COMPOSITIO MATHEMATICA

MARIUS VAN DER PUT

Differential equations in characteristic p

Compositio Mathematica, tome 97, n° 1-2 (1995), p. 227-251
<http://www.numdam.org/item?id=CM_1995__97_1-2_227_0>

Compositio Mathematica **97**: 227–251, 1995.

Differential equations in characteristic p

Dedicated to Frans Oort on the occasion of his 60th birthday

MARIUS VAN DER PUT
Universiteit Groningen, Vakgroup Wiskunde, Groningen, The Netherlands

Received 28 November 1994; accepted in final form 24 April, 1995

Introduction

Let K be a differential field of characteristic $p > 0$. The aim of this paper is to classify differential equations over K and to develop Picard-Vessiot theory and differential Galois groups for those equations.

The conjecture of A. Grothendieck and its generalization by N. Katz on the comparison of differential Galois groups in characteristic 0 with reductions modulo p of differential equations are the motivations for this study of differential equations in characteristic p.

In the sequel we will suppose that $[K : K^p] = p$ and we fix a choice of $z \in K \setminus K^p$. There is a unique derivation $a \mapsto a'$ of K with $z' = 1$. Interesting examples for K are $F(z)$ and $F((z))$, where F is a perfect field of characteristic p. The ring of differential operators $\mathcal{D} = K[\partial]$ is the skew polynomial ring with the multiplication given by $\partial a = a\partial + a'$ for all $a \in K$. This ring does not depend upon the choice of the (non-zero) derivation. A linear differential equation over K is an equation of the form $v' = Av$ where v lies in the d-dimensional vector space K^d and where $A\colon K^d \to K^d$ is a K-linear map. This differential equation translates into a *differential module over* K i.e. a left $\mathcal{D}$-module M which has a finite dimension as vector space over K. We will describe the main results.

$\mathcal{D}$ turns out to be free of rank p^2 over its center $Z = K^p[\partial^p]$. Moreover $\mathcal{D}$ is an Azumaya algebra. This enables us to give a classification of $\mathcal{D}$-modules which is surprisingly similar to formal classification of differential equations in characteristic 0 (i.e. the well known classification of $\mathbf{C}((z))[\partial]$-modules). This classification can be used in the study of a differential module M over the differential field $\mathbf{Q}(z)$ with $' = \frac{d}{dz}$. A module of this type induces for almost all primes p a differential module $M(p)$ over $\mathbf{F}_p(z)$. The classification of the modules $M(p)$ contains important information about M. (See [K1]). Unlike the characteristic 0 case, skew fields appear in the classification of differential modules. The skew fields in question have dimension p^2 over their center, which is a finite extension of K^p. Skew fields of this type were already studied by N. Jacobson in [J]. (See also [A]).

Using Tannakian categories one defines the differential Galois group $D\mathrm{Gal}(M)$ of a $\mathcal{D}$-module M. It turns out that $D\mathrm{Gal}(M)$ is a commutative group of height one and hence determined by its p-Lie algebra. The p-Lie algebra in question is the (commutative) p-Lie algebra in $\mathrm{End}_{K^p}(M)$ generated by ∂^p. Let $\bar{K}$ denote the algebraic closure of K^p. Then $D\mathrm{Gal}(M)\otimes_{K^p}\bar{K}$ is isomorphic to $(\mu_{p,\bar{K}})^a \times (\alpha_{p,\bar{K}})^b$ with numbers a and b which can be obtained from the action of ∂^p on M.

Picard-Vessiot theory tries to find a "minimal" extension R of K of differential rings such that a given differential module M over K has a full set of solutions in this extension R. If one insists that R and K have the same set of constants, namely K^p, then R is a local Artinian ring with residue field K. An extension with this property will be called a minimal Picard-Vessiot ring for M. A minimal Picard-Vessiot ring for a differential equation exists (after a finite separable extension of the base field) and its group scheme of differential automorphisms coincides with the differential Galois group. A minimal Picard-Vessiot ring of a module is however not unique.

