A simple algorithm for cyclic vectors

Khoa Bang Pham
Séminaire, Rennes 1 University

February 14, 2022

Outline

- Hilbert's twenty-first problem asks about the existence of linear differential equations having prescribed monodromic group.

Introduction

- Hilbert's twenty-first problem asks about the existence of linear differential equations having prescribed monodromic group.
- A theorem of Fuchs, Turrittin and Lutz shows that finding regular singular points is equivalent to searching for cyclic vectors.

Introduction

- Hilbert's twenty-first problem asks about the existence of linear differential equations having prescribed monodromic group.
- A theorem of Fuchs, Turrittin and Lutz shows that finding regular singular points is equivalent to searching for cyclic vectors.
- In a paper, Katz gives an explicit formula for cyclic vectors in "good" cases as well as provides a number of examples.

ODE on nonsingular curve

The data in this setting is

- $X/\mathbb{C}$: a complete connected nonsingular curve.

ODE on nonsingular curve

The data in this setting is

- $X/\mathbb{C}$: a complete connected nonsingular curve.
- $U \overset{\text{open}}{\subset} X$: a non-empty Zariski open set.

ODE on nonsingular curve

The data in this setting is

- $X/\mathbb{C}$: a complete connected nonsingular curve.
- $U \overset{\text{open}}{\subset} X$: a non-empty Zariski open set.
- U^{an}: the complex manifold corresponds to U in the GAGA principle.

The data in this setting is

- $X/\mathbb{C}$: a complete connected nonsingular curve.
- $U \overset{\text{open}}{\subset} X$: a non-empty Zariski open set.
- U^{an}: the complex manifold corresponds to U in the GAGA principle.

Definition 2.1

Define an ODE of rank n over U to be a pair of (M, ∇) consisting of a locally free coherent sheaf M of rank n on U together with a connection $\nabla : M \to M \otimes \Omega^1_{U/\mathbb{C}}$. The *solution* of an ODE (M, ∇) is defined to be the kernel of ∇.

Example 2.2

Let $X = \mathbb{P}^1, U \subset \mathbb{P}^1 - \{\infty\}$, then an equation over U is simply means a $(n \times n)$-system

$$\frac{d}{dz}\mathbf{f} = P(z) \cdot \mathbf{f}.$$

Example

Example 2.2

Let $X = \mathbb{P}^1, U \subset \mathbb{P}^1 - \{\infty\}$, then an equation over U is simply means a $(n \times n)$-system

$$\frac{d}{dz}\mathbf{f} = P(z) \cdot \mathbf{f}.$$

This class of equations includes the case linear equations of order n

$$f^{(n)} = p_{n-1} f^{(n-1)} + \cdots + p_1 f' + p_0 f,$$

Example 2.2

Let $X = \mathbb{P}^1, U \subset \mathbb{P}^1 - \{\infty\}$, then an equation over U is simply means a $(n \times n)$-system

$$\frac{d}{dz}\mathbf{f} = P(z) \cdot \mathbf{f}.$$

This class of equations includes the case linear equations of order n

$$f^{(n)} = p_{n-1} f^{(n-1)} + \cdots + p_1 f' + p_0 f,$$

by taking the matrix $P(z)$ to be a particular choice

$$P(z) = \begin{pmatrix} 0 & 1 & ... & 0 & 0 \\ 0 & . & 1 & 0 & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & & 0 & 1 \\ p_0 & p_1 & \cdots & p_{n-2} & p_{n-1} \end{pmatrix}$$

Monodromy representation

Fix a point $z_0 \in U$, denote by S the germ of local holomorphic solutions near z_0, then:

Monodromy representation

Fix a point $z_0 \in U$, denote by S the germ of local holomorphic solutions near z_0, then:

- S is a complex vector space of dimension $\text{rank}(M)$, by the local existence theorem for differential equations.

Fix a point $z_0 \in U$, denote by S the germ of local holomorphic solutions near z_0, then:

- S is a complex vector space of dimension $\mathrm{rank}(M)$, by the local existence theorem for differential equations.
- Given a loop γ in U^{an} starting and ending at z_0, then the analytic continuation along γ defines an *automorphism* of S.

Fix a point $z_0 \in U$, denote by S the germ of local holomorphic solutions near z_0, then:

- S is a complex vector space of dimension $\operatorname{rank}(M)$, by the local existence theorem for differential equations.
- Given a loop γ in U^{an} starting and ending at z_0, then the analytic continuation along γ defines an *automorphism* of S.

