Séminaires & Congrès
13, 2006, p. 263–292

INTEGRAL p-ADIC DIFFERENTIAL MODULES

by

B. H. Matzat

Abstract. — An integral (or bounded) local D-module is a differential module over a local D-ring R having congruence solution bases over R. In case R is equipped with an iterative derivation, such a D-module is an iterative differential module (ID-module) over R. In this paper we solve the connected inverse Galois problem for integral D-modules over fields of analytic elements $K\{t\}$. In case the residue field of K is algebraically closed, we are able to additionally solve the non-connected inverse Galois problem. Further we study the behaviour of ID-modules by reduction of constants.

***Résumé* (Modules différentiels p-adiques bornés).** — Un D-module local borné est un module différentiel sur un anneau local différentiel R qui possède des bases sur R pour les solutions de congruence. Si R est muni d'une dérivation itérative, un tel D-module en plus est un module différentiel itératif (ID-module) sur R. Dans ce texte nous présentons une solution du problème inverse de Galois connexe pour les D-modules bornés sur des corps d'éléments analytiques $K\{t\}$. Dans le cas où le corps résiduel de K est algébriquement clos nous donnons en plus une solution du problème inverse pour les groupes linéaires non connexes. Finalement nous étudions la relation entre les ID-modules locaux et leurs réductions.

0. Introduction

Integral (or bounded) p-adic differential modules are D-modules over a p-adic D-ring having congruence solution bases over the base ring. By [**Chr83**], Theorem 4.8.7, these are solvable in the ring of analytic functions over the open generic disc. Our interest in this special class of p-adic D-modules comes from the fact that they appear as lifts of (iterative) D-modules in characteristic p (see [**MvdP03b**], [**Mat01**]). This property sometimes allows to solve problems using techniques developed for the

2000 ***Mathematics Subject Classification.*** — 12H25, 13N05, 20G25.
Key words and phrases. — p-adic differential equations, locally bounded D-modules, ID-modules (iterative differential modules), linear algebraic groups over local fields and their integers, fields of analytic elements, inverse problem of Galois theory, reduction of ID-modules.

characteristic p theory. Further, this class also contains the category of integral Frobenius modules over a p-adic differential ring (category of integral DF-modules) studied in [**Mat03**].

In §1, from every integral p-adic D-module we derive a projective system of congruence solution modules and obtain an equivalence of categories between the category $\mathbf{DMod}_{\mathcal{O}}$ of integral D-modules over a p-adic D-ring $\mathcal{O}$ and the corresponding category of projective systems $\mathbf{DProj}_{\mathcal{O}}$. As in positive characteristic, the related system of base change matrices $(D_l)_{l\in\mathbb{N}}$ determines the derivation. The formula is given in Theorem 1.7.

In the next §2, the differential Galois group of an integral p-adic D-module is studied. It is a reduced linear algebraic group over the field of constants K and hence a p-adic analytic group. If the matrices D_l belong to a connected group, this group is an upper bound for the differential Galois group, as in the characteristic p case.

In Theorem 3.4 and Theorem 3.6, the inverse problem of differential Galois theory is solved for split connected groups over the field of analytic elements $K\{t\}$ and its finite extensions. At least over $K\{t\}$ this implies an analogue of the Abhyankar conjecture as stated in Corollary 3.5, which again coincides with the characteristic p case.

In §4 embedding problems with connected kernel and finite cokernel are solved over $K\{t\}$ via equivariant realization of (not necessarily split) connected groups. The proof combines techniques from the solution of the inverse problem over rational function fields with algebraically closed field of constants in characteristic zero by J. Hartmann [**Har02**] and in positive characteristic [**Mat01**]. In case the residue field of K is algebraically closed this leads to the solution of the general inverse problem over $K\{t\}$ (for non-connected groups), see Theorem 4.6. This result can be seen as a differential analogue of Harbater's solution of the finite inverse problem over p-adic function fields [**Har87**].

In the last §5, we study reduction of constants. The main result (Theorem 5.4) is that the reduced module of an integral p-adic D-module is an iterative D-module (ID-module) in characteristic p with a related differential Galois group. This answers Conjecture 8.5 in [**MvdP03b**] by the affirmative.

Acknowledgements. I would like to thank G. Christol, D. Harbater, J. Hartmann, M. Jarden and A. Röscheisen for helpful discussions on topics of the paper.

