

Notes for Differential Galois Theory by P. Jossen

Texed by Lin-Da Xiao

November 4, 2017

Contents

1	Differential rings and modules	2
2	Picard-Vessiot extension	5
3	The Differential Galois Groups	10
4	Algebraic Group: A Detour	11
4.1	Application of the fact that differential Galois group is a algebraic group	15
5	The Galois-correspondence of differential equations	17
6	Local theory of differential equations	18
7	Personal Reads	23
7.1	D-module	23
7.2	Monodromy, Riemann-Hilbert Problem	24

About the Course

Classical Galois theory:

- Fields \mathcal{K}
- Fields extensions \mathcal{K}'/\mathcal{K} .
- $Gal(\mathcal{K}'/\mathcal{K}) = Aut_{\mathcal{K}}(\mathcal{K}')$.
- Solution of polynomials, $\mathcal{K}' = \text{"}\mathcal{K}(\text{solutions of polynomials})\text{"}$, which is what we call **splitting field**.

In the Differential setting,

- Fields \mathcal{K} with derivation ∂ , e.g. $\mathbb{Q}(t)$, with usual derivative:
- Differential field extension \mathcal{K}'/\mathcal{K}
- $Gal(\mathcal{K}'/\mathcal{K}) = Aut_{(\mathcal{K}, \partial)}(\mathcal{K}', \partial)$
- Solution of differential equations. $\mathcal{K}' = \text{"}\mathcal{K}(\text{solution of differential equation})\text{"}$, which is called **Picard-Vessiot Field**

1 Differential rings and modules

Convention: Ring= commutative ring with unit.

Definition 1.1. Let \mathcal{R} be a ring. A **derivation** on \mathcal{R} is a map $\partial : \mathcal{R} \rightarrow \mathcal{R}$ s.t.

1. $\partial(a + b) = \partial a + \partial b$,
2. $\partial(ab) = a\partial b + b\partial a$.

then we call (\mathcal{R}, ∂) a differential ring. A morphism of diff-rings $\varphi : (\mathcal{R}_1, \partial_1) \rightarrow (\mathcal{R}_2, \partial_2)$ is a ring morphism s.t. $\partial_2 \varphi = \varphi \partial_1$

Example 1.2. $\mathbb{Q}(t), \mathcal{K}(t)$ with usual derivations and $\mathbb{Q}[t], \mathcal{K}[t], C^\infty([0, 1])$

Definition 1.3. Let (\mathcal{R}, ∂) be a diff-ring, Call $\mathcal{C} \subset \mathcal{R}$ **constant** if $\partial c = 0, \forall c \in \mathcal{C}$.

Proposition 1.4. Let $\mathcal{C} \subset \mathcal{R}$ be the set of constant elements.

1. \mathcal{C} is a subring,

2. If \mathcal{R} is a field, then so is \mathcal{C}

Proof. $1 \in \mathcal{C}$, $\partial 1 = \partial(1 \cdot 1) = 2\partial 1 \implies \partial 1 = 0$

$a, b \in \mathcal{C} \implies a + b \in \mathcal{C}$, and $ab \in \mathcal{C}$ by Leibnitz rule.

Suppose \mathcal{R} is a field, $c \in \mathcal{C}$, $c \neq 0$, $0 = \partial 1 = \partial(c \cdot c^{-1}) = c\partial(c^{-1}) \implies \partial c^{-1} = 0 \quad \square$

Example 1.5. *Caution:* $\mathcal{R} = \mathbb{F}_p[t]$, ∂ is the usual derivative. Here, constant $\mathcal{C} = \mathbb{F}_p[t^p] \supsetneq \mathbb{F}_p$, because

$$\partial(a_0 + a_1 t^p + a_2 t^{2p} + \dots + a_n t^{np}) = 0.$$

Exercise 1.6. Show that $\mathcal{C} \subseteq \mathcal{R}$ is a algebraically closed in \mathcal{R} . i.e. $x \in \mathcal{R}$ algebraic over $\mathcal{C} \implies x \in \mathcal{C}$. (Notice it does not mean $\mathcal{C} = \overline{\mathcal{C}}$ in general)

Exercise 1.7. Show that for differential field \mathcal{K} with constants \mathcal{C} , consider a field extension \mathcal{R}/\mathcal{K} , an element $x \in \mathcal{R}$ satisfying $x' = 0 \in \mathcal{K}$ is algebraic over $\mathcal{K} \implies x$ is algebraic over \mathcal{C} .

Solution:

x is algebraic over \mathcal{K} , consider the minimal monic polynomial $p(X) = X^n + \dots + a_0$ with coefficients in \mathcal{K} . Then $p(x) = 0 \implies p(x)' = (a'_{n-1})x^{n-1} + \dots + (a'_0) = 0$ by the minimality of $p(X)$, we conclude that each $a'_i = 0$, thus finished the proof.

Definition 1.8. A **differential (\mathcal{R}, ∂) -module** (M, ∂) is a \mathcal{R} -module M , together with $\partial : M \rightarrow M$ satisfying:

$$1. \partial(m + n) = \partial m + \partial n$$

$$2. \partial_M(am) = \partial_{\mathcal{R}} a \cdot m + a \cdot \partial_M m.$$

Think of (M, ∂) as a differential equation, with solutions $\ker(\partial : M \rightarrow M)$.

Suppose $\mathcal{R} = \mathcal{K}$ is a field (over that M is free), M has finite dimension. Choose a \mathcal{K} -basis, (e_1, \dots, e_n) of M . Set

$$\partial e_i = - \sum_{j=1}^n a_{ij} e_j,$$

where $A = (a_{ij}) \in M_{n \times n}(\mathcal{K})$. The matrix A characterizes $\partial : M \rightarrow M$, uniquely, by additivity and Leibnitz:

$$m \in M, m = \sum_{i=1}^n \lambda_i e_i,$$

$$\begin{aligned}\partial m &= \sum \partial(\lambda_i e_i) = \sum (\partial \lambda_i) e_i + \sum \lambda_i \partial e_i \\ &= \sum (\partial \lambda_i) e_i - \sum \sum \lambda_i a_{ij} e_j.\end{aligned}$$

The differential equation corresponding to (M, ∂) is the equation

$$u' = Au.$$

Remark 1.9. *the matrix A depends on the choice of the \mathcal{K} -basis of M . Choosing a different basis yields an equation $u' = \tilde{A}u$ with $\tilde{A} = S^{-1}AS - S^{-1}S'$, where $S \in GL_n(\mathcal{K})$ is the base change matrix. we called A, \tilde{A} equivalent*

Remark 1.10. *Let M be a differential \mathcal{K} -module, $\mathcal{C} \subset \mathcal{K}$ be the set of constants, then we have $\partial : M \rightarrow M$. is \mathcal{C} -linear, follows from Leibnitz. In particular $\ker \partial \subseteq M$ is a \mathcal{C} -module (vector space)*

Lemma 1.11. *Let $u' = Au$ be a differential equation with $A \in M_{n \times n}(\mathcal{K})$. Let $v_1, \dots, v_r \in \mathcal{K}^n$ be solutions, i.e. $v'_i = Av_i$. If v_1, \dots, v_r are linear dependent over \mathcal{K} , then they are linear dependent over \mathcal{C} . In particular,*

$$\dim_{\mathcal{C}}(\ker \partial) \leq n.$$

Proof. Induction on r . For $r = 1$, trivial. Fix $r \geq 2$, suppose lemma holds for $< r$ solutions. Suppose w.l.o.g that no proper subset of $\{v_1, \dots, v_r\}$ is linear dependent over \mathcal{K} . We find that there is a unique linear dependence relation

$$v_1 = \sum_{i=2}^r b_i v_i, \quad b_i \in \mathcal{K}$$

$$\begin{aligned}0 &= v'_1 - Av_1 = \sum b'_i v_i + b_i v'_i - \sum_{i=2}^r b_i Av_i \\ &= \sum_{i=2}^r b'_i v_i + \sum_{i=2}^r b_i (v'_i - Av_i) = \sum_{i=2}^r b'_i v_i\end{aligned}$$

so $b'_i = 0$ for $i = 2, \dots, r \implies b_i \in \mathcal{C}$, and v_1, \dots, v_r linear dependent over \mathcal{C} . \square

Compactify the notation, v_1, \dots, v_r columns of a matrix $V \in M_{n \times r}(\mathcal{K})$, then $v'_i = Av_i \implies V' = AV$. Know that $\text{rank}_{\mathcal{C}} V \leq n$. What we usually seek is a $V \in GL_n(\mathcal{K})$ with $V' = AV$. The columns of such V provide a basis of the solution space of the differential equation and thus also a basis of the differential module itself.

