $F(y_i)$ is a differential field and $F(y_i) \supseteq F_i$ is a Picard-Vessiot extension. Then either $G(F(y_i)/F) = 1$

or $G(F(y_i)/F) \simeq \mathbb{G}_m$. Assume the second case. Notice that the field compositum of $F(y_1)$ and $F(y_i)$ is $F(y_1, y_i)$ while $F(y_1) \cap F(y_i) = F$. Then by proposition 4.3.4,

$$G(F(y_1, y_i)/F(y_1)) \simeq G(F(y_i)/F) \simeq \mathbb{G}_m,$$

but this leads to

$$\begin{aligned} 1 = dim\mathbb{G}_m &= trdeg[E : F] \\ &\geq trdeg[F(y_1, y_i) : F] \\ &= trdeg[F(y_1, y_i) : F(y_1)] + trdeg[F(y_1) : F] \\ &= dim\mathbb{G}_m + \mathbb{G}_m = 2 \end{aligned}$$

which is a contradiction. Thus $y_i \in F$, for any $y_i \neq y_1$. Therefore $F(y_1)$ contains a full set of solution of $L(y) = 0$, so by lemma 3.2.6, $E = F(y_1)$ and we are done. □

Proof of Proposition 5.1.2. Let U be the unipotent radical of G (and therefore of G^0) and let T be a maximal torus of G^0. Then $G^0 = U \rtimes T$ by theorem 1.4.18 since G^0 is solvable. By theorem 4.3.3, $\bar{F} := E^{G^0}$ is the algebraic closure of F in E. Consider the chain of subfields

$$E \supseteq E^U \supseteq \bar{F} \supseteq F$$

By theorem 4.3.3, $\bar{F} \supseteq F$ is a finite Galois extension (hence finite separable extension), therefore $\bar{F} = F(c)$ for some $c \in \bar{F}$. Consider

$$\begin{aligned} n = dimG &= trdeg[E : F] = trdeg[E : \bar{F}] \\ &= dimG^0 = dimU \rtimes T = dimU + dimT \\ &= m + dimT \end{aligned}$$

so $dimT = n - m$, but T is a torus hence $T \simeq (\mathbb{G}_m)^{n-m}$. Hence T has a normal closed subgroup S such that $S \simeq (\mathbb{G}_m)^{n-m-1}$, so $T/S \simeq \mathbb{G}_m$ and $E^S \supseteq \bar{F}$ is a Picard-Vessiot extension with $G(E^S/\bar{F}) \simeq \mathbb{G}_m$, by theorem 4.3.2. Then by lemma 5.1.3, $E^S = \bar{F}(a_1)$

such that $a_1'/a_1 \in \bar{F}$ for some $a_1 \in E^S$. Then by induction on $dimT = n - m$, we obtain a chain of subfields

$$\bar{F} \subseteq \bar{F}(a_1) \subseteq \bar{F}(a_1, a_2) \subseteq ... \subseteq \bar{F}(a_1, a_2, ..., a_{n-m})$$

such that $a_i'/a_i \in \bar{F}(a_1, a_2, ..., a_{i-1})$ for each $1 \leq i \leq n - m$. Moreover,

$$\begin{aligned} trdeg[E^U : \bar{F}] &= dimT = n - m \\ &= 1 + 1 + ... + 1 \\ &= dimG(\bar{F}(a_1, ..., a_{n-m})/\bar{F}(a_1, ..., a_{n-m-1})) + ... + dimG(\bar{F}(a_1)/\bar{F}) \\ &= trdeg[\bar{F}(a_1, ..., a_{n-m}) : \bar{F}(a_1, ..., a_{n-m-1})] + ... + trdeg[(\bar{F}(a_1) : \bar{F}] \\ &= trdeg[\bar{F}(a_1, ..., a_{n-m}) : \bar{F}]. \end{aligned}$$