1. Integral Local Differential Modules

1.1. Local Differential Rings. — Let F be a field with a nonarchimedean valuation $|\cdot|$, valuation ring $\mathcal{O}_F$, valuation ideal $\mathcal{P}_F$ and residue field $\mathcal{F} := \mathcal{O}_F/\mathcal{P}_F$. Assume F has a nontrivial continuous derivation

$$(1.1) \qquad \partial_F : F \longrightarrow F \quad \text{with} \quad \partial_F(\mathcal{O}_F) \subseteq \mathcal{O}_F, \partial_F(\mathcal{P}_F) \subseteq \mathcal{P}_F$$

and field of constants $K = K_F$ with $\mathcal{P}_K := \mathcal{P}_F \cap K \neq (0)$. Then $\mathcal{O}_F$ with ∂_F restricted to $\mathcal{O}_F$ is called a *local differential ring*. By definition ∂_F induces a derivation on $\mathcal{F}$. Note that in case the value groups $|F^\times|$ and $|K^\times|$ coincide, the assumption $\partial_F(\mathcal{O}_F) \subseteq \mathcal{O}_F$ in (1.1) already implies $\partial_F(\mathcal{P}_F) \subseteq \mathcal{P}_F$. Now we fix an element $0 \neq r \in \mathcal{P}_K$, for example a prime element of $\mathcal{P}_K$ in the case of a discrete valuation. With respect to r we define *congruence constant rings*

$$\mathcal{O}_l := \{a \in \mathcal{O}_F | \partial_F(a) \in r^l \mathcal{O}_F\} \quad \text{for} \quad l \in \mathbb{N}. \tag{1.2}$$

Obviously the intersection of all these rings is the valuation ring $\mathcal{O}_K$ of K with respect to the restricted valuation, i.e.,

$$\mathcal{O}_K = \bigcap_{l \in \mathbb{N}} \mathcal{O}_l. \tag{1.3}$$

To explain a standard example, let K be a complete p-adic field, i.e., a complete subfield of the p-adic universe $\mathbb{C}_p$. The field $K(t)$ of rational functions over K with the Gauß valuation (extending the maximum norm on $K[t]$) and with the derivation $\partial_t := \frac{d}{dt}$ is a nonarchimedean differential field. Its completion $F = K\{t\} := \widehat{K(t)}$ with respect to the Gauß valuation with the continuously extended derivation $\hat{\partial}_t$ is a complete nonarchimedean differential field, sometimes called the field of analytic elements over K (compare [**Chr83**], Def. 21.3). By definition the valuation ring $\mathcal{O}_F$ is a local differential ring. It contains the Tate algebra

$$K\langle t \rangle := \Big\{ \sum_{i \in \mathbb{N}} a_i t^i | a_i \in K, \lim_{i \to \infty} |a_i| = 0 \Big\} \tag{1.4}$$

which coincides with the ring of analytic functions on the closed unit disc. The residue field $\mathcal{F}$ of $\mathcal{O}_F$ is the field of rational functions over the residue field $\mathcal{K} := \mathcal{O}_K/\mathcal{P}_K$ of K, i.e.,

$$\mathcal{F} := \mathcal{O}_F/\mathcal{P}_F = (\mathcal{O}_K/\mathcal{P}_K)(t) = \mathcal{K}(t). \tag{1.5}$$

In the case $r = p$ we obtain

$$\mathcal{F}_l = \mathcal{O}_l/(\mathcal{O}_l \cap \mathcal{P}_F) = \mathcal{K}(t^{p^l}) \tag{1.6}$$

for the residue fields of the higher congruence constant rings $\mathcal{O}_l$ of $\mathcal{O}_F$.

Now let L/F be a finite extension of $F = K\{t\}$. Then the valuation of $\mathcal{O}_F$ extends uniquely to a valuation of $\mathcal{O}_L$ and the derivation ∂_t has a unique extension ∂_L to L. If we assume

$$\partial_L(\mathcal{O}_L) \subseteq \mathcal{O}_L \quad \text{and} \quad \partial_L(\mathcal{P}_L) \subseteq \mathcal{P}_L, \tag{1.7}$$

$\mathcal{O}_L$ becomes a local D-ring. Such a ring will be called a *p-adic differential ring* in the following, and $\mathcal{O}_L/\mathcal{O}_F$ is an extension of p-adic D-rings. Unfortunately the assumption (1.7) is not vacuous, as the example $L = F(s), s^p = t$ shows. Here s belongs to $\mathcal{O}_L$, but $\partial_L(s) = \frac{s}{pt} \notin \mathcal{O}_L$. The following proposition gives a sufficient condition for (1.7).

