J. reine angew. Math. **557** (2003), 1—52

Journal für die reine und
angewandte Mathematik

Iterative differential equations and the Abhyankar conjecture

By *B. Heinrich Matzat* at Heidelberg and *Marius van der Put* at Groningen

1. Introduction

Higher derivations, here called *iterative derivations*, were introduced by H. Hasse and F. K. Schmidt, [H-S]. The basic example is the iterative derivation $\{\partial_z^{(n)}\}_{n\geqq 0}$, defined on the field $C(z)$, and given by the formulas $\partial_z^{(n)} z^m = \binom{m}{n} z^{m-n}$. If the field C has characteristic 0, then $\partial_z^{(n)}$ is just the operator $\frac{1}{n!}\left(\frac{d}{dz}\right)^n$ on $C(z)$. We are interested in the case where C is an algebraically closed field of characteristic $p > 0$. More generally, we consider a field K with an iterative derivation $\{\partial_K^{(n)}\}_{n\geqq 0}$ such that its field of constants C, i.e., the set of elements $a \in K$ with $\partial_K^{(n)}(a) = 0$ for all $n \geqq 1$, is algebraically closed, has characteristic $p > 0$ and is different from K. A (linear, iterative) differential equation over the iterative differential field K (or ID-field for short) can be given as a vector space M over K of finite dimension, equipped with a sequence of additive maps $\partial_M^{(n)}\colon M \to M$, $n \geqq 0$ satisfying the rules:

(a) $\partial_M^{(0)}$ is the identity.

(b) $\partial_M^{(n)}(fm) = \sum\limits_{a,b\geqq 0,\, a+b=n} \partial_K^{(a)}(f)\partial_M^{(b)}(m)$ for all $n \geqq 0$, $f \in K$, $m \in M$.

(c) $\partial_M^{(a)} \circ \partial_M^{(b)} = \binom{a+b}{b}\partial_M^{(a+b)}$.

As early as 1963, these (linear, iterative) differential equations have been studied by H. Okugawa, [O]. He proposed a Picard-Vessiot theory along the lines of R. E. Kolchin's work. His theory remained incomplete since the existence and uniqueness of a Picard-Vessiot extension for a given (linear, iterative) differential equation could not be established at the time. The paper does not contain explicit examples and there seems to be no sequel to this work. In the present paper we give a full presentation of the Picard-Vessiot theory and relate this to the Tannakian approach. The main part of the paper is concerned with the inverse problem, i.e., with the question:

Which (reduced) linear algebraic group $\mathcal{G}$ over C can be realized as the differential Galois group of some linear, iterative differential equation over K?

For the field $K = C((z))$, with C algebraically closed and provided with the standard iterative differentiation, a complete answer is given in theorem 6.6. The case where K is the function field of an irreducible, smooth, projective curve X over an algebraically closed field C of characteristic $p > 0$ seems the most interesting one. For the iterative differential modules one prescribes a finite, non-empty, singular locus $S \subset X$. Our results and conjecture for this situation are closely related to Abhyankar's conjecture. The latter concerns Galois covers of curves in characteristic $p > 0$ with prescribed ramification. Abhyankar's conjecture has been proved by M. Raynaud [R] and D. Harbater [H1], [H2]. This "conjecture" turns out to be a special case of our conjecture concerning the inverse problem for linear iterative differential equations over function fields.

In this paper we solve the inverse problem for *connected* linear algebraic groups. The final section explores the strong relation between linear iterative differential equations over a field of characteristic p and linear p-adic differential equations. Finally a link between Grothendieck's conjecture on p-curvatures and linear iterative differential modules is described.

2. Iterative derivations and differential equations

2.1. Iterative derivations. For any ring R (commutative and with a unit element) an *iterative derivation* is a sequence of additive maps $\partial^{(n)}: R \to R$, $n \geqq 0$ satisfying:

1. $\partial^{(0)}$ is the identity.
2. $\partial^{(n)}(fg) = \sum_{a,b\geqq 0, a+b=n} \partial^{(a)}(f)\partial^{(b)}(g)$.
3. $\partial^{(n)}\partial^{(m)} = \binom{n+m}{n}\partial^{(n+m)}$.

For the case $\mathbb{Q} \subset R$, one observes that $\partial^{(n)} = \frac{1}{n!}(\partial^{(1)})^n$ and thus the iterative derivation is determined by the ordinary derivation $\partial^{(1)}$. In the sequel we will suppose that the ring R has characteristic $p > 0$.

Some observations and examples of iterative derivations. (1) A nice reformulation of an iterative derivation on R is the following:

Consider for a sequence of maps $\partial^{(n)}: R \to R$ the map $\phi_T: R \to R[[T]]$, given by $\phi_T(a) = \sum_{n\geqq 0} \partial^{(n)}(a)T^n$. Then properties 1. and 2. are equivalent to ϕ_T is a homomorphism of rings such that the composition with the augmentation map, i.e., $R \to R[[T]] \to R$, is the identity. We extend ϕ_T to a map $R[[T]] \to R[[T]]$ (with the same name) by putting

$$\phi_T\left(\sum_{n\geqq 0} a_n T^n\right) = \sum_{n\geqq 0, m\geqq 0} \partial^{(m)}(a_n)T^m T^n$$

and this is equal to $\sum_{n\geqq 0}\left(\sum_{k+l=n} \partial^{(k)}(a_l)\right)T^n$. Again ϕ_T is also a homomorphism of rings. Condition 3. is now equivalent to $\phi_{T_1+T_2} = \phi_{T_1} \circ \phi_{T_2}$, say as maps from R to $R[[T_1, T_2]]$.

(2) One has $\partial^{(n_1)} \cdots \partial^{(n_s)} = \binom{n_1 + \cdots + n_s}{n_1, \ldots, n_s} \partial^{(n_1 + \cdots + n_s)}$ with $\binom{n_1 + \cdots + n_s}{n_1, \ldots, n_s}$ equal to $\dfrac{(n_1 + \cdots + n_s)!}{n_1! \cdots n_s!}$. Write any positive integer n as $a_0 + a_1 p + \cdots + a_k p^k$ with $a_i \in \{0, 1, \ldots, p-1\}$. Then $(\partial^{(1)})^{a_0} \cdots (\partial^{(p^k)})^{a_k} = c \cdot \partial^{(n)}$, where c is some non-zero element of $\mathbb{F}_p$. Thus any iterative derivative is determined by the $\partial^{(p^k)}$ for all $k \geqq 0$. The *ring of constants* is defined as the intersection of the kernels of all $\partial^{(n)}$ with $n \geqq 1$.

(3) Let C be any field of characteristic p and $K = C((z))$. Define the iterative derivation $\{\partial_z^{(n)}\}$ by the formula $\partial_z^{(n)}\Big(\sum_m a_m z^m\Big) = \sum_m \binom{m}{n} a_m z^{m-n}$ (derived from $\dfrac{1}{n!}\left(\dfrac{d}{dz}\right)^n$ in characteristic 0). Then the field of constants is equal to C.

(4) The field $C(z)$ can be seen as a subfield of $C((z))$. The field $C(z)$ is invariant under the maps $\partial_z^{(n)}$ of (3). This induces an iterative derivation on $C(z)$, again denoted by $\{\partial_z^{(n)}\}$. In the terminology of (1), the iterative differential $\{\partial_z^{(n)}\}$ is given by the $\phi_T \colon C(z) \to C(z)[[T]]$ with the formula $\phi_T(z) = z + T$.

(5) Let a separable algebraic field extension $K \subset L$ and an iterative derivation on K be given. Then this iterative derivation extends in a unique way to one of L. This result is due to F. K. Schmidt and the proof can be given as follows:

The iterative derivation on K is equivalent to a $\phi_T \colon K \to K[[T]]$ with the additional property $\phi_{T_1+T_2} = \phi_{T_2} \circ \phi_{T_1}$. The image $\phi_T(K)$ is a coefficient field for $K[[T]]$. The map ϕ_T, considered as a homomorphism $K \to L[[T]]$, extends in a unique way to a homomorphism $\psi_T \colon L \to L[[T]]$ which is modulo (T) the identity. Indeed, the statement translates into the well known fact that the field $\phi_T(K) \subset L[[T]]$ extends in a unique way to a coefficient field for $L[[T]]$. The unicity of ψ_T implies the rule $\psi_{T_1+T_2} = \psi_{T_2} \circ \psi_{T_1}$. For any separable extension $K \subset L$ one can show that any iterative derivation on K extends to one on L. This extension is in general not unique.

Let K/k be a separable field extension of transcendence degree 1. A complete description of all iterative derivations of K/k, i.e., the iterative derivations which are trivial on k, has been given by F. K. Schmidt. The next proposition generalizes this result.

Proposition 2.2. (1) *Let* $\{\partial_K^{(n)}\}$ *be an iterative derivation on the field* K *such that* $\partial_K := \partial_K^{(1)} \neq 0$. *Define for* $s \geqq 1$ *the subfield* K_s *of* K *by* $K_s := \{a \in K \mid \partial_K^{(p^j)} a = 0$ *for* $0 \leqq j \leqq s-1\}$. *There exists an element* $z \in K$ (*depending on* s) *such that* $\{z^j \mid 0 \leqq j < p^s\}$ *is a basis of* K *over* K_s *and* $\partial_K^{(a)} z^b = \binom{b}{a} z^{b-a}$ *for all* b *and all* $a < p^s$.

(2) *Let* K *be a field of characteristic* $p > 0$ *and let a sequence of subfields* $K \supset K_1 \supset K_2 \supset \cdots$ *be given such that, for each* $s \geqq 1$, *the extension* $K \supset K_s$ *is purely inseparable of degree* p^s *and is generated by one element. Then*:

(a) *There exists an iterative derivation* $\{\partial^{(n)}\}$ *on* K *such that, for each* $s \geqq 1$, *one has* $K_s = \{a \in K \mid \partial^{(p^j)} a = 0$ *for* $0 \leqq j \leqq s-1\}$.

(b) *The collection of all iterative derivations on K having the property of* (a) *above is, in a natural way, isomorphic to the set S consisting of the elements in the projective limit $\varprojlim K/K_s$ which map to a non-zero element of K/K_1.*

(3) *Let K/k be a separable extension such that $[K : kK^p] = p$. The set of all iterative derivatives of K/k with $\partial^{(1)} \neq 0$ is, in a natural way, isomorphic to the set S of elements in the projective limit $\varprojlim K/kK^{p^n}$, which map to a non-zero element of K/kK^p.*

Proof. (1) The statement is proved by induction on s. It is given that $\partial_K \neq 0$ and $\partial_K^p = 0$. Choose an element a with $\partial_K a \neq 0$ and let $m > 1$ be minimal such that $\partial_K^m a = 0$. Then $b := \partial_K^{m-1} a \in K_1$ and $z = b^{-1}\partial_K^{m-2} a$ satisfies $\partial_K z = 1$. By induction on n one shows that for $1 \leqq n \leqq p$ the kernel of ∂_K^n is a vector space over K_1 with basis $1, z, \dots, z^{n-1}$. This proves the case $s = 1$. We remark further that the kernel of ∂_K^{p-1} coincides with the image of ∂_K.

The case $s = 2$. Since ∂_K commutes with $\partial_K^{(p)}$ one has that $\partial_K^{(p)}$ maps K_1 into itself. Using the formulas $\partial_K^{(p)}(f^p) = (\partial_K f)^p$ and $(\partial_K^{(p)})^p = 0$ one finds that $z^p \in K_1$, $\partial_K^{(p)} z^p = 1$ and that $1, z^p, z^{2p}, \dots, z^{(p-1)p}$ is a basis of K_1 over K_2. Now we try to find an $x \in K_1$ such that $\partial_K^{(p)}(z - x) = 0$. This amounts to showing that $\partial_K^{(p)} z$ lies in the image of $\partial_K^{(p)}$ on K_1. As before, this image is equal to the kernel of $(\partial_K^{(p)})^{p-1}$ on K_1. The element $\partial_K^{(p)} z$ lies in this kernel since $(\partial_K^{(p)})^p = 0$. After replacing z by $z - x$ we have proved the case $s = 2$. The induction step is proved in the same way.

(2) part (a) An easy calculation shows that the condition on the sequence of fields $K \supset K_1 \supset \cdots$ implies that any field L with $K \supset L \supset K_s$ is equal to either K or some K_j with $1 \leqq j \leqq s$. Take any $z \in K \backslash K_1$. Then $K = K_s(z)$ holds for every $s \geqq 1$. One defines now an iterative derivation, called $\{\partial_z^{(n)}\}$, by the formulas:

For any $s \geqq 1$ the ∂_z^n, with $n < p^s$, are K_s-linear and $\partial_z^{(n)} z^m = \binom{m}{n} z^{m-n}$ for all m and all $n < p^s$.

It is easily verified that the $\{\partial_z^{(n)}\}$ are well defined, form an iterative derivation of K and that $K_s = \{a \in K \mid \partial_z^{(p^j)} a = 0 \text{ for } 0 \leqq j \leqq s-1\}$ holds for every $s \geqq 1$. This proves part (a) of (2).

(2) part (b) For any $x \in K \backslash K_1$ the iterative derivation $\{\partial_x^{(n)}\}$ has been defined in the proof of (2) part (a). One observes further that for elements $x, y \in K \backslash K_1$ the following statements are equivalent:

(i) $x - y \in K_s$.

(ii) $\partial_x^{(n)} = \partial_y^{(n)}$ for all $n < p^s$.

Let now ξ be an element of S, represented by a sequence of elements $x_1, x_2, x_3, \dots$ in K such that $x_1 \notin K_1$ and $x_s - x_{s+1} \in K_s$ for all $s \geqq 1$. One defines an iterative derivation $\{\partial_\xi^{(n)}\}$ on K by the formula:

For every $s \geqq 1$ and every $n < p^s$ the map $\partial_{\xi}^{(n)}$ is equal to $\partial_{x_s}^{(n)}$. From (1) it follows that every iterative derivation $\{\partial^{(n)}\}$ on K such that $K_s = \{a \in K \mid \partial^{(p^j)}a = 0 \text{ for } 0 \leqq j \leqq s-1\}$ holds for all $s \geqq 1$, is equal to some $\{\partial_{\xi}^{(n)}\}$. The unicity of ξ follows from the equivalence of the above properties (i) and (ii).

(3) is the special case of (2) part (b) corresponding to the choice $K_s = kK^{p^s}$ for all $s \geqq 1$. □

The structure of the iterative derivations for a given field is rather complicated. In particular, there seems no possibility to construct a universal iterative derivation. For a field like $K = k\big((x)\big)$ with $k = k^p$, one can give a more or less explicit description of the projective limit $\varprojlim K/K_s$. Consider the collection $\mathcal{Q}$ of all formal expressions $\eta = \sum_{n=-\infty}^{\infty} a_n x^n$ satisfying the conditions:

(i) All $a_n \in k$ and $a_0 = 0$.

(ii) For every $s \geqq 1$ the collection $\{n \in \mathbb{Z} \mid a_n \neq 0, p^s \nmid n\}$ has a minimal element.

Every η as above, induces for every $s \geqq 1$ an element of K/K_s, obtained by deleting the terms $a_n x^n$ with $p^s | n$. In this way, η maps to an element of the above projective limit. This leads to a bijection $\mathcal{Q} \to \varprojlim K/K_s$.

2.2. Iterative differential modules. In the sequel we will work with a fixed field K with a non trivial iterative derivation, denoted by $f \mapsto f^{(n)}$ for all $n \geqq 0$ (or sometimes $f \mapsto \partial_K^{(n)} f$). We will assume that the ordinary derivation $f \mapsto f^{(1)}$ is not the zero map. The field of constants of K will be denoted by C. An *iterative differential module* (or ID-module for short) M is a finite dimensional vector space over K equipped with a set of additive maps $\partial^{(*)}: M \to M$ satisfying the rules:

(1) $\partial^{(0)}$ is the identity.

(2) $\partial^{(n)}(fm) = \sum_{a,b \geqq 0, a+b=n} f^{(a)} \partial^{(b)}(m)$.

(3) $\partial^{(n)}\partial^{(m)} = \binom{n+m}{n} \partial^{(n+m)}$.

After a choice of a basis of M over K one translates this into a set of matrix equations. The solution space of an iterative differential module can be defined as the set $\{m \in M \mid \partial^{(n)}(m) = 0 \text{ for all } n > 0\}$. One can show that the solution space is a vector space over C of dimension less than or equal to the dimension of M over K. In case these dimensions are equal, the iterative module is said to be *trivial*. Thus the iterative differential module is trivial if and only if there is a basis $e_1, \ldots, e_s$ of M over K such that $\partial^{(n)} e_i = 0$ for all $n > 0$ and all i.

One can define iterative differential modules in another way. Consider the skew ring of operators $\mathscr{D} := K[\partial^{(n)}, n \geqq 0]$ defined by the relations:

$$\partial^{(0)} = 1,$$

$$\partial^{(n)}\partial^{(m)} = \binom{n+m}{n}\partial^{(n+m)}$$

and

$$\partial^{(n)}f = \sum_{a,b\geqq 0,\, a+b=n} f^{(a)}\partial^{(b)} \quad \text{with } f \in K.$$

Then a left $\mathscr{D}$-module of finite dimension over K is the same thing as an iterative differential module over K.

The category of all iterative differential modules over K. By ID_K one denotes the category whose objects are the iterative differential modules over K. A morphism f in this category is a K-linear map $f\colon M_1 \to M_2$ between two ID-modules such that $\partial^{(n)} \circ f = f \circ \partial^{(n)}$ for all n. One sees that $\mathrm{Hom}(M_1, M_2)$ is a vector space over C. Kernels, cokernels, direct sums are present and ID_K is an abelian category. Further constructions of linear algebra are:

Internal Hom, $\underline{\mathrm{Hom}}(M_1, M_2)$ which consists of all K-linear maps $l : M_1 \to M_2$. The ID-module structure on $\underline{\mathrm{Hom}}(M_1, M_2)$ is given by the formula

$$\partial^{(n)}(l) = \sum_{a,b\geqq 0,\, a+b=n} (-1)^a \partial^{(a)} \circ l \circ \partial^{(b)}.$$

(The opposite sign can also be chosen.)

Tensor product, $M_1 \otimes M_2$, defined as $M_1 \otimes_K M_2$ with the ID-module structure given by the formula $\partial^{(n)}(m_1 \otimes m_2) = \sum_{a,b\geqq 0,\, a+b=n} (\partial^{(a)}m_1) \otimes (\partial^{(b)}m_2)$.

Symmetric powers, exterior powers et cetera are defined as usual.

The category is a C-linear tensor category in the terminology of [D-M]. For the case that the field of constants C is algebraically closed, it can be derived from Deligne's work (see [D]) on Tannakian categories that ID_K is a neutral Tannakian category. In other words, ID_K is as C-linear tensor category isomorphic to the category Repr_G of the finite dimensional representations of a certain affine group scheme over C. In particular, fix an ID-module M and consider the full subcategory $\{\{M\}\}$ of ID_K generated by all tensor products of M and its dual M^*. Then $\{\{M\}\}$ is also a neutral Tannakian category and isomorphic to Repr_G for a certain linear algebraic group G over C. This group will be called the Galois group of the module M. In the sequel we will treat ID-modules with the more down to earth method of Picard-Vessiot rings.

3. Picard-Vessiot theory

In the sequel we will suppose that the field K of characteristic $p > 0$ is equipped with an iterative derivation such that its field of constants C is algebraically closed and different from K. We will follow the presentation of the classical Picard-Vessiot theory given in [P2] and provide the few adaptions which are needed in the present situation.

Definitions 3.1. An *iterative differential ring* R (or ID-ring for short) over K is a (commutative) K-algebra with 1, having a set of additive maps $\partial^{(n)}: R \to R$, extending the iterative derivation on K, such that:

(1) $\partial^{(0)}$ is the identity.

(2) $\partial^{(n)}(fg) = \sum\limits_{a,b \geqq 0, a+b=n} \partial^{(a)}(f)\partial^{(b)}(g)$.

(3) $\partial^{(n)}\partial^{(m)} = \binom{n+m}{n}\partial^{(n+m)}$.

An *iterative differential ideal* (or ID-ideal for short) $I \subset R$ is an ideal invariant under all $\partial^{(n)}$. R is called *simple* if the only iterative differential ideal $(\neq R)$ is 0.

Lemma 3.2. (1) *A simple iterative differential ring R has no zero divisors.*

(2) *Let R be a simple iterative differential ring which is finitely generated over K. Then its field of fractions* (*equipped with the unique extension of the iterative derivation*) *has C as field of constants.*

Proof. (1) Define $\phi : R \to R[[T]]$ by $\phi(a) = \sum\limits_{n \geqq 0} \partial^{(n)}(a)T^n$. Then ϕ is a homomorphism of rings. Let $\underline{q}$ be any prime ideal of R. The map $\psi : R \xrightarrow{\phi} R[[T]] \to (R/\underline{q})[[T]]$ is again a homomorphism of rings. Let I denote the kernel of ψ. It suffices to show that $I = 0$ since $(R/\underline{q})[[T]]$ has no zero divisors. An element a belongs to I if and only if all $\partial^{(n)}(a) \in \underline{q}$. For $a \in I$ one also has $\partial^{(m)}(a) \in I$ since $\partial^{(n)}\partial^{(m)}(a) = \binom{n+m}{n}\partial^{(n+m)}(a) \in \underline{q}$. Thus I is an iterative differential ideal and is by assumption 0.

(2) Let $a \neq 0$ be an element of the field of fractions of R such that $\partial^{(n)}a = 0$ for all $n \geqq 1$. Let $I := \{b \in R \mid ba \in R\}$. Then for any $b \in I$ (and $n \geqq 1$) one has $\partial^{(n)}(ba) = \partial^{(n)}(b)a \in R$. Thus I is a non-zero iterative differential ideal and is therefore equal to R. Consequently $a \in R$. For any constant c one has that $a - c$ is either invertible or equal to 0. As in the paper [P2] it follows that a lies in the field of constants of K. □

Definition 3.3. Let M be an iterative differential module over K. Let $e_1, \ldots, e_s$ be a basis of M over K. Let $A_n = (A_n(i,j))$ denote the matrix of the map $\partial_M^{(n)}$ with respect to this basis. Thus $\partial_M^{(n)} e_i = \sum\limits_j A_n(j,i)e_j$ for all i, j, n. One considers the vector $y_1e_1 + \cdots + y_se_s \in M$. Let $\partial_M^{(n)}(y_1e_1 + \cdots + y_se_s) = w_1e_1 + \cdots + w_se_s$ and write $y, w \in K^s$ for the column vectors with entries y_i and w_i. Then

$$w = \partial^{(n)}y + A_1\partial^{(n-1)}y + \cdots + A_{n-1}\partial^{(1)}y + A_ny,$$

where each $\partial^{(m)}$ operates coordinatewise on column vectors. The set of equations $\partial_M^{(n)}(y_1e_1 + \cdots + y_se_s) = 0$, $n \geqq 1$ translates into a set of equations for the column vector y which can be rewritten as a sequence of matrix equations $\partial^{(n)}y = B_ny$, $n \geqq 1$ for certain matrices B_n.

A *fundamental matrix* F (with coefficients is some iterative differential ring over K) is an invertible matrix satisfying $\partial^{(n)}F = B_nF$ for all $n \geqq 0$. A *Picard-Vessiot ring* for the above iterative differential module M is an iterative differential ring over K such that:

(1) R is simple.

(2) Over R there exists a fundamental matrix for M.

(3) R is generated over K by the coefficients of a fundamental matrix for M.

A *Picard-Vessiot field* for M is the field of fractions of a Picard-Vessiot ring for M.

Lemma 3.4. *For any iterative differential module there exists a Picard-Vessiot ring. This ring is unique up to a* (*non canonical*) *isomorphism of K-algebras respecting the iterative derivations.*

Proof. After choosing a basis, the iterative differential module translates into a set of matrix equations $\partial^{(n)}y = B_ny$, $n \geqq 0$. The matrices B_n have coefficients in K and satisfy a set of relations, namely the translations of the defining properties of ID-module. One introduces a matrix of indeterminates $(X_{i,j})$ with determinant d and defines the iterative differential ring $R_0 := K\left[\{X_{i,j}\}, \frac{1}{d}\right]$. The iterative derivation on R_0 extends the one of K and is given by $(\partial^{(n)}X_{i,j}) = B_n \cdot (X_{i,j})$ for all $n \geqq 0$. Let $I \subset R_0$ be an ideal which is maximal among the set of all iterative ideals of R_0. Then $R := R_0/I$ is clearly a Picard-Vessiot ring for the given ID-module. For the remaining part of the proof one can copy the proofs of [P2]. □

The *differential Galois group $\mathcal{G}$ of an iterative differential module M* is the group of the differential automorphisms of R/K, where R is a Picard-Vessiot ring for M. Let $V \subset R \otimes M$ denote the solution space of the ID-module M, i.e., V consists of the elements $v \in R \otimes M$ with $\partial^{(n)}v = 0$ for all $n \geqq 1$. Then $\mathcal{G}$ acts faithfully on V and $\mathcal{G}$ can be identified with a *reduced* algebraic subgroup of $\mathrm{GL}(V)$.