But $E \supset \bar{F}$ is purely transcendental and E^U contains $\bar{F}(a_1, a_2, ..., a_{n-m})$, thus

$$E^U = \bar{F}(a_1, a_2, ..., a_{n-m}).$$

By proposition 1.4.7, U has a closed normal subgroup V with codimension 1. Then $U/V \simeq \mathbb{G}_a$ and $E^V \supseteq E^U$ is a Picard-Vessiot extension with $G(E^V/E^U) \simeq \mathbb{G}_a$, by theorem 4.3.2. Then by lemma 5.1.3, $E^V = E^U(b_1)$ such that $b_1' \in E^U$ for some $b_1 \in E^V$. Using proposition 1.4.7, we can make induction on $dimU = m$ and get a chain of subfields

$$E^U \subseteq E^U(b_1) \subseteq E^U(b_1, b_2) \subseteq ... \subseteq E^U(b_1, b_2, ..., b_m)$$

such that $b_j' \in E^U(b_1, b_2, ..., b_{j-1})$ for each $1 \leq j \leq m$. By similar dimension argument as above case, we have

$$E = E^U(b_1, b_2, ..., b_m).$$

□

Theorem 5.1.4. *Let $E \supseteq F$ be a Picard-Vessiot extension with algebraically closed field of constants C and let $G := G(E/F)$. Following are equivalent.*

(i) G^0 *is solvable.*

(ii) $E \supseteq F$ *is liouvillian.*

(iii) E *is contained in a liouvillian extension of* F*.*

Proof of Theorem 5.1.4. (i) implies (ii) by Proposition 5.1.2. (ii) implies (iii), trivially. We will show that (iii) implies (i). Let M be liouvillian extension of F containing E. Consider the chain

$$F \subseteq F(a_1) \subseteq F(a_1, a_2) \subseteq ... \subseteq F(a_1, ..., a_n) = M$$

as in definition 5.1.1. We will make induction on n. The case $n = 0$ i.e. $F = M$ is trivial.

By proposition 4.3.4, the compositum $E \cdot F(a_1) \supseteq F(a_1)$ is a Picard-Vessiot extension and we know that $M \supseteq E \cdot F(a_1) \supseteq F(a_1)$. But $M = F(a_1, ..., a_n) = F(a_1)(a_2, ..., a_n)$ so by induction $G(E \cdot F(a_1)/F(a_1))^0$ is solvable. By proposition 4.3.4, letting H be the image of the injection

$$G(E \cdot F(a_1)/F(a_1)) \to G(E/F)$$

we have an isomorphism

$$G(E \cdot F(a_1)/F(a_1)) \xrightarrow{\sim} H$$

and therefore H^0 is solvable. Again by proposition 4.3.4, the Zariski closure of H is $\bar{H} = G(E/E \cap F(a_1))$. Let $\bar{H^0}$ be the Zariski closure of H^0. By corollary 1.2.14, $\bar{H^0}$ is also solvable. But $[H : H^0]$ is finite, so by proposition 1.2.15, $[\bar{H} : \bar{H^0}]$ is also finite. Hence $\bar{H} = G(E/E \cap F(a_1))$ is virtually solvable, i.e. $G(E/E \cap F(a_1))^0$ is solvable.

Now consider $F(a_1) \supseteq E \cap F(a_1) \supseteq F$. By assumption, either a_1 is algebraic over F or $a_1'/a_1 \in F$ or $a_1' \in F$. Therefore by theorem 4.3.3 and lemma 5.1.3, $G(F(a_1)/F)$ is either finite or isomorphic to $\mathbb{G}_a$ or to $\mathbb{G}_m$. If it is finite, then $E \cap F(a_1) \supseteq F$ is

finite algebraic which implies that $G(E/E \cap F(a_1))$ is of finite index in $G(E/F)$. But $G(E/E \cap F(a_1))$ is virtually solvable, therefore $G = G(E/F)$ is also virtually solvable, i.e. G^0 is solvable. If $G(F(a_1)/F)$ is isomorphic to one of $\mathbb{G}_a$ and $\mathbb{G}_m$, then it is abelian, and every subgroup of it is normal and abelian. Then by theorem 4.3.2 $E \cap F(a_1) \supseteq F$ is a Picard-Vessiot extension with $G(E \cap F(a_1)/F) = G(F(a_1)/F)/G(F(a_1)/E \cap F(a_1))$ which is abelian since $G(F(a_1)/F)$ is abelian. Again by theorem 4.3.2, we have an exact sequence

$$1 \to G(E/E \cap F(a_1)) \to G(E/F) \to G(E \cap F(a_1)/F) \to 1$$

Since $G(E \cap F(a_1)/F)$ is abelian and $G(E/E \cap F(a_1))^0$ is solvable, by corollary 1.2.10, we conclude that $G^0 = G(E/F)^0$ is solvable. □

