A simple algorithm for cyclic vectors

Khoa Bang Pham
Master 2 Séminaire

Université de Rennes 1

Abstract

The notion of regular singular points appeared in the classical theory of complex ODE. Equations with regular singular points can be solved locally by the so-called Frobenius method and behave more nicely than other classes of equations. It is well-known by a theorem of Fuchs, Turrittin and Lutz that finding regular singular points is equivalent to searching for cyclic vectors. This documents, based on a work of Katz, interprets the connection of aforementioned notions and provides an explicit formula for finding cyclic vectors.

Contents

1 Complex ordinary differential equations in one variable

Hilbert's twenty-first problem asks about the existence of linear differential equations having prescribed monodromic group. The main reference for this section is [Kat76]. Let X be a complete connected nonsingular curve over $\mathbb{C}$, whose underlying complex manifold is thus a compact Riemann surface. Let U be a non-empty Zariski open set, the complement in X of a finite (possibly empty) set of closed points. The underlying complex manifolds U^{an} is thus a finitely punctured Riemann surfaces.

Consider a linear homogeneous differential equation of rank n on U. To make this more clear, let us explicate several notions as well as present examples. For instance, if $X = \mathbb{P}^1$ and $U \subset \mathbb{P}^1 - \{\infty\}$, this simply means a $(n \times n)$ system

$$\frac{d}{dz}\mathbf{f} = P(z) \cdot \mathbf{f}. \tag{1.1}$$

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

$$f^{(n)} = p_{n-1} f^{(n-1)} + \cdots + p_1 f' + p_0 f, \tag{1.2}$$

by taking for the matrix $P(z)$ the particular choice

$$P(z) = \begin{pmatrix} 0 & 1 & ... & 0 & 0 \\ 0 & . & 1 & 0 & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & & 0 & 1 \\ p_0 & p_1 & \cdots & p_{n-2} & p_{n-1} \end{pmatrix} \tag{1.3}$$

In case of higher genus, we have no global coordinate z so we are led to define a differential equation on U to be a pair (M, ∇) consisting of a locally free coherent sheaf M on U together with a connection $\nabla : M \to M \otimes \Omega^1_{U/\mathbb{C}}$ (definition 2.1), we then define solutions of this equation to be the kernel of ∇. This is reasonable, at least when one thinks in terms of analytic manifolds. Let's consider the following example.

Example 1.1. Denote $\pi : \mathbb{C}^2 \times \mathbb{C} \to \mathbb{C}$ by the trivial bundle of rank 2 over $\mathbb{C}$. Any connection on π can be expressed as

$$\nabla = d + \begin{pmatrix} -f_{11}(z) & -f_{12}(z) \\ -f_{21}(z) & -f_{22}(z) \end{pmatrix} dz \tag{1.4}$$

where d is the exterior derivative and $f_{ij}(z)$ are analytic functions. A section $a \in \Gamma(\pi)$ may be identified with a map

$$\begin{aligned} &\mathbb{C} \to \mathbb{C}^2 \\ &z \mapsto (a_1(z), a_2(z)), \end{aligned}$$

and then

$$\nabla(a) = \nabla \begin{pmatrix} a_1(z) \\ a_2(z) \end{pmatrix} = \begin{pmatrix} a_1'(z) - f_{11}(z)a_1(z) - f_{12}(z)a_2(z) \\ a_2'(z) - f_{21}(z)a_1(z) - f_{22}(z)a_2(z) \end{pmatrix} dz. \tag{1.5}$$

We can easily see that a being in the kernel of ∇ is essentially equivalent to being a solution of a (2×2) system.

If we fix a point $z_0 \in U$, then the germ S of local holomorphic solutions near z_0 is a complex vector space of dimension $\text{rank}(M)$, 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 1.2. Take the differential equation

$$z\frac{df}{dz} = \alpha f, \ \alpha \in \mathbb{C} \tag{1.6}$$

on the punctured plane $\mathbb{C} - \{0\}$. Fix a point in the punctured plane and choose a branch cut starting from the chosen point then the local solution is the function $z^\alpha = \exp(\alpha \log(z))$. 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 $\mathbb{C}^\times = \text{GL}(1, \mathbb{C})$ is given by $\gamma \mapsto e^{2\pi \mathbf{i}\alpha}$.

Let us recall the notion of a regular singular point before we state the Hilbert's twenty-first problem. Consider a ODE in one complex variable $z \in \mathbb{C}$

$$f^{(n)} = p_{n-1} f^{(n-1)} + \cdots + p_1 f' + p_0 f, \tag{1.7}$$

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

$$D^{(n)} f = b_{n-1} D^{(n-1)} f + ... + b_0 f, \tag{1.8}$$

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.

