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

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

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 $B_l = \{b_{l1}, \ldots, b_{lm}\}$ 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*

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

(c) *Let $\theta : M \to N$ be a morphism in $\mathbf{DMod}_{\mathcal{O}}$ and let $(N_l, \psi_l)_{l\in\mathbb{N}}$ be the projective system associated to N. Then the restrictions $\theta_l : M_l \to N_l$ are $\mathcal{O}_l$-linear D-homomorphisms with the property*

$$\theta_l \circ \varphi_l = \psi_l \circ \theta_{l+1}. \tag{1.19}$$

Proof. — The assertions (a) and (b) immediately follow from the fact that by definition φ_l maps an $\mathcal{O}$-basis B_{l+1} of M (inside M_{l+1}) to an $\mathcal{O}$-basis B_l of M (inside M_l). Assertion (c) finally is a consequence of $\theta \circ \partial_M = \partial_N \circ \theta$. □

Obviously the projective systems of congruence solution modules $(M_l, \varphi_l)_{l\in\mathbb{N}}$ together with the systems $\Theta = (\theta_l)_{l\in\mathbb{N}}$ of $\mathcal{O}_l$-linear D-homomorphisms θ_l form a (tensor) category. In the following, the category of all projective systems $\mathcal{M} = (M_l, \varphi_l)_{l\in\mathbb{N}}$ of $\mathcal{O}_l$-modules M_l with (1.18) and systems $\Theta = (\theta_l)_{l\in\mathbb{N}}$ of $\mathcal{O}_l$-linear homomorphisms with (1.19) is denoted by $\mathbf{DProj}_{\mathcal{O}}$. We want to show that in case $\mathcal{O}$ is complete, any $\mathcal{M} \in \mathbf{DProj}_{\mathcal{O}}$ is isomorphic in $\mathbf{DProj}_{\mathcal{O}}$ to a system of congruence solution modules of some $M \in \mathbf{DMod}_{\mathcal{O}}$. This can be expressed in the following way:

Theorem 1.4. — *Let $(\mathcal{O}, \partial)$ be a complete local D-ring. Then the category $\mathbf{DProj}_{\mathcal{O}}$ is equivalent to the category $\mathbf{DMod}_{\mathcal{O}}$ as a tensor category over $\mathcal{O}_K$.*

Proof. — By Proposition 1.3 any $(M, \partial_M) \in \mathbf{DMod}_{\mathcal{O}}$ defines an object $\mathcal{M} = (M_l, \varphi_l)_{l\in\mathbb{N}} \in \mathbf{DProj}_{\mathcal{O}}$ and any morphism θ in $\mathbf{DMod}_{\mathcal{O}}$ leads to a morphism $\Theta = (\theta_l)_{l\in\mathbb{N}}$ in $\mathbf{DProj}_{\mathcal{O}}$.

Now let $\mathcal{N} = (N_l, \psi_l)_{l\in\mathbb{N}}$ be an object in $\mathbf{DProj}_{\mathcal{O}}$ with $\dim_{\mathcal{O}}(N_0) = m$. We want to show that there exists a unique derivation ∂_M on $M := N_0$ with congruence solution modules $M_l := \psi_0 \circ \cdots \circ \psi_{l-1}(N_l)$. Obviously the modules M_l are $\mathcal{O}_l$-submodules of M containing an $\mathcal{O}$-basis $B_l = \{b_{l1}, \ldots, b_{lm}\}$ of M by property (1.18). Defining base change matrices $D_l \in \mathrm{GL}_m(\mathcal{O}_l)$ by $B_{l+1} = B_l D_l$ we obtain $B_l = BD_0 \cdots D_{l-1}$ with $B = B_0$. Now let $\boldsymbol{y} = (y_1, \ldots, y_m)^{tr}$ be the coordinate vector of $x \in M$ with respect to the basis B, i.e., $x = \sum_{j=1}^{m} b_j y_j = B\boldsymbol{y}$. Then in view of $\partial_M(B_l) \subseteq r^l M$ we define

$$\delta_l(x) := B_l \partial_F(\boldsymbol{y}_l) := BD_0 \cdots D_{l-1} \partial_F(D_{l-1}^{-1} \cdots D_0^{-1} \boldsymbol{y}) \in M. \tag{1.20}$$

Because of $\partial_F(D_l^{-1}) \in r^l \mathcal{O}_l^{m\times m}$, the coefficients of $\delta_l(x)$ converge in $\mathcal{O}$, hence

$$\partial_M(x) := \lim_{l\to\infty} (\delta_l(x)) \in M \tag{1.21}$$

is well defined. It is easy to verify that ∂_M is additive with $\partial_M(ax) = \partial_F(a)x + a\partial_M(x)$ for $F = \mathrm{Quot}(\mathcal{O})$, i.e., ∂_M is a derivation of M. Further from $\partial_M(x) \equiv \delta_l(x) \pmod{r^l M}$ it follows that $\partial_M(B_l) \subseteq r^l M$. Hence the $\mathcal{O}_l$-modules M_l are the congruence solution modules of (M, ∂_M). Moreover, ∂_M is uniquely determined by this property because of

$$\partial_M(x) = \partial_M(B_l \boldsymbol{y}_l) = \partial_M(B_l)\boldsymbol{y}_l + \delta_l(x). \tag{1.22}$$

□

In the following the system of base change matrices $(D_l)_{l\in\mathbb{N}}$ from the proof of Theorem 1.4 is referred to as a *system of representing matrices of M* or $(M_l)_{l\in\mathbb{N}}$,

respectively. For later use we state the explicit congruence formula for ∂_M found in the proof as a corollary.

Corollary 1.5. — *Let $(\mathcal{O},\partial)$ be a complete local D-ring, $(M,\partial_M)\in\mathbf{DMod}_{\mathcal{O}}$ and let $(D_l)_{l\in\mathbb{N}}$ be a system of representing matrices of M. Then the ∂_M-derivative of $x=B\boldsymbol{y}\in M$ has the property*

$$\partial_M(x)\equiv BD_0\cdots D_{l-1}\partial_F(D_{l-1}^{-1}\cdots D_0^{-1}\boldsymbol{y})\pmod{r^lM}. \tag{1.23}$$

1.4. The Solution Space of an Integral Local D-Module. — As usual, the *solution space of* $(M,\partial_M)\in\mathbf{DMod}_{\mathcal{O}}$ over $\mathcal{O}=\mathcal{O}_F$ is defined by

$$\mathrm{Sol}_{\mathcal{O}}(M):=\{x\in M|\partial_M(x)=0\}=\bigcap_{l\in\mathbb{N}}M_l. \tag{1.24}$$

Now let E/F be an integral extension of valued D-fields and $\tilde{\mathcal{O}}:=\mathcal{O}_E$ its valuation ring. Then $M_{\tilde{\mathcal{O}}}:=\tilde{\mathcal{O}}\otimes_{\mathcal{O}}M$ is an integral local D-module over $\tilde{\mathcal{O}}$. By abuse of notation the solution space of $M_{\tilde{\mathcal{O}}}$ is denoted by

$$\mathrm{Sol}_{\tilde{\mathcal{O}}}(M):=\mathrm{Sol}_{\tilde{\mathcal{O}}}(M_{\tilde{\mathcal{O}}})=\bigcap_{l\in\mathbb{N}}(M_{\tilde{\mathcal{O}}})_l. \tag{1.25}$$

The module M is called *trivial over* $\tilde{\mathcal{O}}$ if $\mathrm{Sol}_{\tilde{\mathcal{O}}}(M)$ contains an $\tilde{\mathcal{O}}$-basis of $M_{\tilde{\mathcal{O}}}$.

Proposition 1.6. — *Let $(\mathcal{O},\partial)$ be a local D-ring and $(M,\partial_M)\in\mathbf{DMod}_{\mathcal{O}}$. Then for every extension $\tilde{\mathcal{O}}/\mathcal{O}$ of local D-rings the solution space $\mathrm{Sol}_{\tilde{\mathcal{O}}}(M)$ is a free $\tilde{\mathcal{O}}$-module over the ring $K_{\tilde{\mathcal{O}}}$ of differential constants of $\tilde{\mathcal{O}}$ with*

$$\dim_{K_{\tilde{\mathcal{O}}}}(\mathrm{Sol}_{\tilde{\mathcal{O}}}(M))\le\dim_{\tilde{\mathcal{O}}}(M_{\tilde{\mathcal{O}}})=\dim_{\mathcal{O}}(M). \tag{1.26}$$

The proof is the standard one and follows from the fact that $K_{\tilde{\mathcal{O}}}$-linearly independent solutions in $\mathrm{Sol}_{\tilde{\mathcal{O}}}(M)$ remain linearly independent over $\tilde{\mathcal{O}}$. Further, with the same arguments as in [**Mat03**], Prop. 7.4, we obtain the following characterization of solutions of M over extension rings of $\mathcal{O}$:

Theorem 1.7. — *Let $(\mathcal{O},\partial)$ be a complete local D-ring and let $(M,\partial_M)\in\mathbf{DMod}_{\mathcal{O}}$ with basis B and system of representing matrices $(D_l)_{l\in\mathbb{N}}$. Then for every extension $\tilde{\mathcal{O}}/\mathcal{O}$ of local D-rings the following statements are equivalent:*

(a) $x=B\boldsymbol{y}\in\mathrm{Sol}_{\tilde{\mathcal{O}}}(M)$,
(b) $\partial_{\tilde{\mathcal{O}}}(\boldsymbol{y})\equiv A_l\boldsymbol{y}\pmod{r^{l+1}}$ *for* $l\in\mathbb{N}$ *with* $A_l:=\partial_F(D_0\cdots D_l)(D_0\cdots D_l)^{-1}$,
(c) $\partial_{\tilde{\mathcal{O}}}(\boldsymbol{y})=A\boldsymbol{y}$ *with* $A:=\lim_{l\to\infty}(A_l)\in\mathcal{O}^{m\times m}$.

In Theorem 1.7 the completeness of $\mathcal{O}$ is only needed for the existence of $A\in\mathcal{O}^{m\times m}$ in (c).

Now let $M_F:=F\otimes_{\mathcal{O}}M$ be the extended D-module over the quotient field F of $\mathcal{O}=\mathcal{O}_F$. Then from the general theory of Picard–Vessiot extensions we know that there exists a Picard–Vessiot ring $\tilde{R}$ and a Picard–Vessiot field $\tilde{E}:=\mathrm{Quot}(\tilde{R})$ after a finite extension of constants $\tilde{F}/F$ (see [**Mat03**], Prop. 8.1). Thus in the following,

among other things we have to deal with the question under which conditions a PV-extension E/F of M exists (without introducing new constants) and which linear groups are realizable by integral D-modules as differential Galois groups, for example, over the field of analytic elements $F = K\{t\}$.

2. The Galois Group of a p-adic D-Module

2.1. Solution Fields. — Let $(\mathcal{O}_F, \partial_F)$ be a p-adic D-ring as introduced in Section 1.1 and let (M, ∂_M) be an integral D-module over $\mathcal{O}_F$ with system of representing matrices $(D_l)_{l\in\mathbb{N}}$. Then by Theorem 1.7 the solutions of M in a D-ring extension $\mathcal{O}_E \geq \mathcal{O}_F$ are solutions of a linear differential equation

$$\partial_E(\boldsymbol{y}) = A\boldsymbol{y}, \quad \text{where} \quad A \in \mathcal{O}_F^{m\times m} \tag{2.1}$$

and A can be computed from the matrices D_l. Hence $U := \mathcal{O}_F[\mathrm{GL}_n] = \mathcal{O}_F[x_{ij}, \det(x_{ij})^{-1}]_{i,j=1}^m$ becomes a D-ring by defining

$$\partial_U(X) := A \cdot X \quad \text{for} \quad X = (x_{ij})_{i,j=1}^m. \tag{2.2}$$

The quotient ring R_M of U by a maximal differential ideal $P \trianglelefteq U$ with $P \cap \mathcal{O}_F = (0)$ is a simple D-ring called a *Picard–Vessiot ring of M over $\mathcal{O}_F$*. As in the case of fields, R_M is an integral domain and its quotient field E_M is called a *Picard–Vessiot field of M*. Unfortunately, in case the field of constants K of F is not algebraically closed, R_M and E_M may contain new constants and moreover may be not uniquely determined by M.

Now let $\mathbb{M}_F^*$ be the *field of meromorphic functions on the generic disc with coefficients in F*. This is defined as the quotient field of the ring of analytic functions on the generic disc

$$\mathcal{D}_F^* := \{u \in F\{z\} |\ |u - t| < 1\} \tag{2.3}$$

where z is transcendental over F and $t \in F$ with $\partial_F(t) = 1$. Then the Taylor map

$$\tau_F : F \longrightarrow \mathbb{M}_F^*, \quad f \mapsto \sum_{k\in\mathbb{N}} \frac{1}{k!}\partial_F(f)(z-t)^k \tag{2.4}$$

identifies the valued D-field (F, ∂_F) with the subfield $(F^*, \partial_{F^*}) = (\tau_F(F), \hat{\partial}_z)$ of $\mathbb{M}_F^*$ where the D-structure is translated by

$$\tau_F(\partial_F(f)) = \hat{\partial}_z(\tau_F(f)) \tag{2.5}$$

(compare [**Chr83**], Prop. 2.5.1). Now [**Chr83**], Thm. 4.8.7, or [**MvdP03b**], Thm. 6.3, respectively, immediately give

Theorem 2.1. — *Let $(\mathcal{O}_F, \partial_F)$ be a p-adic D-ring and (M, ∂_M) an integral D-module over $\mathcal{O}_F$. Assume there exists an element $t \in \mathcal{O}_F$ with $\partial_F(t) = 1$. Then (M, ∂_M) possesses a Picard–Vessiot field inside the field $\mathbb{M}_F^*$ of meromorphic functions on the generic disc (by identifying F with F^*).*

Unfortunately the field $\mathbb{M}_F^*$ contains many new constants. In order to obtain a Picard–Vessiot field of (M, ∂_M) over F without new constants, we have to specialize the result above, for example to an ordinary disc. An open disc $\mathcal{D}_K(c) = \{a \in K|\ |a-c| < 1\}$ is called an *ordinary disc with center c for* (M, ∂_M) if M has a basis B such that ∂_M defines a matrix $A \in F^{m\times m}$ with entries a_{ij} belonging to the subring $F_c \leq F$ of analytic functions on $\mathcal{D}_K(c)$ (compare [**Chr83**], 2.2.1). Now [**Chr83**], Prop. 5.1.7, shows

Corollary 2.2. — *Assume in addition that the open disc $\mathcal{D}_K(c)$ with center c is ordinary for (M, ∂_M). Then the integral p-adic D-module has a Picard–Vessiot field inside the field $\mathbb{M}_K(c)$ of meromorphic functions on $\mathcal{D}_K(c)$.*

By Theorem 1.7, in the case $(F, \partial_F) = (K\{t\}, \hat{\partial}_t)$ the assumption in Corollary 2.2 is satisfied with $c = 0$ if the representing matrices D_l belong to $\mathrm{GL}_m(K\langle t^{p^l}\rangle)$ where $K\langle t^{p^l}\rangle$ is the Tate algebra introduced in (1.4).