Definition 1.12. \mathcal{K} is a diff-field, $A \in M_{n \times n}(\mathcal{K})$, let \mathcal{R} be a differential \mathcal{K} -algebra, which means we have a diff-ring morphism from $(\mathcal{R}, \partial_{\mathcal{R}})$ to $(\mathcal{K}, \partial_{\mathcal{K}})$. We also suppose \mathcal{R} has same constants as \mathcal{K} (every constant of \mathcal{R} lies in \mathcal{K}). A matrix $V \in GL_n(\mathcal{R})$ is said to be a **fundamental matrix** of solutions of the differential equation $u' = Au$, if $V' = AV$.

Remark 1.13. Let V, \tilde{V} be fundamental matrices of solutions of $u' = Au$, $V, \tilde{V} \in GL_n(\mathcal{R})$, $\tilde{V} = V \cdot S$ $S = V^{-1}\tilde{V}$

$$A\tilde{V} = \tilde{V}' = (VS)' = V'S + VS' = AVS + VS' = A\tilde{V} + VS'$$

$$\implies VS' = 0, V \text{ is invertible} \implies S' = 0 \implies S \in GL_n(C).$$

Definition 1.14. Let $v_1, \dots, v_n \in \mathcal{K}$, The **Wronski matrix** of $\underline{v} \in \mathcal{K}^n$ is

$$Wr(\underline{v}) = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1^{(1)} & v_2^{(1)} & \cdots & v_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ v_1^{(n-1)} & v_2^{(n-1)} & \cdots & v_n^{(n-1)} \end{pmatrix}$$

the **Wronskian** is the determinant of the Wronski matrix, i.e. $\det(Wr(\underline{v})) =: wr(\underline{v})$.

2 Picard-Vessiot extension

Through out this section, we will assume \mathcal{K} is a differential field with $\text{char}(\mathcal{K}) = 0$ (It contains \mathbb{Q} as subfield). The set of constants $\mathcal{C} \subset \mathcal{K}$ is a field and we assume it to be algebraic closed. For example, think of $\mathcal{K} = \mathbb{C}(t)$, $\partial = d/dt$ and $\mathcal{C} = \mathbb{C}$.

Definition 2.1. Let \mathcal{R} be a diff. \mathcal{K} -algebra. An ideal $I \subset \mathcal{R}$ is a **differential ideal** if $\partial I \subseteq I$. Say that \mathcal{R} is **simple** if $\{0\}$ and \mathcal{R} are the only differential ideal in \mathcal{R}

Remark 2.2. $I \subseteq \mathcal{R}$ is differential ideal, then the derivation on \mathcal{R} induces a derivation on \mathcal{R}/I . Given any morphism of diff. rings $\varphi: \mathcal{R} \longrightarrow \mathcal{R}'$, then $\text{Ker}(\varphi)$ is a differential ideal.

Definition 2.3. Let $A \in M_n(\mathcal{K})$, consider the matrix differential equation

$$u' = Au$$

A differential \mathcal{K} -algebra \mathcal{R} is said to be a **Picard-Vessiot extension** for $u' = Au$ if

1. \mathcal{R} is simple
2. The equation $u' = Au$ admits a fundamental matrix of solution in \mathcal{R} , i.e. $\exists V \in M_n(\mathcal{R})$, invertible such that

$$V' = AV.$$

3. As \mathcal{K} -algebra, \mathcal{R} is generated by the coefficients v_{ij} of V and $\det(V)^{-1}$.

Some references require in addition the constants of \mathcal{R} are \mathcal{C} . We will see this additional requirement can be derived by 1-3 in our setting.

A **Picard-Vessiot extension of a differential module** M is a Picard-Vessiot extension for any of the corresponding matrix differential equation.

Exercise 2.4. Check that any two differential equation corresponding to a same differential module give the same P-V extension.

Alternatively, we can define the Picard-Vessiot extension of a differential module M directly. Given a diff. module (M, ∂_M) , a Picard-Vessiot extension for (M, ∂_M) is a diff. \mathcal{K} -algebra \mathcal{R} s.t.

1. \mathcal{R} is simple
2. $\dim_{\mathcal{C}}(\text{Ker}(\partial_{\mathcal{R} \otimes M})) = \dim_{\mathcal{K}} M$, where $\partial_{\mathcal{R} \otimes M} : \mathcal{R} \otimes M \longrightarrow \mathcal{R} \otimes M$, $\partial_{\mathcal{R} \otimes M}(r \otimes m) = r' \otimes m + r \otimes \partial_M m$.
3. \mathcal{R} is minimal with these properties.

Exercise 2.5. Check that the two definitions of PV extension for diff. module coincide.

Example 2.6. $\mathcal{K} = \mathbb{C}(t), \mathcal{C} = \mathbb{C}$, Consider the 2nd order homogeneous linear differential equation

$$t \cdot u'' + u' = 0.$$

We can set $v := u', v' = u''$, then we have a new 1st order

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & -1/t \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix},$$

where the matrix is called **companion matrix**. What we want is $\mathcal{R} \supseteq \mathbb{C}(t), V \in GL_2(\mathcal{R})$ s.t. $V' = AV$. The general solution of the 2nd order equation is

$$a + b \log(t).$$

Solution to $(u', v')^T = A \cdot (u, v)^T$ are

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \log(t) \\ 1/t \end{pmatrix},$$

The corresponding fundamental matrix

$$V = \begin{pmatrix} 1 & \log(t) \\ 0 & 1/t \end{pmatrix}.$$

A candidate of the Picard-Vessiot ring is

$$\mathcal{R} = \mathbb{C}(t)[X]$$

the Differential on \mathcal{R} , we just need to set $\partial X = X' = 1/t$, in this case, we don't have to adjoint $\det(V)^{-1}$. The only thing left to check is whether \mathcal{R} is simple.

Yes, $I \subseteq \mathcal{R}$ diff. ideal. \mathcal{R} principal $I = f(X)\mathcal{R}$, $\partial I \subset I$, where $\partial I = (\partial f)\mathcal{R}$, derive it sufficiently many times. until $\partial^n f \in \mathbb{C}(t) \implies \mathcal{R} = \partial^n f \mathcal{R} \subseteq I$.

Lemma 2.7. *Let \mathcal{R} be simple diff. \mathcal{K} -algebra. Then*

1. \mathcal{R} is integral domain
2. Suppose \mathcal{R} is finitely generated as \mathcal{K} -algebra, then $\text{Frac}(\mathcal{R}) = \mathcal{L}$ is a differential field with constants equal to \mathcal{C} .

Proof. The proof of the second part relies on the assumption that \mathcal{C} is algebraic closed, we will postpone it a little.

Proof of (1) Pick $a \in \mathcal{R}$ and $a \neq 0$. Consider the ideal $I = \{b \in \mathcal{R} | a^n \cdot b = 0, \text{ for some } n \geq 1\}$. This is a differential ideal. (Check it by derive it and multiply it with a) If a is not nilpotent, then $1 \notin I$ then I has to be $\{0\}$, so a is not a zero divisor. It follows that if a is a zero divisor, then a has to be nilpotent.

Let $I \subset \mathcal{R}$ be the nil radical of \mathcal{R} . Again, I is a diff. ideal. But $1 \notin I$, I has to be $\{0\}$. \square

Lemma 2.8. *(Criterion for Algebraicity) Let \mathcal{K} be a field of char 0. \mathcal{R} is a finitely generated \mathcal{K} -algebra, integral domain, and suppose that $x \in \mathcal{R}$ is such that the set $S := \{c \in \mathcal{K} | x - c \in \mathcal{R}^\times\}$ is infinite. Then x is algebraic over \mathcal{K} .*

For example $\mathcal{K} = \bar{\mathbb{Q}}$, $\mathcal{R} = \bar{\mathbb{Q}}[x, y, 1/x, 1/(x^2 + 2)]$. For $x - c$ to be unit, then only possibility is $c = 0$, which means x is not algebraic over $\bar{\mathbb{Q}}$. While in the case $\mathcal{K} = \mathbb{Q}$, $\mathcal{R} = \mathbb{Q}[\sqrt{2}]$, $\sqrt{2} - c$ is always unit in \mathcal{R}^\times , which means $\sqrt{2}$ is algebraic over \mathbb{Q} .