Example 1.3. If p, q are two holomorphic functions then

$$f^{"}(z) = \frac{p(z)}{z} f'(z) + \frac{q(z)}{z^2} f(z) \tag{1.9}$$

is equivalent to $D^2 f = (p+1)Df + qf$, so we see that this equation has a regular singular point at $z = 0$.

We rewrite the resulting equation into the matrix form

$$D \begin{pmatrix} f \\ Df \\ D^2 f \\ \cdots \\ D^{(n-1)} f \end{pmatrix} = \begin{pmatrix} 0 & 1 & ... & 0 & 0 \\ 0 & . & 1 & 0 & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & & 0 & 1 \\ b_0 & b_1 & \cdots & b_{n-2} & b_{n-1} \end{pmatrix} \begin{pmatrix} f \\ Df \\ D^2 \\ \cdots \\ D^{(n-1)} f \end{pmatrix}. \tag{1.10}$$

Consequently, the original equation does *not* have a regular singular point at a iff $\mathrm{ord}_a(p_i) < 0$ for some i. We shall see this fact again in theorem 2.4. Initially, the concept of regular singular points was defined by requiring the local analytic solution to satisfy certain growth estimates but afterwards Fuchs proved that in fact this notion is purely algebraic, which is precisely the one we just define here.

Remark. Though we do not use this but we recall that once we know our equation has a regular singular point at a, the so-called *Frobenius method* can be used to provide n independent solutions near a.

Now we are in position to state the 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 complex representation of $\pi_1(U^{an})$ can be obtained as the monodromy representation of a differential equation on U with regular singular points.*

If we remove the regular condition, then there may be too many differential equations with given monodromy.

Example 1.4. 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

$$\frac{df}{dz} = P(z).f \tag{1.11}$$

has solution

$$f(z) = \exp\left(\int_0^z P(t)dt\right) \tag{1.12}$$

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

$$w\frac{df}{dw} = -\frac{Q(w)}{w^{\deg(P)+1}}.f \text{ where } w^{\deg(P)}P(1/w) = Q(w) \tag{1.13}$$

has a regular singular point at $w = 0$ iff $Q(w) \equiv 0$. For this reason, one *insists* on regular singular points.

The next section introduces the classical theory of regular singular points and show how it is related to the notion of cyclic vectors. Loosely, once we know that our connection has a cyclic vector, we can use this vector to check the regularity; in this sense, a cyclic vector behaves like a local solution of our differential equation.

2 Classical singular regular theory and Turrittin's theorem

Throughout this section, we suppose k is a field of characteristics 0 and K is a function field in one variable over k; for instance, we can take K to be the function field of a smooth, projective curve over k. Let W a finite-dimensional vector space over K. Denote by n the dimension of W over K.

Definition 2.1 (Connection). A connection ∇ on W is an additive mapping $\nabla : W \to \Omega^1_{K/k} \otimes W$ satisfying the Leibniz rule

$$\nabla(fw) = df \otimes w + f\nabla(w) \ \forall f \in K, w \in W. \tag{2.1}$$

Equivalently, ∇ can be viewed as a K-linear mapping

$$\nabla : \mathrm{Der}_k(K, K) \to \mathrm{End}_k(W) \tag{2.2}$$

such that

$$(\nabla(D))(fw) = D(f)w + f(\nabla(D))w \ \forall D \in \mathrm{Der}_k(K, K), f \in K, w \in W, \tag{2.3}$$

where $\nabla(D)$ is the composite

For simplicity, we can assume that k is algebraically closed then K is the function field of a nonsingular, projective curve. Thus for every closed point $\mathfrak{p}$ (we also call a closed point a *place*) we do have

$$\begin{aligned} \mathcal{O}_\mathfrak{p} &= \{f \in K \mid \mathrm{ord}_\mathfrak{p}(f) \geqslant 0\} \\ \mathfrak{m}_\mathfrak{p} &= \{f \in K \mid \mathrm{ord}_\mathfrak{p}(f) \geqslant 1\}, \end{aligned} \tag{2.5}$$

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

Definition 2.2 (Regular singular point). Let $\mathfrak{p}$ be a place of K/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

$$\nabla\left(h\frac{d}{dh}\right)\mathbf{e} = P\mathbf{e}, \tag{2.6}$$

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

Definition 2.3 (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 $D \in \mathrm{Der}_k(K, K)$ such that

$$\mathrm{Span}_K \left\langle w, (\nabla(D))(w), ..., (\nabla(D))^l(w), ... \right\rangle = W. \tag{2.7}$$

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

We mention Turrittin theorem in the first section. Now we state the theorem partially. Those who are interested in reading its full statement and proof are advised to refer to [Kat70].