2.2. Differential Automorphisms. — As above, (M, ∂_M) is an integral D-module over a p-adic D-ring $(\mathcal{O}_F, \partial_F)$ with quotient field F. After a finite extension of constants $\tilde{F}/F$, there exists a Picard–Vessiot extension $\tilde{E}/\tilde{F}$ (without new constants). Let us assume for the moment that $F = \tilde{F}$, i.e., the existence of a Picard–Vessiot extension E/F for M. If in addition we normalize the fundamental solution matrix $Y \in \mathrm{GL}_m(E)$ to have initial value $Y(c) \in \mathrm{GL}_m(\mathcal{O}_K)$ for some $c \in \mathcal{O}_K$, the field E and the Picard-Vessiot ring $R = R_M$ inside E are uniquely determined up to D-isomorphisms over F or $\mathcal{O}_F$, respectively. Then the group of D-automorphisms

$$\mathrm{Aut}_{\mathrm{D}}(M) := \mathrm{Aut}_{\mathrm{D}}(R_M/\mathcal{O}_F) \tag{2.6}$$

is called the *differential automorphism group over $\mathcal{O}_F$ of M (or R_M, respectively).* In the following $\bar{K}$ denotes an algebraic closure of the field K of constants of F and $\bar{F} := \bar{K} \otimes_K F$ the corresponding extension by constants.

Proposition 2.3. — *Let (M, ∂_M) be an integral D-module over a p-adic D-ring $(\mathcal{O}_F, \partial_F)$ of rank m and $R_M/\mathcal{O}_F$ a Picard–Vessiot ring of M over $\mathcal{O}_F$ and let $M_F := F \otimes_{\mathcal{O}_F} M$.*

(a) *There exists a reduced linear algebraic group $\mathcal{G} \leq \mathrm{GL}_m(K)$ defined over K such that*

$$\mathrm{Aut}_{\mathrm{D}}(M_F) \cong \mathcal{G}(K) \quad \textit{and} \quad \mathrm{Aut}_{\mathrm{D}}(M) \cong \mathcal{G}(\mathcal{O}_K). \tag{2.7}$$

(b) *In case $\mathcal{G}$ is connected we further have $R_M^{\mathrm{Aut}_{\mathrm{D}}(M)} = \mathcal{O}_F$.*

Proof. — Since the field $\bar{K}$ of constants of $\bar{F}$ is algebraically closed, general Picard–Vessiot theory shows the existence of a Picard–Vessiot extension $\bar{E}/\bar{F}$ for $M_{\bar{F}} := \bar{F} \otimes_F M_F$ and a linear algebraic group $\mathcal{G}$ defined over $\bar{K}$ such that $\mathrm{Aut}_{\mathrm{D}}(\bar{E}/\bar{F}) \cong \mathcal{G}(\bar{K})$. The Picard–Vessiot ring $\bar{R}$ inside $\bar{E}$ is D-isomorphic to $\bar{F}[\mathrm{GL}_M]/\bar{P}$, where $\bar{P}$ denotes a maximal D-ideal $\bar{P} \triangleleft \bar{F}[\mathrm{GL}_n]$. Since by assumption the ring $\bar{R}$ and thus the D-ideal $\bar{P}$ are defined over K, the same holds for the defining equations of $\mathcal{G}$ because of

$$\mathcal{G}(\bar{K}) = \{C \in \mathrm{GL}_m(\bar{K}) | q(X \cdot C) \in P \quad \text{for} \quad q(X) \in P\} \tag{2.8}$$

with $X = (x_{ij})_{i,j=1}^m$. This shows (a).

In case $\mathcal{G}$ is connected, the group $\mathcal{G}(K)$ is Zariski–dense in $\mathcal{G}(\bar{K})$ by [**PR94**], Thm. 2.2 and [**Spr98**], Cor. 13.3.10, respectively. Moreover, its p-adic open subgroup of integral points $\mathcal{G}(\mathcal{O}_K) := \mathcal{G}(K) \cap \mathrm{GL}_m(\mathcal{O}_K)$ which coincides with $\mathrm{Aut}_{\mathrm{D}}(M)$ is Zariski–dense in $\mathcal{G}(K)$ by [**PR94**], Lemma 3.2. Hence the subring of R_M of $\mathrm{Aut}_{\mathrm{D}}(M)$-invariant elements equals $R_M \cap F = \mathcal{O}_F$. □

In case $R_M^{\mathrm{Aut}_{\mathrm{D}}(M)} = \mathcal{O}_F$, the group $\mathrm{Aut}_{\mathrm{D}}(M)$ is called the *differential Galois group of M or R_M*, respectively, and is denoted by $\mathrm{Gal}_{\mathrm{D}}(M)$ or $\mathrm{Gal}_{\mathrm{D}}(R_M/\mathcal{O}_F)$, respectively. From the proof we obtain in addition:

Corollary 2.4. — *If in Proposition 2.3 the field K is a finite extension of $\mathbb{Q}_p$, then the differential automorphism group $\mathrm{Aut}_{\mathrm{D}}(M_F)$ is a locally compact p-adic analytic group and $\mathrm{Aut}_{\mathrm{D}}(M)$ is a Zariski–dense compact subgroup of $\mathrm{Aut}_{\mathrm{D}}(M_F)$.*

Unfortunately the connectedness assumption on $\mathcal{G}$ in Proposition 2.3 (b) can not be omitted, as the following example shows. Let E/F be the finite extension $E = F(x)$ defined by $x^n = t$ over $(F, \partial_F) = (K\{t\}, \hat{\partial}_t)$. Then E is a Picard–Vessiot field over F for the 1-dimensional D-module $M = Fx$ with $\partial_M(x) = \frac{1}{nt}x$. Obviously M is integral if p does not divide n. But the subfield of E of $\mathrm{Aut}_{\mathrm{D}}(M_F)$-invariant elements only equals F if K contains a primitive n-th root of unity.

2.3. An Upper Bound. — As in positive characteristic ([**MvdP03b**], Prop. 5.3 or [**Mat01**], Thm. 5.1) a system of representing matrices of an integral D-module gives an upper bound on the D-Galois group. However, before proving the corresponding theorem, we state the following useful triviality criterion:

Proposition 2.5. — *Let (M, ∂_M) be an integral D-module over a p-adic D-ring $(\mathcal{O}_F, \partial_F)$. Assume M has a system of representing matrices $(D_l)_{l\in\mathbb{N}}$ converging to the identity matrix. Then M is a trivial D-module, i.e., F contains a full system of solutions.*

Proof. — Under the assumptions above the matrices $Y_l := \prod_{k=0}^{l} D_l$ converge to a matrix $Y \in F^{m\times m}$, which by Theorem 1.7 is a fundamental solution matrix of M. □

Theorem 2.6. — *Let (M, ∂_M) be an integral p-adic D-module over a p-adic D-ring $(\mathcal{O}_F, \partial_F)$ and let $\mathcal{G}$ be a reduced connected linear group defined over the field of constants K of $F = \mathrm{Quot}(\mathcal{O}_F)$. Assume that there exist bases of the congruence solution modules M_l over $\mathcal{O}_l$ such that the corresponding representing matrices D_l of M belong to the groups $\mathcal{G}(\mathcal{O}_l)$ of $\mathcal{O}_l$-rational points of $\mathcal{G}$, then*

$$\mathrm{Gal}_{\mathrm{D}}(M_F) \le \mathcal{G}(K) \quad \textit{and} \quad \mathrm{Gal}_{\mathrm{D}}(M) \le \mathcal{G}(\mathcal{O}_K). \tag{2.9}$$

Proof. — The matrices $A_l = \partial_F(D_0 \cdots D_l)(D_0 \cdots D_l)^{-1}$ in Theorem 1.7 belong to the Lie algebra $\mathrm{Lie}_F(\mathcal{G})$ of $\mathcal{G}$ over F since they are images of the logarithmic derivative

$$\lambda : \mathcal{G}(F) \longrightarrow \mathrm{Lie}_F(\mathcal{G}), D \mapsto \partial_F(D)D^{-1}. \tag{2.10}$$

Then from the validity of the congruences

$$A_l \equiv A_{l-1} \pmod{r^l\mathcal{O}_F} \tag{2.11}$$

and the completeness of $\mathrm{Lie}_F(\mathcal{G})$ we conclude that $A = \lim_{l\to\infty}(A_l) \in \mathrm{Lie}_F(\mathcal{G})$. But this implies $\mathrm{Gal}_{\mathrm{D}}(M_F) \leq \mathcal{G}(K)$ according to [**vdPS03**], Prop. 1.31, and therefore $\mathrm{Gal}_{\mathrm{D}}(M) \leq \mathcal{G}(\mathcal{O}_K)$. □

An easy example is given by $F = \mathbb{Q}_p\{t\}$ and the 1-dimensional $\mathcal{O}_F$-module $M = \mathcal{O}_F b$ with $D_l = (t^{a_l p^l})$ and $a_l \in \{0, \ldots, p-1\}$. Then

$$A = \left(\frac{\alpha}{t}\right) \quad \text{with} \quad \alpha = \sum_{l\in\mathbb{N}} a_l p^l \in \mathbb{Z}_p. \tag{2.12}$$

A solution $y \in \mathbb{M}_{\mathbb{Q}_p}$ of $\partial(y) = Ay$ is given by

$$y = t^\alpha \quad \text{where} \quad t^\alpha = \lim_{l\to\infty}\left(\prod_{j=0}^{l} t^{a_j p^j}\right). \tag{2.13}$$

Obviously $\mathrm{Gal}_{\mathrm{D}}(M) \leq \mathbb{G}_m(\mathbb{Z}_p) = \mathbb{Z}_p^\times$ and equality holds if and only if $\alpha \notin \mathbb{Q}$.

In the following an integral p-adic D-module (M, ∂_M) over $\mathcal{O}_F$ or its extension M_F over F with $\mathrm{Gal}_{\mathrm{D}}(M) = \mathcal{G}(\mathcal{O}_K)$ or $\mathrm{Gal}_{\mathrm{D}}(M_F) = \mathcal{G}(K)$, respectively, is called an *effective D-module* if, with respect to a suitable basis, ∂_M is given by a matrix $A \in \mathrm{Lie}_F(\mathcal{G})$. Obviously only a D-module with connected D-Galois group can be effective.

2.4. Effective D-Modules. — The following well known criterion gives a sufficient condition for a D-module over a field F to be effective.

Theorem 2.7. — *Let F be a D-field with field of constants K and $M \in \mathbf{DMod}_F$ with connected D-Galois group $\mathrm{Gal}_{\mathrm{D}}(M) = \mathcal{G}(K)$. Assume $H^1(G_F, \mathcal{G}(F^{\mathrm{sep}})) = 0$, then M is effective.*

A proof can be found in [**vdPS03**], Prop. 1.31 in the case of an algebraically closed field of constants and in [**Kol76**], Ch. VI 9, Cor. 1, in the general case. In order to apply this theorem to p-adic D-fields F we recall the following fact which immediately follows from [**Ser97**], II § 4.3, Prop. 12:

Proposition 2.8. — *Let K be a complete p-adic field with respect to a discrete valuation and let F be a finite extension of the field of analytic elements $K\{t\}$.*

(a) *For the cohomological dimension* $\mathrm{cd}(F)$ *we have* $\mathrm{cd}(F) \leq 3$.
(b) *In case the residue field of K is algebraically closed, we obtain* $\mathrm{cd}(F) \leq 2$.

Thus by a theorem of Bayer and Parimala ([**BP99**] or [**Ser97**], III § 3.1, respectively) concerning the cohomological triviality of linear groups over fields F with $\mathrm{cd}(F) \leq 2$, we finally obtain

Corollary 2.9. — *Let K be a complete p-adic field with respect to a discrete valuation and with algebraically closed residue field. Let $\mathcal{G}$ be a simply connected semisimple linear algebraic group over K of classical type (possibly except the triality group* D_4*). Then any $M \in \mathbf{DMod}_F$ over a finite extension $F/K\{t\}$ with* $\mathrm{Gal}_{\mathrm{D}}(M) = \mathcal{G}(K)$ *is effective.*

Under the assumptions of Corollary 2.9 the Bayer–Parimala theorem shows $H^1(G_F, \mathcal{G}(F^{\mathrm{sep}})) = 0$ such that Theorem 2.7 applies.

3. The Connected Inverse Problem

3.1. A Criterion for Effective D-Modules. — The following existence theorem for effective PV-extensions over the field of analytic elements $(K\{t\}, \partial_t)$ is a variant obtained by p-adic approximation of the corresponding theorem for iterative PV-extensions in positive characteristic presented in [**Mat01**], Thm. 7.14.