In this way the fundamental group $\pi_1(U^{an}, z_0)$ acts on S, this is called the *monodromy representation* of the differential equation.

Example 2.3

Consider the differential equation

$$z\frac{df}{dz} = \alpha f,\ \alpha \in \mathbb{C}$$

on the punctured plane $\mathbb{C} - \{0\}$.

Example

Example 2.3

Consider the differential equation

$$z\frac{df}{dz} = \alpha f,\ \alpha \in \mathbb{C}$$

on the punctured plane $\mathbb{C} - \{0\}$. Choose a branch cut, the local solution is easily seen to be

$$z^{\alpha} = \exp(\alpha \log(z)).$$

Example 2.3

Consider the differential equation

$$z\frac{df}{dz} = \alpha f, \ \alpha \in \mathbb{C}$$

on the punctured plane $\mathbb{C} - \{0\}$. Choose a branch cut, the local solution is easily seen to be

$$z^{\alpha} = \exp(\alpha \log(z)).$$

If we take the analytic continuation along the homotopy class of the curve γ looping counterclockwise around the origin an angle of 2π then the solution turns out to be $e^{2\pi \mathbf{i} \alpha} z^{\alpha}$.

Example 2.3

Consider the differential equation

$$z\frac{df}{dz} = \alpha f,\ \alpha \in \mathbb{C}$$

on the punctured plane $\mathbb{C} - \{0\}$. Choose a branch cut, the local solution is easily seen to be

$$z^{\alpha} = \exp(\alpha \log(z)).$$

If we take the analytic continuation along the homotopy class of the curve γ looping counterclockwise around the origin an angle of 2π then the solution turns out to be $e^{2\pi \mathbf{i} \alpha} z^{\alpha}$.
We have $\pi_1(\mathbb{C} - \{0\}) \cong \mathbb{Z}$ with generator $[\gamma]$, the corresponding monodromy representation in $\mathbb{C}^{\times} = \mathrm{GL}(1, \mathbb{C})$ is given by $\gamma \mapsto e^{2\pi \mathbf{i} \alpha}$.

Regular singular points

Consider a ODE in one complex variable $z \in \mathbb{C}$

$$f^{(n)} = p_{n-1} f^{(n-1)} + \cdots + p_1 f' + p_0 f,$$

where p_i are meromorphic functions.

Regular singular points

Consider a ODE in one complex variable $z \in \mathbb{C}$

$$f^{(n)} = p_{n-1} f^{(n-1)} + \cdots + p_1 f' + p_0 f,$$

where p_i are meromorphic functions. The above equation is said to have a *regular singular point* at $a \in \mathbb{C}$ if all p_{n-i} have a pole of order at most i at a.

Consider a ODE in one complex variable $z \in \mathbb{C}$

$$f^{(n)} = p_{n-1} f^{(n-1)} + \cdots + p_1 f' + p_0 f,$$

where p_i are meromorphic functions. The above equation is said to have a *regular singular point* at $a \in \mathbb{C}$ if all p_{n-i} have a pole of order at most i at a. In such a case, by a routine computation, the equation can be transformed into the form

$$D^{(n)} f = b_{n-1} D^{(n-1)} f + ... + b_0 f,$$

where $D = (z-a)\frac{d}{dz}$. The original one has a regular singular point at a iff all b_i are holomorphic at a.

Hilbert's twenty-first problem

Hilbert's twenty-first problem. *Let* X *be a nonsingular curve over* $\mathbb{C}$*,* U *one of its non-empty Zariski open set. Hilbert's twenty-first problem asks whether any finite-dimensional representation of* $\pi_1(U^{an})$ *can be obtained as a monodromy representation of a differential equation on* U *with regular singular points.*

Hilbert's twenty-first problem

Hilbert's twenty-first problem. *Let X be a nonsingular curve over $\mathbb{C}$, U one of its non-empty Zariski open set. Hilbert's twenty-first problem asks whether any finite-dimensional representation of $\pi_1(U^{an})$ can be obtained as a monodromy representation of a differential equation on U with regular singular points.*

Question. Why do we insist on regular singular points?

Hilbert's twenty-first problem. *Let X be a nonsingular curve over $\mathbb{C}$, U one of its non-empty Zariski open set. Hilbert's twenty-first problem asks whether any finite-dimensional representation of $\pi_1(U^{an})$ can be obtained as a monodromy representation of a differential equation on U with regular singular points.*

Question. Why do we insist on regular singular points?