Theorem 2.4 (Fuchs, Turrittin, Lutz). *Suppose that (W, ∇) has a cyclic vector $w \in W$, $\mathfrak{p}$ is a place of K/k, h is a uniformizer at $\mathfrak{p}$ and $n = \dim_K(W)$. Then the following conditions are equivalent:*

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

$$\mathbf{e} = \begin{pmatrix} w \\ \nabla\left(h\frac{d}{dh}\right)(w) \\ \vdots \\ \left(\nabla\left(h\frac{d}{dh}\right)\right)^{n-1}(w) \end{pmatrix} \tag{2.8}$$

of W, the connection matrix is expressed as

$$\nabla\left(h\frac{d}{dh}\right)\mathbf{e} = \begin{pmatrix} 0 & 1 & ... & 0 & 0 \\ 0 & . & 1 & 0 & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & & 0 & 1 \\ p_0 & p_1 & \cdots & p_{n-2} & p_{n-1} \end{pmatrix}\mathbf{e} \tag{2.9}$$

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

Proof. [Kat70], **theorem 11.9**. □

Remark. In this setting, the basis $\mathbf{e}$ plays the role of the tuple $(f, Df, D^2f, ..., D^{(n-1)}f)$ in (1.10).

Having explained why cyclic vectors are important, the next section gives an efficient algorithm for the problem of finding cyclic vectors.

3 A simple algorithm for cyclic vectors

The setting in this section is general as we deal with a large class of rings, not only for fields as before. Let R be a commutative ring with unity, $\partial : R \to R$ is a derivation of R to itself, and $t \in R$ an element with $\partial(t) = 1$. We denote by R^∂ the subring of "constants". For any constant $a \in R^\partial$, the element $t + a$ of R also satisfies $\partial(t + a) = 1$.

Fix an integer $n \geqslant 1$, 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

$$D(fv) = \partial(f)v + fD(v) \tag{3.1}$$

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

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

$$c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} \sum_{k=0}^{j} (-1)^k \binom{j}{k} D^k(e_{n-k}). \tag{3.2}$$

Theorem 3.1 (N. Katz, [Kat87]). *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. We compute the successive derivatives of $c(\mathbf{e}, t-a)$. For convenience, we define the following elements

$$c(i, j) \in V \text{ indexed by } i, j \text{ integers } \geqslant 0,$$

inductively by the formulas

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

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

$$c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(0, j). \tag{3.3}$$

We shall prove by induction that

$$D^i c(\mathbf{e}, t-a) = \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(i, j). \tag{3.4}$$

Before that, we shall show that

(i) $\partial((t-a)^j) = j(t-a)^{j-1}$. This can be proved by induction. Indeed, for $j = 1$, it is true since $\partial(t) = 1, \partial(a) = 0$. Suppose it is true for j, then we have

$$\partial((t-a)^{j+1}) = (t-a)\partial((t-a)^j) + (t-a)^j \partial(t-a)$$

(ii) $c(i,j) = 0$ if $j \geqslant n$. Again, this can be proved by induction because $c(0,j) = 0$ if $j \geqslant n$ and $c(i+1,j) = c(i,j+1) + D(c(i,j))$. In particular, we deduce that $c(i+1,n-1) = D(c(i,j))$ because $c(i,n) = 0$.

The case $i = 0$ is trivial, suppose it is true for i, we shall prove that it holds for $i+1$. Applying D to our induction hypothesis

$$\begin{aligned}
D^{i+1}c(\mathbf{e}, t-a) &= D\left(\sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(i,j)\right) \\
&= \sum_{j=0}^{n-1} \left(\frac{1}{j!}\partial((t-a)^j)c(i,j) + \frac{(t-a)^j}{j!} D(c(i,j))\right) \\
&\overset{(i)}{=} \sum_{j=0}^{n-1} \left(\frac{(t-a)^{j-1}}{(j-1)!} c(i,j) + \frac{(t-a)^j}{j!} D(c(i,j))\right) \\
&= \frac{(t-a)^{n-1}}{(n-1)!} D(c(i,n-1)) + \sum_{j=0}^{n-2} \left(\frac{(t-a)}{j!} c(i,j+1) + \frac{(t-a)^j}{j!} D(c(i,j))\right) \\
&\overset{(ii)}{=} \sum_{j=0}^{n-1} \frac{(t-a)^j}{j!} c(i+1,j).
\end{aligned}$$

