Iterative Differential Equations and Finite Groups

Bernd Heinrich Matzat

It is an old question to characterize those differential equations or differential modules, respectively, whose solution spaces consist of functions which are algebraic over the base field. The most famous conjecture in this context is due to A. Grothendieck and relates the algebraicity property with the p-curvature which appears as the first integrability obstruction in characteristic p. Here we prove a variant of Grothendieck's conjecture for differential modules with vanishing higher integrability obstructions modulo p - these are iterative differential modules - and give some applications.

1. Pseudo Picard-Vessiot Rings over Number Fields

To fix our notation let F/K be a function field of one variable over a number field K with a derivation ∂_F normalized by $\partial_F(t) = 1$ for some $t \in F$. Then $F/K(t)$ is a finite field extension, and ∂_F is the unique extension of $\partial_t := \frac{d}{dt}$ to F. Any linear differential equation over F defines a finite dimensional differential module (D-module) M over F. This is an F-vector space equipped with a derivation $\partial_M : M \to M$ which is an additive map with

$$\partial_M(x \cdot a) = \partial_M(x) \cdot a + x \cdot \partial_F(a) \text{ for } x \in M, a \in F.$$

With respect to some basis $B = \{b_1, ..., b_m\}$ of M the derivation is given by a matrix $A \in F^{m \times m}$.

Now we are interested in finding a minimal differential extension field E/F such that the solution space $\mathrm{Sol}_E(M)$ of M in E, defined by $\partial_E(\underline{y}) = A \cdot \underline{y}$ for $\underline{y} = (y_1, \ldots, y_m)^{\mathrm{tr}} \in E^m$, has dimension m. Such a field can be constructed in the following way (compare [7], Ch. 1.3): The coordinate ring of the affine group GL_m over F

$$U := F[\mathrm{GL}_m] = F[x_{ij}, \det(x_{ij})^{-1}]_{i,j=1}^m$$

becomes a differential ring (D-ring) by defining $\partial_U(X) = A \cdot X$ for $X = (x_{ij})_{i,j=1}^m$. Then the residue ring R of U by a maximal differential ideal $P \triangleleft U$ is a D-ring and a domain containing a matrix $Y \in \mathrm{GL}_m(R)$ with $\partial_R(Y) = A \cdot Y$ and ∂_R obtained from ∂_U. Thus R contains a fundamental solution matrix of M, and for $E := \mathrm{Quot}(R)$ holds $\dim_K(\mathrm{Sol}_E(M)) = m$.

In order to find an R without new constants we assume that F/K contains a prime $\wp$ of degree one which is regular for M, i. e., $\wp$ is a regular point. Since M has only finitely many singular points, such a $\wp$ always exists in the case $F = K(t)$ or after a finite extension by constants. Choosing a local parameter $u \in F$ for $\wp$, the D-module M possesses a fundamental solution matrix $Y \in \mathrm{GL}_m(K[[u]])$ which can be normalized by $Y(\wp) \in \mathrm{GL}_m(K)$. Denoting by P the kernel of the differential homomorphism $\pi : U \to K((u))$ defined by $\pi(X) = Y$, the D-ring $R := U/P$ is regular over K. Obviously all fundamental solution matrices $Y \in \mathrm{GL}_m(K[[u]])$ with $Y(\wp) \in \mathrm{GL}_m(K)$ only differ by matrices $C \in \mathrm{GL}_m(K)$. Hence R is uniquely determined up to differential isomorphisms by the property

above. It further depends neither on the chosen local parameter nor on the chosen regular rational point $\wp$. In the following the D-ring (R, ∂_R) is called a *pseudo Picard-Vessiot ring* (PPV-ring) and its field of fractions (E, ∂_E) a *PPV-field*.