Proof. Say $\mathcal{R} = \mathcal{K}[x_1, \dots, x_n]$ and w.l.o.g. $x_1 = x$. Set $\mathcal{L} = \text{Frac}(\mathcal{R})$ (\mathcal{R} is integral domain), suppose x is **not** algebraic over \mathcal{K} , so x is transcendental. Suppose w.l.o.g. that Reorder x_2, \dots, x_n such that x_1, \dots, x_r are a transcendence base for \mathcal{L}/\mathcal{K} , i.e. x_1, \dots, x_r are algebraic independent and $\mathcal{L}/\mathcal{K}(x_1, \dots, x_r)$ is a finite algebraic extension. Recall the [Lemma of primitive element](#) (every finite field extension of char 0, can be generated by one element). Pick $y \in \mathcal{R}$ such that $\mathcal{L} = \mathcal{K}(x_1, \dots, x_r)[y]$, look at the minimal polynomial of y over $\mathcal{K}[x_1, \dots, x_r]$

$$a_N(x_1, \dots, x_r)T^N + a_{N-1}(x_1, \dots, x_r)T^{N-1} + \dots,$$

where $a_i \in \mathcal{K}[x_1, \dots, x_r]$

Pick $G \in \mathcal{K}[x_1, \dots, x_r]$ s.t.

1) $a_N | G$ and

2) $x_1, \dots, x_n \in \mathcal{K}[x_1, \dots, x_r, y, G^{-1}]$

For $s > r$, $x_s \in \mathcal{R} \subseteq \mathcal{L} = \text{Frac}(\mathcal{K}[x_1, \dots, x_r])[y]$

$$x_s = \frac{P_s(x_1, \dots, x_r, y)}{Q_s(x_1, \dots, x_r)} = \frac{\tilde{P}_s(x_1, \dots, x_r, y)}{G}$$

G has to be a multiple of all those denominators Q_s , it is always possible to pick such a G .

Since the set $S \subseteq \mathcal{K}$ is infinite, we can find $s_1, \dots, s_r \in S$ with $G(s_1, \dots, s_r) \neq 0$. Fix such elements $s_1, \dots, s_r \in S$, we can define a ring homomorphism $\mathcal{K}[x_1, \dots, x_r, y, G^{-1}] \xrightarrow{\varphi} \bar{\mathcal{K}}$ where $x_i \mapsto s_i$, $y \mapsto$ any root of the minimal polynomial evaluated in s_i . $a_N(s_1, \dots, s_r)T^N + \dots$ and $G^{-1} \mapsto G(s_1, \dots, s_r)^{-1}$. since $G(s_1, \dots, s_r) \neq 0$ also we have $a_N(s_1, \dots, s_r) \neq 0$ (The minimal polynomial of y with coefficients evaluated in s_i indeed has nontrivial roots in $\bar{\mathcal{K}}$). The ring homomorphism is well-defined and $\mathcal{R} \subseteq \mathcal{K}[x_1, \dots, x_r, y, G^{-1}]$ $\varphi(x_1 - s_s) = 0$, where $(x_1 - s_s)$ is invertible in \mathcal{R} , which makes the contradiction. \square

Lemma 2.9. (Second half of Lemma 2.7) \mathcal{K} is a differential field and \mathcal{C} is the field of constant, $\mathcal{C} = \bar{\mathcal{C}}$ and $\text{char} \mathcal{C} = 0$. \mathcal{R}/\mathcal{K} simple differential ring which is finitely generated as \mathcal{K} -algebra. \implies the field of constants of \mathcal{R} is \mathcal{C} .

Proof. We already know \mathcal{R} is an integral domain. Let $\mathcal{L} = \text{Frac}(\mathcal{R})$, fix $a \in \mathcal{L}, a \neq 0, a' = 0$. Suppose $a \notin \mathcal{C}$, consider the ideal $I := \{b \in \mathcal{R} | a \cdot b \in \mathcal{R}\} \subseteq \mathcal{R}$. This is a differential ideal because $b \in I \implies ab' = a'b + ab' = (ab)' \in \mathcal{R}$. By the assumption \mathcal{R} is simple differential ring $\implies I = \mathcal{R}$. Then $1 \in I \implies a \cdot 1 \in \mathcal{R}$. a has an inverse in \mathcal{L} , denote it by c . Then $e \neq 0, e' = 0$ we can proceed the similar construction $J := \{b \in \mathcal{R} | e \cdot b \in \mathcal{R}\} \subseteq \mathcal{R}$ it also indicates that $e \in \mathcal{R}$, hence we get the conclusion that $a \in \mathcal{R}^\times$

Same argument for $a + c$ for any $c \in \mathcal{C}$ shows $(a + c) \in \mathcal{R}^\times, \forall c \in \mathcal{C} \implies a$ is algebraic over $\mathcal{K} \xrightarrow{\text{Exercise 1.7}} a$ is algebraic over $\mathcal{C} = \overline{\mathcal{C}} \implies a \in \mathcal{C}$ \square

Proposition 2.10. \mathcal{K} is a differential field with constants $\mathcal{C} = \overline{\mathcal{C}}$ Let $u' = Au$ be a matrix differential equation over \mathcal{K} .

- (1) A Picard-Vessiot extension for $u' = Au$ exists.
- (2) Any two P-V extension for $u' = Au$ are isomorphic.
- (3) The field of constant of any P-V extension is $\mathcal{C} = \overline{\mathcal{C}}$

Proof. The previous Lemma \implies (3)

For (1) consider the ring $\mathcal{R}_0 = \mathcal{K}[(X_{ij})_{1 \leq i, j \leq n}, \det(X)^{-1}]$. Define a differentiation on \mathcal{R}_0 by

$$X' = AX$$

$$X'_{ij} = (AX)_{ij} \text{ a polynomial in } \mathcal{K}[X_{ij}, \dots, X_{nn}]$$

and together with the Leibnitz rule it is a well-defined differentiation on \mathcal{R}_0 .

Pick any maximal differential ideal $I \subseteq \mathcal{R}_0$ and set $\mathcal{R} = \mathcal{R}_0/I$. \mathcal{R} is a P-V ring:

Simple because I is maximal.

Fundamental matrix of solutions is X (the classes of X in \mathcal{R}_0/I)

\mathcal{R} is generated by X_{ij} and $\det(X)^{-1}$.

For (2) Let $\mathcal{R}_1, \mathcal{R}_2$ be P-V rings. Consider $\mathcal{R} = \mathcal{R}_1 \otimes \mathcal{R}_2$ with differential $(a \otimes b)' = a' \otimes b + a \otimes b'$. Choose $I \subseteq \mathcal{R}$ maximal differential ideal. Consider $\varphi_1 : \mathcal{R}_1 \longrightarrow \mathcal{R}/I | \varphi_1(a) = a \otimes 1$ and $\varphi_2 : \mathcal{R}_2 \longrightarrow \mathcal{R}/I | \varphi_2(1) = 1 \otimes b$. φ_1 and φ_2 are morphism of differential rings and since $\mathcal{R}_1, \mathcal{R}_2$ are simple, φ_1, φ_2 are injective. Let $V_1 \in M_n(\mathcal{R}_1), V_2 \in M_n(\mathcal{R}_2)$ be fundamental matrices of solution of $u' = Au$. $\varphi_1(V_1)$ and $\varphi_2(V_2)$ are fundamental matrices of solution in \mathcal{R}/I . \mathcal{R}/I is simple finitely generated \implies constants in \mathcal{R}/I are \mathcal{C} . $\exists S \in GL_n(\mathcal{C})$ with $\varphi_1(V_1) = \varphi_2(V_2)S$

$\varphi_1(\mathcal{R}_1)$ is isomorphic to the algebra in \mathcal{R}/I generated by $\varphi_1(V_{1,ij})$ and $\varphi_1(\det(V_1))^{-1}$ = the algebra in \mathcal{R}/I generated by $\varphi_2(V_{2,ij})$ and $\varphi_2(\det(V_2))^{-1}$ $\cong \varphi_2(\mathcal{R}_2)$

Then $\mathcal{R}_1 \cong \varphi_1(\mathcal{R}_1) = \varphi_2(\mathcal{R}_2) \cong \mathcal{R}_2$ \square

3 The Differential Galois Groups

Assumption: \mathcal{K} - differential field with $\text{char} 0$, \mathcal{C} is the set of constants in \mathcal{K} and $\mathcal{C} = \overline{\mathcal{C}}$.