If one wants that R is a differential field L then there are new constants, at the least L^p. We will call L a Picard-Vessiot field for M if its field of constants is L^p and if L is minimal. A Picard-Vessiot field L for a differential module M also exists and is unique (after a finite separable extension of the base field). The group of differential automorphisms of this field is in general rather complicated. The p-Lie algebra of the derivations of L/K which commute with $'$ is again the (commutative) p-Lie algebra over L^p generated by the action of ∂^p on $L\otimes_K M$.

Y. André [A1,A2] has developed a very general differential Galois theory over differential rings instead of fields. His definition of the differential Galois group does not coincide with ours. However, the results announced in [A2] concerning differential Galois groups in characteristic $p > 0$ are close to our results. (See 3.2.1).

I would like to thank N. Katz for his critical remarks which led to many improvements in this paper.

1. Classification of differential modules

1.1. LEMMA. *Let Z denote the center of $\mathcal{D}$. Then:*
(1) *$Z = K^p[\partial^p]$ is a polynomial ring in one variable over K^p.*
(2) *$\mathcal{D}$ is a free Z-module of rank p^2.*
(3) *Let $Qt(Z)$ denote the field of quotients of Z, then $Qt(Z)\otimes_Z \mathcal{D}$ is a skew field with center $Qt(Z)$ and with dimension p^2 over its center.*

Proof. (1) For any $j \geqslant 1$ one has $\partial^j z = z\partial^j + j\partial^{j-1}$. In particular, $\partial^p \in Z$ and so $K^p[\partial^p] \subset Z$. Any $f \in \mathcal{D}$ can uniquely be written as

$$f = \sum_{0\leqslant i,j<p} f_{i,j} z^i \partial^j \quad \text{with all } f_{i,j} \in K^p[\partial^p].$$

Suppose that $f \in Z$. Then $0 = fz - zf = \sum f_{i,j} z^i j \partial^{j-1}$ implies that $f = \sum_{0 \leqslant i < p} f_{i,0} z^i$. Further $0 = \partial f - f\partial = \sum f_{i,0} i z^{i-1}$ implies $f \in K^p[\partial^p]$.

(2) This is already shown in the proof of (1).

(3) Let "deg" denote the degree of the elements of $\mathcal{D}$ with respect to ∂. Since $\deg(fg) = \deg(f) + \deg(g)$ the ring $\mathcal{D}$ has no zero-divisors. Hence $Qt(Z) \otimes_Z \mathcal{D}$ has no zero-divisors and since this object has dimension p^2 over $Qt(Z)$ it must be a skew field. Its center is $Qt(Z)$ as one easily sees.

1.2. LEMMA. *Let $\underline{m}$ denote a maximal ideal of Z with residue field $L := Z/\underline{m}$. Then $\mathcal{D}/\underline{m}\mathcal{D} = L \otimes_Z \mathcal{D}$ is a central simple algebra over L with dimension p^2.*

Proof. Let $I \neq 0$ be a two-sided ideal of $L \otimes_Z \mathcal{D}$. We have to show that I is the unit ideal. Take some $f \in I,\ f \neq 0$. One can write f uniquely in the form:

$$f = \sum_{0 \leqslant i,j < p} f_{i,j} z^i \partial^j \quad \text{with all } f_{i,j} \in L.$$

Then $fz - zf = \sum f_{i,j} z^i j \partial^{j-1} \in I$. Repeating this trick one obtains a non-zero element of I having the form $g = \sum_{i=0}^{p-1} g_i z^i$ with all $g_i \in L$. The element $\partial g - g\partial = \sum_{i=0}^{p-1} i g_i z^{i-1}$ lies in I. Repeating this process one finds a non-zero element of L belonging to I. This proves the statement. As in 1.1 one verifies that L is the center of $L \otimes_Z \mathcal{D}$. The dimension of $L \otimes_Z \mathcal{D}$ over L is clearly p^2.

1.3. COROLLARY. *With the notations of 1.2 one has that $L \otimes_Z \mathcal{D}$ is isomorphic to either the matrix ring $M(p \times p, L)$ or a skew field of dimension p^2 over its center L.*

Proof. The classification of central simple algebras asserts that $L \otimes_Z \mathcal{D}$ is isomorphic to a matrix algebra $M(d \times d, D)$ over a skew field D containing L. Since p is a prime number the result follows.