Theorem 3.1. — *Let $(F, \partial_F) = (K\{t\}, \partial_t)$ be the field of analytic elements over a complete p-adic field K with discrete valuation, $\mathcal{O} = \mathcal{O}_F$ its valuation ring and $\mathcal{P} = \mathcal{P}_F = r\mathcal{O}_F$ the valuation ideal. Let $\mathcal{A}$ be either $\mathbb{G}_a$ or $\mathbb{G}_m$, set $S_l = \mathcal{O}_K[t^{p^l}]$ or $S_l = \mathcal{O}_K[t^{p^l}, t^{-p^l}]$, respectively, and let $\mathcal{G} \leq \mathrm{GL}_m(K)$ be a reduced connected linear algebraic group defined over $\mathcal{O}_K$. Suppose $M \in \mathbf{DMod}_{\mathcal{O}}$ is an integral local D-module whose system of representing matrices $D_l \in \mathcal{G}(\mathcal{O}_l)$ satisfies the following properties:*

(1) *For all $l \in \mathbb{N}$ there exists a $\gamma_l \in \mathrm{Mor}_K(\mathcal{A}, \mathcal{G})$ such that*

$$D_l = \gamma_l(t^{p^l}) \in \mathcal{G}(S_l) \quad \textit{and} \quad \gamma_l(1) = 1_{\mathcal{G}(K)}.$$

(2) *For all $n \in \mathbb{N}$ the set $\{\gamma_l(\mathcal{A}(K)) | l \geq n\}$ generates $\mathcal{G}(K)$ as an algebraic group over K.*

(3) *There exists a number $d \in \mathbb{N}$ such that the (divisor) degree of γ_l in F is bounded by $d \cdot p^l$ for all $l \in \mathbb{N}$.*

(4) *If $l_0 < l_1 < \ldots$ is the sequence of natural numbers l_i for which $\gamma_{l_i} \neq 1$, then $\lim\limits_{i \to \infty} (l_{i+1} - l_i) = \infty$.*

Then M is an effective D-module with $\mathrm{Gal}_{\mathrm{D}}(M) = \mathcal{G}(\mathcal{O}_K)$.

Proof. — In order to simplify the notation we first assume $r = p$, i.e., $K/\mathbb{Q}_p$ is unramified.

We start with introducing some notation. Let $M_F := F \otimes_{\mathcal{O}} M \in \mathbf{DMod}_F$ be the D-module over F generated by M with $\dim_F(M) = m$. Let $U_K := K[\mathrm{GL}_m]$ and $Q_K \trianglelefteq U_K$ be the defining radical ideal of $\mathcal{G}_K$. The extended ideal $Q_F := Q_K U_F \trianglelefteq U_F := F[\mathrm{GL}_m]$ is a D-ideal according to [**vdPS03**], proof of Prop. 1.31. Therefore $\tilde{R} := F[\mathcal{G}] = U_F/Q_F$ is a D-ring, and it is an integral domain since $\mathcal{G}_K$ is connected. Set $\tilde{E} := \mathrm{Quot}(\tilde{R})$ and denote by $\tilde{K}$ its field of constants. Let $P_F \trianglelefteq U_F$ be a maximal D-ideal containing Q_F, so that $R := U_F/P_F$ is a PV-ring with PV-field $E := \mathrm{Quot}(R)$, and let $\kappa : \tilde{R} \to R$ denote the canonical epimorphism. The D-module $\tilde{M} := \tilde{E} \otimes_F M$ contains a fundamental solution system and thus is trivial. Hence the solution space $\tilde{V} := \mathrm{Sol}_{\tilde{E}}(\tilde{M})$ is an m-dimensional $\tilde{K}$-vector space and a $\mathcal{G}(K)$-module by definition.

First we show that any one-dimensional D-submodule $N \in \mathbf{DMod}_{\mathcal{O}}$ of M or $N_F := F \otimes_{\mathcal{O}} N \leq M_F$, respectively, defines a $\mathcal{G}(K)$-stable line $\tilde{W} \leq \tilde{V}$. Write $M = \bigoplus\limits_{i=1}^{m} b_i \mathcal{O}$ with basis $B = \{b_1, \ldots, b_m\}$. Then $B_l = BD_0 \cdots D_{l-1}$ is a basis of the

congruence solution module M_l with respect to p^l. The corresponding congruence solution module $N_l = N_F \cap M_l$ has a generator $B_l \boldsymbol{h}_l$ with the basis B_l written as a row and $\boldsymbol{h}_l \in \mathcal{O}_l^m$. Let

$$\boldsymbol{h}_l = \sum_{k\in\mathbb{N}} \boldsymbol{h}_l^{(k)} p^k \tag{3.1}$$

be the p-adic expansion of $\boldsymbol{h}_l$ with respect to a given system of residues $\mathcal{R}$ of $\mathcal{O}$ modulo $\mathcal{P}$ (including 0). Without loss of generality we may assume that $\boldsymbol{h}_l^{(0)} \in \mathcal{O}_K[t]^m$ and that the coordinates of $\boldsymbol{h}_l^{(0)}$ modulo p are relatively prime. Then the $\boldsymbol{h}_l$ are unique up to a factor belonging to $\mathcal{O}_K^\times$.

By assumption (1) all representing matrices D_l belong to $\mathcal{G}(\mathcal{O}_K[t^{p^l}, t^{-p^l}])$. They satisfy $B_{l+1}\boldsymbol{h}_{l+1} = B_l D_l \boldsymbol{h}_{l+1} \in N_l$, so there exist elements $u_l \in \mathcal{O}_l^\times$ such that $D_l \boldsymbol{h}_{l+1} = u_l \boldsymbol{h}_l$. By construction the coefficients of $\boldsymbol{h}_{l+1}^{(0)}$ and $\boldsymbol{h}_l^{(0)}$ are polynomials relatively prime modulo p, so in fact u_l is a unit in $\mathcal{O}_K[t^{p^l}, t^{-p^l}]$. Without loss of generality we may therefore assume $u_l = t^{a_l p^l}$ where $a_l \in \mathbb{Z}$ is bounded by property (3). (Observe that in the case $D_l \in \mathcal{G}(\mathcal{O}_K[t^{p^l}])$, the factor u_l is a unit in $\mathcal{O}_K[t^{p^l}]$ and hence $a_l = 0$). Then

$$\boldsymbol{h}_l \equiv \boldsymbol{h}_l^{(0)} \equiv t^{\tilde{a}_l} D_{l-1}^{-1} \cdots D_0^{-1} \boldsymbol{h}_0^{(0)} \pmod{p} \quad \text{with} \quad \tilde{a}_l := \sum_{j=0}^{l-1} a_j p^j. \tag{3.2}$$

From $\boldsymbol{h}_l \in \mathcal{O}_l$ we obtain by induction $\boldsymbol{h}_l^{(0)} \in \mathcal{O}_K[t^{p^l}]$ modulo p. The degree of $\boldsymbol{h}_l^{(0)}$ is bounded by the maximum degree of the polynomial coefficients of $\boldsymbol{h}_0^{(0)}$, the a_{l_i}, and the degrees $\deg(D_{l_i}^{-1}) \le p^{l_i} d^*$ for $l_i < l$, where d^* only depends on d. Thus, for l large enough, we get a contradiction in case $\boldsymbol{h}_l^{(0)}$ has a nonconstant coefficient. Hence there exists an $i_1 \in \mathbb{N}$ such that

$$\boldsymbol{h}_l \equiv \boldsymbol{h}_l^{(0)} \equiv \boldsymbol{h}_l^{(0)}(0) \equiv \boldsymbol{h}_l(0) \in \mathcal{O}_K^m \pmod{p} \quad \text{for} \quad l \ge l_{i_1}. \tag{3.3}$$

Specializing the congruences $\boldsymbol{h}_{l+1} \equiv u_l D_l^{-1} \boldsymbol{h}_l \pmod{p}$ at $t = 1$ by (1) we obtain further

$$\boldsymbol{h}_{l+1}(0) \equiv \boldsymbol{h}_{l+1}^{(0)}(0) \equiv \boldsymbol{h}_l^{(0)}(0) \equiv \boldsymbol{h}_l(0) \pmod{p} \quad \text{for} \quad l \ge l_{i_1} \tag{3.4}$$

and thus

$$\boldsymbol{h}_l \equiv \boldsymbol{h}_{l_{i_1}}(0) \pmod{p} \quad \text{for} \quad l \ge l_{i_1}. \tag{3.5}$$

Now we proceed by induction. Assume there exists an $i_k \in \mathbb{N}$ such that

$$\boldsymbol{h}_l \equiv \boldsymbol{h}_{l_{i_k}}(0) \pmod{p^k} \quad \text{for} \quad l \ge l_{i_k}. \tag{3.6}$$

Then we find an $\tilde{\boldsymbol{h}}_l^{(k)} \in \mathcal{O}_K(t)^m$ with

$$\boldsymbol{h}_l \equiv \boldsymbol{h}_{l_{i_k}}(0) + p^k \tilde{\boldsymbol{h}}_l^{(k)} \pmod{p^{k+1}}. \tag{3.7}$$

As in the first step we obtain by induction $\tilde{\boldsymbol{h}}_l^{(k)} \in \mathcal{O}_K(t^{p^{l-k}})^m$ modulo p which for l large enough, for $l \geq l_{i_{k+1}}$, say, leads to

$$\boldsymbol{h}_l \equiv \boldsymbol{h}_{l_{i_k}}(0) + p^k \tilde{\boldsymbol{h}}_l^{(k)}(0) \equiv \boldsymbol{h}_l(0) \in \mathcal{O}_K^m \pmod{p^{k+1}}. \tag{3.8}$$

By specializing at $t = 1$ as above this proves the next induction step

$$\boldsymbol{h}_l \equiv \boldsymbol{h}_{l_{i_{k+1}}}(0) \pmod{p^{k+1}} \quad \text{for} \quad l \geq l_{i_{k+1}}. \tag{3.9}$$

Thus the limit

$$\boldsymbol{h} := \lim_{k\to\infty}(\boldsymbol{h}_{l_{i_k}}(0)) = \lim_{l\to\infty}(\boldsymbol{h}_l(0)) \in \mathcal{O}_K^m \tag{3.10}$$

is well defined and has the property

$$D_l\boldsymbol{h} \equiv t^{a_l p^l}\boldsymbol{h} \pmod{p^k} \quad \text{for} \quad l \geq l_{i_k}. \tag{3.11}$$

Now by specializing the last congruence at $t = c$ for $c \in \bar{K}$, property (2) shows that $\boldsymbol{h}$ is an eigenvector for $\mathcal{G}(K)$.

Since the integers $a_l \in \mathbb{Z}$ are bounded, $\alpha := \sum_{l\in\mathbb{N}} a_l p^l$ is a p-adic integer and

$$y := t^\alpha = \prod_{l\in\mathbb{N}} t^{a_l p^l} \tag{3.12}$$

describes a solution of N in E and $\tilde{E}$, respectively (compare to the example in Section 2.3). Hence $\tilde{w} := yB_0\boldsymbol{h}$ is an element of $\tilde{V}$, which can easily be verified, and

$$\partial(\tilde{w}) \equiv B_0(\partial(y) - A_l y)\boldsymbol{h} \equiv 0 \pmod{p^{l+1}} \quad \text{for} \quad l \in \mathbb{N}, \tag{3.13}$$

using $A_l = \partial_F(D_0 \cdots D_l)(D_0 \cdots D_l)^{-1}$ from Theorem 1.7. The vector space $\tilde{W} := \tilde{K}\tilde{w}$ spanned by $\tilde{w}$ is a one-dimensional subspace of $\tilde{V}$. It is $\mathrm{Gal}_{\mathrm{D}}(\tilde{E}/F)$-stable with $\mathrm{Gal}_{\mathrm{D}}(\tilde{E}/F) \leq \mathcal{G}(\tilde{K})$ and $\mathcal{G}(K)$-stable (under the action on y and $\boldsymbol{h}$, respectively), and both actions coincide when restricted to $\mathrm{Gal}_{\mathrm{D}}(E/F)$. (Note that $\mathrm{Gal}_{\mathrm{D}}(E/F) \leq \mathcal{G}(K)$ by Theorem 2.6).

Next we show that any $\mathrm{Gal}_{\mathrm{D}}(E/F)$-stable line $\tilde{W} \leq \tilde{V}$ is in fact $\mathcal{G}(K)$-stable. Using the characterization of $\mathrm{Gal}_{\mathrm{D}}(E/F)$ in the proof of [**vdPS03**], Thm. 1.27, we see that Q_F is a $\mathrm{Gal}_{\mathrm{D}}(E/F)$-stable ideal, and so the canonical map $\kappa : \tilde{R} \to R$ is $\mathrm{Gal}_{\mathrm{D}}(E/F)$-equivariant. The image W of $\tilde{W}$ under this map is then $\mathrm{Gal}_{\mathrm{D}}(E/F)$-stable in V. Hence W defines a one-dimensional D-submodule N of M, and by the considerations above, this yields the $\mathcal{G}(K)$-stable line $\tilde{W} \leq \tilde{V}$.

Finally we need to show that E/F is an effective extension with Galois group $\mathcal{G}(K)$. By Chevalley's theorem ([**Spr98**], Thm. 5.5.3), there exists a faithful representation $\varrho : \mathcal{G} \to \mathrm{GL}(V)$ over K and a line $W \leq V$ such that $\mathrm{Gal}_{\mathrm{D}}(E/F)$ is exactly the stabilizer of W in $\mathcal{G}(K)$. The matrices $D_l^\varrho = D(\varrho \circ \gamma_l) := \varrho(\gamma_l(t^{p^l})) \in (\varrho(\mathcal{G}))(S_l)$ define a D-module M^ϱ with system of representing matrices $(D_l^\varrho)_{l\in\mathbb{N}}$, which again satisfies conditions (1) to (4) (possibly with a different degree bound). The vector space $W^\varrho \leq \mathrm{Sol}_E(M^\varrho)$ associated to W by the considerations above is $\mathrm{Gal}_{\mathrm{D}}(E/F)$-stable, and by the above, it is also $\mathcal{G}(K)$-stable. Consequently, $\mathrm{Gal}_{\mathrm{D}}(E/F) = \mathcal{G}(K)$. This ends the proof in the case $r = p$.