Definition 3.1. Let \mathcal{R} be a Picard-Vessiot ring of a differential equation $u' = Au$ or of a differential module (M, ∂) over \mathcal{K} . We call **Galois group of the equation/ module** the group $\text{Aut}^\partial(\mathcal{R}/\mathcal{K}) = \{\mathcal{K}\text{-algebra isomorphism } \varphi : \mathcal{R} \rightarrow \mathcal{R} \text{ compatible with the differentiations}\}$. Usually we denote it with $\text{Gal}^\partial(\mathcal{R}/\mathcal{K})$

Exercise 3.2. Let \mathcal{L}/\mathcal{K} be a finite Galois extension.

- (1) There is unique differentiation on \mathcal{L} extending that of \mathcal{K} .
- (2) Look at \mathcal{L} as a \mathcal{K} -module (differential module), Then a Picard-Vessiot extension fo \mathcal{L} is \mathcal{L} as a \mathcal{K} -algebra.
- (3) $\text{Gal}^\partial(\mathcal{L}/\mathcal{K}) = \text{Gal}(\mathcal{L}/\mathcal{K})$

$\text{Gal}^\partial(\mathcal{R}/\mathcal{K})$ can be seen as a subgroup of $GL_n(\mathcal{C})$. Let $V \in GL_n(\mathcal{R})$ be a fundamental matrix of solutions. Pick $g \in G = \text{Gal}^\partial(\mathcal{R}/\mathcal{K})$. then $gV = g(v_{ij})$ is again a fundamental matrix of solutions.

$$(gV)' = gV' = gAV = A(gV)$$

$$g(V) = V \cdot \gamma(g)$$

$\gamma \in GL_n(\mathcal{C})$ is unique, because two fundamental matrices are linked with a unique matrix in $GL_n(\mathcal{C})$ (Remark 1.13). Then we get a group homomorphism:

$$\begin{aligned} \gamma : G &\hookrightarrow GL_n(\mathcal{C}) \\ g &\longmapsto \gamma(g) \end{aligned}$$

It is injective: $\gamma(g) = \mathbb{1} \implies gV = V$, but \mathcal{R} is generated by entries of $V \implies g = \text{id}_{\mathcal{R}} = \mathbb{1}_G$.

What makes differential Galois groups a powerful tool is that they are linear algebraic groups and, moreover, establish a Galois correspondence, analogous to the classical Galois correspondence. Torsors will explain the connection between the Picard-Vessiot ring and the differential Galois group. The Tannakian approach to linear differential equations provides new insight and useful methods. Some of this is rather technical in nature. We will try to explain theorems and proofs on various levels of abstraction.

Example 3.3. $\mathcal{K} = \mathbb{C}(t), \mathcal{C} = \mathbb{C} \quad u' = Au$

$$A = \begin{pmatrix} 0 & 1 \\ 0 & -1/t \end{pmatrix}$$

$X := \log(t)$. The Picard-Vessiot ring $\mathcal{R} = \mathbb{C}(t)[X]$, with differential defined by $X' = \frac{1}{t} + \text{Leibnitz}$. $\text{Aut}^\partial(\mathcal{R}/\mathcal{K}) \ni g$, the action of g is $\mathbb{C}(t)$ -linear.

$$\begin{aligned} g : \mathbb{C}(t)[X] &\Longrightarrow \mathbb{C}(t)[X] \\ X &\longmapsto g(X) \end{aligned}$$

It is compatible with the differentiation

$$\begin{aligned} g(X)' &= g(X') = g(1/t) = 1/t \\ g(X) &= X + a, \quad a \in \mathbb{C} \end{aligned}$$

For a fundamental matrix

$$V = \begin{pmatrix} 1 & X \\ 0 & 1/t \end{pmatrix}$$

$$g(V) = \begin{pmatrix} 1 & X+a \\ 0 & 1/t \end{pmatrix} = \begin{pmatrix} 1 & X \\ 0 & 1/t \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

Then

$$\text{Gal}^\partial(\mathcal{R}/\mathcal{K}) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{C} \right\} \cong (\mathbb{C}, +)$$

4 Algebraic Group: A Detour

Last week, we introduced differential Galois group, where \mathcal{K} is a differential field with algebraic closed constants $\mathcal{C} = \overline{\mathcal{C}}$. And the Picard-Vessiot extension (for equation or module). $\text{Gal}(\mathcal{R}/\mathcal{K}) = \text{Aut}_{\mathcal{K}}^\partial(\mathcal{R})$. If $F \in GL_n(\mathcal{R})$ is a fundamental matrix, $g \in \text{Gal}(\mathcal{R}/\mathcal{K})$, then gF is again a fundamental matrix,

hence of the form $gF = F\gamma(g)$, where $\gamma(g) \in GL_n(\mathcal{C})$. Then we obtain the embedding of $Gal(\mathcal{R}/\mathcal{K}) \xrightarrow{\gamma} GL_n(\mathcal{C})$.

Intrinsic variant:

If \mathcal{R} is the Picard-Vessiot extension associated to a differential module M , then the $Gal(\mathcal{R}/\mathcal{K})$ acts on $\mathcal{R} \otimes M$ and leaves

$$V = Ker(\mathcal{R} \otimes M \xrightarrow{\partial} \mathcal{R} \otimes M)$$

invariant, notice that the action is \mathcal{C} -linear on V . Which says $Gal(\mathcal{R}/\mathcal{K})$ acts on V , get

$$\gamma : Gal \hookrightarrow GL(V)$$

Exercise 4.1. \mathcal{R} is the Picard-Vessiot extension of \mathcal{K} . $\mathcal{L} := Frac(\mathcal{R})$, show that

$$Aut_{\mathcal{K}}^{\partial}(\mathcal{L}) = Aut_{\mathcal{K}}^{\partial}(\mathcal{R}) = Gal(\mathcal{R}/\mathcal{K})$$

Proof. Consider the group $Gal(\mathcal{L}/\mathcal{K})$ consisting of the \mathcal{K} -linear automorphism on \mathcal{L} , commuting with the differential on \mathcal{L} . Each $\sigma \in Gal(\mathcal{R}/\mathcal{K})$ extends to a unique element $\tilde{\sigma} \in Gal(\mathcal{L}/\mathcal{K})$ by $\tilde{\sigma}\left(\frac{u}{v}\right) = \frac{\sigma(u)}{\sigma(v)}$ and

$$\partial_{\mathcal{L}}\left(\tilde{\sigma}\left(\frac{u}{v}\right)\right) = \frac{\partial_{\mathcal{R}}(\sigma(u))\sigma(v) - \partial_{\mathcal{R}}(\sigma(v))\sigma(u)}{\sigma(v)^2} = \tilde{\sigma}\left(\frac{u'v - v'u}{v^2}\right) = \tilde{\sigma}\left(\partial_{\mathcal{L}}\left(\frac{u}{v}\right)\right)$$

There is an injective homomorphism $\varphi : Gal(\mathcal{R}/\mathcal{K}) \longrightarrow Gal(\mathcal{L}/\mathcal{K}) : \sigma \mapsto \tilde{\sigma}$. φ is in fact an bijective homomorphism because $\sigma = \tilde{\sigma}|_{\mathcal{R}}$ \square

Definition 4.2. A subgroup $G \subseteq GL_n(\mathcal{C})$ is **algebraic** if there exists polynomials $f_1, \dots, f_N \in \mathcal{C}[x_{11}, \dots, x_{nn}, det(X)^{-1}]$ such that $G = \{g \in GL_n(\mathcal{C}) | f_i(g) = 0 \forall i = 1, \dots, N\}$.

Alternatively, because $\mathcal{C}[X, \dots, X]$ is Noetherian:

Definition 4.3. A subgroup $G \subseteq GL_n(\mathcal{C})$ is **algebraic** if there exists an ideal $\mathcal{I} \subset \mathcal{C}[x_{11}, \dots, x_{nn}, det(X)^{-1}]$ s.t. $G = \{g \in GL_n(\mathcal{C}) | f(g) = 0, \forall f \in \mathcal{I}\}$. One can suppose that $\mathcal{I} = \sqrt{\mathcal{I}} = \{f | f^N \in \mathcal{I}\}$.

Example 4.4.