Example 2.4

Let $U = \mathbb{A}^1, U^{an} = \mathbb{C}$, and consider $\pi_1(U^{an}) = 0 \to \mathbb{C}^\times$ the trivial representation. For any polynomial $P \in \mathbb{C}[z]$, the equation

$$\frac{df}{dz} = P(z).f \text{ has solution } f(z) = \exp\left(\int_0^z P(t)dt\right),$$

which is an entire function, so without monodromy. But as differential equations on the algebraic variety $\mathbb{A}^1$, these are pairwise non-isomorphic; only the choice $P \equiv 0$ gives regular singular points (include ∞).

Hilbert's twenty-first problem. *Let X be a nonsingular curve over $\mathbb{C}$, U one of its non-empty Zariski open set. Hilbert's twenty-first problem asks whether any finite-dimensional representation of $\pi_1(U^{an})$ can be obtained as a monodromy representation of a differential equation on U with regular singular points.*
Question. Why do we insist on regular singular points?

Example 2.4

Let $U = \mathbb{A}^1, U^{an} = \mathbb{C}$, and consider $\pi_1(U^{an}) = 0 \to \mathbb{C}^\times$ the trivial representation. For any polynomial $P \in \mathbb{C}[z]$, the equation

$$\frac{df}{dz} = P(z).f \text{ has solution } f(z) = \exp\left(\int_0^z P(t)dt\right),$$

which is an entire function, so without monodromy. But as differential equations on the algebraic variety $\mathbb{A}^1$, these are pairwise non-isomorphic; only the choice $P \equiv 0$ gives regular singular points (include ∞). Indeed, if $z = 1/w$ then the equation

$$\frac{df}{dw} = -\frac{Q(w)}{w^{\deg(P)+2}}.f \text{ where } w^{\deg}P(1/w) = Q(w)$$

has a regular singular point at $w = 0$ iff $Q(w) \equiv 0$.

Connections and regular singular points

Our data in this section includes:

- k: an algebraically closed field of characteristic 0.

Our data in this section includes:

- k: an algebraically closed field of characteristic 0.
- F/k: a function field in one variable over k. For instance, F can be the function field of a smooth, projective curve over k.

Connections and regular singular points

Our data in this section includes:

- k: an algebraically closed field of characteristic 0.
- F/k: a function field in one variable over k. For instance, F can be the function field of a smooth, projective curve over k.
- W: a vector space over F of dimension n.

Connections and regular singular points

Our data in this section includes:

- k: an algebraically closed field of characteristic 0.
- F/k: a function field in one variable over k. For instance, F can be the function field of a smooth, projective curve over k.
- W: a vector space over F of dimension n.

Definition 3.1 (Connections)

A *connection* ∇ on W is an additive mapping $\nabla : W \to \Omega^1_{F/k} \otimes W$ satisfying the Leibniz rule

$$\nabla(fw) = df \otimes w + f\nabla(w) \ \forall f \in K, w \in W.$$

Our data in this section includes:

- k: an algebraically closed field of characteristic 0.
- F/k: a function field in one variable over k. For instance, F can be the function field of a smooth, projective curve over k.
- W: a vector space over F of dimension n.

Definition 3.1 (Connections)

A *connection* ∇ on W is an additive mapping $\nabla : W \to \Omega^1_{F/k} \otimes W$ satisfying the Leibniz rule

$$\nabla(fw) = df \otimes w + f\nabla(w) \ \forall f \in K, w \in W.$$

Equivalently, ∇ can be defined as a F-linear mapping

$$\nabla : \mathrm{Der}_k(F, F) \to \mathrm{End}_k(W)$$

such that

$$(\nabla(D))(fw) = D(f)w + f(\nabla(D))w \ \forall D \in \mathrm{Der}_k(F, F), f \in F, w \in W.$$

For every closed point $\mathfrak{p}$ (we also call a closed point a *place*) we do have

$$\mathcal{O}_{\mathfrak{p}} = \{f \in K \mid \mathrm{ord}_{\mathfrak{p}}(f) \geq 0\}$$
$$\mathfrak{m}_{\mathfrak{p}} = \{f \in K \mid \mathrm{ord}_{\mathfrak{p}}(f) \geq 1\},$$

where $\mathrm{ord}_{\mathfrak{p}} : F \to \mathbb{Z} \cup \{\infty\}$ is the discrete valuation at $\mathfrak{p}$.