The F-automorphisms of E commuting with ∂_E form a group $\mathrm{Aut_D}(E/F)$ and define an affine group scheme $\mathcal{G} \leq \mathrm{GL}_m$ over K with $\mathcal{G}(K) \cong \mathrm{Aut_D}(E/F)$, called the *Galois group scheme of* E/F. In case the fixed field $E^{\mathcal{G}(K)}$ equals F, the ring R/F or E/F respectively are called *Picard-Vessiot ring* (PV-ring) or *PV-field*, and $\mathcal{G}(K) =: \mathrm{Gal_D}(E/F)$ is the *differential Galois group of* E/F. It is well known that for connected groups the notion of a PPV-ring and a PV-ring coincide.

By the assumptions above we obtain the following variant of T. Dyckerhoff of the differential Galois correspondence due to E. Kolchin valid over number fields:

Theorem 1. ([2]): *Let (F, ∂_F) be a D-field of one variable over a number field K and (M, ∂_M) be a D-module over F with regular rational point $\wp$ in F. Then the following hold:*

(a) *There exists a PPV-field E/F for M without new constants. E/F is uniquely determined by $Y(\wp) \in \mathrm{GL}_m(K)$ up to differential isomorphisms.*
(b) *There exists a Galois correspondence between the subgroup schemes of the Galois group scheme $\mathcal{G}$ and the differential intermediate fields of E/F.*

2. Grothendiecks p-Curvature Conjecture

By the first section the algebraicity of the solutions of a D-module, the algebraicity of the corresponding PPV-field E/F and the finiteness of $\mathrm{Gal_D}(E/F)$ are equivalent. In case E/F and thus $E/K(t)$ are algebraic, the property $\partial_t^p \equiv 0 \pmod p$ of $K(t)$ implies $\partial_E^p \equiv 0 \pmod p$ for almost all primes. According to A. Grothendieck (1970), this property should be characteristic. To be more precise, let (M, ∂_M) be a D-module over F. Then the p-curvature of M is the p-th iterate ∂_M^p of ∂_M. It is called trivial in the case $\partial_M^p \equiv 0 \pmod p$.

P-Curvature Conjecture. *Let (F, ∂_F) be a D-field of one variable over a number field K and (M, ∂_M) be a D-module over F. Then the following are equivalent:*

(1) *M admits a full system of algebraic solutions.*
(2) *The p-curvature of M is trivial for almost all primes p.*

An equivalent condition has been detected by P. Cartier using reduction. For this purpose let $\mathfrak{p}$ denote a prime divisor (place) dividing p in K, $\mathfrak{p}_t$ its Gauss extension to $K(t)$ and $\mathfrak{P}$ a place F extending $\mathfrak{p}_t$. Then the reduction $F_\mathfrak{P}$ of F modulo $\mathfrak{P}$ is a function field with finite field of constants. In case (M, ∂_M) is a D-module over F with representing matrix $A \in F^{m \times m}$ of ∂_M, for almost all $\mathfrak{P}$ the reduced matrix $A_\mathfrak{P} \in F_\mathfrak{P}^{m \times m}$ exists and defines the derivation of a D-module $M_\mathfrak{P}$ over $F_\mathfrak{P}$. The same procedure works for any of the matrices $A^{(k)}$ corresponding to the higher derivation $\partial_M^{(k)} := \frac{1}{k!}\partial_M^k$. Fortunately these can be computed iteratively using the so-called Taylor recursion:

$$A^{(0)} = I, A^{(1)} = A, kA^{(k)} = \partial_F\left(A^{(k-1)}\right) + A^{(k-1)} \cdot A.$$

In the case $\partial_M^p \equiv 0 \pmod p$, the formulas above show that

$$Y_{\mathfrak{P}} := (\sum_{k=0}^{p-1} A_{\mathfrak{P}}^{(k)}(-u)^k)^{-1} \in \mathrm{GL}_m(F_{\mathfrak{P}})$$

is a fundamental solution matrix of the reduced D-module $M_{\mathfrak{P}}$, i.e., $M_{\mathfrak{P}}$ is trivial over $F_{\mathfrak{P}}$.