The general case follows from the special case $r = p$ by substituting $\mathcal{O}_l$ by $\mathcal{O}_{le}$ where $|p| = |r^e|$. □

In the special case of the 1-dimensional D-module M at the end of Section 2.3, condition (4) of Theorem 3.1 forces α to be a (p-adic) Liouvillean transcendental number. In particular, the solution $y = t^\alpha$ is not algebraic over F and hence $\mathrm{Gal}_{\mathrm{D}}(M) = \mathbb{Z}_p^\times$.

In the next corollary $F_1 \leq F$ denotes the subring of analytic functions on $\mathcal{D}_K(1)$ and $\mathbb{M}_K(1)$ the field of meromorphic functions on $\mathcal{D}_K(1)$ (which contains $\mathrm{Quot}(F_1)$, see [**Chr83**], 2.4.11).

Corollary 3.2. — *Under the assumptions of Theorem 3.1*

$$Y := \prod_{l\in\mathbb{N}} D_l \in \mathbb{M}_K(1)^{n\times n} \tag{3.14}$$

is a fundamental solution matrix for (M, ∂_M) over F.

Proof. — By the assumptions of Theorem 3.1 the representing matrix $D_l(t)$ is an element of $\mathcal{G}(\mathcal{O}_K[t^{p^l}, t^{-p^l}])$ with $D_l(1) = 1_{\mathcal{G}(K)}$. This implies $D_l(1+q) - 1_{\mathcal{G}(K)} \in \mathcal{P}_F^{m\times m}$ for $q \in \mathcal{P}_K$. Hence $D_l(t), D_l(t^{-1})$ and $\partial_F(D_l(t))$ belong to $F_1^{m\times m}$. Thus the same holds for $A_l = \partial_F(D_0\cdots D_l)(D_0\cdots D_l)^{-1}$ and $A = \lim_{l\to\infty}(A_l)$, since F_1 is complete. Now the result follows from Corollary 2.2 (or [**Chr83**], Prop. 5.1.7, respectively). □

3.2. Realization of Split Connected Groups. — In the following a connected linear group $\mathcal{G}$ over a perfect field K is called K-split if its maximal K-tori are K-split, i.e., are products of multiplicative groups over K. In order to apply Theorem 2.1 we need the following result:

Proposition 3.3. — *Let $\mathcal{G}$ be a reduced connected linear group over a complete p-adic field K which is K-split and defined over $\mathcal{O}_K$.*

(a) *$\mathcal{G}$ is generated as an algebraic group by finitely many maximal K-split tori and finitely many K-split unipotent groups.*

(b) *Each torus $\mathcal{T}$ is generated as an algebraic group by an element $T(t) \in \mathcal{T}(\mathcal{O}_K[t, t^{-1}])$ with $T(1) = 1_{\mathcal{T}}$, i.e.,*

$$\mathcal{T}(K) = \langle T(c) | c \in K\rangle_{\mathrm{alg}}. \tag{3.15}$$

(c) *Each unipotent group $\mathcal{U}$ is generated as an algebraic group by an element $U(T) \in \mathcal{U}(\mathcal{O}_K[t])$ with $U(1) = 1_{\mathcal{U}}$, i.e.,*

$$\mathcal{U}(K) = \langle U(c) | c \in K\rangle_{\mathrm{alg}}. \tag{3.16}$$

Proof. — By [**Spr98**], Thm. 13.3.6, $\mathcal{G}$ is generated by Cartan subgroups $\mathcal{C} = \mathcal{T}\times\mathcal{U}$ belonging to the maximal K-tori $\mathcal{T}$ of $\mathcal{G}$. Since K is perfect, the unipotent part $\mathcal{U}$ of $\mathcal{C}$ is K-split, too (by [**Spr98**], Thm. 14.3.8). Finally, the finiteness of the number of necessary tori and unipotent subgroups follows from the finiteness of $\dim(\mathcal{G})$. This proves (a).

Since $\mathcal{T}$ and $\mathcal{U}$ are K-split, the proof of (b) and (c) can now be copied from the proof of [**MvdP03b**], Thm. 7.3 and Lemma 7.5, respectively (using [**Spr98**], Cor. 14.3.9). □

Theorem 3.4. — *Let $(F, \partial_F) = (K\{t\}, \partial_t)$ be the field of analytic elements over a complete p-adic field K with discrete valuation and $\mathcal{G}$ a K-split reduced connected linear group over K which is defined over $\mathcal{O}_K$. Then $\mathcal{G}(\mathcal{O}_K)$ can effectively be realized as differential Galois group of an integral local D-module $M \in \mathbf{DMod}_{\mathcal{O}_F}$:*

$$\mathrm{Gal}_{\mathrm{D}}(M) = \mathcal{G}(\mathcal{O}_K). \tag{3.17}$$

Proof. — We want to apply Theorem 3.1. By Proposition 3.3, $\mathcal{G}$ is generated by finitely many K-split tori and finitely many K-split unipotent groups. For each torus $\mathcal{T}$ and each unipotent group $\mathcal{U}$ we find $D_l = T(t^{p^l}) \in \mathcal{G}(\mathcal{O}_K[t^{p^l}, t^{-p^l}])$ or $D_l = U(t^{p^l}) \in \mathcal{G}(\mathcal{O}_K[t^{p^l}])$, respectively, with the properties (1) and (3) of Theorem 3.1 according to Proposition 3.3, (b) and (c). Combining these D_l with large gaps as assumed in Theorem 3.1(4), we can still fulfill property (2) of the theorem. Now Theorem 3.1 gives the result. □

Corollary 3.5

(a) *In case the group $\mathcal{G}$ in Theorem 3.4 is generated by unipotent subgroups, $\mathcal{G}(\mathcal{O}_K)$ can be realized with at most one singular point in ∞.*
(b) *In the general case, $\mathcal{G}(\mathcal{O}_K)$ can be realized with singular points at most in $\{0, \infty\}$.*

Proof. — For (a) note that for the proof of Theorem 3.4 we only need $D_l \in \mathcal{G}(\mathcal{O}[t^{p^l}])$. In the general case it is sufficient to choose $D_l \in \mathcal{G}(\mathcal{O}[t^{p^l}, t^{-p^l}])$, so that the singular locus is contained in $\{0, \infty\}$. □

The last corollary proves a p-adic variant of the differential Abhyankar conjecture for connected groups over the affine line which is similar to the characteristic p case (compare [**MvdP03b**], Thm. 7.3). However, it is in contrast to the archimedean case where by a theorem of Ramis over the affine line at most groups generated by tori can be realized without singular points (see [**vdPS03**], Thm. 11.21).

3.3. Connected Groups over Curves. — The result of Theorem 3.4 implies the solution of the connected inverse problem over finite extensions $F/K\{t\}$ in the following form.

Theorem 3.6. — *Let $F/K\{t\}$ be a finite extension of D-fields with $K_F = K$ and $\mathcal{G}$ a K-split reduced connected linear algebraic group over K. Then $\mathcal{G}(K)$ can be realized as D-Galois group of a Picard–Vessiot extension E/F.*

Proof. — Any n-dimensional representation of $\mathcal{G}$ over K defines an $\mathcal{O}_K$-form of $\mathcal{G}$ by $\mathcal{G}(\mathcal{O}_K) = \mathcal{G}(K) \cap \mathrm{GL}_n(\mathcal{O}_K)$ (compare [**PR94**], Ch. 3.3), where $\mathcal{G}(\mathcal{O}_K)$ is Zariski–dense in $\mathcal{G}(K)$ by Proposition 2.3(b). Now Theorem 3.4 proves the existence of an integral local D-module $M \in \mathbf{DMod}_{\mathcal{O}}$ over $\mathcal{O} = \mathcal{O}_{K\{t\}}$ with $\mathrm{Gal}_{\mathrm{D}}(M) = \mathcal{G}(\mathcal{O}_K)$. Then $M_{K\{t\}} := K\{t\} \otimes_{\mathcal{O}} M$ has D-Galois group $\mathcal{G}(K)$ and its solution space generates a Picard–Vessiot extension $E/K\{t\}$ with $\mathrm{Gal}_{\mathrm{D}}(E/K\{t\}| = \mathcal{G}(K)$ (without new

constants by Corollary 3.2). By tensoring with F we finally obtain a PV-extension with

$$\mathrm{Gal}_{\mathrm{D}}(F \otimes_{K\{t\}} E/F) \cong \mathcal{G}(K). \tag{3.18}$$ □

4. Embedding Problems with Finite Cokernel

4.1. Split Embedding Problems with Finite Cokernel. — Unfortunately, up to now in general it is not known if every finite group appears as Galois group of a PV-extension over F (generated by an integral local D-module). Only in case the residue field of F is algebraically closed, we have a positive answer yet. This special case will be discussed in Section 4.4. First we try to solve differential embedding problems with connected kernel and finite cokernel. Before treating the general case we study the case of split embedding problems. This is the case when the D-Galois group $\mathcal{G}$ is a semidirect product $\mathcal{G} = \mathcal{G}^0 \rtimes H$ of the connected component $\mathcal{G}^0$ of $\mathcal{G}$ and a finite group H.

Proposition 4.1. — *Let $\mathcal{G} = \mathcal{G}^0 \rtimes H$ be a linear algebraic group defined over a p-adic field K with regular homomorphic section*

$$\chi : H \longrightarrow \mathcal{G}(K), \eta \mapsto C_\eta. \tag{4.1}$$

Let further $(\mathcal{O}_F, \partial_F)$ be a p-adic D-ring with ring of constants $\mathcal{O}_K$ and let L/F be an integral finite Picard–Vessiot extension with D-Galois group H. Suppose $M \in \mathbf{DMod}_{\mathcal{O}_L}$ defines a PV-extension E/L with D-Galois group $\mathcal{G}^0(K)$ (and no new constants). Assume M has a system of representing matrices $D_l \in \mathcal{G}^0(\mathcal{O}_L)$ which satisfy the equivariance condition

$$\eta(D_l) = C_\eta^{-1} D_l C_\eta \quad \textit{for all} \quad l \in \mathbb{N}, \eta \in H. \tag{4.2}$$

Then E/F is a PV-extension with D-Galois group $\mathcal{G}(K)$.

Proof. — We fix a representation of $\mathcal{G}$ as a closed subgroup of $\mathrm{GL}_m(K)$. By Hilbert's Theorem 90 ([**Ser97**], III.1, Lemma 1) there exists an element $Z \in \mathrm{GL}_m(L)$ with

$$\eta(Z) = Z \cdot C_\eta \quad \text{for all} \quad \eta \in H; \tag{4.3}$$

in particular, Z is a fundamental solution matrix for the PV-extension L/F. Since the representing matrices D_l of M or $M_L := L \otimes_{\mathcal{O}_L} M$, respectively, belong to $\mathcal{G}^0(\mathcal{O}_L)$, M_L is an effective D-module with D-Galois group $\mathcal{G}^0(K)$ by Theorem 2.6. Further, by [**vdPS03**], Prop. 1.31(2) there exists a fundamental solution matrix $Y \in \mathcal{G}^0(E)$ of M or M_L, respectively, with $\partial_E(Y) = A \cdot Y$ for some $A \in \mathcal{O}_L^{m \times m}$ and

$$\varepsilon(Y) = Y \cdot C_\varepsilon \quad \text{for all} \quad \varepsilon \in \mathrm{Gal}_{\mathrm{D}}(E/L), \tag{4.4}$$

where C_ε denotes the matrix of ε in $\mathcal{G}^0(K)$.

Now let (U, ∂_U) be the differential ring $U = L[\mathrm{GL}_m] = L[x_{ij}, \det(x_{ij})^{-1}]_{i,j=1}^m$ with derivation $\partial_U(X) = A \cdot X$ for $X = (x_{ij})_{i,j=1}^m$. Since $Y \in \mathcal{G}^0(E)$, the Picard–Vessiot ring R of M_L has the simple form $R = L[\mathcal{G}^0] = L \otimes_K K[\mathcal{G}^0]$. First we lift

$\eta \in \mathrm{Gal}_{\mathrm{D}}(L/F)$ to an automorphism $\tilde{\eta} = \tilde{\eta}_R$ of R and E by setting

$$\begin{aligned} \tilde{\eta}(f) &:= \eta(f) \quad \text{for} \quad f \in L \quad \text{and} \\ \tilde{\eta}(g(D)) &:= g(C_\eta^{-1} D C_\eta) \quad \text{for} \quad g \in K[\mathcal{G}^0] \end{aligned} \tag{4.5}$$

and then similarly further to an automorphism $\tilde{\eta}_U$ of $U = L \otimes_K K[\mathrm{GL}_m]$. Using Theorem 1.7 and the equivariance, we obtain

$$\begin{aligned} \eta(A) &= \lim_{l\to\infty} (\eta(A_l)) = \lim_{l\to\infty} ((\eta \circ \partial)(D_0 \cdots D_l)\eta(D_0 \cdots D_l)^{-1}) \\ &= \lim_{l\to\infty} (\partial_L(C_\eta^{-1} D_0 \cdots D_l C_\eta) C_\eta^{-1} (D_0 \cdots D_l)^{-1} C_\eta) \\ &= \lim_{l\to\infty} (C_\eta^{-1} A_l C_\eta) = C_\eta^{-1} A C_\eta \end{aligned} \tag{4.6}$$

which leads to

$$\begin{aligned} (\tilde{\eta}_U \circ \partial_U)(X) &= \tilde{\eta}_U(AX) = \eta(A) C_\eta^{-1} X C_\eta = C_\eta^{-1} A X C_\eta \\ &= C_\eta^{-1} \partial_U(X) C_\eta = \partial_U(C_\eta^{-1} X C_\eta) = (\partial_U \circ \tilde{\eta}_U)(X). \end{aligned} \tag{4.7}$$

Hence $\tilde{\eta}_U$ is a differential automorphism of U/K and in fact of U/F. Let $\kappa : U \to R, X \mapsto Y$ denote the canonical epimorphism. Then κ is a D-homomorphism which by construction commutes with $\tilde{\eta}$, i.e., we obtain

$$\partial_R \circ \kappa = \kappa \circ \partial_U \quad \text{and} \quad \tilde{\eta}_R \circ \kappa = \kappa \circ \tilde{\eta}_U. \tag{4.8}$$