Along the lines of [P2], one can show that $Z = \mathrm{Spec}(R)$ is a $\mathcal{G}$-torsor over the field K. The usual Galois correspondence for Picard-Vessiot fields is a consequence of this fact. Especially one has the following results (compare [P2], proposition 3.6 and 3.7 for the classical case):

Theorem 3.5. *Let M be an iterative differential module over K. Let L/K be the corresponding Picard-Vessiot field and $\mathcal{G}$ its differential Galois group. There is a Galois correspondence, given by $\mathcal{H} \mapsto L^{\mathcal{H}}$, between the reduced algebraic subgroups of $\mathcal{G}$ and the intermediate iterative differential fields of L/K.*

4. Examples

4.1. Finite Galois extensions of K. Let $L \supset K$ be a finite Galois extension of K of degree $m > 1$. The iterative derivation of K extends in a unique way to one on L which will be denoted by $\{\partial_L^{(n)}\}$. View now $M := L$ as a vector space over K equipped with the $\{\partial_L^{(n)}\}$. This is an ID-module. The field of constants of L with respect to the iterative differentiation is also C. Indeed, take $x \in L$ with $\partial_L^{(n)} x = 0$ for all $n \geqq 1$. Let $x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0$ be its minimal equation over K. This equation is separable. Let $\tilde{K}$ denote the splitting field of the above polynomial over K. Then, since the Galois action of $\tilde{K}/K$ commutes with the iterative derivation on $\tilde{K}$ we have that all the roots of the polynomial are constants. Therefore all the a_i are constants. Since C is algebraically closed, one has that $x \in C$. We conclude that M is not a trivial module since the solution space of M has dimension 1 over C. The ID-module $L \otimes M$ is trivial, since $L \otimes_K L$ is isomorphic with the direct sum of m copies of L. Thus it contains as set of constants the direct sum of m copies of C. It follows that L contains a Picard-Vessiot ring (actually a field). The Galois group $\mathrm{Gal}(L/K)$ acts faithfully on the solution space of $L \otimes M$. We conclude that L is the Picard-Vessiot field of the ID-module M and that $\mathrm{Gal}(L/K)$ is its differential Galois group.

4.2. Iterative differential modules of dimension one. The one-dimensional ID-module $M = Ke_0$ is equipped with a set of maps $\partial^{(n)}$. We first note that $(\partial^{(1)})^p$ is 0 on M. Thus M, as ordinary differential module over K, has p-curvature 0. This implies that M has a basis e_1 such that $\partial^{(1)} e_1 = 0$. The kernel of $\partial^{(1)}$ on M is clearly $K_1 e_1$ where $K_1 = \{a \in K \mid \partial^{(1)}(a) = 0\}$. The operator $\partial^{(p)}$ commutes with $\partial^{(1)}$. It follows that $K_1 e_1$ is invariant under $\partial^{(p)}$. The restriction of the $\{\partial^{(pn)}\}$ to $K_1 e_1$ defines an ID-module over the field K_1 with as iterative derivation the one induced by K (and a shift of the indices if one wants to be precise). The same argument shows that $K_1 e_1 = K_1 e_2$ for a certain element e_2 such that $\partial^{(p)} e_2 = 0$. One can continue this process and produce a sequence of elements $e_0, e_1, e_2, e_3, \ldots$ such that $Ke_0 = Ke_1, K_1 e_1 = K_1 e_2, K_2 e_2 = K_2 e_3, \ldots$. The fields K_n are defined by: $K_0 = K$, K_1 is the kernel of $\partial^{(1)}$ on $K, \ldots, K_n = \{a \in K \mid \partial^{(m)} a = 0$ for all $0 < m < p^n\}$. We note that K_n is also equal to $\{a \in K \mid \partial^{(p^j)} a = 0$ for all $0 \leqq j < n\}$. Moreover $\partial^{(m)} e_n = 0$ for all $0 < m < p^n$. In other words M is a trivial iterative differential module for every "truncation". If one could find a "limit" f for the sequence e_n then $Ke = Kf$ and $\partial^{(n)} f = 0$ for all $n > 0$. The existence of a limit can be formulated with projective limits. Namely the above sequence $\{e_n\}$ produces w.r.t. a fixed basis $e = e_0$ of the 1-dimensional module an element of the projective limit $\varprojlim K^*/K_n^*$. The set of equivalence classes of 1-dimensional ID-modules is then seen to be the cokernel $\mathrm{Isom}_{K,1}$ of the canonical map $K^* \to \varprojlim K^*/(K_n)^*$. This cokernel has a group structure. The group structure coincides with the tensor product of (isomorphy classes of) the 1-dimensional ID-modules.

Lemma 4.1. *For the field $K := C((z))$ (with the standard iterative derivation) the group $\mathrm{Isom}_{K,1}$ is isomorphic to $\mathbb{Z}_p/\mathbb{Z}$.*

Proof. The group K^* can be decomposed as $C^* \times z^{\mathbb{Z}} \times U$ with $U := 1 + zC[[z]]$. The field K_n is equal to $C((x^{p^n}))$ and thus $K_n^* = C^* \times z^{p^n \mathbb{Z}} \times U^{p^n}$. The projective limit of K^*/K_n^* is thus isomorphic to $\mathbb{Z}_p \times \varprojlim U/U^{p^n}$. It is easily seen that the canonical map $U \to \varprojlim U/U^{p^n}$ is an isomorphism. This proves the statement. □

***Explicit examples for lemma* 4.1.** For any p-adic integer α, i.e., $\alpha \in \mathbb{Z}_p$, the element $\binom{\alpha}{n} := \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$ belongs to $\mathbb{Z}_p$. Its reduction modulo p in $\mathbb{F}_p$ will be denoted by $\overline{\binom{\alpha}{n}}$. One defines the ID-module Ke by the formulas $\partial^{(n)}e = \overline{\binom{\alpha}{n}} z^{-n}e$. It is easily verified that this is indeed an ID-module. The image of this module in the group $\mathrm{Isom}_{K,1}$ can be identified with the image of α in $\mathrm{Isom}_{K,1}$. There are two cases:

In the first case α is a rational number with denominator n (not divisible by p). Then the field extension $C\big((z^{1/n})\big) \supset K$ is the Picard-Vessiot field and the Galois group is cyclic of order n.

In the second case α is not rational. Then the Picard-Vessiot field is the transcendental extension $K(y)$ with extension of the iterative derivation given by $y^{(n)} = \overline{\binom{\alpha}{n}} z^{-n}y$. Its differential Galois group is $\mathbb{G}_{m,C}$ (i.e., the multiplicative group over C).

In general, a one-dimensional ID-module M over any K translates, after a choice of a basis of M, into a set of equations $\partial^{(n)}y = a_n y$. The differential Galois group is a reduced subgroup of $\mathbb{G}_{m,C}$. This group is cyclic of order m (and $p \nmid m$) if and only if $m \geqq 1$ is minimal such that the set of equations $\partial^{(n)}f = ma_n f$ has a non-zero solution g in K. Its Picard-Vessiot field is then $K(\sqrt[m]{g})$. In the opposite case, the Picard-Vessiot field is the transcendental extension $K(y)$ with iterative differentiation given by $\partial^{(n)}y = a_n y$ for all $n \geqq 0$.

Proposition 4.2. *C denotes an algebraically closed field of characteristic $p > 0$. Let X denote a connected, smooth, projective curve over X. The Jacobian variety of X is denoted by J. Let K denote its function field and provide K with a non-trivial iterative derivation. There is a natural exact sequence*

$$0 \to T_p(J) \to \varprojlim K^*/(K^{p^n})^* \to \mathrm{Div}^0(X, \mathbb{Z}_p) \to 0,$$

where $T_p(J)$ is the p-adic Tate-module of J and $\mathrm{Div}^0(X, \mathbb{Z}_p)$ *denotes the group of functions $f : X \to \mathbb{Z}_p$ having the two properties*:

(a) *For every integer $n \geqq 1$, the support of f modulo (p^n) is finite.*

(b) $\sum_{x \in X} f(x) = 0.$

Let $\mathrm{Isom}_{K,1}$ *denote the group of the isomorphy classes of the* 1*-dimensional* ID*-modules over K. There is a natural exact sequence*

$$0 \to T_p(J) \to \mathrm{Isom}_{K,1} \to \mathrm{Div}^0(X, \mathbb{Z}_p)/\mathrm{Prin}(X) \to 0,$$

where $\mathrm{Prin}(X)$ *is the group of the principal divisors on X.*

Proof. For $X = \mathbb{P}^1_C$ we have an obvious isomorphism $K^*/C^* \to \mathrm{Div}^0(X)$ (i.e., the group of the ordinary divisors on X with degree 0) and isomorphisms $K^*/(K^{p^n})^* \to \mathrm{Div}^0(X)/p^n\,\mathrm{Div}^0(X)$. The projective limit of the right hand factors is easily seen to be the group $\mathrm{Div}^0(X, \mathbb{Z}_p)$ as defined above. Thus the proposition is correct in this special case.

Suppose now that the genus of X is $\geqq 1$. Then there is an exact sequence $0 \to K^*/C^* \to \mathrm{Div}^0(X) \to J \to 0$, where we have identified J with its group of points $J(C)$. The multiplication by p^n between two copies of the above sequence and the exactness of $0 \to J[p^n] \to J \overset{p^n\cdot}{\to} J \to 0$ induce the exact sequence

$$0 \to J[p^n] \to K^*/(K^{p^n})^* \to \mathrm{Div}^0(X)/p^n\,\mathrm{Div}^0(X) \to 0.$$

Since the projective system $\{J[p^n]\}$ is a system of finite groups, the Mittag-Leffler condition is satisfied and we conclude that the projective limit of the above sequences is again exact. This implies the first part of the proposition. For the second part we observe that the canonical map of K^*/C^* to the projective limit of the $K^*/(K^{p^n})^*$, combined with the map from this projective limit to $\mathrm{Div}^0(X, \mathbb{Z}_p)$ is injective. This implies the exactness of the second sequence. □

Let C, X, K be as in the proposition 4.2. For any point $x \in X$ we denote the completion of K with respect to the valuation corresponding to x by K_x. The field K_x is isomorphic to $C((t))$, where t is some local parameter at x. The field K_x inherites an iterative derivation from K. The natural map $\mathrm{Isom}_{K,1} \to \mathrm{Isom}_{K_x,1}$, derived from $M \mapsto K_x \otimes M$, has the form

$$\mathrm{Isom}_{K,1} \to \mathrm{Div}^0(X, \mathbb{Z}_p)/\mathrm{Prin}(X) \to \mathbb{Z}_p/\mathbb{Z} \cong \mathrm{Isom}_{K_x,1},$$

where the last arrow is induced by $f \in \mathrm{Div}^0(X, \mathbb{Z}_p) \mapsto f(x) \in \mathbb{Z}_p$.

We note that for any X, even for $\mathbb{P}^1_C$, there are non trivial elements $\xi \in \mathrm{Isom}_{K,1}$ such that the image of ξ in $\mathrm{Isom}_{K_x,1}$ is zero for every $x \in X$. An *explicit example* of this phenomenon is the following:

$X = \mathbb{P}^1_C$ and s_n is a sequence of distinct points in $\mathbb{A}^1_C$. The "divisor" $D = \sum\limits_{n \geqq 0} (p-1)p^n[s_n] + [\infty]$ lies in $\mathrm{Div}^0(X, \mathbb{Z}_p)$. No positive multiple of D is in $\mathrm{Prin}(X)$ and its image in $\mathrm{Isom}_{K_x,1}$ is 0 for all x. A calculation shows that the iterative differential equation corresponding to D is $\partial^{(p^n)} y = (z - s_n)^{-p^n} y$ for all $n \geqq 0$. The differential Galois group of this ID-module is $\mathbb{G}_{m,C}$. For every $x \in \mathbb{P}^1_C$ there is a non trivial solution in K_x. An explicit way to see this is to consider a "symbolic" solution $F = \prod\limits_{n \geqq 0} (z - s_n)^{p^n}$ and to give this expression a meaning in every K_x.

This is in contrast with the situation of complex linear differential equations on $\mathbb{P}^1_C$. In order to stay closer to the complex analytic theory of ordinary differential equations we will in section 7 introduce an adequate notion of "regular at a point $x \in X$" for ID-modules over K.

4.3. Inhomogeneous iterative equations of order one. We consider here ID-modules M of dimension two, which admit a submodule N of dimension 1 such that both N and M/N are trivial. In other words we consider inhomogeneous equations of the form $\partial^{(n)} y = a_n$ with all $a_n \in K$. (The sequence of elements a_n satisfies certain relations corresponding to the definition of ID-module.) The differential Galois group is clearly an algebraic subgroup of the additive group $\mathbb{G}_{a,C}$ over C. As in the last subsection one finds that these equations are classified by the cokernel of the natural map $K \to \varprojlim K/K^{p^n}$. For the field $K = C((z))$ one can make this projective limit somewhat explicit. The elements of the projective limit can be described as the formal series $f = \sum_{n \in \mathbb{Z}} c_n z^n$ having the property that for all $k \geqq 0$ there is an integer N_k such that the support of f is contained in $p^k\mathbb{Z} \cup \{n \in \mathbb{Z} \mid n \geqq N_k\}$. A typical example is $f = \sum_{k \geqq 0} a_k z^{-p^k}$. The corresponding iterative equation is $\partial^{(p^n)} y = \sum_{k=0}^{n} -a_k z^{-p^k - p^n}$ for all $n \geqq 0$. The differential Galois group $\mathcal{G} \subset \mathbb{G}_{a,C}$ of this iterative equation depends on the coefficients a_k (see lemma 5.2).

Let C be an algebraically closed field of characteristic $p > 0$, X an irreducible smooth, projective curve over C with function field K. The field K is provided with an iterative derivation with field of constants C. In this situation, too, one can make the projective limit $\varprojlim K/K^{p^n}$ somewhat explicit. Let O, M and H denote the sheaves of the regular functions, the rational functions and the principal parts on X. The exact sequence

$$0 \to K/C \to H(X) \to H^1(X, O) \to 0$$

induces exact sequences

$$0 \to \ker(\mathrm{Frob}^n, H^1(X, O)) \to K/K^{p^n}$$
$$\to H(X)/H(X)^{p^n} \to \operatorname{coker}(\mathrm{Frob}^n, H^1(X, O)) \to 0.$$

Let $H^1(X, O)_0$ denote the generalized eigenspace for the eigenvalue 0 and the Frobenius action Frob on $H^1(X, O)$. Then one finds an exact sequence

$$0 \to H^1(X, O)_0 \to \varprojlim K/K^{p^n} \to \varprojlim H(X)/H(X)^{p^n} \to H^1(X, O)_0 \to 0.$$

As in the last subsection, there are ID-equations (of the type considered here) which are trivial at each point $x \in X$ and are "globally" non trivial. A *typical example* is given by $X = \mathbb{P}^1_C$, a sequence s_n of distinct points in $\mathbb{A}^1_C$ and $\sum_{n \geqq 0} (z - s_n)^{-p^n}$ seen as element of $\varprojlim H(X)/H(X)^{p^n}$. The corresponding iterative differential equation is given by the formulas:

$$\partial^{(p^n)} y = \sum_{k=0}^{n} -(z - s_k)^{-p^k - p^n} \quad \text{for all } n \geqq 0.$$

The differential Galois group over K is $\mathbb{G}_{a,C}$ and the equation has a solution in K_x for every $x \in X$.

5. Iterative differential modules and projective systems

As before K denotes a field equipped with an iterative derivation and its field of constants C is supposed to be algebraically closed of characteristic $p > 0$. We will use again the notation $K_0 = K$ and for $n \geqq 1$ one defines $K_n = \{a \in K \mid \partial^{(j)} a = 0$ for all $0 < j < p^n\}$. Let M be an ID-module over K. The structure of M is determined by the maps $\partial_M^{(p^n)}: M \to M$ for $n \geqq 0$. The p^{th} power of $\partial_M^{(1)}$ is the zero map. Consider the ordinary differential module (M, ∂_0) over the differential field K with derivation $\partial^{(1)}$, given by $\partial_0 = \partial_M^{(1)}$. Define the K_1 vector space M_1 by $M_1 = \{m \in M \mid \partial_0 m = 0\}$. Since the p-curvature is 0, the canonical map $K \otimes_{K_1} M_1 \to M$ is an isomorphism. Now consider the ordinary differential module (M_1, ∂_1) with $\partial_1 = \partial_M^{(p)}$ restricted to M_1, over the differential field K_1 with derivation $\partial^{(p)}$. Again the p-curvature of this differential module is zero. Put $M_2 := \{m \in M_1 \mid \partial_1 m = 0\}$. Then, as before, the canonical map $K_1 \otimes_{K_2} M_2 \to M_1$ is an isomorphism. More generally, define for $n \geqq 1$ the space $M_n = \{m \in M \mid \partial_M^{(p^l)} m = 0$ for all $l < n\}$ and $M_0 := M$. Then M_n is a vector space over K_n and the canonical map $K_n \otimes_{K_{n+1}} M_{n+1} \to M_n$ is an isomorphism. We will call $\{M_*\}$, as above, the *projective system* of the iterative differential module.

Conversely, let a finite dimensional K-vector space M be given and a collection of subsets $M = M_0 \supset M_1 \supset M_2 \supset M_3 \supset \cdots$ such that:

(a) Each M_n is a vector space over K_n.

(b) The natural maps $K_n \otimes_{K_{n+1}} M_{n+1} \to M_n$ are isomorphisms.

Then this defines a unique ID-module structure $\{\partial_M^{(l)}\}$ on M by requiring that $\partial_M^{(l)}$ is the zero map on M_n if $l < p^n$. Indeed, one defines $\partial_M^{(l)}$ by considering some n with $l < p^n$ and a basis $e_1, \dots, e_d$ of M_n over K_n. Any element $m \in M$ can uniquely be written as $\sum_{i=1}^{d} f_i e_i$ with all $f_i \in K$. One defines $\partial_M^{(l)} \sum_{i=1}^{d} f_i e_i := \sum_{i=1}^{d} (\partial^{(l)} f_i) e_i$. A straightforward verification shows that the definition of $\partial_M^{(l)}$ does not depend on the choices made and that $\{\partial_M^{(l)}\}$ is an iterative differential on M.

In general, we define a *projective system* $\{N_*, \phi_*\}$ *over* K to be a sequence of spaces and maps

$$N_0 \overset{\phi_0}{\leftarrow} N_1 \overset{\phi_1}{\leftarrow} N_2 \overset{\phi_2}{\leftarrow} N_3 \leftarrow \cdots$$

having the properties:

(a) Each N_n is a vector space over K_n of finite dimension and

(b) the maps ϕ_n are K_{n+1}-linear and the canonical K_n-linear maps $K_n \otimes_{K_{n+1}} N_{n+1} \to N_n$ are isomorphisms for $n \geqq 0$.

One associates to a projective system over K, the iterative differential module M given by $M = N_0$ and the sequence of subsets $M_n := \phi_0 \circ \cdots \circ \phi_{n-1}(N_n)$ of M. Clearly M_n is a vector space over K_n and the canonical maps $K_n \otimes_{K_{n+1}} M_{n+1} \to M_n$ are isomorphisms. As above, this defines a unique structure of iterative differential module on M.

A morphism $\alpha : \{N_*, \phi_*\} \to \{M_*, \psi_*\}$ between two projective systems over K is a sequence of K_n-linear maps $\alpha_n : N_n \to M_n$, $n \geqq 0$ such that $\alpha_n \circ \phi_n = \psi_n \circ \alpha_{n+1}$ for all $n \geqq 0$. The collection of all homomorphisms between two projective systems forms a vector space over C. Further one sees that one can perform on projective systems "all operations of linear algebra", including tensor products. One concludes the following.

Proposition 5.1. *The Tannakian categories of the iterative differential modules over K and the projective systems over K are equivalent.*

We omit the obvious proof of this proposition. In order to make a projective system $\{N_*, \phi_*\}$ over K more concrete we choose a C-vector space V of dimension d and identify each N_n with $K_n \otimes_C V$. The maps ϕ_n are now elements in $\mathrm{GL}(K_n \otimes V)$. The iterative differential $\{\partial_M^{(l)}\}$ on $M = N_0 = K \otimes V$ can explicitly be derived from the data $\{\phi_n\}$.

The K_{n+1}-linear map $\phi_0 \circ \cdots \circ \phi_n \colon N_{n+1} \to N_0 = M$ is extended to a K-linear isomorphism $K \otimes N_{n+1} \to M$, which we will give temporarely the name ψ. By definition $\partial_M^{(m)}$ is zero on $\psi(N_{n+1})$ for $m \leqq p^n$. One provides $K \otimes N_{n+1} = K \otimes_C V$ with the trivial structure of ID-module $\{\partial_V^{(m)}\}$ given by $\partial_V^{(m)} v = 0$ for all $v \in V$ and $m \geqq 1$. Then by construction $\partial_M^{(m)} \psi = \psi \partial_V^{(m)}$ holds for all $m \leqq p^n$. Thus $\partial_M^{(m)} = \psi \partial_V^{(m)} \psi^{-1}$ holds for $m \leqq p^n$. Now we fix a basis $e_1, \ldots, e_s$ of V over C. Then this is also a basis of $M = K \otimes_C V$ over K. As in the definition 3.3, A_n for $n \geqq 0$ denotes the matrix of $\partial_M^{(n)}$ with respect to this basis. On all of the spaces $N_m = K_m \otimes V$ we have then also fixed a basis, namely $1 \otimes e_1, \ldots, 1 \otimes e_s$. For any linear map τ between vector spaces with fixed bases, we write $[\tau]$ for the corresponding matrix. Moreover $\partial_V^{(m)} B$ for a matrix B, will mean the matrix obtained by applying $\partial^{(m)}$ to all its entries. In this way one obtains the formula $A_m = [\psi] \partial_V^{(m)} [\psi]^{-1}$ for $m \leqq p^n$. The extension of any ϕ_n to a K-linear isomorphism $K \otimes N_{n+1} \to K \otimes N_n$ will also be denoted by ϕ_n. The formula for the matrix A_m can now be written as $A_m = [\phi_0] \cdots [\phi_n] \partial_V^{(m)} ([\phi_0] \cdots [\phi_n])^{-1}$ if $m \leqq p^n$. We note that the above formulas show that $A_m = 0$ for all $m \geqq 1$ if all $\phi_n \in \mathrm{GL}(V)$.

Example. Take $K = C(z)$ and $\partial^{(l)} = \partial_z^{(l)}$ for all $l \geqq 0$ and consider a two dimensional space V with basis v_1, v_2. All maps are given as matrices with respect to this basis. Let ϕ_n have the matrix $\begin{pmatrix} 1 & a_n z^{p^n} \\ 0 & 1 \end{pmatrix}$ with $a_n \in C$. The matrix A_m is equal to $\begin{pmatrix} 0 & b_m \\ 0 & 0 \end{pmatrix}$ with $b_m = -\partial^{(m)}(a_0 z + \cdots + a_n z^{p^n})$ if $m \leqq p^n$. This iterative differential equation can also be written as a set of inhomogeneous scalar equations $\partial^{(p^n)} y = a_n$. The Picard-Vessiot ring R for this equation can be written as $K[Y]/I$, where $K[Y]$ is given an iterative derivation, which extends the given one on K, by putting $\partial^{(p^n)} Y = a_n$. Further I is a maximal iterative ideal in $K[Y]$. The corresponding differential Galois group consists of the automorphism $Y \mapsto Y + c$, with $c \in C$, of R such that the ideal I is invariant. In case $I = 0$, this group is the additive group $\mathbb{G}_{a,C} = C$. If $I \neq 0$, then the differential Galois group is a finite (reduced) subgroup of $\mathbb{G}_{a,C}$. We continue with this situation. The Picard-Vessiot field of the equation is then R. Consider the completion $C((z-a))$ of $K = C(z)$ with respect to the point $a \in C \subset \mathbb{P}_C^1$. In this field the set of equations has a solution, namely $f := \sum_{n \geqq 0} a_n (z-a)^{p^n}$. This implies that the field extension $K \subset R$ is only ramified above the point $\infty \in \mathbb{P}_C^1$. Furthermore $f \in C((t-a))$ must be algebraic over $C(z)$.

It can be seen that f cannot be algebraic over $C(z)$ if the sequence $\{a_n\}$ has arbitrary large "gaps", which means that there are intervals J in $\mathbb{N}$ of arbitrary length with $a_n = 0$ for $n \in J$. A more precise statement about the algebraicity of f is the following.

Lemma 5.2. $f = \sum_{n \geqq 0} a_n z^{p^n} \in \mathbb{F}_p[[z]]$ *is algebraic over* $C(z)$ *if and only if the power series* $\sum_{n \geqq 0} a_n T^n$ *represents a rational function.*

Proof. Suppose that f is algebraic over $C(z)$. Then there is a non trivial relation $h := b_0(z)f + b_1(z)f^p + \cdots + b_s(z)f^{p^s} \in C[z]$, where $b_0(z), \ldots, b_s(z) \in C[z]$. For $n \gg 0$ one has

$$0 = \partial_z^{(p^n)} h = b_0(z)a_n + b_1(z)a_{n-1} + \cdots + b_s(z)a_{n-s}.$$

We choose $c \in C$ such that not all $b_i(c)$ are 0. Then we obtain the recurrence relation

$$0 = b_0(c)a_n + b_1(c)a_{n-1} + \cdots + b_s(c)a_{n-s} \quad \text{for } n \gg 0.$$

This proves that $\sum_{n \geqq 0} a_n T^n$ is a rational function. The converse can be proved as follows. Let the symbol τ stand for the Frobenius operation $a \mapsto a^p$. Assume $\sum a_n T^n = \dfrac{P(T)}{Q(T)}$ with $P = \sum p_n T^n, Q = \sum q_n T^n \in \mathbb{F}_p[T]$. Then $Q(\tau) \sum a_n \tau^n = P(\tau)$. Apply this formula to the element $z \in \mathbb{F}_p[[z]]$. The result is $\sum q_n f^{p^n} = \sum p_n z^{p^n}$. This shows that f is algebraic. □

Proposition 5.3. *Let V be a finite dimensional vector space over C and $\mathcal{G} \subset \mathrm{GL}(V)$ a reduced algebraic subgroup. Consider a projective system $\{K_n \otimes V, \phi_n\}$ such that $\phi_n \in \mathcal{G}(K_n) \subset \mathrm{GL}(K_n \otimes V)$ for all $n \geqq 0$. Let M be the iterative differential module associated to the projective system. Then the differential Galois group of M is contained in $\mathcal{G}$.*

Proof. The proof that we will give here follows closely 9.2 of [P1]. For any linear algebraic group $\mathcal{H}$ over C, one writes $\mathrm{Repr}_{\mathcal{H}}$ for the Tannakian category of the finite dimensional representations of $\mathcal{H}$ (over the base field C). Further, Vect_C denotes the category of the finite dimensional vector spaces over C. The forgetful functor $\omega : \mathrm{Repr}_{\mathcal{H}} \to \mathrm{Vect}_C$ is the functor which associates to a representation of $\mathcal{H}$ on W the vector space W.