For every closed point $\mathfrak{p}$ (we also call a closed point a *place*) we do have

$$\mathcal{O}_{\mathfrak{p}} = \{f \in K \mid \mathrm{ord}_{\mathfrak{p}}(f) \geq 0\}$$
$$\mathfrak{m}_{\mathfrak{p}} = \{f \in K \mid \mathrm{ord}_{\mathfrak{p}}(f) \geq 1\},$$

where $\mathrm{ord}_{\mathfrak{p}} : F \to \mathbb{Z} \cup \{\infty\}$ is the discrete valuation at $\mathfrak{p}$.

Definition 3.2 (Regular singular points)

Let $\mathfrak{p}$ be a place of F/k, let ∇ be a connection on W. We say that ∇ has a *regular singular point* at $\mathfrak{p}$ if there exists a basis $\mathbf{e}$ of W and a matrix $P \in M_n(\mathcal{O}_{\mathfrak{p}})$ such that

$$\nabla\left(h\frac{d}{dh}\right)\mathbf{e} = P\mathbf{e},$$

where h is an uniformizer at $\mathfrak{p}$.

For every closed point $\mathfrak{p}$ (we also call a closed point a *place*) we do have

$$\mathcal{O}_\mathfrak{p} = \{f \in K \mid \operatorname{ord}_\mathfrak{p}(f) \geq 0\}$$
$$\mathfrak{m}_\mathfrak{p} = \{f \in K \mid \operatorname{ord}_\mathfrak{p}(f) \geq 1\},$$

where $\operatorname{ord}_\mathfrak{p} : F \to \mathbb{Z} \cup \{\infty\}$ is the discrete valuation at $\mathfrak{p}$.

Definition 3.2 (Regular singular points)

Let $\mathfrak{p}$ be a place of F/k, let ∇ be a connection on W. We say that ∇ has a *regular singular point* at $\mathfrak{p}$ if there exists a basis $\mathbf{e}$ of W and a matrix $P \in M_n(\mathcal{O}_\mathfrak{p})$ such that

$$\nabla\left(h\frac{d}{dh}\right)\mathbf{e} = P\mathbf{e},$$

where h is an uniformizer at $\mathfrak{p}$.

Definition 3.3 (Cyclic vectors)

Let ∇ be a connection on W. A vector $w \in W$ is said to be *cyclic* if there exists a non-zero derivation $D \in \operatorname{Der}_k(F, F)$ such that

$$\operatorname{Span}_K \langle w, (\nabla(D))(w), ..., (\nabla(D))^{n-1}(w)\rangle = W.$$

In that case, we call (W, ∇) a *cyclic object*.

Turrittin's theorem

Theorem 3.4 (Fuchs, Turrittin, Lutz, [2])

Turrittin's theorem

Theorem 3.4 (Fuchs, Turrittin, Lutz, [2])

Suppose that (W, ∇) *has a cyclic vector* $w \in W$, $\mathfrak{p}$ *is a place of* F/k, h *is a uniformizer at* $\mathfrak{p}$ *and* $n = \dim_F(W)$. *Then the following conditions are equivalent:*

Theorem 3.4 (Fuchs, Turrittin, Lutz, [2])

Suppose that (W, ∇) has a cyclic vector $w \in W$, $\mathfrak{p}$ is a place of F/k, h is a uniformizer at $\mathfrak{p}$ and $n = \dim_F(W)$. Then the following conditions are equivalent:

- *(W, ∇) does **not** have a regular singular point at $\mathfrak{p}$.*

Turrittin's theorem

Theorem 3.4 (Fuchs, Turrittin, Lutz, [2])

Suppose that (W, ∇) *has a cyclic vector* $w \in W$*,* $\mathfrak{p}$ *is a place of* F/k*,* h *is a uniformizer at* $\mathfrak{p}$ *and* $n = \dim_F(W)$*. Then the following conditions are equivalent:*

- (W, ∇) *does **not** have a regular singular point at* $\mathfrak{p}$*.*
- *In terms of the basis*

$$\mathbf{e} = \begin{pmatrix} w \\ \nabla\left(h\frac{d}{dh}\right)(w) \\ \vdots \\ \left(\nabla\left(h\frac{d}{dh}\right)\right)^{n-1}(w) \end{pmatrix}$$

  of W*, the connection matrix is expressed as*

$$\nabla\left(h\frac{d}{dh}\right)\mathbf{e} = \begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ 0 & . & 1 & 0 & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & & 0 & 1 \\ p_0 & p_1 & \cdots & p_{n-2} & p_{n-1} \end{pmatrix}\mathbf{e}$$

  and, for some value of i*, we have* $\operatorname{ord}_{\mathfrak{p}}(p_i) < 0$*.*

Setting

- R: a commutative ring with unity.