Thus $\tilde{\eta} : R \to R$ is a D-automorphism of R/F by

$$\tilde{\eta} \circ \partial_R \circ \kappa = \kappa \circ \tilde{\eta}_U \circ \partial_U = \kappa \circ \partial_U \circ \tilde{\eta}_U = \partial_R \circ \tilde{\eta} \circ \kappa \tag{4.9}$$

with $\tilde{\eta}|_L = \eta$ and

$$\tilde{\eta}(Y) = \kappa(\tilde{\eta}_U(X)) = \kappa(C_\eta^{-1} X C_\eta) = C_\eta^{-1} Y C_\eta. \tag{4.10}$$

Next we define $\tilde{Y} := ZY$. Then $F(\tilde{Y})$ is a subfield of E and we obtain

$$\partial_E(\tilde{Y}) = \partial_E(ZY) = (\partial_L(Z)Z^{-1} + ZAZ^{-1})\tilde{Y} := \tilde{A}\tilde{Y} \tag{4.11}$$

with $\tilde{A} \in L^{m\times m}$. Because of

$$\eta(\tilde{A}) = \partial_L(ZC_\eta) C_\eta^{-1} Z^{-1} + ZC_\eta \eta(A) C_\eta^{-1} Z^{-1} = \tilde{A} \quad \text{for all} \quad \eta \in H, \tag{4.12}$$

$\tilde{A}$ has entries in F, which implies that $F(\tilde{Y})/F$ is a differential field extension. Further for all $\gamma = (\varepsilon, \eta) \in \mathcal{G}^0 \rtimes H$ we find

$$\gamma(\tilde{Y}) = \varepsilon\tilde{\eta}(ZY) = \varepsilon(ZC_\eta \cdot C_\eta^{-1} Y C_\eta) = Z\varepsilon(Y) C_\eta = ZYC_\varepsilon C_\eta = \tilde{Y} C_\gamma. \tag{4.13}$$

Thus $\tilde{Y}$ does not belong to a proper differential subfield of E containing F, i.e., $F(\tilde{Y}) = E$. Hence E/F is a PV-extension with Galois group $\mathrm{Gal}_{\mathrm{D}}(E/F) = \mathcal{G}^0(K) \rtimes H = \mathcal{G}(K)$. The latter can be verified explicitly by

$$\begin{aligned} (\varepsilon_1, \eta_1)(\varepsilon_2, \eta_2)(\tilde{Y}) &= (\varepsilon_1, \eta_1)(\tilde{Y} C_{\varepsilon_2} C_{\eta_2}) = \tilde{Y} C_{\varepsilon_1} C_{\eta_1} C_{\varepsilon_2} C_{\eta_2} \\ &= \tilde{Y} C_{\varepsilon_1} C_{\varepsilon_2} C_{\eta_1}^{C_{\varepsilon_2}} C_{\eta_2} = \tilde{Y} C_{(\varepsilon_1, \eta_1)\cdot(\varepsilon_2, \eta_2)}. \quad \square \end{aligned} \tag{4.14}$$

Corollary 4.2. — *If the field L in Proposition 4.1 in addition is the solution field of an integral local D-module over $\mathcal{O}_F$, then the differential module $(\tilde{M}, \partial_{\tilde{M}})$ with the representing matrix $\tilde{A} \in \mathcal{O}_F^{m\times m}$ of $\partial_{\tilde{M}}$ again is an integral local D-module, i.e., $\tilde{M} \in \mathbf{DMod}_{\mathcal{O}_F}$.*

Proof. — Let $(C_l)_{l\in\mathbb{N}}$ denote a system of representing matrices of the integral local D-module over $\mathcal{O}_F$ generating L/F with fundamental solution matrix $Z \in \mathrm{GL}_m(\mathcal{O}_L)$. Then with $Z_0 := Z$ we obtain $Z_{l+1} := C_l^{-1} Z_l \in \mathrm{GL}_m(\mathcal{O}_{L,l+1})$. Hence by the equivariance condition the matrices $\tilde{D}_l := Z_l D_l Z_{l+1}^{-1}$ belong to $\mathrm{GL}_m(\mathcal{O}_{F,l})$. Now we want to show that $(\tilde{D}_l)_{l\in\mathbb{N}}$ is a system of representing matrices of $\tilde{M}$. For this purpose let $\tilde{B}$ be a basis of $\tilde{M}$ with $\partial_{\tilde{M}}(\tilde{B}\tilde{Y}) = 0$. Using $\tilde{B}_k := \tilde{B}\tilde{D}_0 \cdots \tilde{D}_{k-1}$ and $\tilde{Y}_k := Z_k Y_k = \tilde{D}_{k-1}^{-1} \cdots \tilde{D}_0^{-1} \tilde{Y}$ we obtain

$$0 = \partial_M(\tilde{B}\tilde{Y}) = \partial_M(\tilde{B}_l \tilde{Y}_l) = (\partial_M(\tilde{B}_l) + \tilde{B}_l \tilde{A}^{(l)})\tilde{Y}_l \tag{4.15}$$

with

$$\tilde{A}^{(l)} = \lim_{k\to\infty} (\partial_F(\tilde{D}_l \cdots \tilde{D}_k)(\tilde{D}_l \cdots \tilde{D}_k)^{-1}) \in r^l \mathcal{O}_F^{m\times m}. \tag{4.16}$$

But this implies $\partial_{\tilde{M}}(\tilde{B}_l) \equiv 0 \pmod{r^l \tilde{M}}$. □

By Proposition 4.1, in order to solve a split differential embedding problem over F with connected kernel $\mathcal{G}^0(K)$ and finite cokernel $H = \mathrm{Gal}_{\mathrm{D}}(L/F)$, it is enough to construct a module $M \in \mathbf{DMod}_{\mathcal{O}_L}$ with $\mathrm{Gal}_{\mathrm{D}}(M) = \mathcal{G}^0(K)$ and representing matrices D_l satisfying the equivariance condition. The latter can be translated into a simpler form. For this purpose we define a new Galois action of $\eta \in \mathrm{Gal}_{\mathrm{D}}(L/F)$ on $\mathcal{G}^0(L)$ via

$$\eta * D := C_\eta \eta(D) C_\eta^{-1} = \chi(\eta)\eta(D)\chi(\eta)^{-1}. \tag{4.17}$$

Then $D_l \in \mathcal{G}^0(L)$ is equivariant if and only if $\eta * D = D$ for all $\eta \in H$. This means that D_l is an F-point of the inner L-form $\mathcal{G}_\chi^0$ of $\mathcal{G}^0$ over F defined by the composed homomorphism of Proposition 4.1.

$$\chi : H \longrightarrow \mathcal{G}(K) \longrightarrow \mathrm{Aut}(\mathcal{G}(K)), \eta \mapsto \chi(\eta) \mapsto \mathrm{Int}(\chi(\eta)) \tag{4.18}$$

(compare [**Spr98**], 12.3.7).

4.2. Equivariant Realization of Connected Groups. — In this section, L is an integral finite Galois extension over the D-field $F = K\{t\}$ of analytic elements with $\partial_F = \partial_t$ and $\mathrm{Gal}_{\mathrm{D}}(L/F) = \mathrm{Gal}(L/F) =: H$. Obviously, ∂_F uniquely extends to L. We suppose that L is equipped with a Frobenius endomorphism ϕ_q^L extending the Frobenius endomorphism ϕ_q^F of F where $\phi_q^F|_K$ is a lift of the Frobenius automorphism of $\mathcal{K} = \mathcal{O}_K/\mathcal{P}_K$ and $\phi_q^F(t) = t^q$. Moreover, we assume that ∂_L and ϕ_q^L are related by formula (1.12), i.e., $(L, \partial_L, \phi_q^L)/(F, \partial_F, \phi_q^F)$ is a finite Galois extension of DF-fields in the sense of [**Mat03**], Ch. 7. By Krasner's Lemma, L/F is generated by the roots of a polynomial $f(X) \in K(t)[X]$. Thus L/F is defined over $F_0 := K(t)$, i.e., there exists a finite extension L_0/F_0 (not necessarily Galois) with $L \cong L_0 \otimes_{F_0} F$. The Frobenius endomorphism ϕ_q^L restricted to L_0 maps L_0 onto a subfield L_1 of L with $K(t^q) \le L_1$.

Proposition 4.3. — *Let $(L, \partial_L, \phi_q^L)$ be an integral finite DF-Galois extension of the DF-field $(F, \partial_F, \phi_q^F)$ of analytic elements $F = K\{t\}$ over K with $\phi_q^F(t) = t^q$ and Galois group $H := \mathrm{Gal}(L/F)$. By the above L/F is defined as a Galois extension over $F_0 = K(t)$ via $L_0 = K(s,t)$. Denote by $\mathcal{C}_l$ an affine model of $\phi_q^l(L_0)/K(t^{q^l})$, where we assume without loss of generality that $\mathfrak{o} = (0,0)$ is a regular point. Let $\mathcal{G} = \mathcal{G}^0 \rtimes H$ be a reduced linear algebraic group over K with regular homomorphic section $\chi : H \to \mathcal{G}$ and let $\mathcal{G}_\chi^0$ be the corresponding L-form of $\mathcal{G}^0$ over F with $\mathcal{G}_\chi^0(F) \leq \mathcal{G}^0(L)$.*

Suppose $M \in \mathbf{DMod}_{\mathcal{O}_L}$ is an integral local D-module over $\mathcal{O}_L$ with system of representing matrices $D_l \in \mathcal{G}^0(\mathcal{O}_L)$ satisfying the following conditions:

1. *For all $l \in \mathbb{N}$ there exists a rational map $\gamma_l : \mathcal{C}_l \to \mathcal{G}_\chi^0$ such that $D_l = \gamma_l(\phi_q^l(s), t^{q^l}) \in \mathcal{G}_\chi^0(\mathcal{O}_K(t^{q^l}))$ and $\gamma_l(\mathfrak{o}) = 1_{\mathcal{G}(K)}$.*
2. *For all $n \in \mathbb{N}$ the algebraic group over L generated by $\{\gamma_l(\mathcal{C}_l(\bar{K})) | l \geq n\}$ contains $\mathcal{G}^0(K)$.*
3. *There exists a number $d \in \mathbb{N}$ such that $\deg(\gamma_l) \leq dq^l$ for all $l \in \mathbb{N}$, where $\deg$ denotes the maximum divisor degree of the matrix entries of D_l with respect to L_0 (or $K(t)$, respectively).*
4. *If $l_0 < l_1 < \dots$ is the sequence of natural numbers l_i for which $\gamma_{l_i} \neq 1$, then $\lim_{i\to\infty}(l_{i+1} - l_i) = \infty$.*

Then M is an effective H-equivariant D-module over $\mathcal{O}_L$ with

$$\mathrm{Gal}_{\mathrm{D}}(M) \cong \mathcal{G}^0(\mathcal{O}_K) \tag{4.19}$$

and the corresponding PV-extension E/L defines a PV-extension over F with

$$\mathrm{Gal}_{\mathrm{D}}(E/F) \cong \mathcal{G}(K). \tag{4.20}$$

Proof. — As in the proof of Theorem 3.1, we assume for simplicity $r = p = q$. We start with fixing some notation. Let $M_L := L \otimes_{\mathcal{O}} M \in \mathbf{DMod}_L$ be the D-module generated by M over L with $m := \dim_L(M)$. Let $U_K := K[\mathrm{GL}_m]$ and $Q_K \trianglelefteq U_K$ be the defining ideal of $\mathcal{G}_K^0$. Then the extended ideal $Q_L := Q_K U_L \trianglelefteq U_L := L[\mathrm{GL}_m]$ is a D-ideal (compare Thm. 3.1). Therefore $\tilde{R} := L[\mathcal{G}^0] = U_L/Q_L$ is a D-ring and in addition an integral domain. Set $\tilde{E} := \mathrm{Quot}(\tilde{R})$ and let $\tilde{K}$ denote its field of constants. Let $P_L \trianglelefteq U_L$ be a maximal D-ideal containing Q_L, then $R := U_L/P_L$ is a PV-ring with PV-field $E := \mathrm{Quot}(R)$, and let $\kappa : \tilde{R} \to R$ denote the canonical epimorphism. Obviously, the D-module $\tilde{M} := \tilde{E} \otimes_L M$ contains a fundamental solution system and thus is trivial. Hence the solution space $\tilde{V} := \mathrm{Sol}_{\tilde{E}}(\tilde{M})$ is an m-dimensional $\tilde{K}$-vector space and a $\mathcal{G}^0(K)$-module by definition.

Again, we first have to show that any one-dimensional D-submodule $N \in \mathbf{DMod}_{\mathcal{O}}$ of M (or $N_L := L \otimes_{\mathcal{O}} N$, respectively) defines a $\mathcal{G}^0(K)$-stable line $\tilde{W} < \tilde{V}$. For this purpose let $B := \{b_1, \dots, b_m\}$ be a basis of M, i.e., $M = \bigoplus_{i=1}^m b_i\mathcal{O}$. Then $B_l := BD_0 \cdots D_{l-1}$ is a basis of the congruence submodule M_l or its submodule $M_l^\phi := \bigoplus_{i=1}^m b_i\mathcal{O}_l$, respectively, where $\mathcal{O}_l = \mathcal{O}_{L_l}$ with $L_l = \phi_q^l(L_0)$. Analogously, we define the

one-dimensional $\mathcal{O}_l$-submodule $N_l^\phi = N_l \cap M_l^\phi$. Then

$$N_l^\phi = B_l \boldsymbol{h}_l \mathcal{O}_l = \sum_{i=1}^{m} b_{l,i} h_{l,i} \mathcal{O}_l \quad \text{for suitable} \quad \boldsymbol{h}_l \in \mathcal{O}_l^m \tag{4.21}$$

(and $B_l = \{b_{l,1}, \dots, b_{l,m}\}$), where for every l at least one of the coefficients $h_{l,i}$ belongs to $\mathcal{O}_l^\times$. It follows from condition (1) that $M_{l+1}^\phi \le M_l^\phi$ and $N_{l+1}^\phi \le N_l^\phi$. Thus there exists an element $u_l \in \mathcal{O}_l^\times$ such that

$$B_{l+1} \boldsymbol{h}_{l+1} = B_l \boldsymbol{h}_l u_l = B_{l+1} D_l^{-1} \boldsymbol{h}_l u_l. \tag{4.22}$$

Together with (4.21) this identity implies that if any non-zero component of an $\mathcal{O}_l$-multiple of $D_l^{-1}\boldsymbol{h}_l$ is in $\mathcal{O}_{l+1}$, then so must be all others.