- $G = GL_2(\mathcal{C}), \mathcal{I} = \{0\}$
- $SL_2(\mathcal{C}), \mathcal{I} = \langle X_{11}X_{22} - X_{12}X_{21} - 1 \rangle$

•

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

$$\mathcal{I} = \langle X_{21}, X_{11} - 1, X_{22} - 1 \rangle$$

FACT:

$G = GL_n(\mathcal{C})$ algebraic, then G is the zero set of the ideal $\{f \in \mathcal{C}[X_{11}, \dots, X_{nn}, \det(X)^{-1}] \mid f(g) = 0, \forall g \in G\}$, i.e. $G = \{g \in GL_n(\mathcal{C}) \mid f(g) = 0 \forall f \in \mathcal{I}\}$. This is what we call **Hilbert Nullstellensatz** (\mathcal{C} is algebraically closed.)

Consider the algebra $\mathcal{O}_G = \mathcal{A} = \mathcal{C}[X_{11}, \dots, X_{nn}, \det(X)^{-1}]/\mathcal{I}$, where we assume $\mathcal{I} = \sqrt{\mathcal{I}}$ is called **algebra of regular functions** on G . Given $a \in \mathcal{A}, a = [f], f \in \mathcal{C}[X_{11}, \dots]$ s.t.

$$\begin{aligned} G &\subseteq GL_n(\mathcal{C}) \longrightarrow \mathcal{C} \\ g &\mapsto G \mapsto f(g) \end{aligned}$$

only depends on a .

Theorem 4.5. *Let \mathcal{R}/\mathcal{K} be a Picard-Vessiot extension with Galois group G . The group G , as a subgroup of $GL_n(\mathcal{C})$, is an algebraic group.*

Proof. (Singer Page 20) W.L.O.G, suppose \mathcal{R} is the P-V ring of an equation $u' = Au$, $A \in M_n(\mathcal{K})$. $\mathcal{R} = \mathcal{R}_0/\mathcal{I}$, where $\mathcal{R}_0 = \mathcal{K}[X_{11}, \dots, X_{nn}, \det(X)^{-1}]$, $X' = AX$. $\mathcal{I} \subseteq \mathcal{R}_0$ maximal differential ideal. Choose generators h_1, \dots, h_N of $\mathcal{I} \subseteq \mathcal{R}_0$. Choose $(e_s)_{s \in S}$ a \mathcal{C} -basis of \mathcal{R} . Can identify the $G \subseteq GL_n(\mathcal{C})$ with the group of matrices M for which

$$\begin{aligned} \sigma_M : \mathcal{R}_0 &\longrightarrow \mathcal{R}_0 \\ X_{ij} &\longmapsto (X \cdot M)_{ij} \end{aligned}$$

sends \mathcal{I} to \mathcal{I} . Write $\sigma_M(h_i) \bmod \mathcal{I} = \sum_{s \in S} c_{i,s}(M)e_s$, where $c_{i,s}(M)$ is uniquely determined.

Claim: $c_{is}(M)$ is a polynomial expression in the coefficients $M_{ij}, \det(M)^{-1}$. i.e. $\exists c_{is}(-) \in \mathcal{C}[Y_{11}, \dots, Y_{nn}, \det(Y)^{-1}]$. Knowing this,

$$G = \{M \in GL_n(\mathcal{C}) \mid c_{is}(M) = 0 \forall i, s\}$$

= zero set of the ideal generated by $\{c_{is}(Y) \in \mathcal{C}[Y_{11}, \dots, \det(Y)^{-1}], \forall i, s\}$.

Verification of claim, For a \mathcal{C} -algebra \mathcal{B} , set $\mathcal{B} \otimes_{\mathcal{C}} \mathcal{K}$ and $\mathcal{B} \otimes_{\mathcal{C}} \mathcal{R}$ to be the differential ring with the differentiation defined by $\partial_{\mathcal{B} \otimes_{\mathcal{C}} \mathcal{R}}(b \otimes x)' = b \otimes x'$. Then

we can define the group $G(\mathcal{B})$ to be the group of $\mathcal{B} \otimes_{\mathcal{C}} \mathcal{K}$ -linear automorphism of $\mathcal{B} \otimes_{\mathcal{C}} \mathcal{R}$ which commutating with the differentiation $\partial_{\mathcal{B} \otimes \mathcal{R}}$.

Alternatively, notice that $\mathcal{B} \otimes_{\mathcal{C}} \mathcal{R}$ is in fact a \mathcal{B} -algebra. $G(\mathcal{B})$ is the group of these matrices $M \in GL_n(\mathcal{B})$ s.t.

$$\begin{aligned}\sigma_M : \mathcal{B} \otimes \mathcal{R}_0 &\longrightarrow \mathcal{B} \otimes \mathcal{R}_0 \\ (X)_{ij} &\longmapsto (XM)_{ij}\end{aligned}$$

sending $\mathcal{B} \otimes \mathcal{I}$ to $\mathcal{B} \otimes \mathcal{I}$ ($\mathcal{B} \otimes_{\mathcal{C}} \mathcal{I}$ is the maximal differential ideal in $\mathcal{B} \otimes_{\mathcal{C}} \mathcal{R}_0$).

Given a morphism of \mathcal{C} -algebras: $\mathcal{B}_1 \xrightarrow{\varphi} \mathcal{B}_2$, we get a group homomorphism

$$\begin{aligned}G(\mathcal{B}_1) &\longrightarrow G(\mathcal{B}_2) \\ M &\longmapsto \varphi(M)\end{aligned}$$

Notice:

$$\begin{array}{ccc}\mathcal{B}_1 \otimes \mathcal{R}_0 & \xrightarrow{\sigma_M} & \mathcal{B}_1 \otimes \mathcal{R}_0 \\ \downarrow \varphi & & \downarrow \varphi \\ \mathcal{B}_2 \otimes \mathcal{R}_0 & \xrightarrow{\sigma_{\varphi(M)}} & \mathcal{B}_2 \otimes \mathcal{R}_0\end{array}$$

commutes.

For $M \in GL_n(\mathcal{B})$ have $\sigma_M(1 \otimes h_i) \bmod \mathcal{B} \otimes \mathcal{I} = \sum_{s \in S} c_{is}(M) e_s$ $c_{is} \in \mathcal{B}$ unique. Given a morphism $\varphi : \mathcal{B} = \mathcal{B}_1 \longrightarrow \mathcal{B}_2$, get: Apply φ to relation, or consider relation for $\varphi(M)$, get $\varphi(c_{is}(M)) = c_{is}(\varphi(M))$. Consider the special case $\mathcal{B} = \mathcal{C}[Y_{11}, \dots, Y_{nn}, \det(Y)^{-1}] \xrightarrow{\varphi} \mathcal{C} : Y \mapsto M$. By the previous result we have $c_{is}(M) = c_{is}(\varphi(Y)) = \varphi(c_{is}(Y))$.

These prove the claim thus conclude the proof that differential Galois group is a algebraic group. \square

Back to the algebraic groups. Let $G \subseteq GL_n(\mathcal{C})$ be an algebraic group (or affine group scheme), with the defining ideal $\mathcal{I} = \sqrt{\mathcal{I}}$ and algebra of regular functions $\mathcal{A} = \mathcal{C}[X_{11}, \dots, X_{nn}, \det(X)^{-1}]/\mathcal{I}$ (A Hopf algebra). We have an canonical isomorphism of groups:

$$\begin{aligned}G &= Hom_{\mathcal{C}}(\mathcal{A}, \mathcal{C}) \\ g \in G &\longmapsto [ev_g : \mathcal{A} \longrightarrow \mathcal{C} | f \mapsto f(g)] \\ \varphi(X) &\longleftarrow [\varphi : \mathcal{A} \longrightarrow \mathcal{C}]\end{aligned}$$

This renders $Hom_{\mathcal{C}}(\mathcal{A}, \mathcal{C})$ a group.

For a \mathcal{C} -algebra \mathcal{B} , consider $G(\mathcal{B}) = \text{Hom}_{\mathcal{C}}(\mathcal{A}, \mathcal{B}) \hookrightarrow GL_n(\mathcal{B}) : \varphi \mapsto \varphi(X)$.

FACT: $G(\mathcal{B}) \subseteq GL_n(\mathcal{B})$ is a subgroup.