Setting

- R: a commutative ring with unity.
- $\partial : R \to R$ is a derivation of R to itself.

Setting

- R: a commutative ring with unity.
- $\partial : R \to R$ is a derivation of R to itself.
- $t \in R$ an element with $\partial(t) = 1$.

Setting

- R: a commutative ring with unity.
- $\partial : R \to R$ is a derivation of R to itself.
- $t \in R$ an element with $\partial(t) = 1$.
- $R^\partial = \{a \in R \mid \partial(a) = 0\}$ the subring of "constants".

Setting

- R: a commutative ring with unity.
- $\partial : R \to R$ is a derivation of R to itself.
- $t \in R$ an element with $\partial(t) = 1$.
- $R^{\partial} = \{a \in R \mid \partial(a) = 0\}$ the subring of "constants".
- A fixed integer $n \geq 1$ and a triple $(V, D, \mathbf{e})$ consisting of a free R-module V of rank n, an additive mapping $D : V \to V$ satisfying

$$D(fv) = \partial(f)v + fD(v)$$

for all $f \in R$, $v \in V$, and a R-basis $\mathbf{e} = (e_0, ..., e_{n-1})$ of V.

Setting

- R: a commutative ring with unity.
- $\partial : R \to R$ is a derivation of R to itself.
- $t \in R$ an element with $\partial(t) = 1$.
- $R^\partial = \{a \in R \mid \partial(a) = 0\}$ the subring of "constants".
- A fixed integer $n \geq 1$ and a triple $(V, D, \mathbf{e})$ consisting of a free R-module V of rank n, an additive mapping $D : V \to V$ satisfying

$$D(fv) = \partial(f)v + fD(v)$$

for all $f \in R$, $v \in V$, and a R-basis $\mathbf{e} = (e_0, ..., e_{n-1})$ of V.

Definition 4.1

An element $v \in V$ is said to be a *cyclic vector* if $v, Dv, ..., D^{n-1}(v)$ is a R-basis of V.

- R: a commutative ring with unity.
- $\partial : R \to R$ is a derivation of R to itself.
- $t \in R$ an element with $\partial(t) = 1$.
- $R^\partial = \{a \in R \mid \partial(a) = 0\}$ the subring of "constants".
- A fixed integer $n \geq 1$ and a triple $(V, D, \mathbf{e})$ consisting of a free R-module V of rank n, an additive mapping $D : V \to V$ satisfying

$$D(fv) = \partial(f)v + fD(v)$$

for all $f \in R$, $v \in V$, and a R-basis $\mathbf{e} = (e_0, ..., e_{n-1})$ of V.

Definition 4.1

An element $v \in V$ is said to be a *cyclic vector* if $v, Dv, ..., D^{n-1}(v)$ is a R-basis of V.

Suppose now that $(n-1)!$ is invertible in R. For each constant $a \in R^\partial$, we define an element $c(\mathbf{e}, t-a)$ in V by the following formula

$$c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} \sum_{k=0}^{j} (-1)^k \binom{j}{k} D^k(e_{n-k}).$$

First main result

Theorem 4.2 (N. M. Katz, [1])

Suppose R is a local $\mathbb{Z}[1/(n-1)!]$-algebra whose maximal ideal contains $t-a$. Then $c(\mathbf{e}, t-a)$ is a cyclic vector.

First main result

Theorem 4.2 (N. M. Katz, [1])

Suppose R is a local $\mathbb{Z}[1/(n-1)!]$-algebra whose maximal ideal contains $t-a$. Then $c(\mathbf{e}, t-a)$ is a cyclic vector.

Proof.