We want to show that we may assume $h_{l,k} = 1$ for some fixed k and all $l \in \mathbb{N}$. By construction there exists an index k for which $h_{0,k} \in \mathcal{O}_0^\times$, so by rescaling we may assume that $h_{0,k} = 1$. Suppose that $h_{j,k} = 1$ for $j \le l$. Then for the k-th component of $D_l^{-1}\boldsymbol{h}_l$ we find $(D_l^{-1}(\mathfrak{o})\boldsymbol{h}_l(\mathfrak{o}))_k = h_{l,k}(\mathfrak{o}) = 1$. This implies that we may choose

$$u_l := (D_l^{-1}\boldsymbol{h}_l)_k^{-1} \in \mathcal{O}_l^\times \tag{4.23}$$

since $u_l(\mathfrak{o}) = 1$ and $(D_l^{-1}\boldsymbol{h}_l u_l)_k = 1 \in \mathcal{O}_{l+1}$. By the remark above, all components of the last vector have to belong to $\mathcal{O}_{l+1}$. This allows us to replace $\boldsymbol{h}_{l+1}$ by

$$\boldsymbol{h}_{l+1} := D_l^{-1}\boldsymbol{h}_l u_l \in \mathcal{O}_{l+1}^m \tag{4.24}$$

with $h_{l+1,k} = 1$ by construction.

Obviously the degree of (the components of) $\boldsymbol{h}_0$ is bounded. The recursion formula (4.24) together with (4.23) then yield bounds on the degree for all $\boldsymbol{h}_l$, namely

(4.25)

$$\deg(\boldsymbol{h}_{l+1}) \le \deg(u_l) + \deg(D_l^{-1}) + \deg(\boldsymbol{h}_l) \le \begin{cases} 2(\deg(D_l^{-1}) + \deg(\boldsymbol{h}_l)) & \text{for} \quad \gamma_l \ne 1 \\ \deg(\boldsymbol{h}_l) & \text{for} \quad \gamma_l = 1. \end{cases}$$

This implies

$$\deg(\boldsymbol{h}_l) \le 2^i \deg(\boldsymbol{h}_0) + \sum_{j=0}^{i-1} 2^{i-j} \deg(D_{l_j}^{-1}) \quad \text{for} \quad l_i \le l < l_{i+1}. \tag{4.26}$$

Using condition (3) and Cramer's rule, we see that the degree of D_j^{-1} is bounded by $dp^j P(m)$ for some polynomial $P(m)$ not depending on j. On the other hand, the degree of any element in $\mathcal{O}_l$ is a multiple of p^l. So we can use condition (3) to conclude that there exists an $n \in \mathbb{N}$ such that $\boldsymbol{h}_l$ has constant coefficients for all $l \ge n$ (compare to the proof of Theorem 3.1). This implies

$$\boldsymbol{h}_l = \boldsymbol{h}_l(\mathfrak{o}) = \boldsymbol{h}_0(\mathfrak{o}) \quad \text{for} \quad l \ge n. \tag{4.27}$$

Thus for $\boldsymbol{h} := \boldsymbol{h}_0(\mathfrak{o})$ we obtain $D_l \boldsymbol{h} = u_l \boldsymbol{h}$, i.e., $\boldsymbol{h}$ is an eigenvector for D_l for all $l \ge n$.

From $u_l \in \mathcal{O}_l$ and $u_l(\mathfrak{o}) = 1$ we derive

$$y := \prod_{l \ge 0} u_l \in \mathbb{M}_K(0). \tag{4.28}$$

For $\tilde{w} := B_0 \boldsymbol{h} y$ we obtain the congruences

$$\partial(\tilde{w}) \equiv B_0(\partial(y) - A_l y)\boldsymbol{h} \equiv 0 \pmod{p^{l+1}} \quad \text{for} \quad l \in \mathbb{N} \tag{4.29}$$

by using the formula for A_l given in Theorem 1.7. Thus $\tilde{w}$ is an element of $\tilde{V}$. The vector space $\tilde{W} := \tilde{K}\tilde{w}$ spanned by $\tilde{w}$ is a one-dimensional subspace of $\tilde{V}$ which is $\mathrm{Gal}_{\mathrm{D}}(\tilde{E}/L)$- and $\mathcal{G}^0(K)$-stable (under the action on y or $\boldsymbol{h}$, respectively,) and both actions coincide when restricted to $\mathrm{Gal}_{\mathrm{D}}(E/F)$.

Next one has to show that any $\mathrm{Gal}_{\mathrm{D}}(E/L)$-stable line $\tilde{W} \leq \tilde{V}$ is $\mathcal{G}^0(K)$-stable. This can be proved using the same arguments as in the proof of Theorem 3.1 as well as the fact that M is effective, showing (4.19). By condition (1), the H-equivariance of M follows from Proposition 4.1, which then immediately implies (4.20). □

Proposition 4.3 leads to the following existence theorem for split extensions.

Theorem 4.4. — *Let $(L, \partial_L, \phi_q^L)$ be an integral finite DF-Galois extension of the DF-field $(F, \partial_F, \phi_q^F)$ of analytic elements $F = K\{t\}$ with $\partial_F = \partial_t$, $\phi_q^F(t) = t^q$ and Galois group H. Let $\mathcal{G}^0$ be a reduced connected linear algebraic group defined over $\mathcal{O}_K$ and let $\mathcal{G} = \mathcal{G}^0 \rtimes H$ be a split extension of linear algebraic groups. Then there exists an effective and H-equivariant PV-extension E/L such that*

$$\mathrm{Gal}_{\mathrm{D}}(E/L) \cong \mathcal{G}^0(K) \quad \textit{and} \quad \mathrm{Gal}_{\mathrm{D}}(E/F) \cong \mathcal{G}(K). \tag{4.30}$$

Proof. — To prove Theorem 4.4 it is enough to show the existence of a D-module $M \in \mathbf{DMod}_{\mathcal{O}_L}$ whose system of representing matrices satisfies conditions (1) – (4) of Proposition 4.3.

The algebraic F-group $\mathcal{G}_\chi^0$ is generated as an algebraic group by its Cartan subgroups, so by finitely many F-tori and finitely many unipotent groups ([**Spr98**], Thm. 13.3.6). By [**Spr98**], Thm. 14.3.8, the unipotent groups are F-split. In the special case $\mathcal{U} = \mathbb{G}_a$ we can certainly find morphisms $\gamma_l : \mathcal{C}_l \to \mathcal{U} \leq \mathcal{G}_l^0$ satisfying property (1) of Proposition 4.3. The general case of unipotent groups follows by solving central embedding problems with kernel $\mathbb{G}_a$ (using [**Spr98**], Cor. 14.3.9, compare [**MvdP03b**], Lemma 7.5 or [**Mat01**], Lemma 7.11, respectively). In the case of a torus $\mathcal{T}$ by a theorem of Tits ([**Tit68**], Ch. III, Prop. 1.6.4) there exists a $T(s,t) \in \mathcal{T}(K(t))$ generating a dense subgroup of $\mathcal{T}(K(t))$. By the proof of that theorem we may assume $T \in \mathcal{T}(\mathcal{O}_K(t))$ and $T(\mathfrak{o}) = 1$. Then the corresponding morphism $\gamma_0 : \mathcal{C}_0 \to \mathcal{T}$ as well as its Frobenius images γ_l again satisfy condition (1) of Proposition 4.3.

Since $\mathcal{G}_\chi^0$ is generated by finitely many tori and finitely many unipotent subgroups and since one morphism for each of these groups suffices to generate $\mathcal{G}_\chi^0$ as an algebraic group, we can splice the corresponding matrices D_l together into a sequence such that conditions (2), (3), and (4) are also satisfied. □

4.3. Non-Split Extensions. — For the realization of non-split group extensions with finite cokernel as D-Galois groups we use the following theorem of Borel and Serre:

Proposition 4.5. — *Let K be a perfect field and $\mathcal{G}$ a linear algebraic group over K. Then there exists a finite subgroup $\mathcal{H} \leq \mathcal{G}$ defined over K with $\mathcal{G} = \mathcal{G}^0 \cdot \mathcal{H}$. Moreover $\mathcal{H}(K) = \mathcal{H}(\bar{K})$ if K contains enough roots of unity.*

Proof. — The proof of the first part is given in [**BS64**], Lemma 5.11 with footnote. The equality $\mathcal{H}(K) = \mathcal{H}(\bar{K})$, where $\bar{K}$ denotes an algebraic closure of K, immediately follows from the representation theory of finite groups. □

This proposition leads to the following generalization of Theorem 4.4.

Theorem 4.6. — *Let K be a complete p-adic field and $\mathcal{G}$ a reduced linear algebraic group over K defined over $\mathcal{O}_K$. Suppose $\mathcal{G}^0$ has a finite supplement $\mathcal{H}$ in $\mathcal{G}$ such that $\mathcal{H}(K) = \mathcal{H}(\bar{K})$ can be realized as a DF-Galois group of an integral extension over the DF-field $F = K\{t\}$ of analytic elements over K. Then $\mathcal{G}(K)$ can be realized as D-Galois group over F.*

Proof. — Let $\tilde{\mathcal{G}}$ be the split extension of the linear algebraic groups $\mathcal{G}^0$ and $\mathcal{H}$ with the action of $\mathcal{H}$ on $\mathcal{G}^0$ given by the supplement. Then by Theorem 4.4 there exists a PV-extension $\tilde{E}/F$ with $\mathrm{Gal}_{\mathrm{D}}(\tilde{E}/F) \cong \tilde{\mathcal{G}}(K)$. The group $\mathcal{G}$ is a linear quotient group of $\tilde{\mathcal{G}}$, so there exists a PV-extension E/F inside $\tilde{E}/F$ with $\mathrm{Gal}_{\mathrm{D}}(E/F) \cong \mathcal{G}(K)$. □

An easy application is the following: Let K be a p-adic field containing the n-th roots of unity, let F be the field of analytic elements over K and let L/F be a cyclic extension given by the equation $s^n = t$. Assume p does not divide n, then $\mathcal{O}_L/\mathcal{O}_F$ is an extension of p-adic D-rings. Hence every linear algebraic group $\mathcal{G}$ over K with a cyclic supplement $H = \mathcal{H}(K)$ of $\mathcal{G}^0$ of order dividing n can be realized as the D-Galois group of an integral D-module M over F, i.e.,

$$\mathrm{Gal}_{\mathrm{D}}(M) \cong \mathcal{G}(\mathcal{O}_K) \quad \text{and} \quad \mathrm{Gal}_{\mathrm{D}}(M_F) \cong \mathcal{G}(K). \tag{4.31}$$

4.4. The Non-Connected Inverse Problem. — Now we assume that the field of differential constants K of the field of analytic elements $F = K\{t\}$ contains the Witt ring $\mathbb{W}(\bar{\mathbb{F}}_p)$, i.e., K contains $\mathbb{E}_p := \mathrm{Quot}(\mathbb{W}(\bar{\mathbb{F}}_p))$. Then the residue field $\mathcal{F}$ of F equals $\bar{\mathbb{F}}_p(t)$. This entails a positive solution of the finite inverse problem over F.

Proposition 4.7. — *Let $F = K\{t\}$ be the field of analytic elements over a complete p-adic field K with $K \geq \mathbb{E}_p$. Then every finite group H can be realized as D-Galois group of an integral DF-extension L/F.*

Proof. — Let F^{ur}/F be the maximal unramified algebraic extension of F. Then the derivation $\partial_F = \partial_t$ as well as the Frobenius endomorphism ϕ_q^F extend uniquely to F^{ur} and the D-Galois group $\mathrm{Gal}_{\mathrm{D}}(F^{\mathrm{ur}}/F)$ coincides with $\mathrm{Gal}(F^{\mathrm{ur}}/F)$. By profinite Galois theory, $\mathrm{Gal}(F^{\mathrm{ur}}/F)$ is isomorphic to the Galois group of the separable closure $\mathcal{F}^{\mathrm{sep}}/\mathcal{F}$ of the residue field $\mathcal{F}$ (see [**Nag91**], Thm. 6.3.2). Now a theorem of Harbater [**Har95**] and Pop [**Pop95**] (compare [**MM99**], Thm. V.2.10) shows that the profinite group $\mathrm{Gal}(\mathcal{F}^{\mathrm{sep}}/\mathcal{F})$ is free of countable rank. In particular, every finite group H can be realized as the Galois group of a Galois extension $\mathcal{L}/\mathcal{F}$ and as the DF-Galois group of a p-adically unramified DF-Galois extension L/F. By the last property and Proposition 1.1 the extension L/F is integral and does not contain new constants. □

Combining the result above with Proposition 4.5 and Theorem 4.6 we obtain the solution of the general inverse problem over F:

Theorem 4.8. — *Let $F = K\{t\}$ be the field of analytic elements over a complete p-adic field K containing $\mathbb{E}_p$ and let $\mathcal{G}$ be a reduced linear algebraic group defined over $\mathcal{O}_K$. Then $\mathcal{G}(K)$ can be realized as D-Galois group over F.*

5. Reduction of Constants

5.1. Iterative D-Modules. — A local D-ring $(\mathcal{O}_F, \partial_F)$ is called a *local iterative D-ring* or a *local ID-ring* for short if

$$\frac{1}{k!}\partial_F^k(\mathcal{O}_F) \subseteq \mathcal{O}_F \quad \text{and} \quad \frac{1}{k!}\partial_F^k(\mathcal{P}_F) \subseteq \mathcal{P}_F \quad \text{for} \quad k \in \mathbb{N}. \tag{5.1}$$

Here again the second condition follows from the first in case the value group $|F^\times|$ of F coincides with the value group $|K^\times|$ of its field of constants. The family of higher derivations $\partial_F^{(k)} := \frac{1}{k!}\partial_F^k : \mathcal{O}_F \to \mathcal{O}_F$ defines an *iterative derivation* $\partial_F^* := (\partial_F^{(k)})_{k\in\mathbb{N}}$ on $\mathcal{O}_F$ as introduced by H. Hasse and F. K. Schmidt [**HS37**] (compare [**MvdP03b**], § 2.1 or [**vdPS03**], Ch. 13.3).