Another straightforward induction shows that

$$c(i,j) = \sum_{k=0}^{j} (-1)^k \binom{j}{k} D(e_{i+j-k}) \ \forall\ i+j \leqslant n-1. \tag{3.5}$$

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

$$D^i c(\mathbf{e}, t-a) \equiv e_i \bmod (t-a)V. \tag{3.6}$$

Denote by I the ideal generated by $D^i c(\mathbf{e}, t-a)$, then we can easily see that

$$V = (t-a)V + I, \tag{3.7}$$

but $(t-a)$ is contained in the maximal ideal of R so we apply Nakayama's lemma (recall that V is finitely generated) to conclude that $V = I$; equivalently, $c(\mathbf{e}, t-a)$ is a cyclic vector. □

Theorem 3.2 (N. Katz, [Kat87]). *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 Zariski locally on $X = \mathrm{Spec}(R)$, one of the vectors $c(\mathbf{e}, t-a_i)$, $i = \overline{0, n(n-1)}$, is a cyclic vector.*

Remark. Here *Zariski locally* literally means there exists an open covering $\mathrm{Spec}(R) = \bigcup_i \mathrm{Spec}(R_i)$ such that the conclusion holds for each R_i.

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

$$c_i(\mathbf{e}, X) = \sum_{j=0}^{n-1} \frac{X^j}{j!} c(i,j). \tag{3.8}$$

Taking wedge product gives us

$$c_0(\mathbf{e}, X) \wedge \cdots \wedge c_{n-1}(\mathbf{e}, X) = P(X) e_0 \wedge \cdots \wedge e_{n-1}, \tag{3.9}$$

where P is a polynomial of degree $\leqslant n(n-1)$. We know in the proof of the previous theorem that $c_i(\mathbf{e}, 0) = e_i$, so $P(0) = 1$. At $X = t - a$, we know from (3.4) that $c_i(\mathbf{e}, t-a) = D^i c(\mathbf{e}, t-a)$; therefore, $c(\mathbf{e}, t-a)$ is a cyclic vector if and only if $P(t-a) \in R^\times$. We must show that the ideal generated by $P(t-a_i)$ is the unit ideal. Let us write explicitly

$$P(X) = \sum_{j=0}^{n(n-1)} r_j X^j. \tag{3.10}$$

If we take r_j as variables then we have a system consisting of $n(n-1)+1$ equations

$$P(t-a_i) = \sum_{j=0}^{n(n-1)} r_j (t-a_i)^j. \tag{3.11}$$

The determinant of this system is the well-known Van der Monde determinant:

$$\det\left((t-a_i)^j_{0\leqslant i,j\leqslant n(n-1)}\right) = \prod_{0\leqslant i<j\leqslant n(n-1)} (a_i - a_j) \in k^\times \subset R^\times. \tag{3.12}$$

From this we see that the ideal generated by $P(t-a_i)$ equals the ideal generated by the coefficients r_i, but $r_0 = P(0) = 1$. □

The proof theorem 3.2 also yields the following variant.

Corollary 3.3. *Let R be a ring in which $(n(n-1))!$ is invertible, then Zariski locally on* $\mathrm{Spec}(R)$*, one of the vectors $c(\mathbf{e}, t-i)$, $i = \overline{0, n(n-1)}$ is a cyclic vector.*

Proof. Since $(n(n-1))!$ is invertible, we deduce that all constants $0, 1, ..., n(n-1)$ are contained in k. Thus, we may apply previous theorem with $a_i = i$. □

Remark.

- Suppose $\mathbf{e} = (e_0, ..., e_{n-1})$ is a cyclic basis to begin with, i.e., e_0 is a cyclic vector and $e_i = D^i e_0$ for $i = \overline{0, n-1}$. Then $c(0,0) = e_0$ and $c(0,j) = 0$ for $j > 0$. Therefore $c(\mathbf{e}, t-a) = e_0$ is the cyclic vector we began with.

- Suppose R is a field, $n \geqslant 2$. If $(n-1)!$ is not invertible in R, (V, D) may admit no cyclic vector. For example, take $R = \mathbb{F}_p(t)$, $\partial = d/dt$, $V = R^n$, $D(f_1, ..., f_n) = (\partial f_1, ..., \partial f_n)$. Because $\partial^p = 0$, so $D^p = 0$, so (V, D) admits no cyclic vector if $p \leqslant n-1$.