REMARK. Théorème 4.5.7 on page 122 of [R] and 1.2 above imply that $\mathcal{D}$ is an Azumaya algebra. This property of $\mathcal{D}$ is one explanation for the rather simple classification of $\mathcal{D}$-modules that will be given in the sequel.

1.4. CLASSIFICATION OF IRREDUCIBLE $\mathcal{D}$-MODULES

In the sequel we will sometimes write t for the element $\partial^p \in \mathcal{D}$. The elements of $Z = K^p[t]$ are seen as polynomials in t. Let M denote an irreducible left $\mathcal{D}$-module which has finite dimension over the field K. Then $\{f \in Z \mid fM = 0\}$ is a non-trivial ideal in Z generated by some polynomial F. Suppose that F has a non-trivial factorisation $F = F_1F_2$. The submodule $F_1M \subset M$ is non-zero and must then be equal to M. Now $F_2M = F_2F_1M = 0$ contradicts the definition of F. It follows that F is an irreducible polynomial. Let $\underline{m}$ denote the ideal generated by F

and let L denote its residue field. Then M can also be considered as an irreducible $L \otimes_Z \mathcal{D}$-module. If $L \otimes_Z \mathcal{D}$ happens to be a skew field then $M \cong L \otimes_Z \mathcal{D}$. If $L \otimes_Z \mathcal{D}$ is isomorphic to the matrix algebra $M(p \times p, L)$ then M is isomorphic to a vector space of dimension p over L with the natural action of $M(p \times p, L)$ on it. This proves the following:

1.4.1. LEMMA. *There is a bijective correspondence between the irreducible $\mathcal{D}$-modules of finite dimension over K and the set of maximal ideals of Z.*

We apply this to $\mathcal{D}$-modules of dimension 1. Let $\{e\}$ be a basis of a such a module. Then $\partial e = be$ for some $b \in K$. The action of ∂^p on Ke is K-linear. One defines $\tau(b)$ by $\partial^p e = \tau(b)e$. Applying ∂ to both sides of the last equation one finds $\tau(b)' = 0$. Hence τ is a map from K to K^p.

1.4.2. LEMMA.

(1) $\tau(b) = b^{(p-1)} + b^p$. *(The Jacobson identity).*

(2) $\tau \colon K \to K^p$ *is additive and its kernel is* $\{\frac{f'}{f} | f \in K^*\}$.

(3) $\tau \colon K \to K^p$ *is surjective if there are no skew fields of degree p^2 over K^p.*

Proof. (1) The map τ is easily seen to be additive. Indeed, let Ke_i denote differential modules with $\partial e_i = b_i e_i$ for $i = 1, 2$. The action of ∂ on $Ke_1 \otimes Ke_2$ is (as usual) given by $\partial(m \otimes n) = (\partial m) \otimes n + m \otimes (\partial n)$. Hence $\partial(e_1 \otimes e_2) = (b_1 + b_2)(e_1 \otimes e_2)$. Then $\partial^p(e_1 \otimes e_2) = \tau(b_1 + b_2)(e_1 \otimes e_2)$. Using that also $\partial^p(m \otimes n) = (\partial^p m) \otimes n + m \otimes (\partial^p n)$ one finds $\tau(b_1 + b_2) = \tau(b_1) + \tau(b_2)$. It suffices to verify the formula in (1) for $b = cz^i$ with $c \in K^p$ and $0 \leqslant i < p$. Let d denote $\frac{d}{dz}$ as operator on K and let cz^i also stand for the multiplication by cz^i on K. Then $\tau(cz^i) = (cz^i + d)^p(1)$. One can write $(cz^i + d)^p$ as

$$
\begin{aligned}
&c^p(z^i)^p + c^{p-1}\sum z^i \cdots z^i \, \mathrm{d}z^i \cdots z^i + c^{p-2}\sum \cdots \\
&\quad + c\sum d \cdots \mathrm{d}z^i d \cdots d + d^p
\end{aligned}
$$

Applied to 1 one finds $c^p(z^i)^p + c^{p-1} * + \cdots + c^2 * + c*$ where each $*$ is a polynomial in z (depending on i). Since $c \mapsto \tau(cz^i)$ is additive, only c and c^p can occur in the formula. The coefficient $*$ of c in the formula is easily calculated. In fact $* = 0$ for $i < p - 1$ and $* = -1$ for $i = p - 1$. This ends the verification of (1).