Now let (M, ∂_M) be an integral local D-module over $\mathcal{O} := \mathcal{O}_F$, i.e., $M \in \mathbf{DMod}_{\mathcal{O}}$. Then (M, ∂_M) is called a *local iterative D-module* or a *local ID-module* if in addition

$$\frac{1}{k!}\partial_M^k(M) \subseteq M \quad \text{for} \quad k \in \mathbb{N}. \tag{5.2}$$

Then the family of maps $\partial_M^* := (\partial_M^{(k)})_{k\in\mathbb{N}}$, where $\partial_M^{(k)} := \frac{1}{k!}\partial_M^k$, is the *iterative derivation on M* induced by ∂_M (compare [**MvdP03b**], § 2.2 or [**vdPS03**], loc. cit.). Obviously, the local ID-modules over $\mathcal{O}$ with D-homomorphisms form a tensor category denoted by $\mathbf{IDMod}_{\mathcal{O}}$.

Proposition 5.1. — *Let $(\mathcal{O}_F, \partial_F)$ be a local ID-ring and (M, ∂_M) a local D-module over $\mathcal{O} := \mathcal{O}_F$. Then (M, ∂_M) is integral if and only if it is an ID-module. More precisely, the tensor categories $\mathbf{DMod}_{\mathcal{O}}$ and $\mathbf{IDMod}_{\mathcal{O}}$ are equivalent.*

The proof immediately follows from [**MvdP03b**], Prop. 8.1.

The ID-structure of M gives rise to a second projective system: For this purpose we define

$$\mathcal{O}_{(0)} := \mathcal{O},\ \mathcal{O}_{(l+1)} := \{a \in \mathcal{O}_{(l)} | \partial_F^{(p^l)}(a) \in \mathcal{P}_F\} \tag{5.3}$$

and, respectively,

$$M_{(0)} := M,\ M_{(l+1)} := \{x \in M_{(l)} | \partial_M^{(p^l)}(x) \in \mathcal{P}_F M\}. \tag{5.4}$$

Then in analogy to Proposition 1.3 the submodules $M_{(l)}$ together with the $\mathcal{O}_{(l+1)}$-linear embeddings $\varphi_{(l)} : M_{(l+1)} \to M_{(l)}$ form a projective system $(M_{(l)}, \varphi_{(l)})_{l\in\mathbb{N}}$ of $\mathcal{O}_{(l)}$-modules. The category of all those projective systems with the properties (1.18) and (1.19) for $M_{(l)}, \varphi_{(l)}$ instead of M_l, φ_l will be denoted by $\mathbf{IDProj}_{\mathcal{O}}$.

Corollary 5.2. — *Let $(\mathcal{O}_F, \partial_F)$ be a local ID-ring, $(M, \partial_M) \in \mathbf{DMod}_{\mathcal{O}}$ and let $(M_l, \varphi_l)_{l\in\mathbb{N}}$, $(M_{(l)}, \varphi_{(l)})_{l\in\mathbb{N}}$ be the induced projective systems in $\mathbf{DProj}_{\mathcal{O}}$ or $\mathbf{IDProj}$, respectively.*

(a) *For all $l \in \mathbb{N}$ there exists a $k(l) \in \mathbb{N}$ such that*

$$\mathcal{O}_{(l)} \geq \mathcal{O}_k \quad \textit{and} \quad M_{(l)} \geq M_k \quad \textit{for all} \quad k \geq k(l).$$

(b) *Then with a basis $B_k = \{b_{k1}, \ldots, b_{km}\}$ of M_k*

$$M_{(l)} = \mathcal{O}_{(l)} \otimes_{\mathcal{O}_k} M_k = \bigoplus_{i=1}^{m} \mathcal{O}_{(l)} b_{k,i}. \tag{5.5}$$

Proof. — By the definition of a local integral D-module there exists an $\mathcal{O}_F$-basis $B_k = \{b_{k1}, \ldots, b_{km}\}$ of M for all $k \in \mathbb{N}$ with $\partial_M(b_{k,i}) \in r^k M$ and thus $\partial_M^{p^j}(b_{k,i}) \in r^k M$ for all $j \in \mathbb{N}$. This implies

$$\partial_M^{(p^j)}(b_{k,i}) = \frac{1}{(p^j)!}\partial_M^{p^j}(b_{k,i}) \in \mathcal{P}_F M \quad \text{for all} \quad j < l \in \mathbb{N} \tag{5.6}$$

in case k is large enough, say, $k \geq k(l)$. This proves (a) and also (b), since $x = \sum_{i=1}^{n} a_i b_{k,i} \in M$ belongs to $M_{(l)}$ if and only if $a_i \in \mathcal{O}_{(l)}$ for $i = 1, \ldots, m$. □

If we let $(D_l)_{l\in\mathbb{N}}$ denote a system of representing matrices of (M, ∂_M) (with respect to bases B_l of M_l), we obtain a system of representing matrices of the second projective system $(M_{(l)}, \varphi_{(l)})_{l\in\mathbb{N}}$ for example by

$$D_{(l)} := D_{k(l-1)} \cdots D_{k(l)-1} \in \mathrm{GL}_m(\mathcal{O}_{k(l-1)}) \quad \text{for} \quad l \in \mathbb{N} \tag{5.7}$$

(with respect to the bases $B_{k(l)}$) and $k(-1) = 0$. Moreover, with the base change matrices $(D_{(l)})_{l\in\mathbb{N}}$ from $(M_{(l)}, \varphi_{(l)})_{l\in\mathbb{N}}$ we can recover the derivation ∂_M which is characterized by the projective system $(M_l, \varphi_l)_{l\in\mathbb{N}}$ according to Theorem 1.4.

5.2. Residue Modules. — The iterative derivation ∂_F^* of a local ID-ring $\mathcal{O}_F = \mathcal{O}$ induces an iterative derivation $\partial_{\mathcal{F}}^*$ on the residue field $\mathcal{F} := \mathcal{O}_{\mathcal{F}}/\mathcal{P}_F$ by

$$\partial_{\mathcal{F}}^{(k)}(a + \mathcal{P}_F) := \partial_F^{(k)}(a) + \mathcal{P}_F \quad \text{for} \quad a \in \mathcal{O}_F \quad \text{and} \quad k \in \mathbb{N}. \tag{5.8}$$

Analogously any $M \in \mathbf{DMod}_{\mathcal{O}} = \mathbf{IDMod}_{\mathcal{O}}$ with $\mathcal{O}$-basis $B = \{b_1, \ldots, b_m\}$ reduces to an $\mathcal{F}$-vector space

$$\tilde{M} := M/\mathcal{P}_F M = \bigoplus_{i=1}^{m} \mathcal{F}\tilde{b}_i \tag{5.9}$$

with basis $\tilde{B} = \{\tilde{b}_1, \ldots, \tilde{b}_m\}$ equipped with an iterative derivation $\partial_{\tilde{M}}^*$ defined by

$$\partial_{\tilde{M}}^{(k)}(x + \mathcal{P}_F M) := \partial_M^{(k)}(x) + \mathcal{P}_F M \quad \text{for} \quad x \in M \quad \text{and} \quad k \in \mathbb{N}, \tag{5.10}$$

i.e., $(\tilde{M}, \partial_{\tilde{M}}^*)$ is an ID-module over $\mathcal{F}$ in the sense of [**MvdP03b**], Ch. 2.2 (compare [**vdPS03**],Ch. 13.3). The next proposition shows that the induced projective systems are compatible with the reduction process.

Proposition 5.3. — *Let $(\mathcal{O},\partial^*)$ be a local ID-ring with residue field $\mathcal{F}$ and $(M,\partial_M^*)\in \mathbf{IDMod}_{\mathcal{O}}$ with associated projective system $(M_{(l)},\varphi_{(l)})_{l\in\mathbb{N}}\in \mathbf{IDProj}_{\mathcal{O}}$. Then the projective system of the reduced ID-module $(\tilde{M},\partial_{\tilde{M}}^*)\in \mathbf{IDMod}_{\mathcal{F}}$ is given by $(\tilde{M}_l,\tilde{\varphi}_l)_{l\in\mathbb{N}}$ where*

$$\tilde{M}_l := M_{(l)}/(M_{(l)}\cap \mathcal{P}_F M) \tag{5.11}$$

and $\tilde{\varphi}_l$ is induced from $\varphi_{(l)}$.

Proof. — Let (for each l) $B_{(l)}$ be an arbitrary $\mathcal{O}_{(l)}$-basis of $M_{(l)}$ and $D_{(l)}\in \mathrm{GL}_m(\mathcal{O}_{(l)})$ with $B_{(l)}=B_{(l-1)}D_{(l-1)}$. For $x\in M$ there exists $\boldsymbol{y}_{(0)}=(y_1,\dots,y_m)\in\mathcal{O}^m$ with $x=B_{(0)}\boldsymbol{y}_{(0)}$ and thus $x=B_{(l)}\boldsymbol{y}_{(l)}$ with $\boldsymbol{y}_{(l)}:=D_{(l-1)}^{-1}\cdots D_{(0)}^{-1}\boldsymbol{y}_{(0)}$. Then obviously for all $k<p^l$ we obtain

$$\begin{aligned}\partial_M^{(k)}(x)&=\partial_M^{(k)}(B_{(l)}\boldsymbol{y}_{(l)})=\sum_{i+j=k}\partial_M^{(i)}(B_{(l)})\partial_F^{(j)}(\boldsymbol{y}_{(l)})\\ &\equiv B_l\partial_F^{(k)}(\boldsymbol{y}_{(l)})=B_0D_{(0)}\cdots D_{(l-1)}\partial_F^{(k)}(D_{(l-1)}^{-1}\cdots D_{(0)}^{-1}\boldsymbol{y}_{(0)})\pmod{\mathcal{P}_FM}.\end{aligned} \tag{5.12}$$

Substituting $B_{(0)}$ by the reduced basis $\tilde{B}$ and $D_{(l)}$ by the reduced base change matrices $\tilde{D}_l$ the above equation yields the formula for the iterative derivation of an ID-module over $\mathcal{F}$ induced from its projective system (see [**Mat01**], Prop. 2.10 or [**MvdP03a**], Ch. 5.5, respectively). □

If we use the bases $B_{k(l)}$ for $M_{(l)}$, the reduced base change matrices $\tilde{D}_l$ of $(\tilde{M}_l,\tilde{\varphi}_l)_{l\in\mathbb{N}}$ are obtained from the representing matrices D_l of $(M_l,\varphi_l)_{l\in\mathbb{N}}$ by

$$\tilde{D}_l=D_{k(l-1)}\cdots D_{k(l)-1}\pmod{\mathcal{P}_F\mathcal{O}_{(l)}^{m\times m}}. \tag{5.13}$$

5.3. Behaviour of the Galois Group. — As before, let $(\mathcal{O}_F,\partial_F^*)$ be a p-adic ID-ring with quotient field F and $(M,\partial_M)\in\mathbf{DMod}_{\mathcal{O}}$ for $\mathcal{O}=\mathcal{O}_F$. As in Section 2.2 we assume the quotient field E_M of a Picard–Vessiot ring R_M of M over $\mathcal{O}_F$ does not contain new constants. Then by Proposition 2.3 there exists a reduced linear algebraic group $\mathcal{G}$ over the field of constants K of F with $\mathrm{Aut}_{\mathrm{D}}(M)\cong\mathcal{G}(\mathcal{O}_K)$. Further, at least in the case when $\mathcal{G}$ is connected, we know $R_M^{\mathrm{Aut}_{\mathrm{D}}(M)}=\mathcal{O}_F$. This fact will be assumed in the next theorem. Since the group of $\mathcal{K}$-rational points $\mathcal{G}(\mathcal{K})$ over a finite field $\mathcal{K}$ is not Zariski dense in $\mathcal{G}(\bar{\mathcal{K}})$, we suppose in addition $\mathcal{K}\geq\bar{\mathbb{F}}_p$ or $K\geq\mathbb{E}_p:=\mathrm{Quot}(\mathbb{W}(\bar{\mathbb{F}}_p))$, respectively.

Theorem 5.4. — *Let (M,∂_M) be an integral p-adic D-module over a discretely valued p-adic ID-ring $(\mathcal{O}_F,\partial_F^*)$ with field of constants $K\geq\mathbb{E}_p$. Assume there exists a Picard–Vessiot ring R_M of M over F without new constants and with $R_M^{\mathrm{Gal}_{\mathrm{D}}(M)}=\mathcal{O}_F$. Then the residue module $(\tilde{M},\tilde{\partial}_M^*)$ of M is an ID-module over the residue field $\mathcal{F}:=\mathcal{O}_F/\mathcal{P}_F$ whose ID-Galois group is bounded by*

$$\mathrm{Gal}_{\mathrm{ID}}(\tilde{M})\leq\mathrm{Gal}_{\mathrm{D}}(M)/\mathrm{Gal}_{\mathrm{D}}(M)_1 \tag{5.14}$$

where $\mathrm{Gal}_{\mathrm{D}}(M)_1$ denotes the principal congruence subgroup of the p-adic analytic group $\mathrm{Gal}_{\mathrm{D}}(M)$.