Explanation: Consider the following algebra morphisms:

$$\mathcal{C}[X_{11}, \dots, \det^{-1}] \longrightarrow \mathcal{C}[Y_{ij}, \det(Y)^{-1}] \otimes \mathcal{C}[Z_{ij}, \det(Z)^{-1}] = \mathcal{C}[Y_{ij}, Z_{ij}, \det(Y)^{-1}, \det(Z)^{-1}]$$

$$\{\text{Polynomial functions: } GL_n(\mathcal{C}) \longrightarrow \mathcal{C}\} \longrightarrow \{\text{Polynomial functions: } GL_n(\mathcal{C}) \times GL_n(\mathcal{C}) \longrightarrow \mathcal{C}\}$$

$$\mu : f \longmapsto [(y, z) \mapsto f(y \cdot z)]$$

$$\mu : I_x \longmapsto I_y \otimes I_z$$

and finally, we get

$$\mu : \mathcal{A} \longrightarrow \mathcal{A} \otimes_{\mathcal{C}} \mathcal{A}$$

where we have constructed the comultiplication explicitly.

Get from μ a composition law on $\text{Hom}_{\mathcal{C}}(\mathcal{A}, \mathcal{B})$, For $\varphi, \psi \in \text{Hom}_{\mathcal{C}}(\mathcal{A}, \mathcal{B})$, define $\varphi \cdot \psi$ as

$$\mathcal{A} \xrightarrow{\mu} \mathcal{A} \otimes \mathcal{A} \xrightarrow{\varphi \otimes \psi} \mathcal{B} \otimes \mathcal{B} \xrightarrow{\text{multiplication}} \mathcal{B}$$

This is compatible with the group law in $GL_n(\mathcal{B}) \supseteq G(\mathcal{B}) = \text{Hom}_{\mathcal{C}}(\mathcal{A}, \mathcal{B})$.

\mathcal{A} is a **Hopf Algebra**.

Then the algebraic group G defines a functor $G\{\mathcal{C}\text{-algebra}\} \longrightarrow \{\text{Groups}\}$, $\mathcal{B} \longmapsto G(\mathcal{B}) = \text{Hom}_{\mathcal{C}}(\mathcal{A}, \mathcal{B})$. I.e. the group functor is represented by $\text{Hom}_{\mathcal{C}}(\mathcal{A}, _)$.

Definition 4.6. A representable functor $G\{\mathcal{C}\text{-algebra}\} \longrightarrow \{\text{Groups}\}$, $\mathcal{B} \longmapsto G(\mathcal{B}) = \text{Hom}_{\mathcal{C}}(\mathcal{A}, \mathcal{B})$ for some unique Hopf algebra \mathcal{A} . is called an **Affine group scheme**. $G = \text{Spec}(\mathcal{A})$. Moreover, if \mathcal{A} is finitely generated, then we call G a **linear algebraic group over \mathcal{C}** . (Which means it can be embedded as a subgroup in $GL_n(\mathcal{C})$ for some n , for a reference that it has a faithful finite dimensional representation, see Milne page 72)

4.1 Application of the fact that differential Galois group is a algebraic group

Last week: \mathcal{R}/\mathcal{K} Picard-Vessiot extension with Galois group $G \subseteq GL_n(\mathcal{C})$. The main message of last week is that G is a algebraic group. you can see it in different ways.

$$G = \text{Spec}(\mathcal{A}),$$

where \mathcal{A} is a Hopf Algebra. Or equivalently, we can see G as a functor:

$$\{\mathcal{C} - \text{algebra}\} \longrightarrow \{\text{Groups}\}$$

$$\mathcal{B} \longmapsto G(\mathcal{B}) = \text{Hom}_{\mathcal{C}\text{-Alg}}(\mathcal{A}, \mathcal{B}).$$

Call **dimension** of G the transcendence degree of \mathcal{A} over \mathcal{C} .

$$\dim(G) \leq n^2$$

This notion of dimension coincides with the intuitive ideas, and with actual dimension as a complex variety if $\mathcal{C} = \mathbb{C}$.

Denote by $G_{\mathcal{K}}$ the base-change of G to \mathcal{K} , i.e.

$$G_{\mathcal{K}} = \text{Spec}(\mathcal{K} \otimes_{\mathcal{C}} \mathcal{A})$$

where $\mathcal{K} \otimes_{\mathcal{C}} \mathcal{A}$ is a Hopf algebra over \mathcal{K} and then $G_{\mathcal{K}}$ defines a functor:

$$\{\mathcal{K} - \text{algebras}\} \longrightarrow \{\text{Groups}\}$$

$$\mathcal{L} \longmapsto \text{Hom}_{\mathcal{K}}(\mathcal{K} \otimes \mathcal{A}, \mathcal{L}) = \text{Hom}_{\mathcal{C}}(\mathcal{A}, \mathcal{L}),$$

where we have the last line because $\text{Hom}_{\mathcal{K}}(\mathcal{K} \otimes_{\mathcal{C}} \mathcal{A}, \mathcal{L}) = \text{Hom}_{\mathcal{C}}(\mathcal{A}, \text{Hom}_{\mathcal{K}}(\mathcal{K}, \mathcal{L}))$.

Set $X = \text{Spec}(\mathcal{R})$, and consider it as a functor from \mathcal{K} -algebra to sets:

$$\{\mathcal{K} - \text{alg}\} \longrightarrow \{\text{Sets}\}$$

$$\mathcal{L} \longmapsto \text{Hom}_{\mathcal{K}}(\mathcal{R}, \mathcal{L})$$

and in fact, for every \mathcal{K} -algebra \mathcal{L} , the group $G_{\mathcal{K}}(\mathcal{L})$ acts on the set $X(\mathcal{L})$

$$\begin{array}{ccc} G_{\mathcal{K}}(\mathcal{L}) \times X(\mathcal{L}) & \longrightarrow & X(\mathcal{L}) \\ \parallel & & \parallel \\ \text{Hom}_{\mathcal{C}}(\mathcal{A}, \mathcal{L}) \times \text{Hom}_{\mathcal{K}}(\mathcal{R}, \mathcal{L}) & \longrightarrow & \text{Hom}_{\mathcal{K}}(\mathcal{R}, \mathcal{L}) \\ \parallel & & \parallel \\ G(\mathcal{L}) \times \text{Hom}_{\mathcal{L}}(\mathcal{R} \otimes \mathcal{L}, \mathcal{L}) & \longrightarrow & \text{Hom}_{\mathcal{L}}(\mathcal{R} \otimes \mathcal{L}, \mathcal{L}) \end{array}$$

where $G(\mathcal{L}) = \text{Aut}(\mathcal{R} \otimes_{\mathcal{K}} \mathcal{L} |_{\mathcal{L}})$

$$(g, x) \longmapsto [\mathcal{R} \otimes \mathcal{L} \xrightarrow{g} \mathcal{R} \otimes \mathcal{L} \xrightarrow{x} \mathcal{L}]$$

This action is natural in \mathcal{L} , An action of the algebraic group G on the algebraic variety X .

Theorem 4.7. For every \mathcal{K} -algebra \mathcal{L} either $X(\mathcal{L}) = \emptyset$ or $G(\mathcal{L})$ acts simply transitively on $X(\mathcal{L})$. In other words:

$$\begin{aligned} G \times X &\longrightarrow G \times X \\ (g, x) &\longmapsto (g, gx) \end{aligned}$$

is a bijection for all \mathcal{L} , i.e. an isomorphism of functors or an isomorphism of affine algebra varieties. X is a G -torsor.

Corollary 4.8. $\dim_{\mathcal{C}}(G) = \dim_{\mathcal{K}}(G_{\mathcal{K}}) = \dim_{\mathcal{K}}(X) = \text{tr.deg}(\mathcal{R}/\mathcal{K})$

Example 4.9. As an illustration: $\mathcal{K} = \mathbb{C}(t), \mathcal{R} = \mathbb{C}(1, \log(t))$. remember that

$$G = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

and $\dim(G) = 1$, then $\text{tr.deg}(\mathbb{C}(t, \log(t))) = 1 \implies \log(t)$ is not algebraic over $\mathbb{C}(t)$

Exercise 4.10. Consider similarly, $\mathcal{R} = (t, \exp(t))$, $G = ?$

5 The Galois-correspondence of differential equations

Recall our setting: \mathcal{K} differential field, \mathcal{C} is constants, $\mathcal{C} = \overline{\mathcal{C}}$ with $\text{char} = 0$

Theorem 5.1. Let \mathcal{R}/\mathcal{K} be a Picard-Vessiot extension, with Galois group G . Set $\mathcal{L} = \text{Frac}(\mathcal{R})$.

$$\left\{ \begin{array}{l} \text{Subfields } M \subseteq \mathcal{L} \\ \text{containing } \mathcal{K}, \text{ stable} \\ \text{under differentiation} \end{array} \right\} \longleftrightarrow \{ \text{algebraic subgroups } H \subseteq G \}$$

$$\begin{aligned} M &\longmapsto \text{Gal}(\mathcal{L}/M) \subseteq \text{Gal}(\mathcal{L}/\mathcal{K}) = G \\ \mathcal{L}^H &\longleftarrow H \end{aligned}$$

where \mathcal{L}^H is the subfield of \mathcal{L} which is fixed under every element of H . These maps are bijective inverse to each other.