(2) $\tau(b) = 0$ if and only if Ke with $\partial(e) = be$ is an irreducible module corresponding to the maximal ideal (t) of $Z = K^p[t]$, where $t = \partial^p$. The trivial module $K\tilde{e}$ with $\partial\tilde{e} = 0$ is also an irreducible module corresponding to the maximal ideal (t). Hence $\tau(b) = 0$ if and only if $Ke \cong K\tilde{e}$. The last condition is equivalent to $b = \frac{f'}{f}$ for some $f \in K^*$.

(3) $a \in K^p$ lies in the image of τ if and only if there is a differential module Ke corresponding to the maximal ideal $(t - a)$ in $Z = K^p[t]$. The last condition is equivalent to $\mathcal{D}/(t - a)$ is not a skew field. This proves (3).

1.4.3. REMARKS. The classification of the irreducible $\mathcal{D}$-modules of finite dimension over K involves the classification of the skew fields of degree p^2 over its center $Z/(F) = L$. From the hypothesis $[K : K^p] = p$ it will follow that the field L can be any finite algebraic extension of K^p. Indeed, one has to show that any finite field extension L of K^p is generated by a single element. There is a sequence of fields $K^p \subset L_1 \subset L_2 \subset \cdots \subset L_n = L$ such that $K^p \subset L_1$ is separable and all $L_i \subset L_{i+1}$ are inseparable of degree p. Write $L_1 = K^p(a)$. Then $a \notin L_1^p$ and $L_2 = K^p(b)$ with $b^p = a$. By induction it follows that $L = K^p(c)$ and $[L : L^p] = p$.

1.5. SKEW FIELDS OF DEGREE p^2 IN CHARACTERISTIC p

Let L be a field of characteristic p such that $[L : L^p] = p$. Let D be a skew field of degree p^2 over its center L. The image of D in the Brauer group of L has order p according to [S2], Exercise 3 on p.167. Then $L^{1/p}$ is a neutralizing field for D, see [S2] Exercise 1 on p.165. According to [B], Proposition 3–4 on p.78, $L^{1/p}$ is a maximal commutative subfield of the ring of all $n \times n$-matrices over D for some n. Since $[L^{1/p} : L] = p$ it follows that $L^{1/p}$ is a maximal commutative subfield of D. Write $L^{1/p} = L(u)$. The automorphism σ of D given by $\sigma(a) = u^{-1}au$ has the property: there exists an element $x \in D$ with $\sigma(x) = x + 1$. (See [B], the proof of Lemma 3.1 on p.73). Hence $D = L[(u^{-1}x), u]$ where the multiplication is given by:

$$(u^{-1}x)u = u(u^{-1}x)u + 1 : \; u^p \in L \setminus L^p; \; (u^{-1}x)^p \in L.$$

Let $'$ denote the differentiation on $L^{1/p}$ given by $u' = 0$, let $\mathcal{D} := L^{1/p}[\partial]$, write $t = \partial^p$ and put $a = (u^{-1}x)^p \in L$. Then D is equal to $\mathcal{D}/(t - a)$. This leads to the following result.

1.5.1. LEMMA. *K denotes as before a field of characteristic p with $[K : K^p] = p$. An element $z \in K$ is chosen with $K = K^p(z)$. The differentiation of K is given by $z' = 1$ and $\mathcal{D} = K[\partial]$. Let F be a monic irreducible polynomial in $Z = K^p[t]$ with $t = \partial^p$.*

(1) *If $Z/(F)$ is an inseparable extension of K^p then $\mathcal{D}/(F)$ is isomorphic to $M(p \times p, Z/(F))$.*

(2) *For every finite separable field extension L of K^p and every skew field D over L of degree p^2 over its center L, there exists a monic irreducible $F \in K^p[t]$ such that $\mathcal{D}/(F) \cong D$.*

Proof. (1) Write $L = Z/(F)$. From $[K : K^p] = p$ and L inseparable over K^p one concludes that $z \in L$. Hence $L \otimes_{K^p} K$ has nilpotent elements. Then also $\mathcal{D}/(F) = L \otimes_Z \mathcal{D} \supset L \otimes_{K^p} K$ has also nilpotents elements. Since $\mathcal{D}/(F)$ can not be a skew field the statement (1) follows from 1.2.