Let M denote the iterative differential module defined by the data of the proposition. One writes M^* for the dual of M and $M^{a,b}$ for the tensor product $M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*$ with a factors M and b factors M^*. Define $\{\{M\}\}$ to be the full subcategory of the category of all iterative differential modules over K, whose objects are the finite direct sums of subquotients of various $M^{a,b}$. Then $\{\{M\}\}$ is a neutral Tannakian category, which means that there is an equivalence $\{\{M\}\} \to \mathrm{Repr}_{\mathcal{H}}$ of Tannakian categories for some affine group scheme $\mathcal{H}$ over C. In fact $\mathcal{H}$ is the differential Galois group of M.

Suppose that we can produce a functor of Tanakian categories $\mathrm{Repr}_{\mathcal{G}} \to \{\{M\}\}$ such that the composition $\mathrm{Repr}_{\mathcal{G}} \to \{\{M\}\} \to \mathrm{Repr}_{\mathcal{H}} \xrightarrow{\omega} \mathrm{Vect}_C$ is the forgetful functor of $\mathrm{Repr}_{\mathcal{G}}$. Then it follows that $\mathcal{H}$ is an algebraic subgroup of $\mathcal{G}$.

Let $\rho : \mathcal{G} \to \mathrm{GL}(W)$ be a representation. Then for any commutative C-algebra F one has an induced homomorphism $\rho : \mathcal{G}(F) \to \mathrm{GL}(F \otimes W)$. One associates to ρ the projective system $\{K_n \otimes W, \rho(\phi_n)\}$ and the corresponding iterative differential module $M(\rho)$ over K. In this way one obtains a functor $\mathcal{F}$ from the Tannakian category $\mathrm{Repr}_{\mathcal{G}}$ to the category of all iterative differential modules over K. Let V denote the given representation of $\mathcal{G}$, i.e., $\mathcal{G}$ is given as an algebraic subgroup of $\mathrm{GL}(V)$. One writes V^* for the dual representation and $V^{a,b}$ for the tensor product $V \otimes \cdots \otimes V \otimes V^* \otimes \cdots \otimes V^*$ with a factors V and b factors V^*. Clearly $\mathcal{F} V^{a,b} = M^{a,b} \in \{\{M\}\}$. Let $\{\{V\}\}$ denote the full subcategory of

$\mathrm{Repr}_{\mathscr{G}}$ whose objects are the finite direct sums of subquotients of various $V^{a,b}$. Then $\mathscr{F}$ maps $\{\{V\}\}$ into the category $\{\{M\}\}$. It is well known that $\{\{V\}\}$ is actually equal to $\mathrm{Repr}_{\mathscr{G}}$ (see [W]). Thus we have constructed the required functor $\mathrm{Repr}_{\mathscr{G}} \to \{\{M\}\}$. □

5.1. Frobenius operators and finite groups. Proposition 5.3 will be used to construct iterative differential modules with $\mathscr{G}$ as prescribed differential Galois group. We note that for a finite group $\mathscr{G}$, the condition $\phi_n \in \mathscr{G}(K_n)$ implies $\phi_n \in \mathscr{G}(C)$. This has as consequence that the iterative differential module is trivial and the differential Galois group is $\{1\}$ (compare with the calculation following proposition 5.1). We will briefly discuss a natural way to produce iterative differential modules with finite groups as differential Galois group. In the sequel we will suppose that the field K is provided with an iterative derivation such that the field of constants C is algebraically closed and $K_n := \{a \in K \mid \partial^{(j)} a = 0$ for all $0 < j < p^n\}$ coincides with the field K^{p^n}.

Let M be a finite dimensional vector space over K. A map $F : M \to M$ will be called a *Frobenius operator* if F is additive, $F(fm) = f^p F(m)$ for all $f \in K$ and $m \in M$ and moreover the determinant of the matrix of F with respect to some basis of M over K is non-zero.

Let a Frobenius operator F on M be given. Then one defines $M_1 = F(M)$. This is a vector space over K_1. Since the determinant of F (w.r.t. some basis) is non-zero, the natural map $K \otimes_{K_1} M_1 \to M$ is an isomorphism. Define $M_n = F^n(M)$, then again $K_{n-1} \otimes M_n \to M_{n-1}$ is an isomorphism. Thus the system $\{M_n\}$ (with inclusion maps) forms a projective system and defines an ID-module structure on M.

Proposition 5.4. *F denotes a Frobenius operator on a vector space M over K of dimension d.*

(1) *The $\mathbb{F}_p$-vector space $\{m \in M \mid F(m) = m\}$ has dimension $\leqq d$.*

(2) *The smallest field extension $L \supset K$ such that the $\mathbb{F}_p$-vector space $\{m \in L \otimes M \mid F(m) = m\}$ has dimension d is a Galois extension. Let G denote its Galois group.*

(3) *Let $\mathscr{G} \subset \mathrm{GL}_{d,\mathbb{F}_p}$ be a linear algebraic group and suppose that the matrix of F with respect to some basis of M lies in $\mathscr{G}(K)$. Then G is a subgroup of $\mathscr{G}(\mathbb{F}_p)$.*

(4) *The Picard-Vessiot field and the differential Galois group of the iterative differential module M are equal to the field L and the group G of* (2).

Proof. (1) Let $e_1, \dots, e_s \in M$ be $\mathbb{F}_p$-linear independent elements with $F(e_i) = e_i$ for all i. By induction on s we will show that the elements are also K-linearly independent. Suppose that there is some relation between the e_i. Then we may assume that this relation has the form $a_1 e_1 + \cdots + a_s e_s = 0$ with $a_1, \dots, a_s \in K$ and $a_s = 1$. By induction we may suppose that $e_1, \dots, e_{s-1}$ are linearly independent and therefore the given relation is unique. Applying F to the identity yields $a_1^p e_1 + \cdots + a_s^p e_s = 0$, which is either a new relation or a relation with coefficients in $\mathbb{F}_p$.

(2) Let $e_1, \dots, e_d$ be a basis of M over K. The set of d additive polynomial equations $x_1 e_1 + \cdots + x_d e_d = x_1^p F(e_1) + \cdots + x_d^p F(e_d)$ in the d variables $x_1, \dots, x_d$ has the identity as Jacobian matrix and defines therefore a finite Galois extension L of K.

(3) Let $A \in \mathscr{G}(K)$ denote the matrix of F with respect to some basis of M over K. One considers *Lang's isogeny* $f: \mathscr{G} \to \mathscr{G}$, given by $(x_{i,j}) \mapsto (x_{i,j}^p)(x_{i,j})^{-1}$. There is an element $(b_{i,j}) \in \mathscr{G}(K^{\mathrm{sep}})$ with $f\big((b_{i,j})\big) = A^{-1}$. In fact, the field extension of K defined by this matrix is L. Indeed, the identity $A(b_{i,j}^p) = (b_{i,j})$ is a solution of the set of equations of (2). For any $\sigma \in G$, the element $(\sigma b_{i,j})$ lies in $\mathscr{G}(L)$ and also satisfies $f\big((\sigma b_{i,j})\big) = A^{-1}$. It follows that $(\sigma b_{i,j}) = C(\sigma)^{-1}(b_{i,j})$ with $C(\sigma) \in \mathscr{G}(\mathbb{F}_p)$. Thus $G \subset \mathscr{G}(\mathbb{F}_p)$.

(4) L denotes the field defined in (2). Let $e_1, \ldots, e_d$ be a basis of $L \otimes M$ satisfying $F(e_i) = e_i$ for all i. Then clearly $L \otimes M$ is a trivial ID-module and so the Picard-Vessiot field of the ID-module M is contained in L. On the other hand, let $\tilde{L}$ denote a Picard-Vessiot field for the ID-module M. Let $e_1, \ldots, e_d \in N := \tilde{L} \otimes M$ be a basis of elements with $\partial^{(n)} e_i = 0$ for all i and all $n \geqq 1$. Then $F^m(N) = \tilde{L}_m e_1 + \cdots + \tilde{L}_m e_d$ for all $m \geqq 0$. The intersection of all $F^m(N)$ is the F-invariant space $Ce_1 + \cdots + Ce_d$. Since C is algebraically closed, the space $Ce_1 + \cdots + Ce_d$ has a basis $\tilde{e}_1, \ldots, \tilde{e}_d$ with $F(\tilde{e}_i) = \tilde{e}_i$ for all i. This implies that $L \subset \tilde{L}$. □

A specialization of proposition 5.4 to the case $K = C(z)$ (with the standard iterative differentiation) produces ID-modules over K which have only one singular point, namely $z = \infty$, and have differential Galois group $\mathscr{G}(\mathbb{F}_p)$ where $\mathscr{G}$ is a semi-simple, simply connected linear algebraic group over $\mathbb{F}_p$. The corresponding Picard-Vessiot extension $L \supset K = C(z)$ is only ramified above $z = \infty$. A small variation on proposition 5.4 produces also differential Galois groups $\mathscr{G}(\mathbb{F}_q)$ with $\mathscr{G}$ as above. We refer to [S3] and [Gi] for more details on Nori's examples.

Corollary 5.5 (Nori). *Let $\mathscr{G}$ be a linear algebraic group defined over $\mathbb{F}_p$, which is semi-simple and simply connected. The field $K = C(z)$ is provided with the standard iterative differentiation. There exists an $A \in \mathscr{G}(K)$ such that the differential Galois group of the iterative differential module corresponding to A is equal to $\mathscr{G}(\mathbb{F}_p)$.*

Examples. (1) $\mathscr{G} = \mathbb{G}_m$ (the multiplicative group) and $A = (z)$ produce the $(p-1)$-cyclic group $\mathbb{G}_m(\mathbb{F}_p)$ and the equation $x = zx^p$.

(2) $\mathscr{G} = \mathbb{G}_a$ (the additive group) and $A = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$ produce the p-cyclic group $\mathbb{G}_a(\mathbb{F}_p)$ and an Artin Schreier equation $x^p - x = -z$.

(3) $\mathscr{G} = \mathscr{B}$, the Borel subgroup of SL(2) and $A = \begin{pmatrix} z^{-1} & 1 \\ 0 & z \end{pmatrix}$ leads to the equation $x^{p^2} - (z^p + z^{-1})x^p + x = 0$ with group $\mathscr{B}(\mathbb{F}_p)$. Indeed, division of this polynomial by $x(x^{p-1} - z)$ produces an irreducible factor of degree $p(p-1)$, which is the order of the group $\mathscr{B}(\mathbb{F}_p)$.

(4) $\mathscr{G} = \mathrm{SL}(2)$ and $A = \begin{pmatrix} 0 & 1 \\ -1 & z \end{pmatrix}$ produce the group $\mathrm{SL}(2, \mathbb{F}_p)$ and the equation is $f(x) = 0$ where $f(x) = x^{p^2} - zx^p + x$. By corollary 5.5, the Galois group G is a subgroup of $\mathrm{SL}(2, \mathbb{F}_p)$. Since the equation $f(x) = 0$ is irreducible over $\mathbb{F}_p(z)$, the order of G is a multiple of $p^2 - 1$. By specializing z to 2 one finds an element of order p (using Dedekind's criterion, see [M-M], I, corollary 9.3). Hence the order of G is a multiple of $p(p^2 - 1)$ and G must be $\mathbf{SL}(2, \mathbb{F}_p)$. See also [A2], Thm. 1.2 for this example.

6. Local iterative differential modules

In this section the field K is $C((z))$, where C algebraically closed of characteristic p and provided with the standard iterative differential $\{\partial_z^{(n)}\}$. Our aim is to classify the iterative differential modules over K and to determine all possible differential Galois groups.

We define the operators $\delta^{(n)} := z^n \partial^{(n)}$, as element of the skew ring $\mathscr{D} = K[\partial^{(n)}, n \geqq 0]$. This skew ring acts faithfully as a ring of operators on K. Using this action one easily verifies the following relation:

$$\delta^{(n)}\delta^{(m)} = \sum_{n+m \geqq k \geqq \max(n,m)} \frac{k!}{(k-n)!(k-m)!(n+m-k)!}\delta^{(k)}.$$

In particular the $\delta^{(n)}$ commute. In the same way one can verify that $(\delta^{(n)})^p = \delta^{(n)}$ holds for all n. The commutative algebra $R := C[\delta^{(n)}, n \geqq 0]$ is rather special. Suppose that R acts on a finite dimensional vector space V over C. Then each $\delta^{(n)}$ acts semi-simple because $(\delta^{(n)})^p = \delta^{(n)}$ holds. Moreover the $\delta^{(n)}$ commute and one concludes that there are unique distinct p-adic numbers $\alpha_1, \dots, \alpha_r$ and a decomposition $V = V_1 \oplus \cdots \oplus V_r$ such that the action of R on each vector space V_j is given by $\delta^{(n)} v = \binom{\alpha_j}{n} v$ for all $v \in V_j$. The $\alpha_1, \dots, \alpha_r \in \mathbb{Z}_p$ will be called the *eigenvalues for R on V*.

Proposition 6.1. *For $\alpha \in \mathbb{Z}_p$ one defines the one dimensional iterative differential module $E(\alpha) = Ke$ by the formulas $\partial^{(n)} e = \binom{\alpha}{n} z^{-n} e$ for all $n \geqq 0$.*

(1) *Suppose that the iterative differential module M contains a lattice Λ over $C[[z]]$, which is invariant under all $\delta^{(n)}$. Then M is isomorphic to a direct sum $E(\alpha_1) \oplus \cdots \oplus E(\alpha_d)$.*

(2) *The differential Galois group $\mathscr{G}$ of $E(\alpha_1) \oplus \cdots \oplus E(\alpha_d)$ is the subgroup of $\mathbb{G}_{m,C}^d$ consisting of the elements $t = (t_1, \dots, t_d)$ satisfying $t_1^{m_1} \cdots t_d^{m_d} = 1$ for all $(m_1, \dots, m_d) \in \mathbb{Z}^d$ such that $m_1\alpha_1 + \cdots + m_d\alpha_d \in \mathbb{Z}$.*

Proof. (1) We consider the action of the $R = C[\delta^{(n)}, n \geqq 0]$ on the vector space $\Lambda/z\Lambda$. The distinct eigenvalues are, say, $\alpha_1, \dots, \alpha_r$ and the direct sum decomposition is $\bigoplus_i \Lambda/z\Lambda(\alpha_i)$. One can lift this direct sum decomposition of $\Lambda/z\Lambda$ to a direct sum decomposition $\bigoplus \Lambda_i$ of the $C[[z]]$-module Λ. The submodule $\Lambda^* := z\Lambda_1 \oplus \Lambda_2 \oplus \cdots$ is again a lattice, invariant under all $\delta^{(n)}$. The action of $C[\delta^{(n)}, n \geqq 0]$ on the vector space $\Lambda^*/z\Lambda^*$ gives rise to new eigenvalues. They are $\alpha_1 + 1, \alpha_2, \dots, \alpha_r$. Of course it is now possible that $\alpha_1 + 1$ coincides with some α_j. This process of changing the invariant lattice can be continued until one arrives at a situation where *the distinct $\alpha_1, \dots, \alpha_r$ do not differ by an integer*. In the sequel we will assume that the α_i have this property.

Now the vector space $\Lambda/z^2\Lambda$ has a similar direct sum decomposition. The corresponding p-adic eigenvalues are the α_i and the $1 + \alpha_i$. Indeed, if e is a simultaneous eigenvector corresponding to the p-adic integer α then ze corresponds to $1 + \alpha$. From our assumption it follows that the canonical map $\Lambda/z^2\Lambda(\alpha_i) \to \Lambda/z\Lambda(\alpha_i)$ is bijective. A similar statement holds for any $\Lambda/z^d\Lambda$. Using that $C[[z]]$ and the lattice Λ are complete with respect to the (z)-topology one finds that Λ has subspaces (linear over C) $\Lambda(\alpha_i)$ which map bijectively to the $\Lambda/z\Lambda(\alpha_i)$. It follows from this that Λ is a direct sum of modules $\Lambda_i := C[[z]] \otimes_C \Lambda(\alpha_i)$. The action of $\delta^{(n)}$ on Λ_i is given by $\delta^{(n)}e = \binom{\overline{\alpha_i}}{n} e$ for all n and $e \in \Lambda(\alpha_i)$.

(2) The Picard-Vessiot ring for the module $E(\alpha_1) \oplus \cdots \oplus E(\alpha_d)$ is

$$K[X_1, X_1^{-1}, \ldots, X_d, X_d^{-1}]/I \quad \text{with } \delta^{(n)}X_j = \binom{\overline{\alpha_j}}{n} X_j \quad \text{for all } n \geqq 0,\ 1 \leqq j \leqq d,$$

and where I is a maximal iterative differential ideal. The ideal J generated by the elements

$$\{X_1^{m_1} \cdots X_d^{m_d} - z^m \,|\, \text{for } m_j \in \mathbb{Z} \text{ with } m_1\alpha_1 + \cdots + m_d\alpha_d = m \in \mathbb{Z}\}$$

is easily seen to be an iterative differential ideal. A longer, however straightforward calculation shows that J is in fact already maximal among the iterative differential ideals. Thus we may take $I = J$. The differential Galois group consists of the K-algebra automorphisms σ of $K[X_1, X_1^{-1}, \ldots, X_d, X_d^{-1}]$ having the form $\sigma X_j = c_j X_j$ with all $c_j \in C^*$ and such that the ideal $I = J$ is invariant. □

An iterative differential module M over K will be called *regular singular* if M contains a lattice which is invariant under all $\delta^{(n)}$. We will call M *regular or trivial* if M has a basis $e_1, \ldots, e_d$ over K such that $\partial^{(n)}e_j = 0$ for all j and $n \geqq 1$. We note that M is trivial if and only if the differential Galois group of M is $\{1\}$.

Corollary 6.2. (1) *M is regular singular if and only if its differential Galois group is a diagonizable group.*

(2) *The* ID*-module M is regular if and only if M contains a lattice Λ over* $C[[z]]$ *which is invariant under all $\partial^{(n)}$.*

(3) *For a regular M the lattice, invariant under all $\partial^{(n)}$, is unique.*

Proof. (1) If M is regular singular then, according to proposition 6.2, M is a direct sum of one-dimensional submodules. Thus its differential Galois group is diagonizable. On the other hand, suppose that the differential Galois group $\mathscr{G}$ of M is diagonizable. Then the action of $\mathscr{G}$ on the solution space of M has a diagonal form and therefore M is the direct sum of one-dimensional submodules. The classification of the one-dimensional ID-modules (see lemma 4.1) yields that M is regular singular.

(2) Suppose that M is regular ID-module of dimension d. Then

$$V := \{m \in M \,|\, \partial^{(n)}m = 0\}$$

is a vector space over C of dimension d, which contains a basis of M. The lattice $C[[z]] \otimes_C V \subset M$ is clearly invariant under all $\partial^{(n)}$. Now suppose that a lattice $\Lambda \subset M$ is invariant under all $\partial^{(n)}$. This lattice is also invariant under all $\delta^{(n)}$. Then M is regular singular and all the attached p-adic numbers (eigenvalues) are 0. The proof of proposition 6.2 implies that Λ contains a subspace V of dimension d over C such that all the $\partial^{(n)}$, $n \geqq 1$ are 0 on V and $C[[z]] \otimes V \to \Lambda$ is an isomorphism. This proves that M is regular.

(3) According to the proof of (2), any lattice Λ, which is invariant under all $\partial^{(n)}$, has necessarily the form $\Lambda = C[[z]] \otimes V$, where $V = \{m \in M \,|\, \partial^{(n)}m = 0 \text{ for all } n \geqq 1\}$. This proves the unicity. □

Proposition 6.3. *Every* ID-*module M over $K = C((z))$ of dimension strictly greater than* 1 *has a non trivial submodule.*

Proof. We fix a lattice Λ_0 for M. For any $n \geqq 1$ we define the subset $\Lambda_n := \{m \in \Lambda_0 \,|\, \delta^{(j)}m \in \Lambda_0 \text{ for all } j < p^{n+1}\}$. It is easily seen that Λ_n is itself a lattice. Take a basis $e_1, \ldots, e_d$ of M over K such that $\partial^{(j)}e_i = 0$ for all i and all $j < p^{n+1}$. The lattice $L_n := C[[z]]e_1 + \cdots + C[[z]]e_d$ is clearly invariant under $\partial^{(j)}$ for all $j < p^{n+1}$. The lattice $z^s L_n$ is then seen to be invariant under $\delta^{(j)}$ for all $j < p^{n+1}$. One chooses s such that $z^s L_n \subset \Lambda_0$ and $z^s L_n$ is not contained in $z\Lambda_0$. Take an element $m \in z^s L_n$ which does not lie in $z\Lambda_0$. From the invariance of $z^s L_n$ under all $\delta^{(j)}$ with $j < p^{n+1}$ it follows that $m \in \Lambda_n$. We conclude that Λ_n is not contained in $z\Lambda_0$. By standard local algebra we conclude that $\Lambda_\infty := \bigcap_{n \geqq 1} \Lambda_n$ is not zero. By definition, Λ_∞ consists of the elements $\xi \in \Lambda_0$ such that $\delta^{(j)}\xi \in \Lambda_0$ for all j. Using the formula for $\delta^{(n)}\delta^{(m)}$ one concludes that for any $\xi \in \Lambda_\infty$ and any $m \geqq 1$ also $\delta^{(m)}\xi \in \Lambda_\infty$. Therefore $K \otimes \Lambda_\infty \subset M$ is a regular singular submodule of M. By proposition 6.2, this submodule and also M contains a one-dimensional submodule. □

For any group G one denotes by $p(G)$ the subgroup generated by all elements which have order a power of the prime number p. Clearly $p(G)$ is a normal subgroup of G. Moreover $G/p(G)$ is the largest factor group of G which has no elements of order p. We refer to section 7, for more details on $p(\mathcal{G})$ and the structure of $\mathcal{G}/p(\mathcal{G})$ for reduced linear algebraic groups $\mathcal{G}$.

Corollary 6.4. (1) *Every iterative differential module over $K = C((z))$ is a multiple extension of one-dimensional iterative differential modules.*

(2) *The differential Galois group $\mathcal{G}$ of an iterative differential module over $K = C((z))$ has the properties*:

(a) *$\mathcal{G}$ is a solvable group.*

(b) *$\mathcal{G}/p(\mathcal{G})$ is commutative.*

(c) *$\mathcal{G}/\mathcal{G}^o$ is an extension of a cyclic group of order prime to p by a p-group.*

Proof. (1) is an immediate consequence of proposition 6.4.

(2) Let an iterative differential module M of dimension d over K be given. Let V denote its solution space and $\mathcal{G} \subset \mathrm{GL}(V)$ its differential Galois group. There exists a sequence $M_1 \subset M_2 \subset \cdots \subset M_d = M$ of ID-submodules such that the dimension of each M_j is j. The solution space V has therefore a sequence $V_1 \subset V_2 \subset \cdots \subset V_d = V$ of $\mathcal{G}$-invariant subspaces such that each V_j has dimension j. Therefore $\mathcal{G}$ is a subgroup of a Borel subgroup $\mathcal{B} \subset \mathrm{GL}(V)$ and $\mathcal{G}$ is solvable. Let $\mathcal{U} \subset \mathcal{B}$ denote the unipotent radical of $\mathcal{B}$. Then one easily sees that $\mathcal{G} \cap \mathcal{U}$ is equal to $p(\mathcal{G})$. Hence $\mathcal{G}/p(\mathcal{G}) \subset \mathcal{B}/\mathcal{U}$ is commutative. Finally, $\mathcal{G}/\mathcal{G}^o$ is the (ordinary) Galois group of a finite Galois extension of K. Moreover any Galois group of a finite Galois extension of K is the differential Galois group of an iterative differential module over K, according to 4.1. It is well known that a finite group G is the Galois group of a finite Galois extensions of K if and only if G is an extension of a cyclic group (of order prime to p) by a p-group. □

The second part of the corollary suggests that a linear algebraic group satisfying (a), (b) and (c) can be realized as differential Galois group over K. This will indeed be proved in theorem 6.6. We start with some useful results on Galois cohomology and cohomology for linear algebraic groups.

Observations 6.5. *The $\mathcal{G}$-torsor $Z = \mathrm{Spec}(R)$ and the groups $H^i(\mathcal{G}, R)$.*

(1) Let M be an iterative differential module over K with Picard-Vessiot ring R and differential Galois group $\mathcal{G}$.

As remarked at the end of section 3, $Z = \mathrm{Spec}(R)$ is a $\mathcal{G}$-torsor over K and determines an element of $H^1\big(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathcal{G}(K^{\mathrm{sep}})\big)$ with K^{sep} the separable algebraic closure of K. It is well known that for the groups $\mathcal{G} = \mathbb{G}_m$, $\mathbb{G}_a$ the cohomology set $H^1\big(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathcal{G}(K^{\mathrm{sep}})\big)$ is trivial, i.e., equal to $\{1\}$. According to corollary 6.4, the group $\mathcal{G}^o$ is solvable. In particular, $\mathcal{G}^o$ is a multiple extension of groups isomorphic to $\mathbb{G}_m$ or $\mathbb{G}_a$. Consequently $H^1\big(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathcal{G}^o(K^{\mathrm{sep}})\big) = \{1\}$. We conclude that for a connected differential Galois group $\mathcal{G}$ the Picard-Vessiot ring R is K-isomorphic to $K \otimes_C C[\mathcal{G}]$, where $C[\mathcal{G}]$ denotes the coordinate ring of $\mathcal{G}$. This isomorphism is $\mathcal{G}$-equivariant.

In the general case, let $\mathcal{G}^o$ denote the component of the identity of $\mathcal{G}$. The ring of invariants $\tilde{K} := R^{\mathcal{G}^o}$ is a field, and moreover a finite Galois extension of K with Galois group $\mathcal{G}/\mathcal{G}^o$. The iterative differential module $\tilde{K} \otimes M$ has again R as Picard-Vessiot ring and $\mathcal{G}^o$ as differential Galois group. Thus R is $\tilde{K}$-isomorphic to $\tilde{K} \otimes_C C[\mathcal{G}^o]$. This isomorphism is $\mathcal{G}^o$-equivariant. It is possible to make the $\mathcal{G}$-action on $\tilde{K} \otimes_C C[\mathcal{G}^o]$ explicit.