If $N \subseteq G$ is normal subgroup, then the map $G \longrightarrow \text{Gal}(\mathcal{L}^N/\mathcal{K})$ is surjective with Kernel N , and \mathcal{L}^N is a Picard-Vessiot extension with Galois group G/N .

For proof see Singer Page 26.

Proposition 5.2. *In the setup of the theorem*

$$L^G = \mathcal{K}$$

Proof. The inclusion \supseteq is evident. For the converse inclusion. Pick $x \in \mathcal{L}, x \notin \mathcal{K}$ and we have to produce $g \in G$ with $gx \neq x$. Set $x = \frac{p}{q}$, $p, q \in \mathcal{R}, q \neq 0$. Consider $r = p \otimes q - q \otimes p \in \mathcal{R} \otimes \mathcal{R}$.

Two easy facts: $r \neq 0$ (because $\frac{p}{q} \notin \mathcal{K}$) and $\mathcal{R} \otimes \mathcal{R}$ has no nilpotents (Char=0)

Choose a maximal differential ideal \mathcal{J} in $\mathcal{R} \otimes \mathcal{R}[1/r]$. Have two canonical morphisms of differential algebras

$$\begin{aligned} \mathcal{R} &\xrightarrow{\varphi_1} \frac{(\mathcal{R} \otimes \mathcal{R})[1/r]}{\mathcal{J}} \xleftarrow{\varphi_2} \mathcal{R} \\ a &\longmapsto (a \otimes 1), (1 \otimes b) \longleftarrow b \end{aligned}$$

φ_1, φ_2 are injective (\mathcal{R} simple) and images of φ_1, φ_2 are equal (c.f. proof of unicity of P-V-extension) denote the image by S

$$\begin{array}{ccc} \mathcal{R} & \xrightarrow{\varphi_1} S & \xleftarrow{\varphi_2} R \\ & \searrow \quad \nearrow & \\ & g = \varphi_2^{-1} \circ \varphi_1 & \end{array}$$

$g \in \text{Gal}(\mathcal{R}/\mathcal{K}) = G$. The class of r in $\mathcal{R} \otimes \mathcal{R}[1/r]/\mathcal{J}$ is a unit

$$\begin{aligned} 0 \neq [p \otimes q - q \otimes p] &= \varphi_1(p)\varphi_2(q) - \varphi_1(q)\varphi_2(p) \\ &= \varphi_1(p \cdot (gq)) - \varphi_1(q \cdot (gp)) \\ &\implies p \cdot gq \neq q \cdot gp \\ &x \neq gx \end{aligned}$$

□

6 Local theory of differential equations

Setups: $\mathcal{C} = \overline{\mathcal{C}}$ field of $\text{char} = 0$. $\mathbb{C} = \mathcal{A}$. choose $\xi_m \in \mathcal{C}$ -primitive m -th roots of unity. $\xi_m^n = \xi_{m/n}$ if $n|m$. e.g. $\xi_m = e^{2\pi i/m}$. $\mathcal{K} = \mathcal{C}((t)) = \text{Frac}(\mathcal{C}[[t]])$ (the formal Laurant series.) with usual derivative. Goal: classify differential equation of differential modules over \mathcal{K} .

Ingredients to classification:

1. Set $\mathfrak{D} = \mathcal{K}[\partial]$ the noncommutative ring of polynomial expressions differential operators $\mathcal{L} = a_n \partial^n + a_{n-1} \partial^{n-1} + \dots + a_0$. \mathfrak{D} =the ring of differential operators. multiplication: $\partial \cdot a = a' + a\partial, a \in \mathcal{K}$. Differential modules over \mathcal{K} are the same as left \mathfrak{D} -modules. Given $L \in \mathfrak{D}$, get a \mathfrak{D} -module

$$\mathcal{K}[\partial]/\mathcal{K}[\partial] \cdot L = \mathfrak{D}/\mathfrak{D}L$$

Claim: This \mathfrak{D} -modules is the differential module of the equation $L(u) = 0$. In general $\{\text{Left } \mathfrak{D}\text{-module}\} = \{\text{Diff. } \mathcal{K}\text{-module}\}$

2. Finite field extension of \mathcal{K} . Let $m \geq 1$ integer. Set $\mathcal{K}_m = \mathcal{C}((t^{1/m})) = \mathcal{C}((t)[s])/\langle s^m - t \rangle$. Clearly $\mathcal{K} \subseteq \mathcal{K}_m$. The field extension $\mathcal{K}_m/\mathcal{K}$ is Galois with group $\mathbb{Z}/m\mathbb{Z}$. For $[a] \in \mathbb{Z}/m\mathbb{Z}$ consider the automorphism

$$\begin{aligned} \mathcal{K}_m &\xrightarrow{\epsilon(a)} \mathcal{K}_m \\ t^{1/m} &\mapsto \xi_m^a \cdot t^{1/m}, \end{aligned}$$

where $\epsilon : \mathbb{Z}/m\mathbb{Z} \xrightarrow{\cong} \text{Gal}(\mathcal{K}_m/\mathcal{K})$ isomorphism.

If $n|m$, then $\mathcal{K}_n \subseteq \mathcal{K}_m$. Can consider $\overline{\mathcal{K}} = \cup_{m \geq 1} \mathcal{K}_m$.

Theorem 6.1. $\overline{\mathcal{K}}$ is algebraically closed!

$$\text{Gal}(\overline{\mathcal{K}}|\mathcal{K}) = \lim_m \mathbb{Z}/m\mathbb{Z} = \widehat{\mathbb{Z}}$$

Theorem 6.2. Consider a matrix differential equation of the form

$$\delta u = Au$$

where $\delta = t \cdot \partial = t \frac{\partial}{\partial t}$. Then there exists an extension $\mathcal{K}_m/\mathcal{K}$ such that the equation $\delta u = Au$ is equivalent to $\delta v = Bv$, with $B \in M_n(\mathcal{K}_m)$ of the form:

$$\begin{pmatrix} B_{11} & 0 & \dots & & & \\ 0 & B_{12} & \dots & & & \\ \vdots & \vdots & \ddots & \vdots & & \\ & & \dots & B_{1m_1} & & \\ & & & & B_{21} & \\ & & & & & B_{22} \\ & & & & & \ddots \\ & & & & & & B_{2m_2} \\ & & & & & & \ddots \\ & & & & & & & B_{s \ m_s} \end{pmatrix}$$

where each B_{ia} , $1 \leq a \leq m_i$ is a block-diagonal matrix of the form

$$\begin{pmatrix} b_i & & & & 0 \\ 1 & \ddots & & & \\ 0 & 1 & \ddots & & \\ & & 0 & 1 & \ddots \\ 0 & & & 0 & 1 & b_i \end{pmatrix}$$

and $b_i \in \mathcal{C}[t^{-\frac{1}{m}}]$ and $b_i - b_j \notin \mathbb{Q}$ for $i \neq j$

Another version of the above theorem:

Theorem 6.3. *Let M be a left \mathfrak{D} -module which is finite dimensional a \mathcal{K} -vector space. There is $\mathcal{K}_m/\mathcal{K}$ and distinct $q_1, \dots, q_s \in t^{-1,m}\mathcal{C}[t^{-1/m}]$ such that*

$$\mathcal{K}_m \otimes_{\mathcal{K}} M = \oplus_{i=1}^s M_i$$

where M_i has the following shape. There exists a \mathcal{C} -vector space W_i finite dimensional and a linear map $l_i : W_i \rightarrow W_i$ s.t.

$$M_i = \mathcal{K}_m \otimes_{\mathcal{C}} W_i$$

with differential on M_i given by

$$\delta_{M_i}(f \otimes w) = q_i f \otimes w + \delta f \otimes w + f \otimes l_i(w)$$

And also another equivalent version

Theorem 6.4. *For any differential operator $L = \partial^n + a_{n-1}\partial^{n-1} + \dots + a_1\partial + a_0$, there exists $\alpha \in \mathcal{K}_m$ s.t. L factors as*

$$L = L_1 \cdot (\partial - \alpha)$$

where $L_1 \in \mathcal{K}_m[\partial]$

We will take the next few weeks to prove the above theorem:

$$\text{6.2} \iff \text{6.3} \implies \text{6.4}$$

are relatively easy and the real difficulty lies in the

$$\longleftarrow \text{6.4}$$

Lets first prove that $\overline{\mathcal{K}}$ is algebraically closed.