(2) This has already been proved above.

1.5.2. LEMMA. *Let L be a finite separable extension of K^p. The cokernel of the map $\tau : L[z] \to L$, given by $\tau(b) = b^{(p-1)} + b^p$, is equal to* $\mathrm{Br}(L)[p] := \{\xi \in \mathrm{Br}(L) | \xi^p = 1\}$, *where* $\mathrm{Br}(L)$ *denotes the Brauer group of* L.

More explicitly: let $a \in L$ generate L over K^p, let the image $\xi \in$ $\mathrm{Br}(L)[p]$ *of a be not trivial and let $F \in K^p[t]$ be the monic irreducible polynomial of a over K^p. Then ξ is the image of the skew field $\mathcal{D}/(F)$ in* $\mathrm{Br}(L)[p]$.

Proof. Let L_{sep} denote the separable algebraic closure of L and let G denote the Galois group of L_{sep}/L. The following sequence is exact (see 1.4.2).

$$1 \to (L_{\mathrm{sep}}[z])^*/L_{\mathrm{sep}}^* \xrightarrow{\frac{f'}{f}} L_{\mathrm{sep}}[z] \xrightarrow{\tau} L_{\mathrm{sep}} \to 0$$

From the exact sequence of G-modules

$$1 \to L_{\mathrm{sep}}^* \to (L_{\mathrm{sep}}[z])^* \to (L_{\mathrm{sep}}[z])^*/L_{\mathrm{sep}}^* \to 1$$

one derives $((L_{\mathrm{sep}}[z])^*/L_{\mathrm{sep}}^*)^G = (L[z])^*/L^*$ and $H^1((L_{\mathrm{sep}}[z])^*/L_{\mathrm{sep}}^*) = \ker(H^2(L_{\mathrm{sep}}^*) \to H^2((L_{\mathrm{sep}}[z])^*)$. Now $H^2(L_{\mathrm{sep}})$ is the Brauer group $\mathrm{Br}(L)$ of L. Since $L_{\mathrm{sep}}[z] = L_{\mathrm{sep}}^{1/p}$ one can apply [S2], Exercice 1 on p.165, and one finds that the kernel consists of the elements $a \in \mathrm{Br}(L)$ with $a^p = 1$.

The last statement of the lemma follows from the link between τ and $\mathcal{D}/(F)$.

1.5.3. *Definition and Remarks*

A field K of characteristic p with $[K : K^p] = p$ will be called *p-split* if there is no irreducible polynomial $F \in Z$ such that $\mathcal{D}/F$ is a skew field, where $\mathcal{D} = K[\partial]$ as before.

Examples of p-split fields are: Let F be an algebraically closed field of characteristic $p > 0$. Then any finite extension K of $F(z)$ or $F((z))$ satisfies $[K : K^p] = p$ and has trivial Brauer group. Indeed, such a field is a C_1-field by Tsen's theorem and hence has trivial Brauer group (See [S1]).

1.6. LEMMA. *Let $F \in Z$ denote an irreducible monic polynomial. Put $L = Z/(F)$ and let t_1 denote the image of ∂^p in L.*

(1) *Then $\mathcal{D}/(F) = L \otimes_Z \mathcal{D}$ is isomorphic to $M(p \times p, L)$ if and only if the equation $c^{(p-1)} + c^p = t_1$ has a solution in $L[z]$. If L is an inseparable extension of K^p then the equation $c^{(p-1)} + c^p = t_1$ has a solution in $L[z]$.*