Define elements $c(i,j)$ inductively by the formulas

$$c(0,j) = \begin{cases} \sum_{k=0}^{j} (-1)^k \binom{j}{k} D^k(e_{j-k}) & j \leq n-1, \\ 0 & j \geq n. \end{cases}$$

$$c(i+1,j) = c(i,j+1) + D(c(i,j)).$$

Theorem 4.2 (N. M. Katz, [1])

Suppose R is a local $\mathbb{Z}[1/(n-1)!]$-algebra whose maximal ideal contains $t-a$. Then $c(\mathbf{e}, t-a)$ is a cyclic vector.

Proof.

Define elements $c(i,j)$ inductively by the formulas

$$c(0,j) = \begin{cases} \sum_{k=0}^{j} (-1)^k \binom{j}{k} D^k(e_{j-k}) & j \leq n-1, \\ 0 & j \geq n. \end{cases}$$

$$c(i+1,j) = c(i,j+1) + D(c(i,j)).$$

By definition of $c(\mathbf{e}, t-a)$, we have

$$c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(0,j).$$

□

First main result

Proof.

By induction,

$$D^i c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(i,j) = c(i,0) + (t-a)(\text{smth}) \ \forall\ i,j \geq 0$$

First main result

Proof.

By induction,

$$D^i c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(i,j) = c(i,0) + (t-a)(\text{smth}) \ \forall\ i, j \geq 0$$

First main result

Proof.

By induction,

$$D^i c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(i,j) = c(i,0) + (t-a)(\text{smth}) \ \forall\ i, j \geq 0$$

$$c(i,j) = \sum_{k=0}^{j} (-1)^k \binom{j}{k} D(e_{i+j-k}) \ \forall\ i+j \leq n-1.$$

First main result

Proof.

By induction,

$$D^i c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(i,j) = c(i,0) + (t-a)(\text{smth}) \ \forall\, i, j \geq 0$$

$$c(i,j) = \sum_{k=0}^{j} (-1)^k \binom{j}{k} D(e_{i+j-k}) \ \forall\, i+j \leq n-1.$$

In particular, $c(i,0) = e_i \ \forall\, i = \overline{0, n-1}$, which implies that

$$D^i c(\mathbf{e}, t-a) \equiv e_i \bmod (t-a)V.$$

First main result

Proof.

By induction,

$$D^i c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(i,j) = c(i,0) + (t-a)(\text{smth}) \ \forall\ i,j \geq 0$$

$$c(i,j) = \sum_{k=0}^{j} (-1)^k \binom{j}{k} D(e_{i+j-k}) \ \forall\ i+j \leq n-1.$$

In particular, $c(i,0) = e_i \ \forall\ i = \overline{0, n-1}$, which implies that

$$D^i c(\mathbf{e}, t-a) \equiv e_i \mod (t-a)V.$$

Hence,

$$V = (t-a)V + \left\langle D^i c(\mathbf{e}, t-a) \right\rangle \subset \mathfrak{m}V + \left\langle D^i c(\mathbf{e}, t-a) \right\rangle \subset V.$$

First main result

Proof.

By induction,

$$D^i c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(i,j) = c(i,0) + (t-a)(\text{smth}) \ \forall\ i, j \geq 0$$

$$c(i,j) = \sum_{k=0}^{j} (-1)^k \binom{j}{k} D(e_{i+j-k}) \ \forall\ i + j \leq n-1.$$

In particular, $c(i,0) = e_i \ \forall\ i = \overline{0, n-1}$, which implies that

$$D^i c(\mathbf{e}, t-a) \equiv e_i \mod (t-a)V.$$

Hence,

$$V = (t-a)V + \left\langle D^i c(\mathbf{e}, t-a) \right\rangle \subset \mathfrak{m}V + \left\langle D^i c(\mathbf{e}, t-a) \right\rangle \subset V.$$

Since V is finitely generated, we can apply Nakayama's lemma to conclude that $V = \langle D^i c(\mathbf{e}, t-a) \rangle$; in other words, $c(\mathbf{e}, t-a)$ is a cyclic vector. □

Second main result

Theorem 4.3 (N. M. Katz, [1])

Let R be a ring in which $(n-1)!$ is invertible, and let k be a subfield of R^{∂}. Suppose that $|k| > n(n-1)$, and let $a_0, a_1, ..., a_{n(n-1)}$ be $n(n-1)+1$ distinct elements of k. Then Zarisky locally on $\mathrm{Spec}(R)$, one of the vectors $c(\mathbf{e}, t-a_i)$, $i = \overline{0, n(n-1)}$, is a cyclic vector.