(2) Let $\mathcal{G}$ be any linear algebraic group over C. A finite dimensional $\mathcal{G}$-module is a finite dimensional vector space V over C on which $\mathcal{G}$ acts via a homomorphism of algebraic groups $\mathcal{G} \to \mathrm{GL}(V)$. A *general $\mathcal{G}$-module* is a vector space V over C with a $\mathcal{G}$-action such that V is the union of finite dimensional subspaces which are $\mathcal{G}$-modules. An example of a general $\mathcal{G}$-module is $C[\mathcal{G}]$, the ring of the regular functions on $\mathcal{G}$.

For any $\mathcal{G}$-module V one defines $V^{\mathcal{G}}$ to be the subspace of the elements invariant under $\mathcal{G}$. The functor $V \mapsto V^{\mathcal{G}}$, from $\mathcal{G}$-modules to C-vector spaces, is left-exact. The derived functors are denoted by $V \mapsto H^i(\mathcal{G}, V)$.

Let, as in (1) above, M denote an iterative differential module over K, $\mathcal{G}$ its differential Galois group and R its Picard-Vessiot ring. From the description $R \cong \tilde{K} \otimes_C C[\mathcal{G}^o]$ and the well known $\mathcal{G}^o$-structure of $C[\mathcal{G}^o]$, it follows that R is a $\mathcal{G}^o$-module. It is also a $\mathcal{G}$-module since $\mathcal{G}/\mathcal{G}^o$ is a finite group. We will prove a result which will be used for the construction of iterative differential modules over K with prescribed differential Galois group (see theorem 6.6).

Let E be any one-dimensional $\mathcal{G}$-module over C, then the cohomology groups $H^i(\mathcal{G}, R \otimes_C E)$ are 0 for $i \geqq 1$. The same holds if one replaces R by $R_s = \{a \in R \mid \partial^{(p^m)} a = 0$ for all $m < s\}$.

Proof. It is known that for any linear algebraic group $\mathcal{H}$ over C and any $\mathcal{H}$-module F, the cohomology groups $H^i(\mathcal{H}, F \otimes_C C[\mathcal{H}])$ are 0 for $i \geqq 1$ (see [J], lemma 4.7 on page 59). This implies that $H^i(\mathcal{G}^o, R \otimes E) = 0$ for $i \geqq 1$. Then

$H^i(\mathcal{G}, R \otimes E) = H^i\big(\mathcal{G}/\mathcal{G}^o, (R \otimes_C E)^{\mathcal{G}^o}\big)$. One observes that $(R \otimes_C E)^{\mathcal{G}^o}$ is a 1-dimensional vector space over $\tilde{K} = R^{\mathcal{G}^o}$ and has therefore the form $\tilde{K}e$. The action of $\sigma \in \mathcal{G}/\mathcal{G}^o$ satisfies the formula $\sigma(fe) = \sigma(f)\sigma(e)$. Then the map $\sigma \mapsto a(\sigma) \in \tilde{K}^*$, defined by $\sigma(e) = a(\sigma)e$, is a 1-cocycle. By Hilbert 90, this 1-cocycle is trivial and we may suppose that $\sigma(e) = e$ for all $\sigma \in \mathcal{G}/\mathcal{G}^o$. The additive form of Hilbert 90 implies that the $H^i(\mathcal{G}/\mathcal{G}^o, \tilde{K}e) = 0$ for $i \geqq 1$. Finally, consider $M_s := \{m \in M \mid \partial^{(p^i)}m = 0 \text{ for all } i < s\}$ as an iterative differential module over K_s. It is easily seen that its Picard-Vessiot ring is R_s and that its differential Galois group is $\mathcal{G}$.

The next theorem refines corollary 6.4. The result can be seen as an analogue of Turritin's classification of the (ordinary) differential modules over the differential field $\mathbb{C}\big((z)\big)$.

Theorem 6.6. *Let the reduced linear algebraic group $\mathcal{G}$ satisfy*:

(a) *$\mathcal{G}$ is solvable.*

(b) *$\mathcal{G}/p(\mathcal{G})$ is commutative.*

(c) *$\mathcal{G}/\mathcal{G}^o$ is an extension of a cyclic group of order prime to p by a p-group.*

Then there exists an iterative differential module over $K = C\big((z)\big)$ with differential Galois group isomorphic to $\mathcal{G}$.

Remarks. One may ask a more precise question namely, given a linear algebraic group $\mathcal{G}$ satisfying the above properties (a), (b) and (c) and a representation V of $\mathcal{G}$, i.e., a finite dimensional vector space V over C and a morphism of algebraic groups $\mathcal{G} \to \mathrm{GL}(V)$, does there exist an iterative differential module M over K such that the action of the differential Galois group on the solution space is isomorphic to the representation V of $\mathcal{G}$?

Suppose that this question has a positive answer for a single faithful representation W of $\mathcal{G}$ (i.e., $\mathcal{G} \to \mathrm{GL}(W)$ is injective). Let M be the corresponding iterative differential module. It is known (see [W], section 3.5) that any representation V of $\mathcal{G}$ can be obtained as a direct sum of subquotients of representations $W \otimes \cdots \otimes W \otimes W^* \otimes \cdots \otimes W^*$. Then the Tannakian approach produces an iterative differential module N, which is a similar direct sum of subquotients of the iterative differential modules $M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*$, such that the action of $\mathcal{G}$ on its solution space is isomorphic to the given representation V. Thus the more precise question has a positive answer if the original question has a positive answer. Now we start the proof of theorem 6.6.

Proof. (1) Consider a reduced linear algebraic group $\mathcal{G}$, satisfying (a), (b) and (c). If $\mathcal{G}^o$ happens to be $\{1\}$, then $\mathcal{G}$ is a finite group, occurs as a Galois group of a finite Galois extension of K and is, according to subsection 4.1, also a differential Galois group.

Suppose now that $\mathcal{G}^o$ is a torus. The p-group $p(\mathcal{G})$ is a normal subgroup which maps bijectively to $p(\mathcal{G}/\mathcal{G}^o)$. By assumption (b) one has that $\mathcal{G}/p(\mathcal{G})$ is commutative and is, according to (c), equal to $\mathcal{G}^o \times C_m$ where C_m denotes a cyclic group of order m (not divisible by p). The group C_m is the image of a cyclic group of order m in $\mathcal{G}$. Thus $\mathcal{G}$ is the semi-direct product of the finite normal p-group $p(\mathscr{G})$ and $\mathscr{G}^o \times C_m$. The action (by conjugation) of $\mathscr{G}^o$ on $p(\mathscr{G})$ is trivial since any $\mathscr{G}^o$-orbit (for the conjugation) is connected. Thus $\mathscr{G}$ is isomorphic to the product of $\mathscr{G}^o$ and the finite group $\mathscr{G}/\mathscr{G}^o$. Both groups are differential Galois groups (see proposition 6.1). Then this product is also a differential Galois group.

Suppose now that $\mathscr{G}^o$ is not a torus. Define a sequence of connected normal subgroups $\mathscr{H}_1 \supset \mathscr{H}_2 \supset \cdots$ of $\mathscr{G}$ by $\mathscr{H}_1$ is the unipotent radical of $\mathscr{G}^o$ and for $i \geqq 1$ the group $\mathscr{H}_{i+1} := [\mathscr{H}_1, \mathscr{H}_i]$, i.e., the group generated by $\{ghg^{-1}h^{-1} \mid g \in \mathscr{H}_1, h \in \mathscr{H}_i\}$. Let $s \geqq 1$ be such that $\mathscr{H}_s \neq 1$ and $\mathscr{H}_{s+1} = 1$. Then $\mathscr{H}_s$ is a connected commutative unipotent group and thus isomorphic to $\mathbb{G}_a^d$ for some $d \geqq 1$. The group $\mathscr{G}$ acts on $\mathscr{H}_s$ by conjugation. This action is trivial for $\mathscr{H}_1$ and we have to study the action of the group $\mathscr{G}_1 := \mathscr{G}/\mathscr{H}_1$ on $\mathscr{H}_s$. As we have seen above the group $\mathscr{G}_1$ is a product $E \times \mathscr{T}$, where E is the finite group $\mathscr{G}/\mathscr{G}^o$ and $\mathscr{T}$ is the torus $\mathscr{G}^o/\mathscr{H}_1$. Let $\mathscr{H}_s$ have the coordinate ring $C[x_1, \dots, x_d]$ and the comultiplication given by $x_i \mapsto x_i \otimes 1 + 1 \otimes x_i$ for all i. The action of E on $C[x_1, \dots, x_d]$ respects the comultiplication and therefore the ring of invariants $C[x_1, \dots, x_d]^E$ is the coordinate ring of a connected commutative unipotent group. Therefore the quotient $\mathscr{H}_s/E$ exists and is isomorphic to the algebraic group $\mathbb{G}_a^d$. The torus $\mathscr{T}$ acts on $\mathscr{H}_s/E \cong \mathbb{G}_a^d$ and it can be seen that there exists a subgroup $\mathscr{N}_1 \subset \mathscr{H}_s/E$, isomorphic to $\mathbb{G}_a$ and invariant under the action of $\mathscr{T}$. We will give an explicit proof of this.

Let $A := C[y_1, \dots, y_d]$ denote the coordinate ring of $\mathscr{H}_s/E$ and let the comultiplication m be given by $y_i \mapsto y_i \otimes 1 + 1 \otimes y_i$. The character group of $\mathscr{T}$ is denoted by $X(\mathscr{T})$. The action of $\mathscr{T}$ on $\mathscr{H}_s/E$ translates into a direct sum decomposition $A = \bigoplus\limits_{\chi} A_\chi$, taken over all $\chi \in X(\mathscr{T})$. The action of $\mathscr{T}$ respects the comultiplication. This yields that m maps A_χ into the direct sum $\bigoplus\limits_{\chi_1 + \chi_2 = \chi} A_{\chi_1} \otimes A_{\chi_2}$. Write each y_i as the finite sum $y_i = \sum\limits_{\chi} y_i(\chi)$ with $y_i(\chi) \in A_\chi$. One finds that $m(y_i(\chi)) = y_i(\chi) \otimes 1 + 1 \otimes y_i(\chi)$. Let S denote a finite set of characters such that all $y_i(\chi)$ are 0 for $\chi \notin S$. Consider the free polynomial ring $B = C[\{Z_i(\chi)\}_{i=1,\dots,d;\chi \in S}]$ and define the comultiplication $B \to B \otimes B$ by $Z_i(\chi) \mapsto Z_i(\chi) \otimes 1 + 1 \otimes Z_i(\chi)$ for all $Z_i(\chi)$. Then $\mathrm{Spec}(B)$ is the direct sum of the $d \cdot \# S$ additive groups $\mathscr{M}_{i,\chi} := \mathrm{Spec}(C[Z_i(\chi)])$. The action of $\mathscr{T}$ on $\mathrm{Spec}(B)$ is induced by an action of $\mathscr{T}(C)$ on the C-algebra B. The latter is defined by $t \cdot Z_i(\chi) = \chi(t) Z_i(\chi)$ for all $t \in \mathscr{T}(C)$ and all i, χ. In particular $\mathrm{Spec}(B)$ is the direct sum of the $\mathscr{T}$-invariant subgroups $\mathscr{M}_{i,\chi}$. Consider now the surjective C-algebra homomorphism $B \to A$ which sends each $Z_i(\chi)$ to $y_i(\chi)$. This morphism respects the comultiplication and the $\mathscr{T}$-action. There results a closed, $\mathscr{T}$-equivariant immersion $\mathscr{H}_s/E \subset \bigoplus \mathscr{M}_{i,\chi}$. One considers a minimal subset T of $\{(i,\chi) \mid i = 1, \dots, d; \chi \in S\}$ such that $\mathscr{N}_0 := (\mathscr{H}_s/E) \cap \bigoplus\limits_{(i,\chi) \in T} \mathscr{M}_{i,\chi}$ is an infinite group. Clearly $\mathscr{N}_0$ has dimension 1 and is $\mathscr{T}$-invariant. Then $\mathscr{N}_1 := \mathscr{N}_0^o$ is isomorphic to $\mathbb{G}_a$ and is $\mathscr{T}$-invariant.

The preimage $\mathscr{N}_2 \subset \mathscr{H}_s$ of $\mathscr{N}_1$ has dimension 1 and is invariant under the action of $\mathscr{G}$ on $\mathscr{H}_s$. The same holds for $\mathscr{N} := \mathscr{N}_2^o$. The latter group is clearly isomorphic to $\mathbb{G}_a$. Thus we have proved that $\mathscr{G}$ contains a normal subgroup $\mathscr{N}$ isomorphic to $\mathbb{G}_a$. In the remaining part of the proof we will show that $\mathscr{G}$ is a differential Galois group over K if the group $\mathscr{G}/\mathscr{N}$ is a differential Galois group over K. By induction (on the dimension of the group $\mathscr{G}$) the theorem follows.

(2) Let a linear algebraic group $\mathscr{G}$ and a one dimensional $\mathscr{G}$-module E be given. One identifies E with the linear algebraic group $\mathbb{G}_{a,C}$ and considers exact sequences of linear algebraic groups $1 \to E \to \tilde{\mathscr{G}} \to \mathscr{G} \to 1$ such that the action by conjugation of $\mathscr{G}$ on E is the given $\mathscr{G}$-module structure on E. There is a regular function on $\tilde{\mathscr{G}}$ which restricts to the identity on E. Thus the exact sequence has a section which is a morphism of algebraic varieties over C. Using this section, the group law on $\tilde{\mathscr{G}}$ can be expressed by a 2-cocycle. In fact, the isomorphy classes of these exact sequences are classified by the cohomology group $H^2(\mathscr{G}, E)$. Suppose that $\mathscr{G}$ can be realized as the differential Galois group of some iterative differential module over K. Then we want to show that any $\tilde{\mathscr{G}}$ as above can also be realized.

Let M be an iterative differential module over K which realizes $\mathscr{G}$ and let R denote its Picard-Vessiot ring and L the field of fractions of R. Consider an inhomogeneous iterative differential equation $\partial^{(p^n)}y = a_n$, $n \geqq 0$ over L with differential Galois group $\mathbb{G}_{a,C}$. The inhomogeneous equation is given by some element $\xi \in \mathscr{L} := \varprojlim L/L_s$ which is unique up to an element in L. The group $\mathscr{G}$ acts on $L, \mathscr{L}$ and $\mathscr{L}/L$. Let $\bar{\xi}$ denote the image of ξ in $\mathscr{L}/L$. We require that the $\mathscr{G}$ action on $C\bar{\xi}$ is isomorphic to the $\mathscr{G}$-module E^*, the dual of E.

First we observe that (under this hypothesis) any $\sigma \in \mathscr{G}$ extends to a K-linear differential automorphism $\tilde{\sigma}$ of $L(x)$. It suffices to define $h := \tilde{\sigma}x$. By construction $\partial^{(p^n)}x = a_n$ for all $n \geqq 0$. The element h should satisfy $\partial^{(p^n)}h = \sigma(a_n)$ for all $n \geqq 0$. It is given that $\sigma\bar{\xi} = c\bar{\xi}$ for some $c \in C^*$ depending on σ. Thus $\sigma(\xi) = c\xi + f$ for certain $f \in L$ and $h = cx + f$ has the required property. For the special ξ's that will be considered, we will show that $L(x)$ is the Picard-Vessiot field of some iterative differential equation over K. Let $\mathscr{G}_\xi$ be the group of all the K-linear differential automorphisms of $L(x)$. By construction there is an exact sequence $1 \to E \to \mathscr{G}_\xi \to \mathscr{G} \to 1$ and so ξ determines a 2-cocycle and its class $c_2(\xi)$ in the cohomology group $H^2(\mathscr{G}, E)$. In the sequel we will make $c_2(\xi)$ more or less explicit and prove that any element in this cohomology group is a $c_2(\xi)$.

The field L with its natural $\mathscr{G}$-action is not a $\mathscr{G}$-module because for a general $a \in L$ the C-vector space generated by the $\{g(a) \mid g \in \mathscr{G}\}$ is not finite dimensional. The Picard-Vessiot ring $R \subset L$ is a $\mathscr{G}$-module and has trivial $\mathscr{G}$-cohomology according to 6.5. The same holds for $R_s = \{a \in R \mid \partial^{(p^n)}a = 0 \text{ for } n < s\}$. The projective limit $\varprojlim R/R_s$ has a natural $\mathscr{G}$-action. It is not a $\mathscr{G}$-module since the $\mathscr{G}$-orbit of an element need not be contained in a finite dimensional C-vector space. We will replace $\varprojlim R/R_s$ by a subspace $\mathscr{R}$, which is actually a $\mathscr{G}$-module. For this purpose we consider finite dimensional $\tilde{K}$-linear subspaces $W \subset R$ which are invariant under the action of $\mathscr{G}$ and under all $\partial^{(p^n)}$. From the form of the Picard-Vessiot ring one sees that R is a filtered countable union of such spaces W. To W one associates $\mathscr{W} = \varprojlim W/W_s$. This is a $\mathscr{G}$-invariant subspace of $\varprojlim R/R_s$ and also a $\mathscr{G}$-module. Then $\mathscr{R}$ will denote the union of all $\mathscr{W}$. Our aim is to show that $H^i(\mathscr{G}, \mathscr{R} \otimes E) = 0$ for all $i \geqq 1$ and every 1-dimensional $\mathscr{G}$-module E.

First we consider the $\mathscr{G}^o$-structure of $\mathscr{R}$. The $\mathscr{G}^o$-modules R and $\tilde{K} \otimes_C C[\mathscr{G}^o]$ are isomorphic. One deduces from this that $\mathscr{R}$ is isomorphic to a $\mathscr{G}^o$-module of the form $T \otimes_C C[\mathscr{G}^o]$, where T is some vector space over C. The conclusion is that $H^i(\mathscr{G}^o, \mathscr{R} \otimes E) = 0$ for all $i \geqq 1$ and therefore $H^i(\mathscr{G}, \mathscr{R} \otimes E) \cong H^i\big(\mathscr{G}/\mathscr{G}^o, (\mathscr{R} \otimes E)^{\mathscr{G}^o}\big)$ for all $i \geqq 0$. Now we have to study $(\mathscr{R} \otimes E)^{\mathscr{G}^o}$ in some detail.

By construction $\varprojlim \tilde{K}/\tilde{K}_s \subset \mathscr{R} \subset \varprojlim R/R_s$. Using observation 6.5, one finds that the set of the $\mathscr{G}^o$-invariants of the last $\mathscr{G}^o$-module is $\varprojlim \tilde{K}/\tilde{K}_s$. Therefore $\mathscr{R}^{\mathscr{G}^o} = \varprojlim \tilde{K}/\tilde{K}_s$.

Using that for all $0 \leqq s < t$ the $\mathscr{G}/\mathscr{G}^o$-module $\tilde{K}_s/\tilde{K}_t$ has trivial cohomology, one finds that also $\varprojlim \tilde{K}/\tilde{K}_s$ has trivial cohomology and consequently $H^i(\mathscr{G}, \mathscr{R}) = 0$ for $i \geqq 1$. A slight variation of the above reasoning shows that also $H^i(\mathscr{G}, \mathscr{R} \otimes E) = 0$ for $i \geqq 1$.

Consider an element $\xi \in \mathscr{R}$, with image $\bar{\xi}$ in $\mathscr{R}/R$, such that:

(i) The elements $\{\bar{\xi}^{p^n} \mid n \geqq 0\}$ are linearly independent over C (in order to obtain a transcendental extension).

(ii) $C\bar{\xi}$ is invariant under the action of $\mathscr{G}$.

We claim that the corresponding extension $L(x) \supset K$ is a Picard-Vessiot extension. The collection $\sigma(\xi) - c\xi$, with $\sigma \in \mathscr{G}$ and $c \in C^*$ such that $\sigma(\bar{\xi}) = c\bar{\xi}$, lies in a finite dimensional C-vector subspace of R/C. The inhomogeneous equation attached to ξ is $\partial^{(p^n)}y = a_n$, $n \geqq 0$ with all $a_n \in R$. For any $\sigma \in \mathscr{G}$ one considers the transformed equation $\partial^{(p^n)}y = \sigma(a_n)$, $n \geqq 0$. The set of all these equations forms a finite dimensional C-vector space of equations. Let N be the corresponding iterative differential module over L. Then $\mathscr{G}$ acts on N. This action commutes with all $\partial^{(p^m)}$ and moreover $\sigma(fn) = \sigma(f)\sigma(n)$ for all $f \in L$ and $n \in N$. The K-vector space $N^{\mathscr{G}}$ is an iterative differential module over K such that $L \otimes_K N^{\mathscr{G}}$ is isomorphic to N. Let M denote, as before, the iterative differential module over K with Picard-Vessiot field L. Then one finds that the Picard-Vessiot field of $M \oplus N^{\mathscr{G}}$ is $L(x)$.

One considers the exact sequence of $\mathscr{G}$-modules $0 \to R/C \to \mathscr{R} \to \mathscr{Q} \to 0$, which defines the $\mathscr{G}$-module $\mathscr{Q}$. The exact sequence

$$0 \to R/C \otimes E \to \mathscr{R} \otimes E \to \mathscr{Q} \otimes E \to 0$$

induces a surjective map $H^0(\mathscr{G}, \mathscr{Q} \otimes E) \to H^1(\mathscr{G}, R/C \otimes E)$. The exact sequence of $\mathscr{G}$-modules $0 \to E \to R \otimes E \to R/C \otimes E \to 0$ induces a surjective map

$$H^1(\mathscr{G}, R/C \otimes E) \to H^2(\mathscr{G}, E).$$

In total we have found a surjective map $H^0(\mathscr{G}, \mathscr{Q} \otimes E) \to H^2(\mathscr{G}, E)$. An element on the left hand side can be interpreted as an element $\xi \in \mathscr{R} \subset \mathscr{L}$ such that the $\mathscr{G}$-module $C\bar{\xi} \subset \mathscr{L}/L$ is isomorphic to E^*. The kernel of the map $H^0(\mathscr{G}, \mathscr{Q} \otimes E) \to H^2(\mathscr{G}, E)$ is very large. After adding to $\bar{\xi}$ a suitable element in this kernel, one obtains a ξ such that the elements $\bar{\xi}, \bar{\xi}^p, \bar{\xi}^{p^2}, \ldots$ are linearly independent over C. Using the explicit interpretation of the cohomology groups and the maps between them, one finds that its image in $H^2(\mathscr{G}, E)$ coincides with the 2-cocycle $c_2(\xi)$. This ends the proof of part (2) and completes the proof of the theorem. □

7. Global iterative differential modules

In this section X is an irreducible projective smooth curve over C and K denotes the function field of X. The field K is provided with an iterative derivation such that $\partial^{(1)}$ is not trivial. The theme of this section is the study of the iterative differential modules over K and their differential Galois groups.

We start with the following observations. A linear differential equation of order d on the curve X and with poles in the points $x_1, \dots, x_s$ with order $n_1, \dots, n_s$ can be described by a connection

$$\nabla : \mathscr{M} \to \Omega_X(n_1[x_1] + \cdots + n_s[x_s]) \otimes \mathscr{M},$$

where $\mathscr{M}$ is a vector bundle on X of rank d, Ω_X is the sheaf of holomorphic differential forms on X and $\Omega_X(n_1[x_1] + \cdots + n_s[x_s])$ is the sheaf of the differential forms on X with divisor greater than or equal to $-(n_1[x_1] + \cdots + n_s[x_s])$. Further ∇ is required to satisfy the usual rules. In particular the connection is regular outside the set $\{x_1, \dots, x_s\}$. This natural definition of "regular" for a differential equation at a point or on some open affine subset of X does not carry over to iterative differential modules over K. Indeed, there is no universal iterative differential available and thus no equivalent for the sheaf Ω_X. We will use another method to give a reasonable definition of the regularity at a point $x \in X$ for an iterative differential module over K.

An iterative differential module M over K is, according to proposition 5.1, equivalent to a projective system of subspaces $\{M_n\}$. Each M_n is a vector space over K_n and the canonical maps $K_{n-1} \otimes M_n \to M_{n-1}$ are isomorphisms. In our special situation the field K_n is equal to K^{p^n} and in particular does not depend on the chosen iterative derivation on K provided that $\partial^{(1)} \neq 0$. For any other iterative derivation $\{\tilde{\partial}^{(n)}\}$ on K with $\tilde{\partial}^{(1)} \neq 0$ we can use the above projective system $\{M_n\}$ to define a structure of ID-module on M with respect to new iterative derivation $\{\tilde{\partial}^{(n)}\}$ on K. This change does not effect solution spaces and the differential Galois group of M.

For any point $x \in X$ we can consider a local parameter t at x. The field extension $C(t) \subset K$ is finite and separable and the unique iterative derivation on K with $\partial^{(n)} t^m = \binom{m}{n} t^{m-n}$ for all $n, m \geqq 0$ is denoted by $\{\partial_t^{(n)}\}$. We note that the local ring O_x at x is invariant under all $\partial_t^{(n)}$. The same holds for the coordinate ring $O(U)$ of a suitable affine neighbourhood U of the point x. We can now give the following *definition*:

Let M be an ID-module over K and let x be a point of X. One considers a local parameter t at x, the iterative derivation $\{\partial_t^{(n)}\}$ on K and the corresponding structure $\{\partial_{M,t}^{(n)}\}$ on M. Then x is called a *regular point of M* if there is an open affine subset U containing x and an $O(U)$-lattice $N \subset M$ (i.e., $O(U)$ is the coordinate ring of U and $K \otimes_{O(U)} N \to M$ is an isomorphism) which is invariant under all $\partial_{M,t}^{(n)}$.

It can be seen that this definition is independent of the choice of t. We note further that this property is stronger than the statement that $K_x \otimes M$ is a regular ID-module over K_x (where K_x denotes the completion of the function field K at the place x). Indeed, in section 4.2 we have given examples concerning this statement.

Let M be an iterative differential module over $C(z)$ which is regular outside $S = \{a, \dots, a_r, \infty\}$. Since z is everywhere on $Y := \mathbb{P}_C^1 \backslash S$ a local parameter, there are open affine sets $U_1, \dots, U_s$ with union Y and invariant $O(U_i)$-lattices Λ_i for $i = 1, \dots, s$ and w.r.t. the iterative derivation $\{\partial_z^{(n)}\}$ on $C(z)$. Above the intersection $U_i \cap U_j$ we find by localization two invariant $O(U_i \cap U_j)$-lattices. From the unicity of corollary 6.2, part (3), we conclude that those two lattices coincide. Thus the lattices Λ_i glue to an invariant $O(Y)$-lattice Λ for M.