(2) *Assume that $\mathcal{D}/(F)$ is not a skew field. Let $\hat{Z}_F$ denote the completion of the localisation $Z_{(F)}$. Then the algebra $\hat{Z}_F \otimes_Z \mathcal{D}$ is isomorphic to $M(p \times p, \hat{Z}_F)$. Further there exist an element $c_\infty \in \hat{Z}_F[z]$ satisfying the equation $c_\infty^{(p-1)} + c_\infty^p = t_\infty$, where t_∞ denotes the image of ∂^p in $\hat{Z}_F$. The element c_∞ can be chosen to be a unit.*

(3) *Assume that $\mathcal{D}/(F) = Z/(F) \otimes_Z \mathcal{D}$ is a skew field. Let $Qt(\hat{Z}_F)$ denote the field of fractions of $\hat{Z}_F$. Then $Qt(\hat{Z}_F) \otimes_Z \mathcal{D}$ is a skew field of degree p^2 over*

its center $Qt(\hat{Z}_F)$. This skew field is complete with respect to a discrete valuation. The (non-commutative) valuation ring of $Qt(\hat{Z}_F) \otimes_Z \mathcal{D}$ is $\hat{Z}_F \otimes_Z \mathcal{D}$.

Proof. (1) This has already been proved. (See 1.3 and 1.5.2.)

(2) For $m \geqslant 1$ the image of ∂^p in $Z/(F^m)$ will be denoted by t_m. By induction one constructs a sequence of elements $c_m \in Z/(F^m)[z]$ such that: c_1 is the c from part (1); $c_m^{(p-1)} + c_m^p = t_m$ and $c_{m+1} \equiv c_m$ modulo F^m for every $m \geqslant 1$.

Let c_m already be constructed. Take some $d \in Z/(F^{m+1})[z]$ with image c_m and put $c_{m+1} = d + F^m e \in Z/(F^{m+1})[z]$. Write $d^{(p-1)} + d^p = t_{m+1} + F^m f$. The derivative of the left-hand side is zero and hence $f \in Z/(F^{m+1})$. Define $e = -f z^{p-1}$. Then one verifies that $c_{m+1}^{(p-1)} + c_{m+1}^p = t_{m+1}$.

The projective limit $c_\infty \in \hat{Z}_F[z]$ of the c_m satisfies again $c_\infty^{(p-1)} + c_\infty^p = t_\infty$. The ring $\hat{Z}_F[z]$ is a complete discrete valuation ring with residue field $Z/(F)[z]$. The element $c_\infty \in \hat{Z}_F[z]$ is not unique since one can add to c_∞ any element a such that $a^{(p-1)} + a^p = 0$. If c_∞ is not a unit then $d := c_\infty - z^{-1}$ is a unit and satisfies again $d^{(p-1)} + d^p = t$. Hence one can produce a c_∞ which is a unit.

On the free module $\hat{Z}_F[z]e$ over $\hat{Z}_F[z]$ of rank 1, one defines the operator ∂ by $\partial(e) = c_\infty e$. The equality $c_\infty^{(p-1)} + c_\infty^p = t_\infty$ implies that $\hat{Z}_F[z]e$ is a left $\hat{Z}_F \otimes_Z \mathcal{D}$-module. The natural map

$$\hat{Z}_F \otimes_Z \mathcal{D} \to \mathrm{End}_{\hat{Z}_F}(\hat{Z}_F[z]e) \cong M(p \times p, \hat{Z}_F)$$

is a homomorphism of $\hat{Z}_F$-algebras. It is an isomorphism because it is an isomorphism modulo the ideal (F).

(3) $\hat{Z}_F$ is a discrete complete valuation ring. A multiplicative valuation of its field of fractions can be defined by: $|0| = 0$ and $|a| = 2^{-n}$ if $a = uF^n$, where $n \in \mathbf{Z}$ and where u is a unit of $\hat{Z}_F$.

Every element a of $Qt(\hat{Z}_F) \otimes_Z \mathcal{D}$ has uniquely the form $a = \sum_{0 \leqslant i < p; 0 \leqslant j < p} a_{i,j} z^i \partial^j$. The norm of a is defined as $\|a\| = \max_{i,j}(|a_{i,j}|)$. This norm satisfies

- $\|a\| = 0$ if and only if $a = 0$.
- $\|a + b\| \leqslant \max(\|a\|, \|b\|)$.
- $Qt(\hat{Z}_F) \otimes_Z \mathcal{D}$ is complete with respect to $\| \ \|$.
- $\|ab\| = \|a\| \, \|b\|$.

