



A Simple Algorithm for Cyclic Vectors

Nicholas M. Katz

American Journal of Mathematics, Vol. 109, No. 1. (Feb., 1987), pp. 65-70.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9327%28198702%29109%3A1%3C65%3AASAFCV%3E2.0.CO%3B2-A>

American Journal of Mathematics is currently published by The Johns Hopkins University Press.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/journals/jhup.html>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

The JSTOR Archive is a trusted digital repository providing for long-term preservation and access to leading academic journals and scholarly literature from around the world. The Archive is supported by libraries, scholarly societies, publishers, and foundations. It is an initiative of JSTOR, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology. For more information regarding JSTOR, please contact support@jstor.org.

A SIMPLE ALGORITHM FOR CYCLIC VECTORS

By NICHOLAS M. KATZ

Statement of Results. Let R be a commutative ring with unit, $\partial: R \rightarrow R$ a derivation of R to itself, and $t \in R$ an element with $\partial(t) = 1$. We denote by $R^\partial = \text{Ker}(\partial)$ 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 $n \geq 1$, and a triple (V, D, \vec{e}) consisting of a free R -module V of rank n , an additive mapping $D: V \rightarrow V$ satisfying

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

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

An element $v \in V$ is said to be a cyclic vector for (V, D) if $v, Dv, \dots, D^{n-1}(v)$ is an R -basis of V ; a basis of this form is called a cyclic basis.

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

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

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

THEOREM 2. *Let R be a ring in which $(n-1)!$ is invertible, and let k be a sub-field of R^∂ . Suppose that $\#(k) > n(n-1)$, and let $a_0, a_1, \dots, a_{n(n-1)}$ be $1 + n(n-1)$ distinct elements of k . Then Zariski locally on $\text{Spec}(R)$, one of the vectors $c(\vec{e}, t - a_i)$, $0 \leq i \leq n(n-1)$, is a cyclic vector.*

Proofs. We first compute the derivatives of $c(\vec{e}, t - a)$. For this, we introduce the elements

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

defined inductively as follows:

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

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

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

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

Successively applying D , we easily verify by induction on i that for $i \geq 0$ we have

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

A straightforward induction on $i + j$ shows that for $i + j \leq n - 1$, we have

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

and so in particular we have

$$(***) \quad c(i, 0) = e_i \quad \text{for } i = 0, 1, \dots, n-1.$$

Therefore (**) yields the congruence

$$D^i c(\vec{e}, t - a) \equiv e_i \pmod{(t-a)V}, \quad \text{for } 0 \leq i \leq n-1,$$

from which Theorem 1 follows, by Nakayama's lemma.

To prove Theorem 2, we argue as follows. For $0 \leq i \leq n - 1$, and variable $X \in R$, we define elements $c_i(\vec{e}, X)$ in V by

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

In $\Lambda''(V)$, we visibly have

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

with $P(X)$ the value at X of a polynomial $P(T) \in R[T]$ of degree $\leq n(n - 1)$. By (**), we have $c_i(\vec{e}, 0) = e_i$, so

$$P(0) = 1.$$

At $X = t - a$ with a constant, (**) gives

$$c_i(\vec{e}, t - a) = D^i c(\vec{e}, t - a).$$

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

We must show that the ideal I in R generated by the $1 + n(n - 1)$ values $P(t - a_i)$ is the unit ideal. Let us write explicitly

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

Then

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

But for $i \neq j$, the differences $(t - a_i) - (t - a_j) = a_j - a_i$ lie in k^\times , so in R^\times ; hence the van der Monde determinant

$$\det((t - a_i)_{0 \leq i, j \leq n(n-1)}^j)$$

lies in R^\times . Therefore the ideal I is equal to the ideal generated by the coefficients $r_0, \dots, r_{n(n-1)}$ of $P(X)$. But $r_0 = P(0) = 1$. Q.E.D.

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

(2) Suppose R is a field, and $n \geq 2$. If $(n-1)!$ is not invertible in R , (V, D) may admit no cyclic vector. For take a prime number p , $R = \mathbf{F}_p(t)$, $\partial = d/dt$, $V = R^n$, $D(f_1, \dots, f_n) = (\partial f_1, \dots, \partial f_n)$. Because $\partial^p = 0$, we have $D^p = 0$, so (V, D) admits no cyclic vector if $p \leq n-1$.

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

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

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

(4) If R is a field in which $(n-1)!$ is invertible, and which is a finitely generated extension of an algebraically closed subfield k of R^∂ , then we can use Theorem 1 to produce cyclic vectors. Notice first that for any finite subset S of R , there exists a ∂ -stable k -subalgebra R_0 of R which is finitely generated as a k -algebra, and which contains S (in terms of generators x_1, \dots, x_N of R/k , write each $\partial(x_i)$ and each $s \in S$ as a ratio of k -polynomials in the x_j 's whose denominators are nonzero in R ; then take for R_0 the k -subalgebra of R generated by the x_i and by the inverses of the denominators of both the $\partial(x_i)$ and the $s \in S$). Given (V, D, \vec{e}) over R , we apply this to the set S consisting of t and of the n^2 coefficients a_{ij} of the connection matrix, defined by

$$De_j = \sum_i a_{ij} e_i.$$

Over the resulting R_0 , we have a canonical descent (V_0, D, \vec{e}) of the original (V, D, \vec{e}) over R . For any k -valued point of $X = \text{Spec}(R_0)$, we have ring inclusions $R_0 \subset \mathcal{O}_{X,x} \subset R$, and by Theorem 1 we know that $c(\vec{e}, t - t(x))$ is a cyclic vector for $V_0 \otimes_{R_0} \mathcal{O}_{X,x}$, so a fortiori $c(\vec{e}, t - t(x))$ is a cyclic vector for $V = V_0 \otimes_{R_0} R$ itself.

(5) The heuristic which leads to considering $c(\vec{e}, t)$ is the following. Suppose $R = \mathbf{C}[[t]]$, $\partial = d/dt$. If h_0, \dots, h_{n-1} is a horizontal R -basis of V , i.e., an R -basis with $Dh_i = 0$ for $0 \leq i \leq n-1$, then

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

is obviously a cyclic vector. Now given any $v \in V$, the t -adically convergent series (cf. [2], proof of 8.9)

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

is the unique solution of

$$\tilde{v} \equiv v \pmod{tV}, \quad D(\tilde{v}) = 0.$$

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

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

is a cyclic vector. But if $v \in V$ 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 $0 \leq i \leq n-1$,

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

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 $c(\vec{e}, t)$.

(6) The proof of Theorem 2 also yields the following variant: If R is a ring in which $(n(n-1)!)!$ is invertible, then Zariski locally on $\text{Spec}(R)$, one of the vectors $c(\vec{e}, t-i)$, $0 \leq i \leq n(n-1)$, is a cyclic vector.

REFERENCES

-
1. F. T. Cope, Formal solutions of irregular linear differential equations, Part II, *Amer. J. Math.*, **58** (1936), 130–140.
 2. P. Deligne, *Equations différentielles à points singuliers réguliers*, Springer Lecture Notes in Mathematics, **163** (1970).
 3. N. Katz, Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin, *Pub. Math. I.H.E.S.*, **39** (1970), 175–232.