Lemma of Cartier: *Let (F, ∂_F) be a D-field of one variable over a number field K and (M, ∂_M) be a D-module over F. Then (2) is equivalent to:*

(3) *The reduced D-module $M_{\mathfrak{P}}$ is trivial for almost all $\mathfrak{P}$.*

The Lemma of Cartier shows that in this way D-modules over F with algebraic solutions are reduced to D-modules over $F_{\mathfrak{P}}$ with rational (=trivial) solutions. Comparing with algebraic field extensions this property looks quite unnatural.

3. Iterative Differential Modules

In order to preserve by reduction the degree of algebraicity we have to use in addition higher derivations. But then we have to work with infinitely many $\partial_F^{(k)}$ and $A^{(k)}$ and thus to give more care on our D-rings. For this purpose let $\mathbb{P}'_K \subseteq \mathbb{P}_K$ be a cofinite set of primes $\mathfrak{p}$ in K and $\mathcal{O}'_K$ the intersection of their valuation rings $\mathcal{O}_{\mathfrak{p}}$. Further let $\mathbb{P}'_F$ be the set of all places $\mathfrak{P}$ in F extending the Gauss valuation $\mathfrak{p}_t$ in $K(t)$ for $\mathfrak{p} \in \mathbb{P}'_K$. Then $\mathcal{O}'_F := \bigcap_{\mathfrak{P} \in \mathbb{P}'_F} \mathcal{O}_{\mathfrak{P}}$ is a Dedekind ring in F. It is called a *global iterative differential ring* (ID-ring) if

$$\partial_F^{(k)}(\mathcal{O}'_F) \subseteq \mathcal{O}'_F \text{ and } \partial_F^{(k)}(\mathfrak{P}) \subseteq \mathfrak{P} \text{ for all } k \in \mathbb{N} \text{ and } \mathfrak{P} \in \mathbb{P}'_F.$$

Obviously any function field of one variable F/K contains infinitely many such global ID-rings. In a similar way we define *global ID-modules* M to be free $\mathcal{O}'_F$-modules of finite rank with higher derivations $\partial_M^{(k)} := \frac{1}{k!}\partial_M^k : M \to M$.

Under these assumptions we can follow Section 1 in order to construct a PPV-ring R for M now over the global ID-ring $\mathcal{O}'_F$ with a fundamental solution matrix $Y \in \mathrm{GL}_m(R)$ and with $Y(\wp) \in \mathrm{GL}_m(\mathcal{O}'_K)$ for some regular prime $\wp$ of degree one of F/K. Since by definition all matrices $A^{(k)}$ belong to $(\mathcal{O}'_F)^{m\times m}$, this PPV-ring R is equipped with an iterative derivation $\left(\partial_R^{(k)}\right)_{k\in\mathbb{N}}$ and thus is itself an ID-ring. In all we obtain the following ID-analogue of Theorem 1.

Theorem 2. ([4])*: Let $(\mathcal{O}'_F, \partial_F)$ be a global ID-ring and (M, ∂_M) be a global ID-module over $\mathcal{O}'_F$ with regular rational prime $\wp$ in $\mathcal{O}'_F/\mathcal{O}'_K$. Then there exists a PPV-ring R_M over $\mathcal{O}'_F$ with ring of constants $\mathcal{O}'_K$. Moreover R_M is unique up to D-isomorphisms by assuming $Y(\wp) \in \mathrm{GL}_m(\mathcal{O}'_K)$.*

If in addition the spezialized matrix $A(\wp)$ belongs to $(\mathcal{O}'_K)^{m\times m}$ - this can be reached by removing a finite set of primes $\mathfrak{P}$ from $\mathbb{P}'_F$ - then $A^{(k)}(\wp) \in (\mathcal{O}'_K)^{m\times m}$ holds for all $k \in \mathbb{N}$ by Taylor recursion. This leads to

Corollary 1. *Assuming in addition $A(\wp) \in (\mathcal{O}'_K)^{m\times m}$, the Taylor expansion of Y for a local parameter u for $\wp$ belongs to $\mathrm{GL}_m(\mathcal{O}'_K[[u]])$.*

In particular, the Taylor expansions in u of the entries y_{ij} of Y are globally bounded in the sense of G. Christol (compare [1], Ch. 4.1). It should be mentioned that any finite Galois extension E/F without new constants can be obtained as field of fractions of a PPV-ring R_M of some global ID-module M over a global ID-ring $\mathcal{O}'_F$. Thus any finite group appears as differential Galois group of such a global ID-module.