The following theorem extends proposition 4.2.

Theorem 7.1. *Let X be an irreducible smooth projective curve over C with function field K and J its Jacobian variety. $S \subset X$ will be a finite set with cardinality $r+1 \geqq 0$. Let* $\mathrm{Isom}_{X,S,1}$ *denote the subgroup of* $\mathrm{Isom}_{K,1}$ *consisting of the (isomorphy classes of) one dimensional iterative differential modules over K which are regular outside S. Let* $\mathrm{Div}^0(X,S,\mathbb{Z}_p)$ *denote the subgroup of* $\mathrm{Div}^0(X,\mathbb{Z}_p)$ *consisting of the elements D which have finite support and such that $D(x) \in \mathbb{Z}$ for all $x \in X\backslash S$.*

(1) *There exists an exact sequence*

$$0 \to T_p(J) \to \mathrm{Isom}_{X,S,1} \to \mathrm{Div}^0(X,S,\mathbb{Z}_p)/\mathrm{Prin}(X) \to 0.$$

(2) *For any integer $n > 0$, not divisible by p, the elements of* $\mathrm{Isom}_{X,S,1}$ *with order divisible by n form a group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^c$ with $c = 2g + r$ if $r \geqq 0$ and $c = 2g$ for $r = -1$.*

(3) *The group* $\mathrm{Isom}_{X,S,1}$ *has no elements of infinite order precisely in the following cases*:

(a) *$g > 0$, $r \leqq 0$, $T_p(J) = 0$ and C is the algebraic closure of $\mathbb{F}_p$.*

(b) *$g = 0$ and $r \leqq 0$.*

(4) *Suppose that* $\mathrm{Isom}_{X,S,1}$ *contains an element of infinite order, then the dimension of the $\mathbb{Q}$-vector space* $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Isom}_{X,S,1}$ *is infinite.*

Proof. (1) Let M be a one-dimensional ID-module over K, given by the projective system $\{M_n\}$. Choose a point $x \in X\backslash S$, a local parameter t at x, a small enough open U containing x and a basis $\{e\}$ for M over K. The iterative derivation on K is taken to be $\{\partial_t^{(n)}\}$. We will abbreviate $\partial_t^{(n)}(f)$ for $f \in K$ by $f^{(n)}$. The corresponding ID-structure on M is denoted $\{\partial^{(n)}\}$. We want to investigate the invariance of $O(U)e$ under all $\partial^{(n)}$. Write $M_n = K_n f_n e$ for certain elements $f_n \in K^*$. From $\partial^{(1)}(f_1 e) = 0$ it follows that $\partial^{(1)} e = -\frac{f^{(1)}}{f} e$. The coefficient $-\frac{f^{(1)}}{f}$ belongs to $O(U)$ if and only if the restriction of the divisor of f to U is a multiple of p. More generally, $-\partial^{(p^n)} e = \sum_{a+b=p^n, a>0} \frac{f_n^{(a)}}{f_n} \partial^{(b)} e$. One concludes that $O(U)e$ is invariant under all $\partial^{(k)}$ if and only if for every $n \geqq 1$ the restriction of the divisor of f_n to U is a multiple of p^n. Let $D_e \in \mathrm{Div}^0(X,\mathbb{Z}_p)$ denote the projective limit of the divisors of the f_n modulo p^n. Then the invariance of the lattice $O(U)e$ by all $\partial^{(n)}$ is equivalent to the support of D_e lies in $X\backslash U$.

A change of the basis element of M, changes D_e by a principal divisor. The above and the proposition 4.2 prove now (1).

(2) The p-adic Tate module $T_p(J)$ is isomorphic to $\mathbb{Z}_p^s$ with $0 \leqq s \leqq g$ and has no elements of finite order. The other component $\mathrm{Div}^0(X, S, \mathbb{Z}_p)/\mathrm{Prin}(X)$ of $\mathrm{Isom}_{X,S,1}$ is equal to the Jacobian variety J of X for $r = -1, 0$. For $r > 0$ the considered there is an exact sequence

$$0 \to J \to \mathrm{Div}^0(X, S, \mathbb{Z}_p)/\mathrm{Prin}(X) \to (\mathbb{Z}_p)^r \to 0.$$

Part (2) of the theorem now follows.

(3) and (4) follow from the following observation: If the field C is the algebraic closure of $\mathbb{F}_p$, then all the elements of J (or better of $J(C)$) have finite order. For an algebraically closed field $C \supset \mathbb{F}_p$ which contains transcendental elements over $\mathbb{F}_p$ the group $J(C)$ is large and in particular $\mathbb{Q} \otimes J(C)$ has an infinite dimension over $\mathbb{Q}$. □

In order to state our conjecture we will use the following notion. For any group G, let $p(G)$ denote the subgroup generated by all elements which have as order a power of the prime p. Clearly $p(G)$ is a normal subgroup and $G/p(G)$ is the largest factor group which does no have elements with order p. Consider a linear algebraic group $\mathscr{G}$.

We claim that $p(\mathscr{G})$ is an algebraic subgroup of $\mathscr{G}$ and that the quotient $\mathscr{H} := \mathscr{G}/p(\mathscr{G})$ satisfies: $\mathscr{H}^o$ is either 1 *or a torus and $\mathscr{H}/\mathscr{H}^o$ is a finite group whose order is not divisible by p.*

Every unipotent element of $\mathscr{G}$ has order a power of p. In particular, $p(\mathscr{G})$ contains the unipotent radical $R_u(\mathscr{G})$ of $\mathscr{G}$. After dividing by the unipotent radical we may suppose that $\mathscr{G}$ is reductive. Further it suffices to consider the case where $\mathscr{G}$ is connected. By [Sp], corollary 8.1.6, $\mathscr{G} = R(\mathscr{G}) \cdot [\mathscr{G}, \mathscr{G}]$ where $R(\mathscr{G})$ is a central torus and the commutator subgroup $[\mathscr{G}, \mathscr{G}]$ of $\mathscr{G}$ is a semi-simple algebraic group. By [Sp], theorem 8.1.5, the latter group is generated by unipotent elements and lies therefore in $p(\mathscr{G})$. The central torus $R(\mathscr{G})$ has no elements of order p and we conclude $p(\mathscr{G}) = [\mathscr{G}, \mathscr{G}]$ and $\mathscr{G}/p(\mathscr{G})$ is an image of the central torus, hence either 1 or a torus.

Conjecture. *Let g denote the genus of X and let $S \subset X$ be a finite subset with cardinality $r + 1 \geqq 1$. A linear algebraic group $\mathscr{G}$ can be realized for the pair (X, S), i.e., is the differential Galois group of an iterative differential module over K which is regular outside S, if and only if the group $\mathscr{H} := \mathscr{G}/p(\mathscr{G})$ can be realized for the pair (X, S).*

Remarks. (1) The implication ⇒ in the conjecture follows from the Tannakian approach to iterative differential modules. Indeed, this point of view shows that if a group $\mathscr{G}$ occurs as a differential Galois group for an iterative differential module which is regular outside S, then the same holds for any image of $\mathscr{G}$.

(2) If one specializes the conjecture to the case of finite groups, then one obtains the well known conjectures of Abhyankar, proved by M. Raynaud and D. Harbater (see [A], [R], [H1], [H2]).

(3) The complex analogue of the above conjecture, is a theorem of J.-P. Ramis. In this analogue the expression $p(\mathscr{G})$ is replaced by $L(\mathscr{G})$, which is the subgroup generated by all subtori of $\mathscr{G}$. See for an exposition of this work [Ra1], [Ra2], [P1].

(4) In the sequel we will investigate when a linear algebraic group $\mathscr{H}$, which has no elements of order p, can be realized as a differential Galois group for the pair (X, S). Further we will give a complete answer to the question which *connected* linear algebraic group $\mathscr{G}$ can be realized as a differential Galois group for a pair (X, S) with non-empty S.

Theorem 7.2. *The pair (X, S) represents a smooth, irreducible, projective algebraic curve over C of genus g and a finite subset of cardinality $r + 1 \geqq 1$. Let $\mathscr{H}$ be a linear algebraic group which has no elements of order p.*

(1) *If $\mathscr{H}$ is finite then $\mathscr{H}$ is realizable if and only if $\mathscr{H}$ can be generated by $\leqq 2g + r$ elements.*

(2) *If $\mathscr{H}$ is connected then $\mathscr{H}$ is realizable if and only if* $\mathrm{Isom}_{X,S,1}$ *contains an element of infinite order.*

(3) *Suppose $1 \neq \mathscr{H}^o \neq \mathscr{H}$ and $\mathscr{H}$ commutative. Then $\mathscr{H}$ is realizable if and only if* $\mathrm{Isom}_{X,S,1}$ *contains an element of infinite order and $\mathscr{H}/\mathscr{H}^o$ can be generated by $\leqq 2g + r$ elements.*

(4) *Suppose that $1 \neq \mathscr{H}^o \neq \mathscr{H}$ and that $\mathscr{H}$ is not commutative. Let a denote the minimum number of generators of $\mathscr{H}/\mathscr{H}^o$. If $\mathscr{H}$ is realizable then $a \leqq 2g + r$. If $\mathscr{H}$ is realizable and $a = 1$ (i.e., $\mathscr{H}/\mathscr{H}^o$ is cyclic), then $2 \leqq 2g + r$.*

Proof. We start with *some observations.*

(i) The finite group $\mathscr{H}/\mathscr{H}^o$ is again the differential Galois group of some iterative differential modules M over K which is regular outside S. The Picard-Vessiot extension $L \supset K$ for M is a finite Galois extension with group $\mathscr{H}/\mathscr{H}^o$ and is unramified outside S. According to Grothendieck's work on étale coverings (see [G]), the groups $\mathscr{H}/\mathscr{H}^o$ are characterized as the groups having no elements of order p and generated by at most $2g + r$ elements.

(ii) Consider the case $2g + r = 1$, i.e., $g = 0$ and $r = 1$ and an ID-module M such that its differential Galois group $\mathscr{H}$ has no elements of order p. We may suppose that the affine curve $X\backslash S$ is $\mathbb{A}^1_C\backslash\{0\}$. By assumption the ID-module M admits a lattice Λ over $C[z, z^{-1}]$, which is invariant under all $\partial^{(n)}$. We claim that the point 0 is a regular singular point. Indeed, the differential Galois group $\tilde{\mathscr{H}}$ of the ID-module $C((z)) \otimes M$ over $C((z))$ is a subgroup of $\mathscr{H}$ and has therefore no elements of order p. According to corollary 6.4, $\tilde{\mathscr{H}}$ is also a solvable group. Since it has no elements of order p, the group $\tilde{\mathscr{H}}$ contains no unipotent elements $\neq 1$ and the group $\tilde{\mathscr{H}}$ is diagonalizable. By corollary 6.2, $C((z)) \otimes M$ is regular singular and there are lattices in $C((z)) \otimes M$ over $C[[z]]$, invariant under all $\delta^{(n)}$. The same holds for the point ∞. For both $z = 0$ and $z = \infty$ one has some freedom in the choice of the lattices, invariant under all $\delta^{(n)}$. Using this freedom one concludes that there exists a free vector bundle $\mathscr{M}$ on $\mathbb{P}^1_C$ such that $\mathscr{M}(\mathbb{P}^1_C\backslash\{0, \infty\}) = \Lambda$ and the completions $\hat{\mathscr{M}}_0$, $\hat{\mathscr{M}}_\infty$ are lattices, invariant under all $\delta^{(n)}$. Let V denote the vector space of the global sections of $\mathscr{M}$. Then clearly $M = C(z) \otimes V$ and V is invariant under all $\delta^{(n)}$. The algebra $R = C[\delta^{(n)},\ n \geqq 0]$, introduced in section 6, acts on V. There correspond eigenspaces $V_1, \ldots, V_r$ and eigenvalues $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}_p$ for this action of R on V. The differential Galois group $\mathscr{H}$ of M can be identified with the group of the automorphisms of V consisting of the elements h such that:

(a) The restriction of h to each V_i is multiplication by some $t_i \in C^*$.

(b) For every tuple $(n_1, \dots, n_r) \in \mathbb{Z}^r$ with $n_1\alpha_1 + \cdots + n_r\alpha_r \in \mathbb{Z}$ one has $t_1^{n_1} \cdots t_r^{n_r} = 1$.

We conclude that $\mathscr{H}$ can be any commutative group such that $\mathscr{H}^o$ is a torus and $\mathscr{H}/\mathscr{H}^o$ is cyclic with order not divisible by p.

(iii) We consider the case $g = r = 0$ and an ID-module M with a differential Galois group $\mathscr{H}$ which has no elements of order p. This is a special case of (ii) where now the point $z = 0$ is regular. It follows that all the α_i are in $\mathbb{Z}$ and therefore $\mathscr{H} = \{1\}$.

Now we have all the ingredients for the proof, namely:

(1) follows from observation (i). (2) follows from part (4) of theorem 7.1. (3) follows from part (2) and part (4) of theorem 7.1. (4) follows from observations (i), (ii) and (iii). □

Now we start the proof of the other implication of the conjectures for connected groups $\mathscr{G}$ and $g = 0$. Define $U(\mathscr{G})$ to be the subgroup of $\mathscr{G}$ generated by all its connected unipotent subgroups. The group $U(\mathscr{G})$ is a connected normal algebraic subgroup of $\mathscr{G}$ and the factor group $\mathscr{G}/U(\mathscr{G})$ is either trivial or a torus. (See [Sp].) Clearly $U(\mathscr{G}) \subset p(\mathscr{G})$ and since the factor group has no elements of order p we have $U(\mathscr{G}) = p(\mathscr{G})$.

Theorem 7.3. *Every connected linear algebraic group $\mathscr{G} \subset \mathrm{GL}(V)$, with V a finite dimensional vector space over C, can be realised as a differential Galois group of an iterative differential module M over $C(z)$ such that the action of $\mathscr{G}$ on its solution space is isomorphic to the given representation of $\mathscr{G}$ on V. Moreover*:

(1) *If the group $\mathscr{G}$ is generated by its connected unipotent subgroups* (*or equivalently $\mathscr{G}/p(\mathscr{G}) = \{1\}$*), *then M can be chosen with only one singular point.*

(2) *In the other case* (*i.e., $\mathscr{G}/p(\mathscr{G})$ is a non-trivial torus and hence as algebraic group generated by one element*) *M can be chosen with two singular points.*

The following example illustrates the rather involved proof. We take $\mathscr{G} = \mathrm{SL}(2, C)$ and we use proposition 5.3 in order to produce an iterative differential module M over $C(z)$ which is regular outside $z = \infty$ and has differential Galois group $\mathrm{SL}(2, C)$. This module is given by a sequence of matrices $\phi_n \in \mathrm{SL}(2, C[z^{p^n}])$ which are supposed to satisfy:

(a) ϕ_n is either 1 or $\begin{pmatrix} 1 & z^{p^n} \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ z^{p^n} & 1 \end{pmatrix}$.

(b) The sequence $n_1 < n_2 < n_3 < \cdots$ of elements with $\phi_n + 1$ has "arbitrary large gaps", say defined by $\lim(n_{i+1} - n_i) = \infty$.

(c) For every integer $N \geqq 0$, there are infinitely many $n \geqq N$ with $\phi_n + 1$ and ϕ_n upper triangular and also infinitely many $n \geqq N$ such that $\phi_n + 1$ is lower triangular.

We claim that the differential Galois group of M is $\mathrm{SL}(2,C)$. We will write $V = C^2$ and describe a canonical way to identify the solution space of M with V. The $C[z]$-lattice $C[z] \otimes V = M$ is embedded into the $C[[z]]$-lattice $M_0 := C[[z]] \otimes V \subset C\bigl((z)\bigr) \otimes_{C(z)} M$. The ID-module $C\bigl((z)\bigr) \otimes M$ is regular and has a solution space $\tilde{V} \subset M_0$. The map $\tilde{V} \to M_0 \to M_0/zM_0 \cong V$ produces this canonical identification. Here the expression "canonical" means that the construction respects "all constructions of linear algebra".

According to proposition 5.3, the differential Galois group is a subgroup $\mathscr{H}$ of $\mathrm{SL}(2,C)$. Let us first assume that $\mathscr{H}$ leaves a line in the solution space of M invariant. This implies that M contains an ID-submodule $N \subset M$ of dimension 1. Write $\{N_n\}$ for the projective system induced by N. Each $N_n \subset K_n \otimes V = M_n$ is a vector of dimension 1 over $K_n = C(z^{p^n})$ and is given a basis element $q_n = (a_n, b_n) \in (C[z^{p^n}])^2$ such that the g.c.d. of the two polynomials a_n and b_n is 1. The element q_n is unique up to a constant. Since $\phi_n N_{n+1} \subset N_n$, one has $\phi_n q_{n+1} = u q_n$ for some $u \in K_n^*$. The two coordinates of $\phi_n q_{n+1}$ have again g.c.d. 1 and we conclude that $u \in C^*$.

The degree of q_n is defined as the maximum of the degrees of a_n and b_n w.r.t. the variable z. Thus the degree of q_n is $d_n p^n$ for some integer $d_n \geqq 0$. From $\phi_n q_{n+1} = u q_n$ and the form of the ϕ_n's one concludes that $d_n p^n \geqq d_{n+1} p^{n+1}$. This is only possible if all d_n are 0 for all $n \geqq N$ and some integer N. Therefore $q_n \in V$ for $n \geqq N$. Suppose that ϕ_n, with $n > N$, has the form $\begin{pmatrix} 1 & 0 \\ z^{p^n} & 1 \end{pmatrix}$ then $q_{n+1} = c(0,1)$ with $c \in C^*$ and $q_n = q_{n+1}$. If one supposes that ϕ_n has the form $\begin{pmatrix} 1 & z^{p^n} \\ 0 & 1 \end{pmatrix}$ then $q_{n+1} = c(1,0)$ with $c \in C^*$ and $q_n = q_{n+1}$. Condition (c) yields a contradiction.

Now we suppose that the differential Galois group $\mathscr{H}$ is some proper subgroup of $\mathrm{SL}(2,C)$. There is a symmetric power $W := \mathrm{sym}^d(V)$ and a line $L \subset W$ such that L is invariant under $\mathscr{H}$ and not invariant under $\mathrm{SL}(2,C)$. With this symmetric power one associates ID-module $\mathrm{sym}^d(M)$, which is the d^{th} symmetric power of M and the projective system $\{\psi_n\}$ with $\psi_n := \mathrm{sym}^d(\phi_n) \in \mathrm{GL}(C[z^{p^n}] \otimes W)$. We note that the degree of the coefficients of the matrix ψ_n is bounded by dp^n. The $\mathscr{H}$-invariant line L in $\mathrm{sym}^d(V)$ implies the existence of a one-dimensional ID-submodule D of $\mathrm{sym}^d(M)$. This D is given by a projective system $\{D_n\}$ and each D_n is given a generator $q_n \in C[z^{p^n}] \otimes W$ such that the g.c.d. of its coordinates with respect to some basis of W is 1. The degree of q_n is the maximum of the degrees of those coordinates of q_n with respect to the variable z. Thus the degree of q_n is $d_n p^n$ for some integer $d_n \geqq 0$. As before, one has $\psi_n q_{n+1} = u q_n$ with $u \in C^*$. Further $d_n q_n \geqq d_{n+1} q_{n+1}$ holds for sufficiently large n, since the condition on the gaps does not allow for cancellation of the terms with highest degrees. One concludes that $d_n = 0$ and thus $q_n \in W$ for large enough n. Moreover q_n must be an eigenvector for the eigenvalue 1 for ψ_n and n large. We draw the conclusion that $q_n = w \in W$ and $D_n = K_n w$ for $n \geqq N$. Clearly $L = Cw$. The algebraic subgroup of $\mathrm{SL}(2,C)$ generated by $\phi_n(1)$ with $n \geqq N$ is equal to $\mathrm{SL}(2,C)$. From $\psi_n(w) = w$ for $n \geqq N$ it follows that L is also invariant under the action of $\mathrm{SL}(2,C)$ on W. This contradicts the hypothesis concerning L.

The idea for the construction of M (in the general case) is again proposition 5.3, i.e., M is given by a projective system $\{K_n \otimes V, \phi_n\}$. The ϕ_n's have to be chosen carefully in order to assure that the differential Galois group of M is not a proper subgroup of $\mathscr{G}$. In case $\mathcal{G}$ is generated by its connected unipotent subgroups we define the ring R as $C[z]$ and in the other case we take for R the ring $C[z, z^{-1}]$. Put $R_n = R^{p^n}$.

Lemma 7.4. *Let the connected $\mathcal{G} \subset \mathrm{GL}(V)$ be given and let R be either $C[z]$ or $C[z, z^{-1}]$. Suppose that the elements $\phi_n \in \mathcal{G}(R_n)$ satisfy:*

(a) $\phi_n(1) = 1 \in \mathcal{G}$.

(b) *For any integer $N \geqq 0$ the group $\mathcal{G}$ is generated as an algebraic group by the images of the maps ϕ_n: $\mathbb{A}^1_C$ or $\mathbb{A}^1_C \backslash \{0\} \to \mathcal{G}$ with $n \geqq N$.*

(c) *The "degrees" of all $\phi_n \in \mathrm{GL}(R_n \otimes V)$ in the variable z^{p^n} are bounded by some integer B.*

(d) *Let $n_0 < n_1 < n_2 < \cdots$ denote the $n \in \mathbb{N}$ such that $\phi_n \neq 1$. We require that $\lim(n_{i+1} - n_i) = \infty$.*

Then the differential Galois group of the corresponding modular differential module $M = K \otimes V$ is equal to $\mathcal{G}$ and its action on the solution space of M coincides with the given action of $\mathcal{G}$ on V.

First we explain the notion of "degree" used in part (c) of the lemma. Any $f \in C[z] \otimes V$ can be written as $\sum f_n z^n$ with the $f_n \in V$. The degree of f will be $\max\{n \mid f_n \neq 0\}$. Any $f \in C[z, z^{-1}] \otimes V, f \neq 0$ can be written as $\sum\limits_{n=n_0}^{n_1} f_n z^n$ with $f_n \in V$ and $f_{n_0} \neq 0 \neq f_{n_1}$. The degree of f is defined as $n_1 - n_0$. Further ϕ_n induces a map of V into $R_n \otimes V$.

The degree of ϕ_n (w.r.t. z^{p^n}) is defined as the maximum of the degrees of the $\phi_n(v)$ with $v \in V$ (w.r.t. z^{p^n}).

Proof. (1) We consider the case $R = C[z]$ and start by proving that any one dimensional ID-submodule $N \subset M$ has the form $K \otimes L$, where $L \subset V$ is an $\mathcal{G}$-invariant one dimensional subspace.

The ID-submodule N gives rise to a sequence of subspaces $N_n \subset K_n \otimes V$ of dimension 1 over K_n, such that $\phi_n N_{n+1} \subset N_n$ for all $n \geqq 0$. The space N_n is given a generator $q_n \in C[z^{p^n}] \otimes V$ such that the g.c.d. of the coordinates of q_n with respect to a basis of V is 1. This generator is unique up to multiplication by an element in C^*. Then $\phi_n q_{n+1} = u q_n$ for some element $u \in K_n^*$. Since $\phi_n \in \mathrm{GL}(C[z^{p^n}] \otimes V)$ we have that $\phi_n(q_{n+1}) \in C[z^{p^n}] \otimes V$ and the g.c.d. of the coefficients of $\phi_n(q_{n+1})$ w.r.t. a basis of V is again 1. We conclude that $u \in C^*$.

Now we consider the positive integers $n_0 < n_1 < n_2 < \cdots$ of condition (d). Assume that q_{n_i} has the form $\sum\limits_{j=0}^{d} v_j t^j$ with $t = z^{p^{n_i}}$, $d > 0$ and $v_d \neq 0$. Then $q_{n_{i-1}+1} = q_{n_i}$ and $q_{n_{i-1}} = c \sum\limits_{j=0}^{d} \phi_{n_{i-1}}(v_j) t^j$ with $c \in C^*$. The degrees of $\phi_{n_{i-1}}(v_j)$ in z are bounded by $Bp^{n_{i-1}}$

and the degree of $\phi_{n_{i-1}}(v_d)t^d$ is $\geqq dp^{n_i}$. For i with $p^{n_i-n_{i-1}} > B$ we find that $q_{n_{i-1}}$ has degree $\geqq dp^{n_i}$. This implies that also q_0 has degree $\geqq dp^{n_i}$. We conclude that for large enough i the element q_{n_i} has degree 0. As a consequence, there is an integer N such that $q_n \in V$ for $n \geqq N$. The equality $\phi_n(z^{p^n})q_{n+1} = cq_n$ for $n \geqq N$ can be specialized at $z = 1$ and yields $q_{n+1} = q_n$ and $c = 1$. Further the substitution $z^{p^n} = s \in C$ yields that q_n is also an eigenvector for $\phi_n(s)$ for any $s \in C$. Write $q_n = v \in V$ for $n \geqq N$. Property (b) implies that the line $L := Cv \subset V$ is invariant under $\mathscr{G}$. We conclude that N is the one-dimensional submodule associated with this $\mathscr{G}$-invariant line.

(2) In order to show that the differential Galois group $\mathscr{H}$ of M is not a proper subgroup of $\mathscr{G}$, one has to prove that for any representation $\rho : \mathscr{G} \to \mathrm{GL}(W)$, any $\mathscr{H}$-invariant line $L \subset W$ is also $\mathscr{G}$-invariant. One associates with this representation the projective system $\{K_n \otimes W, \psi_n\}$, where $\psi_n = \rho(\phi_n)$. Let $\tilde{M}$ denote the corresponding iterative differential module. The $\mathscr{H}$-invariant line L provides a one dimensional iterative submodule N of $\tilde{M}$. The conditions (a)–(d) are again satisfied in this new situation and according to part (1) of the proof we conclude that N is associated with a $\mathscr{G}$-invariant line $L_1 \subset V$. Clearly $L = L_1$ and thus L is invariant under $\mathscr{G}$. We conclude that $\mathscr{H} = \mathscr{G}$.