5.2 Solvability by Elementary Functions

Definition 5.2.1. Let C be an algebraically closed field with trivial derivation, and let $F = C(x)$ be the field of rational functions with derivation $x' = 1$.

$$F(a_1, a_2, ..., a_n, b_1, b_2, ..., b_m) \supseteq F$$

is called a *field of elementary functions* if

(i) $a_i' \in F$, for all i and

(ii) for all j, either $b_j'/b_j \in F(b_1, b_2, ..., b_{j-1})$ or b_j is algebraic over $F(b_1, b_2, ..., b_{j-1})$.

An *elementary function* is an element of a field of elementary functions.

Now consider a field of elementary functions $F(a_1, a_2, ..., a_n, b_1, b_2, ..., b_m) \supseteq F$ and a Picard-Vessiot extension $E \supseteq F$ such that $G = G(E/F)$ and

$$F(a_1, a_2, ..., a_n, b_1, b_2, ..., b_m) \supseteq E \supseteq F.$$

Our second main theorem states that G^0 is abelian.

We already showed that the differential Galois group of $\int e^{-x^2}$ over $\mathbb{C}(x)$ is (connected and) not abelian. Thus we conclude that $\int e^{-x^2}$ is not an elementary function.

Theorem 5.2.2. *Let C be an algebraically closed field with trivial derivation, and let $F = C(x)$ be the field of rational functions with derivation $x' = 1$. Let*

$$\mathscr{C} = F(a_1, a_2, ..., a_n, b_1, b_2, ..., b_m) \supseteq F$$

be a field of elementary functions. Suppose $E \supseteq F$ be a Picard-Vessiot subextension contained in $\mathscr{C}$ and let $G := G(E/F)$. Then G^0 is abelian.

Proof. Being the compositum of the Picard-Vessiot extensions $F \subseteq F(a_i)$, the extension $F \subseteq F(a_1, a_2, ..., a_n)$ is also Picard-Vessiot. Call $G_u = G(F(a_1, a_2, ..., a_n)/F)$. Let $\sigma \in G$. Since $a_i' \in F$, we have $(\sigma(a_i) - a_i)' = \sigma(a_i') - a_i' = a_i' - a_i' = 0$, so $\sigma(a_i) - a_i \in C$. Therefore we have the injection of linear algebraic groups

$$\begin{aligned} G_u &\to \mathbb{G}_a^n \\ \sigma &\mapsto (\sigma(a_i) - a_i). \end{aligned}$$

Hence G_u is unipotent, connected and abelian.

$EF(a_1, a_2, ..., a_n) \supseteq F$ is the compositum of the Picard-Vessiot extensions $E \supseteq F$ and $F(a_1, a_2, ..., a_n) \supseteq F$, then it is also Picard-Vessiot. Call $A = G(EF(a_1, a_2, ..., a_n)/F)$, $G = G(E/F)$ and $N = G(EF(a_1, a_2, ..., a_n)/E)$. Since $E \supset F$ is Picard-Vessiot, N is normal in A and $G \simeq A/N$. By theorem 1.2.11, $G^0 \simeq A^0/N^0$. Then it sufficies to show that A^0 is abelian. So we can assume that $A = G$ and $EF(a_1, a_2, ..., a_n) = E$, or equivalently $F(a_1, ..., a_n) \subseteq E$.

Let $T = G(E/F(a_1, ..., a_n))$. By theorem 5.1.4 and theorem 1.4.18, T^0 is a torus. Since $F(a_1, ..., a_n) \supseteq F$ is Picard-Vessiot, T is normal in G and $G/T \simeq G_u$. Let U^0 be the unipotent radical of G^0 (and therefore is of G). Since T does not have any unipotent element, $T \cap U^0 = 1$. Since G_u is unipotent, restriction $\tilde{\pi}$ of the quotient map $\pi : G \to G_u$ to U^0 is still onto. Notice that $\ker \tilde{\pi} = U^0 \cap \ker \pi = U^0 \cap T = 1$, so $\tilde{\pi} : U^0 \to G_u$ is an isomorphism.