4. Reduction of Global ID-Modules.

Let (M, ∂_M) be a global ID-module over a global ID-ring $(\mathcal{O}'_F, \partial_F)$. Then by Theorem 2 there exists a PPV-ring $R_M/\mathcal{O}'_F$ for M. As before, for all $\mathfrak{P} \in \mathbb{P}'_F$ the residue field $F_\mathfrak{P} := \mathcal{O}'_F/\mathfrak{P}$ is a function field of one variable over the finite field $K_\mathfrak{p} := \mathcal{O}'_K/\mathfrak{p}$ and the residue ring $(R_M)_\mathfrak{P} := R_M/R_M\mathfrak{P}$ is an $F_\mathfrak{P}$-algebra.

On the other side the reduced matrices $A_\mathfrak{P}^{(k)} \in F_\mathfrak{P}^{m\times m}$ define an iterative derivation $(\partial_{M_\mathfrak{P}}^{(k)})_{k\in\mathbb{N}}$ on some $F_\mathfrak{P}$-vector space $M_\mathfrak{P}$. Thus $M_\mathfrak{P}$ is an ID-module over $F_\mathfrak{P}$ as studied for example in [5], Ch. 5. By [5], Prop. 6.1, there exists a PV-ring for $M_\mathfrak{P} \otimes_{K_\mathfrak{p}} \overline{K_\mathfrak{p}}$ over $F_\mathfrak{P} \otimes_{K_\mathfrak{p}} \overline{K_\mathfrak{p}}$. In case $F_\mathfrak{P}$ contains a regular point $\tilde{\wp}$ of degree one for $M_\mathfrak{P}$, an argument like the one given in Section 1 shows that there exists an iterative PPV-ring $R_{M_\mathfrak{P}}$ over $F_\mathfrak{P}$ without new constants. Further $R_{M_\mathfrak{P}}$ is uniquely determined up to ID-isomorphisms by the property that a fundamental solution matrix $Y_\mathfrak{P}$ of $M_\mathfrak{P}$ in $R_{M_\mathfrak{P}}$ at $\tilde{\wp}$ has initial values in $\mathrm{GL}_m(K_\mathfrak{p})$. The next theorem shows that for almost all $\mathfrak{P} \in \mathbb{P}'_F$ the reduced PPV-ring $(R_M)_\mathfrak{P}$ and the PPV-ring $R_{M_\mathfrak{P}}$ constructed from the reduced matrices $A_\mathfrak{P}^{(k)}$ coincide.

Theorem 3. ([4]): *Let (M, ∂_M) be a global ID-module over a global ID-ring $(\mathcal{O}'_F, \partial_F)$. Then for almost all $\mathfrak{P} \in \mathbb{P}'_F$ the reduced PPV-ring $(R_M)_\mathfrak{P}$ and the PPV-ring of the reduced ID-module $M_\mathfrak{P}$ are isomorphic as ID-rings.*

The proof of Theorem 3 relies on the compatibility of the Taylor expansions in different characteristics based on the globally boundedness. By the Generic Flatness Lemma then follows

Corollary 2. *For almost all $\mathfrak{P} \in \mathbb{P}'_F$ holds*

$$\dim(R_{M_\mathfrak{P}}) = \dim(R_M) - 1 = \dim(R_M/\mathcal{O}'_F).$$

Thus Corollary 2 proves the last conjecture statet in [5]. A D-module is called algebraic if it admits a full system of algebraic solutions over the base ring.