(3) The case $R = C[z, z^{-1}]$ can be treated in a similar way. We will omit the details.

(4) The module M has $R \otimes V$ as R-lattice, invariant under all ϕ_n and all $\partial^{(j)}$. The solution space for M can be realized as a C-vector space $W \subset C[[z-1]] \otimes V$. The evaluation map $C[[z-1]] \otimes V \to V$ (i.e., dividing by $(z-1)$) induces an isomorphism $W \to V$. The last statement of the lemma follows from the canonical (i.e., compatible with all constructions of linear algebra) identification of the solution space for M with V. □

***Continuation of the proof of theorem* 7.3.** *We consider the case where $\mathscr{G}$ is generated as an algebraic group by its connected unipotent subgroups.* We will need the following lemma.

Lemma 7.5. *Let $\mathscr{U}$ be a connected unipotent group over the field C. There exists a morphism $\alpha : \mathbb{A}^1_C \to \mathscr{U}$ of C-varieties with $\alpha(1) = 1 \in \mathscr{U}$ and such that $\mathscr{U}$ is generated as an algebraic group by the image of α.*

Proof. We will prove this by induction on the dimenson of $\mathscr{U}$. If the dimension of $\mathscr{U}$ is 1, then $\mathscr{U}$ is isomorphic to the additive group $\mathbb{G}_a$ and the statement is trivial. If the dimension of $\mathscr{U}$ is greater than 1, then the centralizer of $\mathscr{U}$ contains a subgroup $\mathscr{C}$ isomorphic to $\mathbb{G}_a$. By induction there is a morphism $\alpha_1 \colon \mathbb{A}^1_C \to \mathscr{U}/\mathscr{C}$ with the required properties. It is known that the morphism $\mathscr{U} \xrightarrow{\pi} \mathscr{U}/\mathscr{C}$ admits a section $r : \mathscr{U}/\mathscr{C} \to \mathscr{U}$. This means that r is a morphism of C-varieties such that $\pi \circ r$ is the identity on $\mathscr{U}/\mathscr{C}$. The map $\alpha_2 := r \circ \alpha_1 \colon \mathbb{A}^1_C \to \mathscr{U}$ has the property that the Zariski closure $\mathscr{U}_1$ of the group generated by $\alpha_2(C)$ maps surjectively to $\mathscr{U}/\mathscr{C}$. If $\mathscr{U}_1$ happens to be $\mathscr{U}$, then α_2 has (after a shift in order to assure $\alpha_2(1) = 1$) the required properties. If $\mathscr{U}_1 \neq \mathscr{U}$ then we may consider instead of $\mathscr{U}$ the direct product $\mathscr{C} \times \mathscr{U}_1$. Indeed, this group maps surjectively to $\mathscr{U}$ and has the same dimension as $\mathscr{U}$. We propose here a map $\alpha_3 \colon \mathbb{A}^1_C \to \mathscr{C} \times \mathscr{U}_1$ of the form $\alpha_3(c) = \big(\beta(c), \alpha_2(c)\big)$ for a suitable β. Let $\mathscr{U}_2$ denote the Zariski closure of the group generated by $\alpha_3(C)$. It suffices to choose β such that the map $\mathscr{U}_3 \to \mathscr{C} \times \mathscr{U}_1/[\mathscr{U}_1, \mathscr{U}_1]$ is surjective. Indeed, it will follow that the kernel of the projection map $\mathscr{U}_2 \to \mathscr{U}_1$ is not finite and thus $\mathscr{U}_2 = \mathscr{C} \times \mathscr{U}_1$.

Write $\mathscr{H} := \mathscr{U}_1/[\mathscr{U}_1, \mathscr{U}_1]$ and α for the induced map $\mathbb{A}^1_C \to \mathscr{H}$. The group $\mathscr{H}$ is isomorphic to a product $\mathbb{G}_a^m$. The image of α does not lie in a proper algebraic subgroup of $\mathscr{H}$ and we have to produce a $\beta : \mathbb{A}^1 \to \mathscr{C} \cong \mathbb{G}_a$ such that the image of $(\beta, \alpha) : \mathbb{A}^1_C \to \mathscr{C} \times \mathscr{H}$ does not lie in a proper algebraic subgroup. One knows that any proper algebraic subgroup of $\mathbb{G}_a^{m+1}$ is contained in the zero set of some additive polynomial $f := \sum\limits_{n \geqq 0} (a_{0,n} x_0^{p^n} + \cdots + a_{m,n} x_m^{p^n})$, where $x_0, \ldots, x_m$ denote the standard coordinates for $\mathbb{G}_a^{m+1}$. One easily sees that β given by $\beta(c) = c^d$ with suitable $d > 1$ and $p \not| \, d$, has the required property. □

Corollary 7.6. *Suppose that $\mathscr{G}$ is generated by its connected unipotent subgroups. Then there are finitely many morphisms of C-varieties $\alpha_j : \mathbb{A}^1_C \to \mathscr{G}$, $j = 1, \ldots, s$ with $\alpha_j(1) = 1 \in \mathscr{G}$ such that $\mathscr{G}$ is generated as an algebraic group by the union of the images of the α_j.*

Proof. Let $\mathscr{U}$ be a maximal connected unipotent subgroup of $\mathscr{G}$. Then every maximal connected unipotent subgroup of $\mathscr{G}$ is conjugated to $\mathscr{U}$. The group $\mathscr{G}$ is already generated by finitely many conjugates of $\mathscr{U}$. Let $\alpha : \mathbb{A}^1_C \to \mathscr{U}$ satisfy the properties of lemma 7.5. Then for finitely many $g_1, \ldots, g_s \in \mathscr{G}$, the maps $\alpha_j = g_j \alpha g_j^{-1}$ have the properties of the lemma. □

We apply lemma 7.4 with the following data:

(i) Any sequence $n_0 < n_1 < n_2 < \cdots$ with $\lim(n_{i+1} - n_i) = \infty$.

(ii) $\phi_n = 1$ if n is not equal to some n_i.

(iii) $\phi_{n_i} = \alpha_j(z^{p^{n_i}})$ such that every α_j occurs infinitely often.

The conditions (a)–(d) are obviously satisfied and the first part of the theorem is proved.

We suppose now that $\mathscr{G}$ is a connected linear algebraic group. Fix a maximal connected unipotent subgroup $\mathscr{U}$ and a maximal torus $\mathscr{T}$. It is well known that $\mathscr{G}$ is generated as an algebraic group by finitely many conjugates of $\mathscr{U}$ and of $\mathscr{T}$. The morphism $\alpha : \mathbb{A}^1_C \to \mathscr{U}$ of lemma 7.5 has also the property that the Zariski closure of the group generated by $\alpha(C^*)$ is equal to $\mathscr{U}$. Indeed, $\alpha(0)$ lies in the Zariski closure of $\alpha(C^*)$. There is a morphism of $\beta : \mathbb{A}^1 \backslash \{0\} \to \mathscr{T}$ such that $\beta(1) = 1$ and the group generated by $\beta(C^*)$ is Zariski-dense in $\mathscr{T}$. Indeed, it suffices to produce a map β such that $\chi \circ \beta$ is not the constant map with image $\{1\}$ for any non trivial character of $\mathscr{T}$. Let Γ be a suitable finite set of conjugates of α and β. Then one applies lemma 7.4 with the following data:

(i) and (ii) as before and (iii) $\phi_{n_i} = \gamma(z^{p^{n_i}})$ with $\gamma \in \Gamma$ and such that every $\gamma \in \Gamma$ occurs infinitely often. The second part of the theorem now follows.

Corollary 7.7. *Let X be a* (*smooth, irreducible, projective*) *curve over C with function field K and let $S \subset X$ be a non-empty finite set.*

(1) *Then any connected algebraic group $\mathscr{G}$ such that $\mathscr{G}/p(\mathscr{G}) = \{1\}$ can be realized as a differential Galois group of an iterative differential module over K, which is regular outside S.*

(2) *Suppose moreover that there exists a non constant regular function on $X\backslash S$ without zeros. Then any connected linear algebraic group $\mathscr{G}$ can be realized as a differential Galois group of an iterative differential module over K which is regular outside S.*

(3) *Any connected linear algebraic group can be realized for the pair (X, S) if and only if* $\mathrm{Isom}_{X,S,1}$ *contains an element of infinite order.*

Proof. (1) The coordinate ring $O(X\backslash S)$ of $X\backslash S$ is a finite extension of some ring $C[z]$. The corresponding morphism $\psi : X \to \mathbb{P}^1_C$ has the property that $\psi^{-1}(\infty) = S$. Let N be an ID-module over $C(z)$ which is regular outside ∞ and has the required differential Galois group $\mathscr{G}$ and representation. Since $\mathscr{G}$ is connected, the ID-module $M = K \otimes_{C(z)} N$ has the same differential Galois group and representation.

The proof of (2) is deduced from the existence of a non constant morphism $f : X \to \mathbb{P}^1_C$ with $S \subset f^{-1}(0) \cup f^{-1}(\infty)$.

(3) According to theorem 7.1, the condition that $\mathrm{Isom}_{X,S,1}$ contains an element of infinite order is necessary since $\mathbb{G}_m$ is supposed to be realizable. Suppose that this condition is satisfied and let $\mathscr{G}$ be a connected linear algebraic group. $\mathscr{T}$ denotes a maximal torus of $\mathscr{G}$ and $U(\mathscr{G})$ is the normal algebraic subgroup generated by all the connected unipotent subgroups of $\mathscr{G}$. The assumption on (X, S) implies that $\mathscr{T}$ can be realized as differential Galois group. The same holds for $U(\mathscr{G})$. An interlacing of the two projective systems for $\mathscr{T}$ and $U(\mathscr{G})$ with "gaps" as in lemma 7.4, provides a projective system with differential Galois group $\mathscr{G}$. We will omit the details. □

8. *p*-adic differential equations

Let $\mathbb{C}_p$ denote the completion of the algebraic closure of $\mathbb{Q}_p$. On the field $\mathbb{C}_p(z)$ one considers a valuation which is called the *Gauss norm*. The Gauss norm $\|P\|_{\mathrm{gauss}}$ of a polynomial $P = \sum c_i z^i \in \mathbb{C}_p[z]$ is defined as the maximum of the absolute value of its coefficients. The Gauss norm $\left\|\frac{T}{N}\right\|_{\mathrm{gauss}}$ of a rational function is defined as $\frac{\|T\|_{\mathrm{gauss}}}{\|N\|_{\mathrm{gauss}}}$. The completion of the field $\mathbb{C}_p(z)$ with respect to this Gauss norm is denoted by $\widehat{\mathbb{C}_p(z)}_{\mathrm{gauss}}$. The differentiation $\frac{d}{dz}$ on $\mathbb{C}_p(z)$ is continuous with respect to the Gauss norm and extends to a continuous derivation of $\widehat{\mathbb{C}_p(z)}_{\mathrm{gauss}}$. The field of constants of both differential fields $\mathbb{C}_p(z)$ and $\widehat{\mathbb{C}_p(z)}_{\mathrm{gauss}}$ is the algebraically closed field $\mathbb{C}_p$. The valuation rings of both $\mathbb{C}_p(z)$ and $\widehat{\mathbb{C}_p(z)}_{\mathrm{gauss}}$ are invariant under the operations $\frac{1}{n!}\left(\frac{d}{dz}\right)^n$. The residue field of both fields is $\overline{\mathbb{F}}_p(z)$. This field inherites an iterative differentiation, induced by the $\frac{1}{n!}\left(\frac{d}{dz}\right)^n$, which coincides with the $\{\partial_z^{(n)}\}$.

A *p-adic differential equation* is a differential equation over either the differential field $\mathbb{C}_p(z)$ or $\widehat{\mathbb{C}_p(z)}_{\mathrm{gauss}}$. The aim of this section is to investigate the relation between differential equations over $\widehat{\mathbb{C}_p(z)}_{\text{gauss}}$ and iterative differential equations over $\overline{\mathbb{F}}_p(z)$. In our setup we will be slightly more general and allow other residue fields than $\overline{\mathbb{F}}_p(z)$ and slightly less general in the sense that we will avoid non-discrete valuation rings like the ring of integers of $\mathbb{C}_p$.

The setup and some notations. R is a complete discrete valuation ring. Its field of fractions F has characteristic 0 and is equipped with a differentiation ∂_F, which induces the iterative derivation $\{\partial_F^{(n)}\}$ with $\partial_F^{(n)} = \frac{\partial_F^n}{n!}$. The residue field K of R has characteristic p. Further $\pi \in R$ denotes a generator of the maximal ideal of R. The *absolute ramification index e of R* is given by $\pi^e R = pR$. Then we assume the following:

(a) R is invariant under all $\partial_F^{(n)}$.

(b) $\partial_F \pi = 0$.

(c) The iterative derivation on K, induced by the $\{\partial_F^{(n)}\}$ is denoted by $\{\partial_K^{(n)}\}$. We require that $\partial_K^{(1)} \neq 0$.

Example. Let L be any complete discretely valued field of characteristic 0 and with a residue field of characteristic $p > 0$. One considers the Gauss norm on $L(z)$ and the completion F of $L(z)$ with respect to the Gauss norm. The differentiation $f \mapsto \frac{df}{dz}$ on $L(z)$ is continuous with respect to the Gauss norm and extends to a differentiation on F. Now F satisfies all conditions above. Thus the usual p-adic differential equations are present in our setup.

Let (M, ∂) be a differential module over F. We investigate R-lattices of M, i.e., the R-submodules of M generated by a basis of M over F.

Proposition 8.1. *Let a differential module (M, ∂) over F of dimension d be given. Let $k \geqq 0$ be an integer. The following properties of an R-lattice Λ of M are equivalent.*

(1) *There exists an R-basis $\{e_j\}$ of Λ such that all $\partial e_j \in p^k \Lambda$.*

(2) *Λ is invariant under the $\partial^{(n)} := \frac{\partial^n}{n!}$ for all $n < p^{k+1}$.*

Proof. (1) $\Rightarrow$ (2) will be proved by induction on k. Take $k = 0$. Then $\partial \sum_j r_j e_j$, with all $r_j \in R$, belongs to Λ since $\partial e_j \in \Lambda$ and $\partial_F(r_j) \in R$. Thus Λ is invariant under ∂ and also under $\partial^{(n)} = \frac{\partial^n}{n!}$ for $n < p$.

Suppose that (1) $\Rightarrow$ (2) holds for $k-1$ and that (1) holds for k. Then Λ is invariant under $\partial^{(n)}$ for $n < p^k$ and we only have to show that Λ is also invariant under $\partial^{(p^k)}$.

From $\partial e_j \in p^k \Lambda$ one concludes that $\partial^{(p)} e_j \in p^{k-1} \Lambda$. Indeed, $p! \partial^{(p)} e_j = \partial^p e_j \in p^k \Lambda$. The same reasoning implies that $\partial^{(p^2)} e_j \in p^{k-2} \Lambda$, $\partial^{(p^3)} e_j \in p^{k-3} \Lambda$ and finally $\partial^{(p^k)} e_j \in \Lambda$.

Any element of Λ has the form $\sum r_j e_j$ with $r_j \in R$. Now $\partial^{(p^k)} r_j e_j = \sum\limits_{a+b=p^k} \partial_F^{(a)} r_j \partial^{(b)} e_j$ shows that Λ is invariant under $\partial^{(p^k)}$.

(2) $\Rightarrow$ (1) is also proved by induction on k. The induction step contains again other induction steps. We will indicate the procedure. The case $k = 0$ is trivial. Consider $k = 1$. Put $W := \Lambda/\pi\Lambda$ and let ∂_W on W be induced by ∂ on Λ. Then (W, ∂_W) is an ordinary differential module over the field K. Its p-curvature is 0 since Λ is invariant under $\partial^{(p)}$. There exists a basis $w_1, \dots, w_d$ of W over K such that all $\partial_W w_j = 0$. Choose representatives $e_1, \dots, e_d \in \Lambda$ of $w_1, \dots, w_d$. They form a free basis of Λ over R and $\partial e_j \in \pi\Lambda$ for all j. If the absolute ramification index e is 1, then we are finished. Suppose now $e > 1$. Then one considers a new basis $e_1 + \pi a_1, \dots, e_d + \pi a_d$ with all $a_j \in \Lambda$ and require that $\partial(e_j + \pi a_j) \in \pi^2\Lambda$. This amounts to relations $\partial a_j \equiv -\dfrac{\partial e_j}{\pi}$ modulo $\pi\Lambda$. One can see this as equations $\partial_W \bar{a}_j = b_j$ in W where b_j denotes the image of $-\dfrac{\partial e_j}{\pi}$ in W. Since the differential module (W, ∂_W) is trivial, one concludes from property (c) that the image of ∂_W on W is equal to the kernel of ∂_W^{p-1}. In particular, there is a solution $\bar{a}_j$ if $\partial_W^{p-1} b_j = 0$. The latter condition is satisfied since $\partial^{p-1}\left(\dfrac{\partial e_j}{\pi}\right) = \dfrac{p!}{\pi}\partial^{(p)} e_j \in \pi^{e-1}\Lambda$. This procedure is repeated until a basis $e_1, \dots, e_d$ is found with $\partial e_j \in p\Lambda$ for all j.

Consider the case $k = 2$. Let $W = \Lambda/\pi\Lambda$. On this K-vector space we have a "truncated" iterative differential module structure. By this we mean that the $\partial_W^{(n)}$ are defined for $n < p^3$ and satisfy the usual rules. There is a basis $w_1, \dots, w_d$ of W such that $\partial_W w_j = \partial_W^{(p)} w_j = 0$.

The *first step* is to produce elements $e_1, \dots, e_d \in \Lambda$ with images $w_1, \dots, w_d$ such that $\partial^{(p)} e_j \in p\Lambda$.

If the ramification index e is 1, then any choice for the e_j has this property. If $e > 1$, then we have that $\partial^{(p)} e_j = \pi^m a_j$ for some $m \geqq 1$ and elements $a_j \in \Lambda$. For $m < e$, one tries to find elements $\{e_1 - \pi^m b_1, \dots, e_d - \pi^m b_d\}$ such that $\partial^{(p)}(e_j - \pi b_j) \in \pi^{m+1}\Lambda$. For this one has to solve the equations $\partial^{(p)} \bar{b}_j = \bar{a}_j$ in the space W. As before, K_1 denote the subfield $\{f \in K \mid \partial_K f = 0\}$. The pair $(W, \partial_W^{(p)})$ is now considered as a differential module over the field K_1. This is again a trivial differential module since $(\partial^{(p)})_W^p = 0$. Therefore a solution $\bar{b}_j$ exists if $(\partial^{(p)})_W^{p-1} \bar{a}_j = 0$. Since Λ is invariant under $\partial^{(p^2)}$ one has that $(\partial^{(p)})^{p-1} \partial^{(p)} e_j \in p\Lambda$ and thus $(\partial^{(p)})^{p-1} a_j \in \pi^{e-m}\Lambda$.

We conclude that there are elements e_j with $\bar{e}_j = w_j$ such that $\partial^{(p)} e_j \in p\Lambda$. The *next step* concerns ∂e_j. One has $\partial e_j = \pi^m a$ with $a \in \Lambda$ and $m \geqq 1$. For $m < 2e$, one wants to change e_j into $e_j - \pi^m b$ with $b \in \Lambda$ such that $\partial(e_j - \pi^m b) \in \pi^{m+1}\Lambda$ and $\partial^{(p)}(e_j - \pi^m b) \in p\Lambda$. If $m \geqq e$, then the second condition is automatically satisfied and one can proceed as before. Suppose now that $1 \leqq m < e$. Then a satisfies two properties namely:

(i) $\partial^{p-1} a \in \pi^{2e-m}\Lambda$. This follows from $\partial^{(p)} e_j \in p\Lambda$.

(ii) $\partial^{(p)} a \in \pi^{e-m}\Lambda$. This follows from $\pi^m \partial^{(p)} a = \partial\partial^{(p)} e_j \in p\Lambda$.

Thus $\partial_W^{p-1}\bar{a} = 0$ and $\partial_W^{(p)}\bar{a} = 0$. We recall that $K_2 = \{f \in K_1 \mid \partial_K^{(p)} f = 0\}$ and that for a good choice of z the field K has basis $\{z^j \mid 0 \leqq j < p^2\}$ over K_2 and that $\partial_K^{(n)} z^m = \binom{m}{n} z^{m-n}$ holds for all $n < p^2$ (see proposition 2.2). Then $\bar{a}$ can be written as $\sum_{i=1,\dots,d;\,0 \leqq j < p^2} a(i,j) z^j w_i$ with all $a(i,j) \in K_2$. From $\partial_W^{p-1}\bar{a} = 0$ and $\partial_W^{(p)}\bar{a} = 0$ one deduces that $a(i,j) = 0$ for $j \geqq p-1$. Thus a solution $\bar{b}$ of $\partial_W \bar{b} = \bar{a}$ has the form $\sum_{i=1,\dots,d;\,0 \leqq j < p-1} \frac{a(i,j)}{j+1} z^{j+1} w_i$. Therefore $\partial(e_j - \pi^m b) \in \pi^{m+1}\Lambda$ and $\partial^{(p)}(e_j - \pi^m b) \in p\Lambda$, as required. This ends the proof of the case $k = 2$.

We sketch the case $k = 3$. One takes a basis $w_1, \dots, w_d$ of W with

$$\partial w_j = \partial^{(p)} w_j = \partial^{(p^2)} w_j = 0 \quad \text{for all } j.$$

The elements $w_1, \dots, w_d$ are first lifted to elements $e_1, \dots, e_d \in \Lambda$ such that $\partial^{(p^2)} e_j \in p\Lambda$. The next step is to modify the e_j such that the additional property $\partial^{(p)} e_j \in p^2\Lambda$ holds. The final step modifies the e_j again in order to obtain $\partial e_j \in p^3\Lambda$. Each of the steps involves smaller steps, where a congruence modulo $\pi^m\Lambda$ is refined to a congruence modulo π^{m+1}. The same pattern can be followed to give a proof for general k. □

Let M be a finite dimensional vector space over the valued field F. A norm on M is a map $\|\ \|: M \to \mathbb{R}_{\geqq 0}$ such that:

(i) $\|m\| = 0$ if and only if $m = 0$.

(ii) $\|m_1 + m_2\| \leqq \max(\|m_1\|, \|m_2\|)$.

(iii) $\|fm\| = |f| \cdot \|m\|$ for $f \in F$ and $m \in M$.

All norms on M are equivalent since F is complete and the dimension of M is finite. This means that for any two norms $\|\ \|$ and $\|\ \|^*$ there are positive constants d, D such that $d\|m\|^* \leqq \|m\| \leqq D\|m\|^*$ holds for all $m \in M$. In the sequel we will only consider norms such that the values $\|m\|$ are contained in $|F|$. One associates with a norm $\|\ \|$ the R-lattice $\{m \in M \mid \|m\| \leqq 1\}$. This produces a bijection between norms and R-lattices. An orthonormal basis $\{m_1, \dots, m_d\}$ for M with respect to a given norm is defined by the property that $\|f_1 m_1 + \cdots + f_d m_d\| = \max(|f_j|)$ holds for all $f_1, \dots, f_d \in F$. In other words $\{m_1, \dots, m_d\}$ is an orthonormal basis if and only if it is a free basis of the R-lattice $\{m \in M \mid \|m\| \leqq 1\}$.

For an additive map $A : M \to M$ and a given norm $\|\ \|$ on M, one defines $\|A\| := \sup\left\{\frac{\|Am\|}{\|m\|} \mid m \in M, m \neq 0\right\}$. A priori, $\|A\|$ can be ∞. For two additive maps A, B with $\|A\|, \|B\| < \infty$ one has $\|AB\| \leqq \|A\| \cdot \|B\|$. With this terminology we can now formulate a limit case of proposition 8.1.

Theorem 8.2. *Let (M, ∂) be a differential module of dimension d over F. One writes $\partial^{(n)}$ for the operator $\frac{\partial^n}{n!}$ on M. The following conditions on M are equivalent.*

(1) *There exists an R-lattice invariant under all* $\partial^{(n)}$.

(2) *There exists a norm* $\| \ \|$ *on* M *such that* $\|\partial^{(n)}\| \leqq 1$ *for all* $n \geqq 0$.

(3) *There exists a norm* $\| \ \|$ *on* M *such that* $\sup\limits_{n \geqq 0} \|\partial^{(n)}\| < \infty$.

(4) *Fix a norm* $\| \ \|$ *on* M. *There exists a constant* $c > 1$ *and for every* $\varepsilon > 0$ *a basis* $\{m_1, \ldots, m_d\}$ *(depending on* ε*) such that*:

(a) $C^{-1} \max(|f_j|) \leqq \|f_1 m_1 + \cdots + f_d m_d\| \leqq C \max(|f_j|)$ *for all* $f_1, \ldots, f_d \in F$.

(b) $\|\partial m_j\| \leqq \varepsilon$ *for all* j.

(5) *There exists a norm* $\| \ \|$ *and for every* $\varepsilon > 0$ *an orthonormal basis* $\{m_1, \ldots, m_d\}$ *such that* $\|\partial m_j\| \leqq \varepsilon$ *for all* j.

Proof. We note that conditions (3) and (4) are independent of the chosen norm since all norms are equivalent.

(1) ⇒ (5). Let $\| \ \|$ denote the norm with $\Lambda = \{m \in M \mid \|m\| \leqq 1\}$ invariant under all $\partial^{(n)}$. Apply now proposition 8.1.

(5) ⇒ (4) is obvious.

(4) ⇒ (3). We will show by induction that $\|\partial^{(n)} m\| \leqq c^2 \|m\|$ holds for all $n \geqq 0$ and all $m \in M$. Suppose this formula holds for $n < N$. Take $\varepsilon > 0$ such that $(c^2)^{N-1} \varepsilon \leqq 1$ and let $m_1, \ldots, m_d$ be the corresponding basis of M. Write $m = \sum\limits_j f_j m_j$. Then $\partial^{(N)} \sum\limits_j f_j m_j = \sum\limits_j \sum\limits_{a+b=N} \partial^{(a)} f_j \partial^{(b)} m_j$. One has $|\partial^{(a)} f_j| \leqq |f_j|$. For $b > 0$ one has $\|\partial^{(b)} m_j\| \leqq (c^2)^{b-1} \varepsilon \leqq 1$ and $\|m_j\| \leqq c$. From this the inequality $\|\partial^{(N)} m\| \leqq c^2 \|m\|$ follows.