Theorem 4.3 (N. M. Katz, [1])

Let R be a ring in which $(n-1)!$ is invertible, and let k be a subfield of R^{∂}. Suppose that $|k| > n(n-1)$, and let $a_0, a_1, ..., a_{n(n-1)}$ be $n(n-1)+1$ distinct elements of k. Then Zarisky locally on $\operatorname{Spec}(R)$, one of the vectors $c(\mathbf{e}, t-a_i)$, $i = \overline{0, n(n-1)}$, is a cyclic vector.

Proof.

For $i = \overline{0, n-1}$, $X \in R$, we define elements $c_i(\mathbf{e}, X)$ by

$$c_i(\mathbf{e}, X) = \sum_{j=0}^{n-1} \frac{X^j}{j!} c(i,j).$$

Theorem 4.3 (N. M. Katz, [1])

Let R be a ring in which $(n-1)!$ is invertible, and let k be a subfield of R^{∂}. Suppose that $|k| > n(n-1)$, and let $a_0, a_1, ..., a_{n(n-1)}$ be $n(n-1)+1$ distinct elements of k. Then Zarisky locally on $\operatorname{Spec}(R)$, one of the vectors $c(\mathbf{e}, t-a_i)$, $i = \overline{0, n(n-1)}$, is a cyclic vector.

Proof.

For $i = \overline{0, n-1}$, $X \in R$, we define elements $c_i(\mathbf{e}, X)$ by

$$c_i(\mathbf{e}, X) = \sum_{j=0}^{n-1} \frac{X^j}{j!} c(i,j).$$

Taking wedge product gives us

$$c_0(\mathbf{e}, X) \wedge \cdots \wedge c_{n-1}(\mathbf{e}, X) = P(X) e_0 \wedge \cdots \wedge e_{n-1},$$

where P is a polynomial of degree $\leq n(n-1)$ in $R[T]$. □

Proof.

We do have

$$c_i(\mathbf{e}, 0) = e_i \Rightarrow P(0) = 1$$
$$c_i(\mathbf{e}, t-a) = D^i c(\mathbf{e}, t-a).$$

Therefore, $c(\mathbf{e}, t-a)$ is cyclic if and only if $P(t-a) \in R^\times$.

Proof.

We do have

$$c_i(\mathbf{e}, 0) = e_i \Rightarrow P(0) = 1$$
$$c_i(\mathbf{e}, t - a) = D^i c(\mathbf{e}, t - a).$$

Therefore, $c(\mathbf{e}, t - a)$ is cyclic if and only if $P(t - a) \in R^\times$. We must show that $\langle P(t - a_i) \rangle = R$. Let's write explicitly

$$P(X) = \sum_{j=0}^{n(n-1)} r_j X^j.$$

Proof.

We do have

$$c_i(\mathbf{e}, 0) = e_i \Rightarrow P(0) = 1$$
$$c_i(\mathbf{e}, t-a) = D^i c(\mathbf{e}, t-a).$$

Therefore, $c(\mathbf{e}, t-a)$ is cyclic if and only if $P(t-a) \in R^\times$. We must show that $\langle P(t-a_i) \rangle = R$. Let's write explicitly

$$P(X) = \sum_{j=0}^{n(n-1)} r_j X^j.$$

This yields a system of equations $P(t-a_i) = \sum_{j=0}^{n(n-1)} r_j (t-a_i)^j$, whose determinant is the well-known Van der Monde one

Frame Title

Proof.

We do have

$$c_i(\mathbf{e}, 0) = e_i \Rightarrow P(0) = 1$$
$$c_i(\mathbf{e}, t-a) = D^i c(\mathbf{e}, t-a).$$

Therefore, $c(\mathbf{e}, t-a)$ is cyclic if and only if $P(t-a) \in R^\times$. We must show that $\langle P(t-a_i)\rangle = R$. Let's write explicitly

$$P(X) = \sum_{j=0}^{n(n-1)} r_j X^j.$$

This yields a system of equations $P(t-a_i) = \sum_{j=0}^{n(n-1)} r_j (t-a_i)^j$, whose determinant is the well-known Van der Monde one

$$\det\left((t-a_i)^j_{0\le i,j\le n(n-1)} \right) = \prod_{0\le i<j\le n(n-1)} (a_i - a_j) \in k^\times \subset R^\times.$$

Consequently, $R \overset{P(0)=1}{=} \langle P(0)\rangle \overset{r_0=P(0)}{=} \langle r_i\rangle = \langle P(t-a_i)\rangle$. □

Motivation for the chosen formula

Consider $R = \mathbb{C}[[t]]$, the formal power series over $\mathbb{C}$ in one variable, $\partial = d/dt$ is the formal derivative. If $(h_0, ..., h_{n-1})$ is a horizontal basis of V, i.e. a R-basis such that $Dh_i = 0 \ \forall \ i = \overline{0, n-1}$. Then it can be seen easily that

$$\sum_{j=0}^{n-1} \frac{t^j}{j!} h_j$$

is a cyclic vector.