By theorem 1.2.11, T^0 is normal in G^0. Moreover

$$G^0/T^0 \simeq (G/T)^0 \simeq (G_u)^0 = G_u \simeq U^0 \simeq T^0U^0/T^0.$$

Hence $G^0 = T^0U^0 \simeq T^0 \times U^0$ is abelian. □

Example 5.2.3. Let $t := \int e^{-x^2}$. In example 4.1.1, we have showed that the Picard-Vessiot extension $\mathbb{C}(x,t,t') \supseteq \mathbb{C}(x)$ has differential Galois group

$$\{\begin{bmatrix} 1 & 0 \\ a & b \end{bmatrix} : a, b \in \mathbb{C}, b \neq 0\}$$

whose identity component, which is itself, is not abelian. Then by theorem 5.2.2, $\mathbb{C}(x,t,t')$ cannot be embedded in any field of elementary functions over $\mathbb{C}(x)$. Thus we conclude that

$$\int e^{-x^2} \text{ is not an elementary function.}$$

Remark 5.2.4. Note that the inverse of theorem 5.2.2 is not always true. More precisely, given a Picard-Vessiot extension $E \subseteq F$ with $G(E/F)^0$ is abelian, it is not necessarily true that E is a field of elementary functions (or contained in a field of elementary functions). See the example below for a counterexample.

Example 5.2.5. Consider $t := \int \sqrt{1-x^4}$ over the differential field $\mathbb{C}(x)$ with derivation $x' = 1$. t satisfies the linear differential equation $(1-x^4)y'' + 2x^3y' = 0$ whose solution space has a basis $\{1, t\}$. Therefore the Picard-Vessiot extension for this equation is $\mathbb{C}(x,t,t') \supseteq \mathbb{C}(x)$. If $\varphi \in G(\mathbb{C}(x,t,t')/\mathbb{C}(x))$, then

$$\varphi : 1 \mapsto 1 \text{ and } \varphi : t \mapsto a + bt$$

for some $a, b \in \mathbb{C}$. Then,

$$\varphi : \sqrt{1-x^4} = t' \mapsto bt' = \sqrt{1-x^4}$$

and

$$\varphi : 1 - x^4 \mapsto b^2(1-x^4).$$

So, $b^2 = 1$ and a is any complex number. Hence

$$G(\mathbb{C}(x,t,t')/\mathbb{C}(x)) = \{\begin{bmatrix} 1 & 0 \\ a & b \end{bmatrix} : a \in \mathbb{C}, b \in \{-1, 1\}\}$$

and

$$G(\mathbb{C}(x,t,t')/\mathbb{C}(x))^0 = \{ \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} : a \in \mathbb{C}\} \simeq \mathbb{G}_a$$

is abelian. However, $\int \sqrt{1-x^4}$ is not an elementary function.

BIBLIOGRAPHY

[1] Crespo, T., Hajto, Z., *Algebraic Groups and Differential Galois Theory*, American Mathemaical Society, United States 2011.

[2] Deligne, Pierre, Catégories Tannakiennes, *Grothendieck Festschrift vol II. Progress in Mathematics*, **87**(1990), no.9, 111-195.

[3] Deligne, P., Milne, J.S., *Tannakian Categories*, preprint(2012), available at `http://mtm.ufsc.br/~ebatista/2016-2/tannakian_categories.pdf` (accessed December 19, 2018).

[4] Humphreys, James E., *Linear Algebraic Groups*, Springer-Verlag, New York 1975.

[5] Magid, Andy R., *Lectures on Differential Galois Theory*, American Mathemaical Society, United States 1994.

[6] Magid, Andy R., Differential Galois Theory, *Notices of the AMS*, **46**(1999), no.9, 1041-1049.

[7] Malle, G., Testerman, D., *Linear Algebraic Groups and Finite Groups of Lie Type*, Cambridge University Press, Cambridge, 2011.

[8] Put, M., Singer M., *Galois Theory of Linear Differential Equations*, Springer, 2003

[9] Szamuely, Tamás, *Galois Groups and Fundamental Groups*, Cambridge Studies in Advanced Mathematics, 2003

[10] Waterhouse, William C. , *Introduction to Affine Group Schemes*, Springer-Verlag, New York 1979.