(3) ⇒ (2). One defines the function $\| \ \|^*$ on M by the formula $\|m\|^* = \max(\|\partial^{(n)} m\|)$. It is easily verified that $\| \ \|^*$ is a norm on M and takes its values in $|F|$. Now $\|\partial^{(a)} m\|^* = \max(\|\partial^{(n)} \partial^{(a)} m\|)$ and this is $\leqq \|m\|^*$ since $\partial^{(n)} \partial^{(a)} = \binom{n+a}{n} \partial^{(n+a)}$ and $\left|\binom{n+a}{n}\right| \leqq 1$.

(2) ⇒ (1). The lattice $\Lambda = \{m \in M \mid \|m\| \leqq 1\}$ is invariant under all $\partial^{(n)}$. □

Another limit form of proposition 8.1 is the following.

Theorem 8.3. *Let* (M, ∂) *be a differential module over* F *of dimension* d. *The following statements are equivalent.*

(1) *For every integer* $k \geqq 0$ *there is an R-lattice which is invariant under all* $\partial^{(n)}$ *with* $n < p^{k+1}$.

(2) *For every integer* $k \geqq 0$ *there is a basis* $m_1, \ldots, m_d$ *of* M *such that* $\partial m_j \in p^k (R m_1 + \cdots + R m_d)$.

(3) *Let* $\| \ \|^*$ *be any norm on* M. *For every* $r > 1$ *there exists a positive constant* $C(r)$ *such that* $\|\partial^{(n)}\|^* \leqq C(r)r^n$ *holds for all* $n \geqq 0$.

Proof. The equivalence between (1) and (2) is just proposition 8.1.

$(1) \Rightarrow (3)$. Let $\| \ \|$ be the norm corresponding to the lattice Λ. Then $\|\partial^{(n)}\| \leqq 1$ for all $n < p^{k+1}$. We will give an estimate for $\|\partial^{(m)}\|$ for all $m \geqq 0$.

Define the real number $w(s)$ by $\|\partial^{(p^s)}\| = p^{w(s)}$. The equality $\partial^{(p^{s+1})} = \dfrac{(p^s!)^p}{p^{s+1}!}(\partial^{(p^s)})^p$ implies $\|\partial^{(p^{s+1})}\| = p\|(\partial^{(p^s)})^p\|$ and thus $w(s+1) \leqq 1 + pw(s)$. It is given that $w(j) \leqq 0$ for $0 \leqq j \leqq k$. One deduces from this that $w(s) \leqq \dfrac{p^{s-k}-1}{p-1}$ for $s > k$. In order to give an estimate for $\|\partial^{(m)}\|$ we write m as $m_0 + m_1 p + \cdots + m_s p^s$ with all $m_i \in \{0, 1, \ldots, p-1\}$. One has $\|\partial^{(m)}\| \leqq \|\partial^{(p^0)}\|^{m_0} \cdots \|\partial^{(p^s)}\|^{m_s}$. Then

$$ {}^{p}\log\|\partial^{(m)}\| \leqq \frac{1}{p-1}\big(m_{k+1}(p-1) + \cdots m_s(p^{s-k}-1)\big) $$

and the latter is $\leqq \dfrac{m}{(p-1)p^k}$. Thus $\|\partial^{(m)}\| \leqq r_k^m$ with $r_k = p^{\frac{1}{(p-1)p^k}}$ holds for all $m \geqq 0$ and the special norm we started with. For the given norm on M, which is equivalent to this special norm, we find $\|\partial^{(m)}\|^* \leqq C_k r_k^m$ for all $m \geqq 0$ and a constant C_k which depends on the comparison between $\| \ \|$ and $\| \ \|^*$. Further $\lim\limits_{k\to\infty} r_k = 1$.

$(3) \Rightarrow (1)$. We fix an integer $k \geqq 0$ and consider the collection of additive maps S on M given by

$$ S := \{(\partial^{(p^0)})^{a_0} \cdots (\partial^{(p^{k-1})})^{a_{k-1}}(\partial^{(p^k)})^{a_k} \mid a_0, \ldots, a_{k-1} \in \{0, 1, \ldots, p-1\}, a_k \geqq 0\}. $$

We claim that $\lim\limits_{s\in S}\|s\|^* = 0$. It suffices to prove that $\lim\limits_{n\to\infty}\|(\partial^{(p^k)})^n\| = 0$. We write $n = n_0 + n_1 p + \cdots + n_s p^s$ with all $n_i \in \{0, 1, \ldots, p-1\}$. Then

$$ \|(\partial^{(p^k)})^n\|^* \leqq (\|\partial^{(p^k)}\|^*)^{n_0} \cdots \big(\|(\partial^{(p^k)})^{p^s}\|^*\big)^{n_s}. $$

As in the proof of $(1) \Rightarrow (3)$ one derives the equality $\|(\partial^{(p^k)})^{p^s}\|^* = \|p^{\frac{p^s-1}{p-1}}\partial^{(p^{k+s})}\|^*$. We are given the inequalities $\|\partial^{(m)}\|^* \leqq C(r)r^m$, in which we make the choice $r = p^{\frac{1}{p^{k+1}(p-1)}}$. This yields $\|\partial^{(p^{k+s})}\|^* \leqq C(r)p^{p^{-s}}$ for every $s \geqq 0$. One derives that for n (as above) that ${}^{p}\log\|(\partial^{(p^k)})^n\|^* \leqq -n + s \cdot p\log C(r)$ and moreover $s \leqq {}^{p}\log n$. Thus $\lim\limits_{n\to\infty}\|(\partial^{(p^k)})^n\|^* = 0$ and we have proved our claim.

Now we introduce a new norm $\| \ \|$ on M by the formula:

$$ \|m\| = \sup\{\|s(m)\|^* \mid s \in S\}. $$

This expression is finite since $\lim\limits_{s\in S}\|s\|^* = 0$. It is easily verified that $\| \ \|$ is actually a norm. Now we observe that for $s \in S$ and any j with $0 \leqq j \leqq k$ there is an integer N

and an element $s' \in S$ such that $\partial^{(p^j)}s = Ns'$. This implies that $\|\partial^{(p^j)}m\| \leqq \|m\|$ if $0 \leqq j \leqq k$. Let Λ be the R-lattice $\{m \in M \mid \|m\| \leqq 1\}$. Then clearly Λ is invariant under $\partial^{(n)}$ for all $n < p^{k+1}$. □

We now describe a tool of Dwork's theory of p-adic differential equations, namely the "generic disk" (see for instance [D-G-S], p. 92 and [C]). For this we specialize F to be the completion of $L(z)$ with respect to the Gauss norm, where L is a complete, discretely valued, subfield of $\mathbb{C}_p$. The norm $\|A\|$ of a matrix $A = (A_{i,j})$ with coefficients in F is defined by $\|A\| = \max(\|A_{i,j}\|)$. Consider a matrix differential equation $y' = Ay$ over F of size d. The iterated equations have the form $\frac{1}{n!}\left(\frac{d}{dz}\right)^n y = A_n y$. One introduces a larger complete valued field $\Omega \supset L$ which contains an element t of absolute value 1 such that its image in the residue field is transcendental over the residue field of L. The field F is mapped into Ω by sending z to t. The open disk $\{a \in \Omega \big| |a - t| < 1\}$ is called the *generic disk*. The differential equation $y' = Ay$ has a formal fundamental solution U at the point t with $U(t) = 1$. This is the expression $U = 1 + \sum_{n \geqq 1} A_n(t)(z - t)^n$, where $A_n(t)$ denotes the image of A_n under the map $F = L(z) \to \Omega$. The verification of this formula is straightforward. The convergence of U on (part of) the generic disk and the behaviour of the absolute values of the coefficients, i.e., the $\|A_n(t)\| = \|A_n\|$ has been studied in detail by B. Dwork, Ph. Robba, G. Christol, B. Chiarellotto et al. Corollary 4.8.8, p. 142 of [C] states that U converges on the full generic disk if and only if for every positive ε there is an $H_\varepsilon \in \mathrm{GL}(d, F)$ such that upon posing $y = H_\varepsilon f$, the transformed equation $f' = \tilde{A}f$ with $\tilde{A} := H_\varepsilon^{-1}AH_\varepsilon - H_\varepsilon^{-1}H_\varepsilon'$ satisfies $\|\tilde{A}\| < \varepsilon$. The convergence on the full generic disk means that for every $r > 1$ there is some constant $C(r)$ with $\|A_n\| \leqq C(r)r^n$ for all $n \geqq 0$. The other condition in the cited Corollary 4.8.8 translates into statement (2) of theorem 8.3. Thus theorem 8.3 implies this result of [C].

A special case of the other limit situation, namely the equivalence of (3) and (4) in theorem 8.2, can be translated into proposition 4.8.9 of [C] (see also [Ro]) which states that the boundedness of the fundamental solution U on the generic disk is equivalent to the assertion:

There exists a positive δ and for every $\varepsilon > 0$ an $H_\varepsilon \in \mathrm{GL}\big(d, L(z)\big)$ such that $\|H_\varepsilon\| \leqq 1$, $|\det H_\varepsilon| \geqq \delta$ and $\|H_\varepsilon' H_\varepsilon^{-1} - A\| \leqq \varepsilon$.

It seems that, apart from the above criterion by Robba, p-adic differential equations of this type have not been studied extensively.

For the next theorem we make the following assumptions on F, K and the derivation ∂_F on F:

Let R_0 be a complete discrete valuation ring with maximal ideal pR_0, residue field $k = R_0/pR_0$ and field of fractions L. The field $L(z)$ is provided with the Gauss norm and the derivation $\frac{d}{dz}$. Then F is the completion of $L(z)$ and ∂_F is the continuous extension of $\frac{d}{dz}$ to F.

The valuation ring of F will be denoted as before by R. We observe that the residue field R/pR of F is equal to $K = k(z)$ and that the induced iterative derivation $\{\partial_K^{(n)}\}$ on K coincides with $\{\partial_z^{(n)}\}$.

Theorem 8.4. *Let F, K and ∂_F be as above and let N be an iterative differential module over K. Then there exists a differential module (M, ∂_*) over F and an R-lattice $\Lambda \subset M$ invariant under all $\partial_*^{(n)}$ such that the induced iterative differential module $\Lambda/p\Lambda$ over K is isomorphic to N.*

Proof. Define, as before, the subfields K_s of K by $K_1 = \{a \in K \mid \partial_K(a) = 0\}$ and $K_{s+1} = \{a \in K_s \mid \partial_K^{(p^s)} a = 0\}$. Clearly $K_s = k(z^{p^s})$. Let R_s be the completion of the valuation ring $R_0[z^{p^s}]_{(p)}$ and let F_s be the field of fractions of R_s. Then one has the properties:

(i) $R_s/pR_s = K_s$.

(ii) $F_{s+1} \subset F_s \subset F$.

(iii) R_s is free over R_{s+1} with basis $1, z^{p^s}, z^{2p^s}, \dots, z^{(p-1)p^s}$.

(iv) $\partial_F R_s \in p^s R$.

Let Λ denote a free R-module with basis $e_1, \dots, e_d$. Then $\Lambda/p\Lambda$ is a vector space over K with basis $f_1, \dots, f_d$, the images of $e_1, \dots, e_d$. We identify $\Lambda/p\Lambda$ with N and regard $f_1, \dots, f_d$ as a basis of N over K. Further M will be $F \otimes_R \Lambda$. The aim is to produce a structure of differential module (M, ∂_*) such that Λ is invariant under all $\partial_*^{(n)}$ and such that the induced iterative differential module $\Lambda/p\Lambda$ is isomorphic to N.

Define $N_1 = \{n \in N \mid \partial^{(p^0)} n = 0\}$ and by induction $N_{s+1} = \{n \in N_s \mid \partial^{(p^s)} n = 0\}$. Each N_s is a vector space of dimension d over the field K_s and $K \otimes_{K_s} N_s \to N$ is an isomorphism. Let $f_1(s), \dots, f_d(s)$ denote a basis of N_s over K_s. Now we will make a sequence of choices:

(1) Elements $e_1(1), \dots, e_d(1) \in \Lambda$ with images $f_1(1), \dots, f_d(1)$ in N. Put $\Lambda_1 = R_1 e_1(1) + \cdots + R_1 e_d(1) \subset \Lambda$. Then Λ_1 maps surjectively to N_1.

(2) Choose elements $e_1(2), \dots, e_d(2) \in \Lambda_1$ with images $f_1(2), \dots, f_d(2) \in N_2 \subset N_1$. Define $\Lambda_2 = R_2 e_1(2) + \cdots + R_2 e_d(2)$. Then Λ_2 maps surjectively to N_2.

(3) By induction on s, one defines $\Lambda_s = R_s e_1(s) + \cdots + R_s e_d(s)$ such that the images of the $e_i(s)$ are the $f_i(s)$ and $\Lambda_s \subset \Lambda_{s-1}$ for all $s \geqq 2$.

We want to define $\partial_* \colon \Lambda \to \Lambda$ by the properties:

(a) ∂_* is additive and $\partial_*(rm) = \partial_F(r)m + r\partial_*(m)$ for all $m \in \Lambda$ and $r \in R$.

(b) $\partial_*\bigl(e_i(s)\bigr) \in p^s\Lambda$ for $i = 1, \dots, d$ and all $s \geqq 1$.

Fix an $m \in \Lambda$. Write $m = \sum c_j(s) e_j(s)$ with $c_j(s) \in R$. Then $\partial_* m$ should be $\sum \partial_F\bigl(c_j(s)\bigr) e_j(s) + \sum c_j(s) \partial_*\bigl(e_j(s)\bigr)$. Thus we want to define $\partial_* m$ by the sequence of congruence relations: $\partial_* m \equiv \sum \partial_F\bigl(c_j(s)\bigr) e_j(s)$ modulo $p^s\Lambda$ for $s \geqq 1$. The only thing to verify is that these congruence relations are compatible.

Write $e_j(s) = \sum_i r(i,j) e_i(s+1)$ with all $r(i,j) \in R_s$.

Then one has $m = \sum_i \left(\sum_j c_j(s) r(i,j) \right) e_i(s+1)$ and we have to show that $\sum_i \left(\sum_j \partial_F\bigl(c_j(s) r(i,j)\bigr) \right) e_i(s+1)$ is congruent to $\sum_j \partial_F\bigl(c_j(s)\bigr) e_j(s)$ modulo $p^s \Lambda$. This follows at once from $r(i,j) \in R_s$ and $\partial_F\bigl(r(i,j)\bigr) \in p^s R$.

We conclude that $\partial_* : \Lambda \to \Lambda$ is well defined and has the properties (a) and (b). From proposition 8.1 it follows that Λ is invariant under all $\partial_*^{(n)}$. Let $\{\partial_*^{(n)}\}$ also denote the induced iterative differential structure on $\Lambda/p\Lambda = N$. From the construction it follows that $\partial_*^{(p^{s-1})}$ maps Λ_s into $p\Lambda$. Since Λ_s maps to N_s, one finds that any $n \in N_s$ satisfies $\partial_*^{(p^j)} n = 0$ for $j = 0, \ldots, s-1$. Therefore the $\{\partial_*^{(n)}\}$ coincide with the given $\{\partial^{(n)}\}$ on N. □

Let (M, ∂) be a differential module over F and Λ an R-lattice which is invariant under all $\partial^{(n)}$. Denote by N the induced iterative differential module over K. The module (M, ∂) has a differential Galois group $\mathcal{G}$ over the algebraic closure $\bar{C}$ of the field of constants C of F. The iterative differential module N has a differential Galois group $\mathcal{H}$ over the algebraic closure of the field of constants of K. These two groups are obviously related. One suspects that "$\mathcal{H}$ is the reduction of $\mathcal{G}$ modulo p". We will make this more precise.

The field C is a complete valued subfield of F. We assume that the valuation ring of C maps surjectively to the field of constants of K, i.e., the residue field of F. Let $O_{\bar{C}}$ denote the valuation ring of $\bar{C}$ and let $\underline{m}$ be its maximal ideal. Then $O_{\bar{C}}/\underline{m}$ is the algebraic closure of the field of constants of K.

Conjecture 8.5. *After replacing the given differential module (M, ∂) over F by some equivalent differential module there exists an R-lattice Λ, invariant under all $\partial^{(n)}$, which determines a linear algebraic group $\mathcal{G}_O$ over $O := O_{\bar{C}}$ such that:*

(1) $\bar{C} \otimes_{O_{\bar{C}}} \mathcal{G}_O = \mathcal{G}$ *and*

(2) $O_{\bar{C}}/\underline{m} \otimes_{O_{\bar{C}}} \mathcal{G}_O$ *contains $\mathcal{H}$ as algebraic subgroup.*

Moreover if $\mathcal{G}$ is a finite group then $\mathcal{G}$ and $\mathcal{H}$ coincide.

We will indicate the way an R-lattice Λ, invariant under all $\partial^{(n)}$, determines a linear algebraic group over $O_{\bar{C}}$. Choose a basis of Λ over R. The differential module (M, ∂) is represented by a differential equation in matrix form $y' = Ay$. The iterative differential equations are $\partial^{(n)} y = A_n y$ for $n \geqq 1$. The coefficients of the matrices A_n are in R. Consider a matrix of indeterminates $(X_{i,j})$ and let D be its determinant. The F-algebra $F\left[\{X_{i,j}\}, \frac{1}{D}\right]$ is made into a differential algebra over F by $(\partial X_{i,j}) = A(X_{i,j})$. We note that $(\partial^{(n)} X_{i,j}) = A_n(X_{i,j})$ holds for any $n \geqq 1$. Let $I \subset F\left[\{X_{i,j}\}, \frac{1}{D}\right]$ be a maximal differential ideal. Then the factor ring $F\left[\{X_{i,j}\}, \frac{1}{D}\right]/I$ is "almost" a Picard-Vessiot for (M, ∂) over F. The "almost" comes from the fact that the field of constants C of F is not algebraically closed. After replacing F by the compositum of F and a finite extension of C, we may regard $F\left[\{X_{i,j}\}, \frac{1}{D}\right]/I$ as a Picard-Vessiot ring. The elements σ of the differential

Galois group $\mathscr{G}$ can be represented by the invertible matrices B with coefficients in $\bar{C}$ such that the automorphism σ of $\bar{C}F\left[\{X_{i,j}\}, \frac{1}{D}\right]$ given by $(\sigma X_{i,j}) = (X_{i,j})B^{-1}$ leaves the ideal generated by I invariant. The linear algebraic group $\mathscr{G}_O$ over $O_{\bar{C}}$ is the one induced by the σ such that B and B^{-1} have their coefficients in $O_{\bar{C}}$. Now we consider the ring $R\left[\{X_{i,j}\}, \frac{1}{D}\right]$ and the ideal $J = I \cap R\left[\{X_{i,j}\}, \frac{1}{D}\right]$. This ring and its ideal J are stable under all $\partial^{(n)}$ and under the action of $\mathscr{G}_O$. Let π denote a generator of the maximal ideal of the valuation ring of C. Then $R\left[\{X_{i,j}\}, \frac{1}{D}\right]/(\pi) = K\left[\{X_{i,j}\}, \frac{1}{D}\right]$ is an iterative differential ring over K. The image $J_1 \subset K\left[\{X_{i,j}\}, \frac{1}{D}\right]$ of the ideal J is an iterative differential ideal and moreover stable under the action of $\overline{\mathscr{G}} := \mathscr{G}_O \otimes O_{\bar{C}}/\underline{m}$. Let $J_2 \supset J_1$ be a maximal iterative differential ideal. Then $K\left[\{X_{i,j}\}, \frac{1}{D}\right]/J_2$ is “almost” a Picard-Vessiot ring of the iterative differential module $N = \Lambda/\pi\Lambda$. The finite extension of C, considered above, can be taken sufficiently large such that $K\left[\{X_{i,j}\}, \frac{1}{D}\right]/J_2$ can be seen as a Picard-Vessiot ring. The algebraic group $\mathscr{H}$ consists of the invertible matrices B such that the K-algebra automorphism σ of $K\left[\{X_{i,j}\}, \frac{1}{D}\right]$, described by $(\sigma X_{i,j}) = (X_{i,j})B^{-1}$, leaves the ideal J_2 invariant. It can be shown that $\mathscr{H}$ leaves every iterative differential ideal invariant. In particular, the ideal J_1 is invariant. Thus J_1 is invariant by both $\mathscr{H}$ and $\overline{\mathscr{G}}$. Neither inclusion seems evident. The above conjecture states however that for good choices of a differential module over F equivalent to the given one and a good choice of an R-lattice invariant under all $\partial^{(n)}$ the two groups $\mathscr{H}$ and $\overline{\mathscr{G}}$ coincide.

Examples 8.6. (1) The following example was analyzed in discussions with B. Chiarellotto and N. Tsuzuki. One considers the equation $\partial y = Ay$ with a constant matrix A with coefficients, say, in $\mathbb{C}_p$. We take F to be the completion of $\mathbb{C}_p(z)$ with respect to the Gauss norm. The residue field of F is $K = \overline{\mathbb{F}}_p(z)$. Then $\partial^{(n)}y = \frac{A^n}{n!}y$. Using the Jordan normal form of A one easily verifies that the following conditions are equivalent:

(i) The equation satisfies for every $k \geqq 1$ condition (1) of proposition 8.1.

(ii) The fundamental solution $U = 1 + \sum_{n \geqq 1} \frac{A^n}{n!}(z-t)^n$ on the generic disk has bounded coefficients.

(iii) Every eigenvalue α of A satisfies $|\alpha| \leqq p^{-1/(p-1)}$.

Suppose that A has the above equivalent properties. Then the iterative differential module over K is trivial. Indeed, this follows from $\left|\frac{\alpha^n}{n!}\right| < 1$ for all $n \geqq 1$ and all eigenvalues α of A. The determination of the differential Galois group over F is more subtle. The fundamental matrix e^{Az} is convergent and bounded by 1 for $|z| < 1$. If all the eigenvalues of A

have absolute value strictly less than $p^{-1/(p-1)}$, then e^{Az} is convergent for $|z| \leqq r$ for some $r > 1$. From this it follows that e^{Az} has its coefficients in F. If some eigenvalue α of A has absolute value $p^{-1/(p-1)}$, then this is no longer true.

To understand this situation we analyze the expression $e^{\pi z}$, where π is defined by the equation $\pi^{p-1} = -p$. In order to see that $e^{\pi z}$ does not belong to F one embeds this field into a certain algebra B. This algebra consists of the Laurent series $\sum\limits_{n=-\infty}^{\infty} a_n z^n$ having the properties:

(a) The set $\{|a_n|\}$ is bounded.

(b) $\lim\limits_{n\to+\infty} |a_n| = 0$.

A straightforward calculation shows that the equation $y' = \pi y$ has no solution $\neq 0$ in B. Thus the equation $y' = \pi y$ has only the trivial solution 0 in F. The p^{th} power of $e^{\pi z}$ is $e^{p\pi z}$ and lies in F, since its radius of convergence is strictly larger than 1. Thus the Picard-Vessiot field $F(e^{\pi z})$ of the equation $y' = \pi y$ is a p-cyclic extension of F. The equations $\partial^{(n)} y = \frac{\pi^n}{n!} y$ induce an iterative differential module over $F_p(z)$ which is trivial since $\left|\frac{\pi^n}{n!}\right| < 1$ for all $n \geqq 1$. This unsatisfactory result is due to the fact that the multiplicative group over $\overline{\mathbb{F}}_p$ has no cyclic subgroup of order p. A remedy is to consider the inhomogeneous equation $y' = \pi y + 1$ or (equivalently) the matrix differential equation $v' = \begin{pmatrix} \pi & 1 \\ 0 & 0 \end{pmatrix} v$. This matrix differential equation is the direct sum of the trivial 1-dimensional equation with the equation $y' = \pi y$. This leads to equations $\partial^{(n)} v = \begin{pmatrix} \frac{\pi^n}{n!} & \frac{\pi^{n-1}}{n!} \\ 0 & 0 \end{pmatrix} v$. The induced iterative differential equation over $\overline{\mathbb{F}}_p(z)$ has the form $\partial^{(p^k)} v = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} v$ for all $k \geqq 0$. This corresponds to the inhomogeneous iterative differential equation $\partial^{(p^k)} y = 1$ for all $k \geqq 0$. The solution $x = \sum\limits_{n \geqq 0} z^{p^n}$ is algebraic over $\overline{\mathbb{F}}_p(z)$ and satisfies the equation $x - x^p = z$ (compare with lemma 5.2). We conclude that this iterative differential equation has a p-cyclic differential Galois group. The corresponding extension is precisely the residue field extension of the above Picard-Vessiot extension $F \subset F(e^{\pi z})$.

Now we return to the general case $y' = Ay$ where all the eigenvalues of A have absolute value less than or equal to $p^{-1/(p-1)}$. Let $\alpha_1, \ldots, \alpha_s$ denote the distinct eigenvalues with absolute value $p^{-1/(p-1)}$. The Picard-Vessiot extension for the equation $y' = Ay$ is the field $F(e^{\alpha_1 z}, \ldots, e^{\alpha_s z})$. Each element $e^{\alpha_i z}$ defines a p-cyclic extension of F. These p-cyclic equations can be dependent. The differential Galois group G is the quotient of $\mathbb{F}_p^s$ with respect to the $\mathbb{F}_p$-subspace $\{(m_1, \ldots, m_s) \,|\, |m_1\alpha_1 + \cdots + m_s\alpha_s| < p^{-1/(p-1)}\}$.