Proof. — For the proof we follow the construction of a Picard–Vessiot ring R_M of M over $\mathcal{O}_F$ (compare [**Mat03**], Thm. 10.2). Let $(M_l, \varphi_l)_{l\in\mathbb{N}} \in \mathbf{DProj}_{\mathcal{O}}$ and $(M_{(l)}, \varphi_{(l)})_{l\in\mathbb{N}} \in \mathbf{IDProj}_{\mathcal{O}}$ be the respective projective systems associated to (M, ∂_M) with systems of representing matrices $(D_l)_{l\in\mathbb{N}}$ and $(D_{(l)})_{l\in\mathbb{N}}$, where $D_{(l)} = D_{k(l-1)} \cdots D_{k(l)-1}$ according to Corollary 5.2. Then the derivative ∂_M of M with respect to the basis $B = B_0 = \{b_1, \ldots, b_m\}$ of M is given by

$$\partial_M(B) = -B \cdot A \tag{5.15}$$

with the matrix $A \in \mathcal{O}_F^{m\times m}$ constructed in Theorem 1.7. Analogously, the higher derivations on M are given by

$$\partial_M^{(k)}(B) = \frac{1}{k!}\partial_M^k(B) = -B \cdot A^{(k)} \tag{5.16}$$

with

$$A^{(k)} = \lim_{l\to\infty} (\partial_F^{(k)}(D_0 \cdots D_l)(D_0 \cdots D_l)^{-1}) \in \mathcal{O}_F^{m\times m}. \tag{5.17}$$

The ring $U := \mathcal{O}_F[\mathrm{GL}_m] = \mathcal{O}_F[x_{ij}, \det(x_{ij})^{-1}]_{i,j=1}^m$ becomes an ID-ring via

$$\partial_U^{(k)}(X) = A^{(k)}X \quad \text{for} \quad X = (x_{ij})_{i,j=1}^m. \tag{5.18}$$

Now let $P \trianglelefteq U$ be a maximal differential ideal with $P \cap \mathcal{O}_F = (0)$, which is an ID-ideal by (5.17). Then the $\mathcal{O}_F$-algebra $R_M := U/P$ is an "integral PV-ring" with quotient field $E := E_M$ (up to differential isomorphism) and there exists a fundamental solution matrix $Y = (y_{ij})_{i,j=1}^m \in \mathrm{GL}_m(R_M)$ with $\partial_E(Y) = A \cdot Y$. By assumption E and R_M do not contain new constants and $\mathrm{Gal_D}(M) := \mathrm{Aut_D}(R_M/\mathcal{O}_F)$ has the property $R_M^{\mathrm{Gal_D}(M)} = \mathcal{O}_F$. A matrix representation of $\mathrm{Gal_D}(M)$ on the solution space is given by

$$\Gamma : \mathrm{Gal_D}(M) \longrightarrow \mathrm{GL}_m(\mathcal{O}_K), \gamma \mapsto C_\gamma \tag{5.19}$$

where $\gamma(Y) = YC_\gamma$.

Now let $\tilde{U} := \mathcal{F} \otimes_{\mathcal{O}} U = \mathcal{F}[\tilde{x}_{ij}, \det(\tilde{x}_{ij})^{-1}]_{i,j=1}^m$ and let $\tilde{R}_M := \mathcal{F} \otimes_{\mathcal{O}} R_M$ be the residue ring of R_M over $\mathcal{F}$, i.e., $\tilde{R}_M = \mathcal{F}[\tilde{y}_{ij}, \det(\tilde{y}_{ij})^{-1}]_{i,j=1}^m$ with $\tilde{y}_{ij} = 1 \otimes y_{ij} \in \tilde{R}_M$. Then the residue matrices $\tilde{D}_l$ of $D_{(l)} \in \mathrm{GL}_m(\mathcal{O}_F)$ define an iterative derivation $\partial^*_{\tilde{R}_M}$ on $\tilde{R}_M$ by

$$\partial_{\tilde{R}_M}^{(k)}(\tilde{Y}) := \partial_{\mathcal{F}}^{(k)}(\tilde{D}_0 \cdots \tilde{D}_l)(\tilde{D}_0 \cdots \tilde{D}_l)^{-1}\tilde{Y} \quad \text{for} \quad k < p^l \tag{5.20}$$

where $\tilde{Y} = (\tilde{y}_{i,j})_{i,j=1}^m$, i.e., $\tilde{R}_M$ is an ID-ring. Hence $\tilde{R}_M$ can be obtained as a quotient of $\tilde{U}$ by an ID-ideal $\tilde{P}$:

$$\tilde{R}_M = \tilde{U}/\tilde{P}. \tag{5.21}$$

The group of iterative differential automorphisms $\mathrm{Aut_{ID}}(\tilde{R}_M/\mathcal{F})$ is a linear algebraic group over $\bar{\mathbb{F}}_p = \mathcal{O}_K/\mathcal{P}_K$ since

$$\mathrm{Aut_{ID}}(\tilde{R}_M/\mathcal{F}) = \{\tilde{C} \in \mathrm{GL}_m(\bar{\mathbb{F}}_p) | \tilde{p}(X\tilde{C}) = 0 \quad \text{for all} \quad \tilde{p} \in \tilde{P}\}. \tag{5.22}$$

Because of $\widetilde{\gamma(Y)} = \widetilde{YC_\gamma} = \tilde{Y}\tilde{C}_\gamma$ for $\gamma \in \mathrm{Gal_D}(M)$, the restriction map

$$\tilde{} : \mathrm{Gal_D}(M) \longrightarrow \mathrm{Aut_{ID}}(\tilde{R}_M/\mathcal{F}), C_\gamma \mapsto \tilde{C}_\gamma \tag{5.23}$$

is a group homomorphism with kernel $\mathrm{Gal_D}(M)_1$ whose image is denoted by $\tilde{G}$. By construction we obtain $\tilde{R}_M^{\tilde{G}} = \mathcal{F}$. Thus $\tilde{G}$ is Zariski dense in $\mathrm{Aut_{ID}}(\tilde{R}_M/\mathcal{F})$ and the restriction map is surjective. This proves

$$\mathrm{Aut_{ID}}(\tilde{R}_M/\mathcal{F}) = \tilde{G} \cong \mathrm{Gal_D}(M)/\mathrm{Gal_D}(M)_1. \tag{5.24}$$

Now let $\tilde{Q} \trianglelefteq \tilde{U}$ be a maximal ID-ideal containing $\tilde{P}$. Then $R_{\tilde{M}} := \tilde{U}/\tilde{Q}$ is an iterative Picard-Vessiot ring for $\tilde{M}$ with

$$\begin{aligned} \mathrm{Gal_{ID}}(\tilde{M}) = \mathrm{Gal_{ID}}(R_{\tilde{M}}/\mathcal{F}) &\cong \{\tilde{\gamma} \in \mathrm{GL}_m(\bar{\mathbb{F}}_p) | \tilde{\gamma}(\tilde{Q}) \subseteq \tilde{Q}\} \\ &\leq \{\tilde{\gamma} \in \mathrm{GL}_m(\bar{\mathbb{F}}_p) | \tilde{\gamma}(\tilde{P}) \subseteq \tilde{P}\} \cong \mathrm{Aut_{ID}}(\tilde{R}_M/\mathcal{F}) \\ &\cong \mathrm{Gal_D}(M)/\mathrm{Gal_D}(M)_1, \end{aligned} \tag{5.25}$$

since every ID-ideal $\tilde{P} \trianglelefteq \tilde{U}$ is left invariant by $\mathrm{Gal_{ID}}(\tilde{M})$ (by the correspondence of ID-ideals and $\mathrm{Gal_{ID}}$-stable ideals in $\tilde{U}$, compare [**vdPS03**], proof of Thm. 1.28). □

The question remains under which conditions equality holds in (5.14) (compare [**MvdP03b**], Conjecture 8.5).

5.4. Example SL_2**.** — As an example, let K be $\mathbb{E}_p = \mathrm{Quot}(\mathbb{W}(\bar{\mathbb{F}}_p))$ and let $F = K\{t\}$ be the field of analytic elements over K. Let further (M, ∂_M) be a 2-dimensional $\mathcal{O}_F$-module with associated projective system $(M_l, \varphi_l)_{l\in\mathbb{N}}$ and system of representing matrices

$$D_l = \begin{pmatrix} 1 & a_l t^{p^l} \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad D_l = \begin{pmatrix} 1 & 0 \\ a_l t^{p^l} & 1 \end{pmatrix} \tag{5.26}$$

with $a_l \in \mathcal{O}_K = \mathbb{W}(\bar{\mathbb{F}}_p)$. For the sequence of natural numbers $l_0 < l_1 < \dots$ with $a_{l_i} \neq 0$ we assume $\lim_{i\to\infty}(l_{i+1} - l_i) = \infty$. We further assume that there exist infinitely many l with $D_l \neq I$ which are upper triangular and infinitely many $D_l \neq I$ which are lower triangular. Then from Theorem 3.1 it follows that

$$\mathrm{Gal_D}(M) = \mathrm{SL}_2(\mathcal{O}_K) = \mathrm{SL}_2(\mathbb{W}(\bar{\mathbb{F}}_p)). \tag{5.27}$$

Now let $(\tilde{M}, \partial^*_{\tilde{M}})$ be the reduced ID-module over $\mathcal{F} = \bar{\mathbb{F}}_p(t)$ with system of representing matrices $\tilde{D}_l := \tilde{D}_{(l)}$ where $D_{(l)} = D_l$. In case all $a_{l_i} \neq 0$ are units in $\mathcal{O}_K$, i.e., $\tilde{a}_{l_i} \neq 0$, the properties above for $(D_l)_{l\in\mathbb{N}}$ entail the corresponding properties for $(\tilde{D}_l)_{l\in\mathbb{N}}$. Hence we obtain, by [**MvdP03b**], Lemma 7.4,

$$\mathrm{Gal_{ID}}(\tilde{M}) = \mathrm{SL}_2(\bar{\mathbb{F}}_p), \tag{5.28}$$

i.e., in Theorem 5.4 we have equality by

$$\mathrm{Gal_{ID}}(\tilde{M}) = \mathrm{SL}_2(\bar{\mathbb{F}}_p) \cong \mathrm{SL}_2(\mathbb{W}(\bar{\mathbb{F}}_p))/\mathrm{SL}_2(\mathbb{W}(\bar{\mathbb{F}}_p))_1 = \mathrm{Gal_D}(M)/\mathrm{Gal_D}(M)_1. \tag{5.29}$$

References

[BP99] E. Bayer & R. Parimala – Galois cohomology of classical groups over fields of cohomological dimension, *Invent. math.* **122** (1999), p. 195–229.

[BS64] A. Borel & J.-P. Serre – Théorèmes de finitude en cohomologie galoisienne, *Comment. Math. Helvet.* **39** (1964), p. 111–164.

[Chr83] G. Christol – *Modules différentiels et équations différentielles p-adiques*, Queen's Papers in Pure and Applied Mathematics, vol. 66, Queen's University, Kingston, 1983.

[Col03] P. Colmez – Les conjectures de monodromie p-adiques, *Astérisque* **290** (2003), p. 53–101.

[Har87] D. Harbater – Galois coverings of the arithmetic line, in *Number Theory, New York 1984–1985* (D. Chudnovsky et al., eds.), Springer–Verlag, Berlin etc., 1987, p. 165–195.

[Har95] ———, Fundamental groups and embedding problems in characteristic p, in *Recent Developments in the Inverse Galois Problem* (M. Fried et al., eds.), Contemporary Math., vol. 186, AMS, Providence, 1995, p. 353–369.

[Har02] J. Hartmann – On the inverse problem in differential galois theory, Ph.D. Thesis, Univ. Heidelberg, 2002.

[HS37] H. Hasse & F. Schmidt – Noch eine Begründung der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten, *J. reine angew. Math.* **177** (1937), p. 215–237.

[Kol76] E. Kolchin – *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1976.

[Mat01] B. Matzat – *Differential Galois theory in positive characteristic*, IWR Preprint 2001-35, 2001.

[Mat03] ———, Frobenius Modules and Galois Groups, in *Galois Theory and Modular Forms* (K. Hashimoto et al., eds.), Kluwer, Boston, 2003, p. 233–268.

[MM99] G. Malle & B. Matzat – *Inverse Galois Theory*, Springer–Verlag, Berlin etc., 1999.

[MvdP03a] B. Matzat & M. van der Put – Constructive differential Galois theory, in *Galois Groups and Fundamental Groups* (L. Schneps, ed.), MSRI Publications, vol. 41, Cambridge UP, 2003, p. 425–467.

[MvdP03b] ———, Iterative differential equations and the Abhyankar conjecture, *J. reine angew. Math.* **257** (2003), p. 1–52.

[Nag91] M. Nagata – *Theory of commutative fields*, AMS, Providence, 1991.

[Pop95] F. Pop – Étale Galois covers of affine smooth curves, *Invent. Math.* **120** (1995), p. 555–578.

[PR94] V. Platonov & A. Rapinchuk – *Algebraic Groups and Number Theory*, Academic Press, Boston etc., 1994.

[Ser62] J.-P. Serre – *Corps Locaux*, Hermann, Paris, 1962.

[Ser97] ———, *Galois Cohomology*, Springer–Verlag, Berlin etc., 1997.

[Spr98] T. Springer – *Linear Algebraic Groups*, Birkhäuser, Boston, 1998.

[Tit68] J. Tits – *Lectures on Algebraic Groups*, Lecture Notes, Yale Univ., 1968.

[vdP01] M. van der Put – Bounded p-adic differential equations, in *Circumspice, Various Papers in and Around Mathematics in Honor of Arnoud van Rooij*, Subfaculteit Wiskunde, Katholieke Universiteit Nijmegen, 2001.

[vdPS03] M. VAN DER PUT & M. SINGER – *Galois Theory of Linear Differential Equations*, Springer–Verlag, Berlin etc., 2003.

B. H. MATZAT, IWR, Universität Heidelberg, Im Neuenheimer Feld 368, D–69120 Heidelberg
E-mail : matzat@iwr.uni-heidelberg.de