Definition 6.5. *Valuations: An element α of $\overline{\mathcal{K}}$ can be written as*

$$\alpha = \sum_{n=N}^{\infty} a_n t^{n/m}$$

*with some fixed m , ($\alpha \in \mathcal{K}_m$). If $\alpha \neq 0, a_N \neq 0, N \in \mathbb{Z}$. we define the **valuation***

$$v(\alpha) := \begin{cases} N/m & \text{if } \alpha \neq 0 \\ \infty & \text{if } \alpha = 0 \end{cases}$$

Call $v(\alpha)$ the valuation of α

$$v : \mathcal{K}_m \longrightarrow \frac{1}{m}\mathbb{Z} \cup \{\infty\}$$

“the valuation”

$$v : \mathcal{K} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

$$v : \overline{\mathcal{K}} \longrightarrow \mathbb{Q} \cup \{\infty\}.$$

Obvious properties:

$$(i) \quad v(\alpha\beta) = v(\alpha) + v(\beta)$$

$$(ii) \quad v(1) = 0$$

$$(iii) \quad v(\alpha + \beta) \geq \min(v(\alpha), v(\beta)) \quad \text{equality if } v(\alpha) \neq v(\beta)$$

Definition 6.6. *Based one only the properties we define: $\mathcal{O}_m = \{\alpha \in \mathcal{K}_m | v(\alpha) \geq 0\}$ is a subring of \mathcal{K}_m **Valuation ring** and $\mathcal{O}_m \supseteq \mathfrak{m}_m := \{\alpha \in \mathcal{K}_m | v(\alpha) > 0\}$ the **valuation ideal**.*

In this case they have the explicit form

$$\mathcal{O}_m = \mathcal{C}[t^{1/m}]$$

$$\mathcal{O}_m \supseteq \mathfrak{m}_m = t^{1/m} \mathcal{C}[t^{1/m}]$$

\mathfrak{m} is maximal. quotient $\mathcal{O}_m/\mathfrak{m}_m = \mathcal{C}$, $f \longmapsto f(v)$ and \mathcal{O}_m is a local ring. (\mathcal{O}_m, v) is a DVR **discrete valuation ring** and $(\overline{\mathcal{O}} = \cup \mathcal{O}_m, v)$ is a valuation ring.

The valuation on \mathcal{K}_m induces a norm:

$$|\alpha| = e^{-v(\alpha)}$$

$$|0| = 0$$

check that $|\alpha\beta| = |\alpha||\beta|$, $|\alpha + \beta| \leq |\alpha| + |\beta|$ and $|1| = 1$. In this way, we get a metric

$$\text{dist}(\alpha - \beta) = |\alpha - \beta|$$

get a topology.

Exercise 6.7. *Prove that:*

- \mathcal{K}_m is complete (Every Cauchy sequence converges)
- $\mathcal{O}_m \subseteq \mathcal{K}_m$ is compact.

Lemma 6.8. (Hensel's Lemma) \mathcal{O} a valuation ring with maximal ideal \mathfrak{m} . Let $P \in \mathcal{O}[X]$ ($\mathcal{O} \subseteq \mathcal{K}$) is a monic polynomial, whose reduction mod \mathfrak{m} factors as

$$P \bmod \mathfrak{m} = F = F_1 F_2$$

with $F_i \in \mathcal{C}[X]$ both monic and coprime. Then there exist $P_1, P_2 \in \mathcal{O}[X]$ with $P = P_1 P_2$ with $F_i = P_i \bmod \mathfrak{m}$

Proof. Let $Q_1^{(1)}$ and $Q_2^{(2)}$ be the polynomials F_1 and F_2 seen elements of $\mathcal{O}[X]$ ($F_i \in \mathcal{C}[X]$). Suppose that we have constructed polynomials $Q_1^{(N)}$ and $Q_2^{(N)} \in \mathcal{O}[X]$ with the properties:

- $(Q_i^{(N)} \bmod \mathfrak{m}) = F_i$
- $(Q^{(N)})_i \bmod \mathfrak{m}^M = Q_i^{(M)}, 1 \leq M \leq N$.
- $P = Q_1^{(N)} Q_2^{(N)} \bmod \mathfrak{m}^N$

For $N = 1$, done. Set $Q_i^{(N+1)} = Q_i^{(N)} + t^N R_i$ with $R_i \in \mathcal{C}[X]$ polynomials satisfying

$$R_1 F_1 + R_2 F_2 = \frac{P - Q_1^{(N)} Q_2^{(N)}}{t^N} \bmod \mathfrak{m}$$

is still $\in \mathcal{O}[X]$, because F_1, F_2 coprime we can always find such R_i . We can check that the 3 properties hold for $Q_i^{(N+1)}$. The sequence $(Q_i^{(N)})_{N=1}^\infty$ are Cauchy and setting $P_i = \lim_{N \rightarrow \infty} Q_i^{(N)}$ get what we want.

For any complete DVR, we can conduct the above proof \square

Exercise 6.9. Look up Hensel's lemma for \mathbb{Z}_p p -adic integers, with \mathcal{C} replaced by \mathbb{F}_p

Theorem 6.10. *The field $\overline{\mathcal{K}} = \cup \mathcal{K}_m$ is algebraically closed.*

Definition 6.11. *Let M be a finite dimensional \mathcal{K} -vector space. A **Lattice** in M is a \mathcal{O} -submodule of M generated by a \mathcal{K} -basis of M . Typically, $M = \mathcal{K}^n$, Lattice $L = \mathcal{O}^n \subseteq \mathcal{K}^n$*

Exercise 6.12. *Show that Lattice can also be defined as*

*Any finitely generated \mathcal{O} -submodule of M containing a \mathcal{K} -basis of M
i.e. $L \subseteq M$ finitely generated as \mathcal{O} -module. $KL = M$
Any open and compact \mathcal{O} -submodule of $M \cong \mathcal{K}^n$*

7 Personal Reads

7.1 D-module

\mathfrak{D} is defined to be the ring of differential operators with coefficients in the differential field \mathcal{K} .

Lemma 7.1. *For differential operators L_1, L_2 in \mathfrak{D} , with $L_1 \neq 0$, there are unique differential operator Q, R such that*

$$L_2 = QL_1 + R$$

and $\deg R < \deg L_1$. This could be proved algorithmically because every \mathcal{K} is a field.

In other word, \mathfrak{D} is an Euclidean domain.

Corollary 7.2. *For every left ideal $I \subseteq \mathcal{K}[\partial]$, there is a unique differential operator L such that $I = \mathcal{K}[\partial] \cdot L$*

Proof. Euclidean domain are principal ideal domain: see [the proofwiki page](#)

□

Lemma 7.3. *Every finitely generated left \mathfrak{D} -module is of the form $\oplus_i M_i$, where each M_i is of isomorphic to either \mathfrak{D} or $\mathfrak{D}/\mathfrak{D}L$ for some differential operator L .*

7.2 Monodromy, Riemann-Hilbert Problem

U is an open connected subset of the complex sphere \mathcal{P}^1 and let $Y' = AY$ be a differential equation on U , with A a $n \times n$ matrix with coefficients that are meromorphic functions on U . We assume that the equation is regular at every point $p \in U$ (might be regular singular point (which means the growth of solutions is bounded)). Let F_p be a matrix whose columns are the n independent solutions, then F_p is a fundamental matrix with entries in $\mathbb{C}(\{z - p\})$

Does there exist on all of U , a solution space for the equation having dimension n

Definition 7.4. Two differential operators $\frac{d}{dz} - A$ and $\frac{d}{dz} - B$ are called *equivalent* if there exists a $F \in GL_n(\mathcal{K})$ s.t., $F^{-1}(\frac{d}{dz} - A)F = \frac{d}{dz} - B$. A matrix differential operator $\frac{d}{dz} - A$ is called **regular singular** if the equation is equivalent to $\frac{d}{dz} - B$ such that the entries of B have poles at $z = 0$ of order at most 1.