After adding to the equation $y' = Ay$ a trivial differential equation (i.e., the differential module M of the equation $y' = Ay$ is replaced by $M \oplus Fe_1 \oplus \cdots \oplus Fe_s$ with $\partial e_i = 0$ for all i), one can produce a matrix differential equation $y' = By$ and an induced iterative differential equation over $\overline{\mathbb{F}}_p(z)$ which has the same differential Galois group as the equation

$y' = Ay$ over F. Moreover the Picard-Vessiot field of the iterative differential equation is the residue field extension of the Picard-Vessiot field of $y' = Ay$ over F. We note that our ad hoc method is related to the "deformation of Artin-Schreier to Kummer", or in other words the deformation of the additive group $\mathbb{G}_a$ in characteristic p to the multiplicative group $\mathbb{G}_m$ in characteristic 0 (see [S-O-S]).

(2) $\partial y = Az^{-1}y$ with A a constant matrix with coefficients in $\mathbb{C}_p$. Then $\partial^n y = A(A-1)\cdots(A-n+1)z^{-n}y$ for all n. One can verify the following results:

(i) The conditions of proposition 8.1 are satisfied for all $k \geqq 1$ if and only if the eigenvalues of A are in $\mathbb{Z}_p$.

(ii) There exists an invariant lattice if and only if A is semi-simple and all its eigenvalues are in $\mathbb{Z}_p$.

Suppose that A is a diagonal matrix with diagonal entries $\alpha_1, \dots, \alpha_d \in \mathbb{Z}_p$. The differential Galois group $\mathcal{G}$ over the field $F = \mathbb{C}_p(z)$ (or over its completion $\hat{F}$) is the subgroup of the torus $\mathbb{G}^d_{m,\mathbb{C}_p}$ consisting of the elements $(t_1, \dots, t_d)$ satisfying $t_1^{m_1} \cdots t_d^{m_d} = 1$ if and only if $m_1\alpha_1 + \cdots + m_d\alpha_d \in \mathbb{Z}$. The iterative differential module N over $K = \overline{\mathbb{F}}_p(z)$ has a basis $w_1, \dots, w_d$ such that $\partial^{(n)} w_i = \binom{\alpha_i}{n} z^{-n} w_i$ for every i and n. This example appeared already after lemma 4.1. It is easily seen that the differential Galois group $\mathcal{H}$ is the subgroup of the torus $\mathbb{G}^d_{m,\overline{\mathbb{F}}_p}$ defined by the same equations as the above group $\mathcal{G}$.

Example 8.7 (p-adic hypergeometric differential equations)**.** The hypergeometric differential equation $HG(a,b,c)$ has the form

$$z(z-1)F'' + \big((a+b+1)z - c\big)F' + abF = 0.$$

We consider this equation for $a, b, c \in \mathbb{Z}_p$ and are interested in the behaviour of the fundamental solution matrix on the "generic disk". Let $y' = Ay$ be a matrix equation representing $HG(a,b,c)$. Define the matrices A_n by the formula $\frac{1}{n!}\left(\frac{d}{dz}\right)^n y = A_n y$. The fundamental matrix on the generic disk has the form $U = 1 + \sum\limits_{n \geqq 1} A_n(t)(z-t)^n$. According to [D-G-S], proposition 8.1, U converges on the open generic disk $\{z \,\|z-t| < 1\}$ if $a, b, c \in \mathbb{Z}_p$. For $a, b, c \in \mathbb{Z}_p \cap \mathbb{Q}$ (and some further conditions on a, b, c), theorem 9.2 of [Dw] produces cases for which the fundamental matrix is also bounded on the generic disk. This is the inspiration for the next theorem. It seems possible to deduce our result as a limit case of [Dw], theorem 9.2. However we present here an elementary proof, found in discussions with F. Beukers. We start with a lemma, which is probably known.

Lemma 8.8. *Let v_p be the additive p-adic valuation on $\mathbb{Q}_p$. Let $x \in \mathbb{Z}_p$ and let n be a positive integer. Let $x = \sum x_i p^i$ and $n = \sum n_i p^i$ denote the usual p-adic expansions. A negative interval of length k for x is a sequence $i_0, i_0+1, \dots, i_0+k-1$ of non-negative integers such that*:

(a) *$x_{i_0-1} > n_{i_0-1}$ or $x_i \geqq n_i$ for all $i < i_0$.*

(b) *$x_{i_0} < n_{i_0}$.*

(c) $x_{i_0+j} \leqq n_{i_0+j}$ *for* $j = 1, \ldots, k-1$.

(d) $x_{i_0+k} > n_{i_0+k}$.

(*The length k is allowed to be infinite, in which case condition* (d) *is empty.*) *Then* $v_p\left(\binom{x}{n}\right)$ *is the sum of the lengths of the negative intervals.*

Proof. Let $\sum y_i p^i$ be the p-adic expansion of $y := x - n$. Suppose first that y is a non-negative integer. Then

$$\begin{aligned} v_p\left(\binom{x}{n}\right) &= v_p(x!) - v_p(n!) - v_p(y!) \\ &= \frac{x - \sum x_i}{p-1} - \frac{n - \sum n_i}{p-1} - \frac{y - \sum y_i}{p-1} = \frac{\sum_i (n_i + y_i - x_i)}{p-1}. \end{aligned}$$

The latter formula is easily seen to be valid in general, i.e., without assuming that x, y are non-negative integers.

One has that $n_0 + y_0$ is equal to x_0 if $n_0 \leqq x_0$ and is equal to $x_0 + p$ if $n_0 > x_0$. One concludes that $v_p\left(\binom{x}{n}\right) = 0$ if there is no negative interval. Let now $i_0, \ldots, i_0 + k - 1$ denote the first negative interval. For notational convenience we suppose $i_0 = 0$ and that k is finite. Then one has that

$$\begin{gathered} x_0 = n_0 + y_0 - p, \quad x_1 = n_1 + y_1 + 1 - p, \ldots, \\ x_{k-1} = n_{k-1} + y_{k-1} + 1 - p, \quad x_k = n_k + y_k + 1. \end{gathered}$$

This gives the contribution k for the formula of $v_p\left(\binom{x}{n}\right)$. If k is infinite then clearly x is an integer and $< n$. Thus $v_p\left(\binom{x}{n}\right) = +\infty$ as required.

After this one can make the same calculation for the next negative interval. By induction (and since n is a non-negative integer) the lemma follows. □

Theorem 8.9. *Put $X = -a$, $Y = -b$, $Z = -c$ and let the p-adic expansions of X, Y, Z be $\sum X_n p^n$, $\sum Y_n p^n$, $\sum Z_n p^n$. Suppose that for every i one has either $X_i < Z_i < Y_i$ or $Y_i < Z_i < X_i$. Then the fundamental solution of $HG(a, b, c)$ is bounded on the generic disk* (*or in other terms the matrices A_n are uniformly bounded*).

Proof. Let $y' = Ay$ be the matrix form of $HG(a, b, c)$ and, as above, the matrices A_n are given by $\frac{1}{n!}\left(\frac{d}{dz}\right)^n y = A_n y$. Let F_1, F_2 denote two independent solutions (to be specified later) of the scalar equation $HG(a, b, c)$, then $M := \begin{pmatrix} F_1 & F_2 \\ F_1' & F_2' \end{pmatrix}$ is a fundamental matrix for the equation and $\frac{1}{n!}\left(\frac{d}{dz}\right)^n M = A_n M$. F_1 satisfies the scalar equation $HG(a,b,c)$. By differentiating this equation one finds $a_m, b_m \in \mathbb{Q}_p(z)$ such that $\frac{1}{m!}\left(\frac{d}{dz}\right)^m F_1 = a_m F_1 + b_m F_1'$. The same equations hold for F_2. One concludes that A_m has the form

$$\begin{pmatrix} a_m & b_m \\ (m+1)a_{m+1} & (m+1)b_{m+1} \end{pmatrix}$$

and that

$$\begin{pmatrix} a_m \\ b_m \end{pmatrix} = \frac{1}{F_1F_2' - F_1'F_2}\begin{pmatrix} F_2' & -F_1' \\ -F_2 & F_1 \end{pmatrix}\begin{pmatrix} \frac{1}{m!}\left(\frac{d}{dz}\right)^m F_1 \\ \frac{1}{m!}\left(\frac{d}{dz}\right)^m F_2 \end{pmatrix}.$$

It suffices to show that the $\frac{1}{m!}\left(\frac{d}{dz}\right)^m F_i$, for $i = 1, 2$, are uniformly bounded with respect to the Gauss norm. We take for F_1, F_2 standard solutions of $HG(a,b,c)$ given as expansions in z, namely

$$F_1 = \sum_{n \geqq 0} \frac{(a)_n (b)_n}{(c)_n n!} z^n \quad \text{and} \quad F_2 = z^{1-c}(1-z)^{c-a-b} \sum_{n \geqq 0} \frac{(1-a)_n (1-b)_n}{(2-c)_n n!} z^n.$$

The condition on X, Y, Z implies that c is not an integer and the two series are the local solutions of $HG(a,b,c)$ at the point $z = 0$. It is easily seen that the Gauss norms of the a_m, b_m are uniformly bounded if the coefficients of these two series are uniformly bounded.

The coefficients of F_1 can be written as $\dfrac{\binom{X}{n}\cdot\binom{Y}{n}}{\binom{Z}{n}}$. A factor p in the denominator of this expression corresponds with an index i which lies in a negative interval for Z. The assumption $X_i < Z_i < Y_i$ or $Y_i < Z_i < X_i$ implies that i lies in a negative interval for X or Y. One concludes that $\dfrac{\binom{X}{n}\cdot\binom{Y}{n}}{\binom{Z}{n}} \in \mathbb{Z}_p$.

For the second hypergeometric function F_2 the X, Y, Z are replaced by $\tilde{X}, \tilde{Y}, \tilde{Z}$ with $X + \tilde{X} = -1$, $Y + \tilde{Y} = -1$, $Z + \tilde{Z} = -2$. It follows that for every i one has $\tilde{X}_i < \tilde{Z}_i < \tilde{Y}_i$ or $\tilde{Y}_i < \tilde{Z}_i < \tilde{X}_i$. This implies that the coefficients of F_2 are also in $\mathbb{Z}_p$. □

8.1. A link with Grothendieck's conjecture. One considers a number field $F \subset \bar{\mathbb{Q}}$. Its ring of integers will be denoted by O_F. For every non-zero pime ideal $\underline{p}$ of O_F we denote by $\mathbb{F}(\underline{p})$ the residue field. The field $F(z)$ is provided with the differentiation $a \mapsto \frac{da}{dz}$ and the field $\mathbb{F}(\underline{p})(z)$ is provided with the "standard" iterative derivation with respect to z. Let M

be a differential module over $F(z)$ such that its differential Galois G is finite. We note that differential Galois groups are only well defined if the field of constants is algebraically closed. In particular, the above G is actually defined as the differential Galois group of $\bar{\mathbb{Q}}(z) \otimes_{F(z)} M$ over the differential field $\bar{\mathbb{Q}}(z)$.

Proposition 8.10. (1) *For almost every non-zero prime ideal $\underline{p}$ of the ring of integers of F, the differential module M induces an iterative differential module $M(\underline{p})$ over the field $\mathbb{F}(\underline{p})(z)$ which has a finite differential Galois group.*

(2) *Let a finite Galois extension $E \supset F(z)$ be given such that $\bar{\mathbb{Q}}(z) \otimes_{F(z)} E$ is isomorphic to the Picard-Vessiot field of $\bar{\mathbb{Q}}(z) \otimes_{F(z)} M$ over $\bar{\mathbb{Q}}(z)$. Then for almost every non-zero prime ideal $\underline{p}$ the differential Galois group of $\overline{\mathbb{F}(\underline{p})}(z) \otimes M(\underline{p})$ over $\overline{\mathbb{F}(\underline{p})}(z)$ is equal to G.*

Proof. (1) Let R denote the localization of $O_F[z]$ with respect to the multipicative set of all primitive polynomials. The non-zero prime ideals of R have the form $\underline{p}R$ where $\underline{p}$ runs in the set of the non-zero prime ideals of O_F. One can show that R is invariant under all $\partial^{(n)} = \dfrac{1}{n!}\left(\dfrac{d}{dz}\right)^n$. The same holds for any localization of R. Let $E \supset F(z)$ denote a Galois extension, with Galois group H, such that the compositum $\bar{\mathbb{Q}}E$ is the Picard-Vessiot field of $\bar{\mathbb{Q}}(z) \otimes_{F(z)} M$ and such that $E \otimes_{F(z)} M$ has a basis $e_1, \ldots, e_d$ of elements with $\partial e_j = 0$ for all j. Let $\tilde{R}$ denote the integral closure of R in E. Let S denote the set of the rational prime numbers p such that p divides the order of the Galois group of E over $F(z)$ or such that there exists a prime ideal $\underline{p}$ of O_F above p for which $\underline{p}R$ ramifies in $\tilde{R}$. We claim that $\tilde{R}_S := \tilde{R}\left[\dfrac{1}{p}, p \in S\right]$ is invariant under all $\partial^{(n)}$.

Proof of the claim. Let p be a rational prime number with $p \notin S$. Consider a prime ideal $\underline{p}$ of O_F above p and a discrete valuation ring V of E lying above $R_{\underline{p}}$. It suffices to show that V is invariant under all $\partial^{(n)}$. In proving this we may replace the discrete valuation rings $R_{\underline{p}} \subset V$ by their completions $A \subset B$. The ideals $\underline{p}A$ and $\underline{p}B$ are the maximal ideals of A and B. The residue fields are $\mathbb{F}(\underline{p})(z) \subset L$. Since this extension is separable we may write $L = \mathbb{F}(\underline{p})(z)[T]/Q$ where $Q = T^d + b_{d-1}T^{d-1} + \cdots + b_0$ is a separable polynomial and the derivative of Q is invertible. Then also $B = A[t] = A[T]/P$, with $P = T^d + a_{d-1}T^{d-1} + \cdots + a_0$ such that $\bar{a}_i = b_i$ holds for all i. The derivative $P(t)'$ is invertible in B. It suffices now to prove that $\partial^{(n)}t \in B$ for all $n \geqq 0$. We will prove this by induction on n. In proving the induction step we apply $\partial^{(n)}$ to the identity $t^d + a_{d-1}t^{d-1} + \cdots + a_0 = 0$. This yields that $P(t)' \cdot \partial^{(n)}t$ is equal to a polynomial expression involving $\partial^{(i)}t$ for $i = 0, \ldots, n-1$ and some $\partial^{(m)}a_j$. This ends the proof of the claim.

We continue with the above finite set of primes S and allow S to grow in the course of the construction. Consider a lattice Λ of M over R_S which is invariant under ∂ on M (here S has grown somewhat).

Choose a basis $e_1, \ldots, e_d$ of $E \otimes M$ over E with $\partial e_j = 0$ for all j. The lattice Λ' generated over $\tilde{R}_S$ by $e_1, \ldots, e_d$ is invariant under H and all $\partial^{(n)}$. Indeed, the action of H commutes with ∂ and the kernel of ∂ on $E \otimes M$, which is $(\bar{\mathbb{Q}}e_1 + \cdots + \bar{\mathbb{Q}}e_d) \cap (E \otimes M)$, is H-invariant. Further $\tilde{R}_S$ is invariant under all $\partial^{(n)}$.

The set of H-invariant elements of Λ' is an R_S-lattice, invariant under all $\partial^{(n)}$. After enlarging S, the two lattices coincide. It follows that for every prime $p \notin S$ and prime ideal $\underline{p}$ above p, the operators $\partial^{(n)}$ induce a structure of iterative differential module on $\Lambda/\underline{p}\Lambda$. In order to see that this iterative differential module has a finite differential Galois group, we observe that the ring $\tilde{R}_S/(\underline{p})$ is isomorphic to $L \times L \times \cdots \times L$, where L is a finite Galois extension of $\mathbb{F}(\underline{p})(z)$ with Galois group equal to the decomposition subgroup of H for the prime ideal $\underline{p}$. Moreover $\Lambda/\underline{p}\Lambda \otimes \tilde{R}_S/(\underline{p})$ is isomorphic to the module $\Lambda'/\underline{p}\Lambda'$ as iterative differential modules. Therefore the iterative differential module $\Lambda/\underline{p}\Lambda \otimes L$ is trivial. In particular the differential Galois group of the iterative module $\Lambda/\underline{p}\Lambda$ is a *subgroup* of $\mathrm{Gal}\big(L/\mathbb{F}(\underline{p})(z)\big)$, the decomposition subgroup of H w.r.t. $\underline{p}$.

(2) We keep the notations of (1) above, but write G for the Galois group of E over $F(z)$. The asumption that $\bar{\mathbb{Q}}(z) \otimes_{F(z)} E = \bar{\mathbb{Q}} \otimes_F E$ is the Picard-Vessiot field of $\bar{\mathbb{Q}}(z) \otimes_{F(z)} M$ over $\bar{\mathbb{Q}}(z)$ implies that G is the differential Galois group of M. Moreover, $E \supset F(z)$ is a "geometric Galois extension". This has the consequence that for almost all primes $\underline{p}$ of O_F the ideal $\underline{p}\tilde{R}$ is prime and the residue field $\tilde{R}/\underline{p}\tilde{R}$ is a geometric Galois extension of $R/\underline{p}R = \mathbb{F}(\underline{p})(z)$. The latter means that the extension remains a Galois extension of fields after tensorization with $\overline{\mathbb{F}(\underline{p})}$ over $\mathbb{F}(\underline{p})$. See for these statements [M-M], section 10.4, p. 87. We note further that $\mathrm{Gal}\big(\bar{\mathbb{Q}} \otimes_F E/F(z)\big)$ is isomorphic to $\mathrm{Gal}(\bar{\mathbb{Q}}/F) \times \mathrm{Gal}\big(E/F(z)\big)$.

The solution space V of M is, as usual, $\ker\big(\partial, (\bar{\mathbb{Q}} \otimes_F E) \otimes_{F(z)} M\big)$. The group $\mathrm{Gal}\big(\bar{\mathbb{Q}} \otimes_F E/F(z)\big)$ acts on $(\bar{\mathbb{Q}} \otimes_F E) \otimes_{F(z)} M$ and this action commutes with ∂. Thus $\mathrm{Gal}\big(\bar{\mathbb{Q}} \otimes_F E/F(z)\big)$ acts as a group of F-linear automorphisms of V. This is also the case for the subgroup $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$. Using Hilbert 90, one finds that the F-vector space $W \subset V$, consisting of the $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$-invariant elements, has the property that the canonical map $\bar{\mathbb{Q}} \otimes_F W \to V$ is an isomorphism. The group G operates faithfullly on W as F-linear automorphisms. Fix a basis $w, \ldots, w_d$ of W and a basis $m_1, \ldots, m_d$ of M over $F(z)$. Write $w_i = \sum_j \lambda_{i,j} m_j$ with $\lambda_{i,j} \in \bar{\mathbb{Q}} \otimes_F E$. Since the w_i and the m_j are invariant under $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$, the same holds for the $\lambda_{i,j}$. Therefore the $\lambda_{i,j}$ belong to E. Further $E = F(z)(\{\lambda_{i,j}\})$ since the action of G on W is faithful.

As is part (1) of this proof, we fix an R_S-lattice $\Lambda \subset M$. After extending S, we may suppose that Λ is invariant under ∂ and $W_0 := \ker(\partial, \tilde{R}_S \otimes \Lambda)$ is a free $(O_F)_S$-module in $W = \ker(\partial, E \otimes M)$ such that the natural map $F \otimes_{(O_F)_S} W_0 \to W$ is an isomorphism. The group G acts clearly on W_0 and we may suppose (again after enlarging S) that for every prime ideal $\underline{p}$ of $(O_F)_S$ the action of G on $W_0/\underline{p}W_0$ is faithful. This $\mathbb{F}(\underline{p})$-vector space coincides with $\{a \in \tilde{R}_S/\underline{p}\tilde{R}_S \otimes_{\mathbb{F}(\underline{p})(z)} \Lambda/\underline{p}\Lambda \mid \partial^{(n)}a = 0 \text{ for all } n \geqq 1\}$. Then $\overline{\mathbb{F}(\underline{p})} \otimes W_0/\underline{p}W_0$ is the solution space of the iterative differential module $\Lambda/\underline{p}\Lambda$. Using that the action of G on this space is faithful and that the Galois extension $\tilde{R}_S/\underline{p}\tilde{R}_S \supset \mathbb{F}(\underline{p})(z)$ is "geometric", one finds that G is the differential Galois group of the iterative differential module $\Lambda/\underline{p}\Lambda$. □

A rather simple illustration of proposition 8.10 is: $M = \mathbb{Q}(z)e$ and $\partial e = \frac{t}{n} z^{-1} e$ with $t, n \in \mathbb{Z}$ having g.c.d. 1 and $n > 1$. We take $\Lambda = R_S e$ where S is the set of prime divisors of n. For a prime p not dividing n the iterative differential module $\Lambda/p\Lambda$ is given by

$\partial^{(m)} e = \binom{\overline{t/n}}{m} z^{-m} e$. The Galois group of this iterative differential module is equal to the cyclic group of order n.

Remarks. Grothendieck's p-curvature conjecture asserts that the differential Galois group of M is finite if for almost all primes p the p-curvature is zero. In our case, the p-curvature is the map $(\partial^{(1)})^p = 0$ on $\Lambda/p\Lambda$.

A variation, which might be easier to prove, of this conjecture is:

Let a differential module M over $\mathbb{F}(z)$ be given. Suppose that for almost all primes $\underline{p}$, the iterative differential module w.r.t. $\underline{p}$ exists and has a finite differential Galois group G, then the differential Galois group of M is isomorphic to G.

References

[A1] *S. Abhyankar*, Coverings of algebraic curves, Amer. J. Math. **79** (1957), 825–856.

[A2] *S. Abhyankar*, Nice equations for nice groups, Israel J. Math. **88** (1994), 1–23.

[C] *G. Christol*, Modules différentiels et Equations différentielles p-adiques, Queen's papers pure appl. math. **66** (1983).

[D] *P. Deligne*, Catégories Tannakiennes, in: The Grothendieck Festschrift 2, Progr. Math. **87** (1990), 111–195.

[D-M] *P. Deligne* and *M. Milne*, Tannakian categories, Lect. Notes Math. **900** (1982), 101–228.

[Dw] *B. Dwork*, Lectures on p-adic Differential Equations, Grundl. math. Wiss. **253**, Springer Verlag, 1982.

[D-G-S] *B. Dwork*, *G. Gerotto* and *F. J. Sullivan*, An Introduction to G-Functions, Ann. Math. Stud. **133**, Princeton University Press, 1994.

[Gi] *Ph. Gilles*, Le groupe fondamental sauvage d'une courbe affine en caractéristique $p > 0$, Courbes semi-stables et groupe fondamental en géométrie algébrique, J.-B. Bost, F. Loeser, M. Raynaud, éds., Progr. Math. **187** (1998).

[G] *A. Grothendieck*, Géométrie formelle et géométrie algébrique, Séminaire Bourbaki, exposé no 182, volume 1958/1959, Benjamin, 1966.

[H1] *D. Harbater*, Abhyankar's conjecture on Galois groups over curves, Invent. Math. **117** (1994), 1–25.

[H2] *D. Harbater*, Fundamental Groups of Curves in Characteristic p, Proceedings of the International Congress of Mathematicians, Zürich 1994, Birkhäuser Verlag, Basel (1995), 656–666.

[H-S] *H. Hasse* and *F. K. Schmidt*, Noch eine Begründung der Theorie der höhere Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten, J. reine angew. Math. **177** (1937), 215–237.

[Hu] *J. E. Humphreys*, Linear Algebraic Groups, Grad. Texts Math. **21**, Springer Verlag, 1981.

[J] *J. C. Jantzen*, Representations of Algebraic Groups, Academic Press, Inc., 1987.

[M-M] *G. Malle* and *B. H. Matzat*, Inverse Galois Theory, Springer Verlag, Berlin 1999.

[O] *K. Okugawa*, Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory, J. Math. Kyoto Univ. **2–3** (1963), 295–322.

[P1] *M. van der Put*, Recent work on differential Galois theory, Séminaire Bourbaki, 50ème année, 1997–98, no 849, Astérisque **252** (1998).

[P2] *M. van der Put*, Galois theory of differential equations, Algebraic Groups and Lie Algebras, J. Symb. Comp. **28** (1999), 441–472.

[Ra1] *J.-P. Ramis*, About the Inverse Problem in Differential Galois Theory: The Differential Abhyankar Conjecture, in: The Stokes Phenomenon and Hilbert's 16th Problem, World Scientific Publ., B. L. J. Braaksma, G. K. Immink, M. van der Put, eds., Singapore (1996), 261–278.

[Ra2] *J.-P. Ramis*, About the Inverse Problem in Differential Galois Theory: The Differential Abhyankar Conjecture, Astérisque, to appear.

[R] *M. Raynaud*, Revêtements de la droite affine en caractéristique p, Invent. Math. **116** (1994), 425–462.

[Ro] *Ph. Robba*, Solutions bornées des systèmes différentiels linéairs. Application aux fonctions hypergéométriques, Groupe d'étude d'Analyse ultramétrique **5** (1975/76), 16 p.

[S-O-S] *T. Sekiguchi*, *F. Oort* and *N. Suwa*, On the deformation of Artin-Schreier to Kummer, Ann. sci. Éc. Norm. Sup. (4) **22** (1989), 345–375.

[S1] *J.-P. Serre*, Cohomologie Galoisienne, Lect. Notes Math. **5**, Springer Verlag, 1973.

[S2] *J.-P. Serre*, Construction de revêtements étales de la droite affine en caractéristique *p*, C.R. Acad. Sci. Paris **331** (I) (1990), 341–346.

[S3] *J.-P. Serre*, Revêtements de courbes algébriques, Séminaire Bourbaki, 44ème année, 1991/92, no 749, Astérisque **206** (1992).

[Sp] *T. A. Springer*, Linear Algebraic Groups, Second Edition, Progr. Math. **9**, Birkhäuser, Boston 1998.

[W] *W. C. Waterhouse*, Introduction to Affine Group Schemes, Grad. Texts Math. **66**, Springer Verlag, 1979.

Mathematischs Institut, Universität Heidelberg, 69120 Heidelberg
e-mail: matzat@iwr.uni-heidelberg.de

University of Groningen, Department of Mathematics, P.O. Box 800, 9700 AV Groningen, The Netherlands
e-mail: mvdput@math.rug.ne

Eingegangen 12. März 2001