Theorem 4. ([4]): *Let (M, ∂_M) be a global ID-module over a global ID-ring $(\mathcal{O}'_F, \partial_F)$. Then the following hold:*

(a) *$M/\mathcal{O}'_F$ is algebraic if and only if the reduced ID-modules $M_\mathfrak{P}/F_\mathfrak{P}$ are algebraic for almost all $\mathfrak{P} \in \mathbb{P}'_F$.*

(b) *$\mathrm{Gal}_\mathrm{D}(R_M/\mathcal{O}'_F)$ is a finite group G if and only if $\mathrm{Gal}_\mathrm{ID}(R_{M_\mathfrak{P}}/F_\mathfrak{P}) \cong G$ for almost all $\mathfrak{P} \in \mathbb{P}'_F$.*

For global ID-modules this theorem refines Cartier's Lemma in Section 2

5. The Link with Grothendieck's Conjecture

According to Grothendieck's conjecture the following conjecture should be true:

Conjecture 1. *Any global ID-module (M, ∂_M) over a global ID-ring $(\mathcal{O}'_F, \partial_F)$ is algebraic.*

To prove Conjecture 1, by Theorem 4 it would be enough to show that reductions modulo $\mathfrak{P}$ lying in $K_{\mathfrak{p}}[[u]]$ of globally bounded solutions of linear differential equations at a regular point are algebraic over $K_{\mathfrak{p}}(u)$.

The truth of Conjecture 1 would already imply an interesting algebraicity criterion for formal power series over number fields.

Eisenstein's Algebraicity Criterion. *Let $f = \sum_{k\in\mathbb{N}} a_k t^k$ be a formal power series over a number field K. Then the following are equivalent:*

(a) *f is algebraic over $K(t)$,*

(b) *f is regularly differentially finite and globally bounded.*

Here an element $f \in K[[t]]$ is called regularly differentially finite if it is a solution of a linear differential equation over $K(t)$, which is regular at 0. The proof that (a) implies (b) is due to G. Eisenstein (reported in [3]). Eisenstein's intention was to develop at least a necessary condition for the algebraicity of solutions of differential equations. The converse implication (b) to (a) would follow from Conjecture 1. It is known that the property being globally bounded is not sufficient at singular points.

The link with Grothendieck's p-curvature conjecture would then be given by the following second conjecture:

Conjecture 2. *Let (M, ∂_M) be a global D-module over a global D-ring $(\mathcal{O}'_F, \partial_F)$ with vanishing p-curvature for almost all primes $p \in \mathbb{Z}$. Then the solutions of M near a non singular prime $\wp$ of degree one in F for M are given by locally bounded power series over the field of constants K of F.*

Obviously Grothendieck's p-curvature conjecture follows from Conjecture 1 and 2. Thus these two conjectures could indicate a way of approaching its proof.

References

[1] André, Y.: *G-functions and Geometry.* Vieweg, Wiesbaden 1989.

[2] Dyckerhoff, T.: *Picard–Vessiot Extensions over Number Fields.* Diplomarbeit, Heidelberg 2005.

[3] Eisenstein, G.: Über eine allgemeine Eigenschaft der Reihen-Entwicklungen algebraischer Funktionen (Bericht von 1852). *Mathematische Werke II*, S. 765–767, Chelsea Publ. Comp., New York 1975.

[4] Matzat, B. H.: Differential equations and finite groups. J. Algebra, to appear.

[5] Matzat, B. H.; van der Put, M.: Iterative differential equations and the Abhyankar conjecture. J. reine angew. Math. **257** (2003), 1-52.

[6] Matzat, B. H.; van der Put, M.: Constructive differential Galois theory. Pp. 425-467 in L. Schneps (Ed.): *Galois Groups and Fundamental Groups*, MSRI Publications 41, Cambridge Univ. Press 2003.

[7] van der Put, M.; Singer, M.F.: *Galois Theory of Linear Differential Equations.* Springer-Verlag, Berlin etc. 2003.