Motivation for the chosen formula

Consider $R = \mathbb{C}[[t]]$, the formal power series over $\mathbb{C}$ in one variable, $\partial = d/dt$ is the formal derivative. If $(h_0, ..., h_{n-1})$ is a horizontal basis of V, i.e. a R-basis such that $Dh_i = 0 \; \forall \; i = \overline{0, n-1}$. Then it can be seen easily that

$$\sum_{j=0}^{n-1} \frac{t^j}{j!} h_j$$

is a cyclic vector. Given any $v \in V$, the t-adic sequence

$$\widetilde{v} = \sum_{k \geq 0} (-1)^k \frac{t^k}{k!} D^k(v)$$

is the unique solution of

$$\widetilde{v} \equiv v \bmod tV, \;\; D(\widetilde{v}) = 0.$$

Motivation for the chosen formula

Consider $R = \mathbb{C}[[t]]$, the formal power series over $\mathbb{C}$ in one variable, $\partial = d/dt$ is the formal derivative. If $(h_0, ..., h_{n-1})$ is a horizontal basis of V, i.e. a R-basis such that $Dh_i = 0 \ \forall \ i = \overline{0, n-1}$. Then it can be seen easily that

$$\sum_{j=0}^{n-1} \frac{t^j}{j!} h_j$$

is a cyclic vector. Given any $v \in V$, the t-adic sequence

$$\widetilde{v} = \sum_{k \geq 0} (-1)^k \frac{t^k}{k!} D^k(v)$$

is the unique solution of

$$\widetilde{v} \equiv v \bmod tV, \ D(\widetilde{v}) = 0.$$

Therefore if $\mathbf{e} = (e_0, ..., e_{n-1})$ is any R-basis of V, then $(\widetilde{e}_0, ..., \widetilde{e}_{n-1})$ is, by Nakayama's lemma, a horizontal R-basis, and consequently

$$\sum_{j=0}^{n-1} \frac{t^j}{j!} \widetilde{e}_j = \sum_{j=0}^{n-1} \frac{t^j}{j!} \sum_{k \geq 0} (-1)^k \frac{t^k}{k!} D^k(e_j)$$

is a cyclic vector.

Motivation for the chosen formula

But if v is a cyclic vector, then so, by Nakayama's lemma, is $v + t^n v_0$ for any $v_0 \in V$, simply because, for $i = \overline{0, n-1}$,

$$D^i(v + t^n v_0) \equiv D^i v \bmod t^{n-i} V.$$

Motivation for the chosen formula

But if v is a cyclic vector, then so, by Nakayama's lemma, is $v + t^n v_0$ for any $v_0 \in V$, simply because, for $i = \overline{0, n-1}$,

$$D^i(v + t^n v_0) \equiv D^i v \mod t^{n-i} V.$$

Therefore in the above double sum, we may neglect all terms with $j + k \geq n$, to conclude that

$$\sum_{j=0}^{n-1} \frac{t^j}{j!} \sum_{k=0}^{n-1-j} (-1)^k \frac{t^k}{k!} D^k(e_j)$$

is a cyclic vector. But this last vector is easily seen to be $c(\mathbf{e}, t)$.

Thank you for your listening!

[1] Nicholas M. Katz. “A simple algorithm for cyclic vectors”. **in** *Amer. J. Math.*: 109.1 (1987), **pages** 65–70. ISSN: 0002-9327. DOI: 10.2307/2374551. URL: https://doi.org/10.2307/2374551.

[2] Nicholas M. Katz. “Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin”. **in** *Inst. Hautes Études Sci. Publ. Math.*: 39 (1970), **pages** 175–232. ISSN: 0073-8301. URL: http://www.numdam.org/item?id=PMIHES_1970__39__175_0.