Proposition 1.1. — *Let $(\mathcal{O}_F, \partial_F)$ be a local D-ring in a discretely valued D-field F, let L/F be a finite field extension and $\mathcal{O}_L/\mathcal{O}_F$ an extension of valuation rings. Assume that the corresponding extension of residue fields $\mathcal{L}/\mathcal{F}$ is separable and the different $\mathcal{D}_{L/F}$ of L/F is trivial. Then $\mathcal{O}_L$ is a local D-ring extending $\mathcal{O}_F$.*

Proof. — By the assumptions above there exists an element $y \in \mathcal{O}_L$ with $\mathcal{O}_L = \mathcal{O}_F[y]$ ([**Ser62**], § 6, Prop. 12). Let $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathcal{O}_F[X]$ be the minimal polynomial of y. Then the derivative of y is given by

$$\partial_L(y) = -\frac{\partial_F(f)(y)}{\partial_X(f)(y)}, \tag{1.8}$$

with the partial derivations ∂_F and ∂_X, respectively. Because of $\mathcal{D}_{L/F} = \partial_X(f)(y)\mathcal{O}_L$ ([**Ser62**], § 6, Cor. 2), our assumptions give $\partial_X(f)(y) \in \mathcal{O}_L^\times$. But this entails $\partial_L(\mathcal{O}_L) \subseteq \mathcal{O}_L$ and in the case $y \in \mathcal{O}_L^\times$ additionally $\partial_L(\mathcal{P}_L) \subseteq \mathcal{P}_L$. In the case $y \in \mathcal{P}_L$ we have $a_0 \in \mathcal{P}_F$. But this implies $\partial_F(a_0) \in \mathcal{P}_F$, thus $\partial_F(f)(y) \in \mathcal{P}_L$ and $\partial_L(y) \in \mathcal{P}_L$ showing $\partial_L(\mathcal{P}_L) \subseteq \mathcal{P}_L$. □

In the following an extension L/F of valued D-fields is called an *integral extension* if $\mathcal{O}_L/\mathcal{O}_F$ is an extension of local D-rings.

1.2. Local Differential Modules. — Now let $(\mathcal{O}_F, \partial_F)$ be a local D-ring as defined above. Then a free $\mathcal{O}_F$-module M of finite rank m together with a map $\partial_M : M \to M$, which is additive and has the defining property

$$\partial_M(ax) = \partial_F(a)x + a\partial_M(x) \quad \text{for} \quad a \in F, x \in M \tag{1.9}$$

is called a *local differential module* (local D-module) over $\mathcal{O}_F$. The pair (M, ∂_M) is called an *integral local D-module* here (instead of *bounded local D-module* as in [**Mat01**], [**vdP01**]) if for every $l \in \mathbb{N}$ there exists an $\mathcal{O}_F$-basis $B_l = \{b_{l1}, \dots, b_{lm}\}$ such that $\partial_M(B_l) \subseteq r^l M$. Then the submodules

$$M_l := \bigoplus_{i=1}^{m} \mathcal{O}_l b_{li} \subseteq M \tag{1.10}$$

are *congruence solution modules of* M (with respect to r). Obviously these are characterized by the property

$$M_l = \{x \in M | \partial_M(x) \in r^l M\}. \tag{1.11}$$

At first glance the defining property of an integral local D-module looks very strong. However, it generalizes the notion of an integral p-adic differential module with Frobenius structure (DF-module) as studied in [**Mat03**]. There, $(F, \partial_F, \phi_q^F)$ is a complete p-adic field with derivation ∂_F and Frobenius endomorphism ϕ_q^F which are related by the formula

$$\partial_F \circ \phi_q^F = z_F \phi_q^F \circ \partial_F \quad \text{with} \quad z_F = \frac{\partial_F(\phi_q^F(t))}{\phi_q^F(\partial_F(t))} \in \mathcal{P}_F \tag{1.12}$$

for some nonconstant $t \in F$ ([**Mat03**], § 7.1 or [**Col03**], § 0.2). Assume $(\mathcal{O}_F, \partial_F)$ is a local D-ring for $r \in \mathcal{P}_K$ with $|r| = |z_F|$. Let (M_F, Φ_q^F) be an integral (or étale) Frobenius module over F with associated derivation ∂_M (as introduced in [**Mat03**], § 7.3). Then a Frobenius lattice M inside M_F (compare [**Mat03**], § 6.3) together with ∂_M restricted to M defines an integral local D-module over $\mathcal{O}_F$ (with Frobenius structure). Moreover, the image $\Phi_q^l(M)$ of the l-th power of the Frobenius endomorphism $\Phi_q = \Phi_q^F$ on M is contained in the congruence solution module M_l, and the derivation ∂_M on M is uniquely determined by this property ([**Mat03**], Thm. 7.2).