- Suppose R is a field, $n \geqslant 2$, and $(n-1)!$ is invertible in R. For a suitably chosen basis $\mathbf{e}$, $c(\mathbf{e}, t)$ can vanish. Indeed, if e_0 is a cyclic vector, and if $e_i = D^i e_0$ for $i = \overline{0, n-2}$ then

$$c(\mathbf{e}, t) = e_0 + \frac{t^{n-1}}{(n-1)!}(e_{n-1} - D^{n-1} e_0),$$

  so we can solve for e_{n-1} to force $c(\mathbf{e}, t) = 0$.

- If R is a field in which $(n-1)!$ is invertible, and which is finitely generated extension of an algebraically closed subfield k of R^{∂}. Given $(V, D, \mathbf{e})$ over R, write the connection in the matrix form

$$De_j = \sum_j a_{ij} e_i. \tag{3.13}$$

There exists a ∂-stable k-subalgera R_0 of R which is finitely generated as a k-algebra, and which contains t and all entrices a_{ij}. We have a canonical descent $(V_0, D, \mathbf{e})$ of $(V, D, \mathbf{e})$, here by V_0 we mean V but it is considered as a R_0-module. For every k-point x of $X = \mathrm{Spec}(R_0)$, we have inclusions

$$R_0 \subset \mathcal{O}_{X,x} \subset R, \tag{3.14}$$

where the first inclusion follows from the fact that R_0 is a domain while the second one is obvious as well since R is a field. Since x is a k-point, we denote by $t(x)$ the image of t in k under the canonical morphism. By theorem 3.1 we know that $c(\mathbf{e}, t - t(x))$ is a cyclic vector for $V_0 \otimes_{R_0} \mathcal{O}_{X,x}$ because $t - t(x)$ is zero in the residue field and hence contained in the maximal ideal. Therefore, à fortiori $c(\mathbf{e}, t - t(x))$ is a cyclic vector for $V = V_0 \otimes_{R_0} R$ itself.

- The formula (3.2) is not randomly chosen. A heuristic reason to write such a cumbersome formular is the following. 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

$$\sum_{j=0}^{n-1} \frac{t^j}{j!} h_j \tag{3.15}$$

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

$$\widetilde{v} = \sum_{k \geqslant 0} (-1)^k \frac{t^k}{k!} D^k(v) \tag{3.16}$$

is the unique solution of

$$\widetilde{v} \equiv v \bmod tV, \ D(\widetilde{v}) = 0. \tag{3.17}$$

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

$$\sum_{j=0}^{n-1} \frac{t^j}{j!} \widetilde{e}_j = \sum_{j=0}^{n-1} \frac{t^j}{j!} \sum_{k \geqslant 0} (-1)^k \frac{t^k}{k!} D^k(e_j) \tag{3.18}$$

is a cyclic vector. 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 $i = \overline{0, n-1}$,

$$D^i(v + t^n v_0) \equiv D^i v \bmod t^{n-i} V. \tag{3.19}$$

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

$$\sum_{j=0}^{n-1} \frac{t^j}{j!} \sum_{k=0}^{n-1-j} (-1)^k \frac{t^k}{k!} D^k(e_j) \tag{3.20}$$

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

There is another variant which improves Katz's results in the case of a differential system over a field $R = K$. The ring of constants K^{∂} turns out to be a field, so it contains a prime field (either $\mathbb{Z}/p$ or $\mathbb{Q}$), this prime field is denoted K_C.

Theorem 3.4. *Suppose $R = K$ is a field, and K_C contains at least n non-zero elements and that the extension K/K_C is either infinite or of degree at least n. Then every n-dimensional differential K-space (V, ∂, D) admits a cyclic vector.*

Proof. [GCKS02], *Cyclic Vectors*, **theorem 3.11**. □

Remark. The hypotheses of the above theorem are essential, R. C. Churchill and Jerald J. Kovacic constructed counterexamples in case we dismiss either hypothesis of the cardinality of K_C or the degree of the extension K/K_C.

References

[GCKS02] Li Guo, Phyllis J. Cassidy, William F. Keigher, and William Y. Sit, editors. *Differential algebra and related topics*. World Scientific Publishing Co., Inc., River Edge, NJ, 2002. ↑10

[Kat70] Nicholas M. Katz. Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin. *Inst. Hautes Études Sci. Publ. Math.*, (39):175–232, 1970. ↑5

[Kat76] Nicholas M. Katz. An overview of Deligne's work on Hilbert's twenty-first problem. In *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*, pages 537–557, 1976. ↑1

[Kat87] Nicholas M. Katz. A simple algorithm for cyclic vectors. *Amer. J. Math.*, 109(1):65–70, 1987. ↑6 , ↑7