Now let (M, ∂_M) and (N, ∂_N) be two integral local D-modules over a local D-ring $(\mathcal{O}_F, \partial_F)$. Then an $\mathcal{O}_F$-linear map $\theta : M \to N$ is called a *D-homomorphism* if and only if $\theta \circ \partial_M = \partial_N \circ \theta$. The integral local D-modules over $\mathcal{O} = \mathcal{O}_F$ together with the D-homomorphisms form a category which will be denoted by $\mathbf{DMod}_{\mathcal{O}}$ in the sequel.

Proposition 1.2. — *Let $(\mathcal{O}_F, \partial_F)$ be a local D-ring. Then the category $\mathbf{DMod}_{\mathcal{O}}$ of integral local D-modules over $\mathcal{O} = \mathcal{O}_F$ is a tensor category over the ring $\mathcal{O}_K$ of differential constants in $\mathcal{O}$.*

Proof. — Obviously $\mathbf{DMod}_{\mathcal{O}}$ is an abelian category of $\mathcal{O}$-modules. For (M, ∂_M), $(N, \partial_N) \in \mathbf{DMod}_{\mathcal{O}}$, the tensor product in $\mathbf{DMod}_{\mathcal{O}}$ is given by $M \otimes N := M \otimes_{\mathcal{O}} N$. It becomes a local D-module over $\mathcal{O}$ via

$$\partial_{M\otimes N}(x \otimes y) := \partial_M(x) \otimes y + x \otimes \partial_N(y). \tag{1.13}$$

This module is integral because

$$M_l \otimes N_l \subseteq (M \otimes N)_l. \tag{1.14}$$

Further the dual module $M^* := \mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O})$ is a D-module with

$$(\partial_{M^*}(f))(x) := \partial_F(f(x)) - f(\partial_M(x)) \quad \text{for} \quad f \in M^*, x \in M. \tag{1.15}$$

The evaluation $\varepsilon : M \otimes M^* \to \mathbf{1}_{\mathbf{DMod}_{\mathcal{O}}} = \mathcal{O}$ sends $x \otimes f$ to $f(x)$, and the coevaluation $\delta : \mathcal{O} \to M^* \otimes M$ is defined by the map $1 \mapsto \sum_{i=1}^{m} b_i^* \otimes b_i$, where $B = \{b_1, \ldots, b_m\}$ denotes a basis of M and $B^* = \{b_1^*, \ldots, b_m^*\}$ the corresponding dual basis of M^*. (Note that the definition of δ does not depend on the basis chosen.) By immediate calculations it follows (compare, for example, [**Mat01**], Ch. 2.1) that ε and δ are D-homomorphisms with

$$(\varepsilon \otimes \mathrm{id}_M) \circ (\mathrm{id}_M \otimes \delta) = \mathrm{id}_M \quad \text{and} \quad (\mathrm{id}_{M^*} \otimes \varepsilon) \circ (\delta \otimes \mathrm{id}_{M^*}) = \mathrm{id}_{M^*}\,. \tag{1.16}$$

Thus by definition $\mathbf{DMod}_{\mathcal{O}}$ is a tensor category defined over $\mathcal{O}_K$ because of

$$\mathrm{End}_{\mathbf{DMod}_{\mathcal{O}}}(\mathbf{1}_{\mathbf{DMod}_{\mathcal{O}}}) = \mathrm{End}_{\mathbf{DMod}_{\mathcal{O}}}(\mathcal{O}) = \mathcal{O}_K. \tag{1.17}$$

□

1.3. The Projective System of Congruence Solution Modules. — In analogy to the differential modules in positive characteristic with respect to an iterative derivation, the so-called ID-modules (see [**MvdP03b**] or [**Mat01**]), to any integral local D-module we can associate a projective system of congruence solution modules.

Proposition 1.3. — *Let $(\mathcal{O}, \partial)$ be a local D-ring and $(M, \partial_M), (N, \partial_N) \in \mathbf{DMod}_{\mathcal{O}}$ with congruence solution modules M_l or N_l over $\mathcal{O}_l$, respectively.*

(a) *Let $\varphi_l : M_{l+1} \to M_l$ be the $\mathcal{O}_{l+1}$-linear embedding. Then $(M_l, \varphi_l)_{l\in\mathbb{N}}$ forms a projective system.*

(b) *In (a) any φ_l can be extended to an $\mathcal{O}$-isomorphism*

$$\tilde{\varphi}_l : M = \mathcal{O} \otimes_{\mathcal{O}_{l+1}} M_{l+1} \longrightarrow \mathcal{O} \otimes_{\mathcal{O}_l} M_l = M. \tag{1.18}$$