The last statement follows from the assumption that $Z/(F) \otimes \mathcal{D}$ is a skew field. The other properties are trivial. The last property implies that $Qt(\hat{Z}_F) \otimes_Z \mathcal{D}$ is a skew field. Its subring of the elements of norm $\leqslant 1$ is $\hat{Z}_F \otimes \mathcal{D}$.

1.6.1. EXAMPLE. For $F = t$ the ring $\hat{Z}_F[z]$ is equal to $K[[t]]$. The expression

$$c_\infty = -\sum_{n \geqslant 0} z^{p^{n+1}-1} t^{p^n} = -z^{-1}\left(\sum_{n \geqslant 0} (z^p t)^{p^n}\right) \text{ satisfies } c_\infty^{(p-1)} + c_\infty^p = t.$$

1.7. CLASSIFICATION OF $\mathcal{D}$-MODULES OF FINITE DIMENSION

Before starting to describe the indecomposable left $\mathcal{D}$-modules of finite dimension over K, we make a general remark and introduce the notation Diff_K.

The category of the left $\mathcal{D}$-modules which are of finite dimension over K will be denoted by Diff_K. This category has a natural structure as tensor category. The tensor product $M \otimes N$ of two modules is defined to be $M \otimes_K N$ with an operation of ∂ given by

$$\partial(m \otimes n) = (\partial m) \otimes n \ + m \otimes (\partial n).$$

One easily sees that Diff_K is a rigid abelian K^p-linear tensor category in the sense of [DM].

Let M be a left $\mathcal{D}$-module of finite dimension over K. The annihilator of M is the principal ideal $(F) = \{b \in Z \mid bM = 0\}$. If F factors as F_1F_2 with coprime F_1, F_2 then the module M can be decomposed as $M = F_1M \oplus F_2M$. Indeed, write $1 = F_1G_1 + F_2G_2$ then any $m \in M$ can be written as $F_1G_1m + F_2G_2m$. Further an element in the intersection $F_1M \cap F_2M$ is annihilated by F_1 and F_2 and is therefore 0. It follows that the annihilator of an indecomposable module must have the form (F^m) where F is a monic irreducible element in Z. An indecomposable left $\mathcal{D}$-module can therefore be identified with an indecomposable finitely generated $\hat{Z}_F \otimes_Z \mathcal{D}$, annihilated by some power of a monic irreducible polynomial $F \in Z$.

Suppose that $F \in Z$ is a monic irreducible polynomial and that $\mathcal{D}/(F)$ is a skew field. $\hat{Z}_F \otimes_Z \mathcal{D}$ is, according to 1.6, a non-commutative discrete valuation ring. As in the case of a commutative discrete valuation ring one can show that every finitely generated indecomposable module, which is annihilated by a power of F, has the form

$$I(F^m) := (\hat{Z}_F \otimes_Z \mathcal{D})/(F^m) \cong \mathcal{D}/(F^m).$$

Suppose that $F \in Z$ is a monic irreducible polynomial and that $\mathcal{D}/(F)$ is not a skew field. According to 1.6, $\hat{Z}_F \otimes_Z \mathcal{D} \cong M(p \times p, \hat{Z}_F)$. Morita's theorem (See [R], Théorème 1.3.16 and Proposition 1.3.17, p. 18,19) gives an equivalence between $\hat{Z}_F$-modules and $M(p \times p, \hat{Z}_F)$-modules. In particular, every finitely generated indecomposable module over $\hat{Z}_F \otimes_Z \mathcal{D} \cong M(p \times p, \hat{Z}_F)$, which is annihilated by a power of F, has the form

$$I(F^m) := (\hat{Z}_F[z]e)/(F^m) \cong Z/(F^m)[z]e_m.$$

The structure as left $\mathcal{D}$-module is given by $\partial(e) = c_\infty e$ and $\partial(e_m) = c_m e_m$ where $c_m \in Z/(F^m)[z]$ is the image of c_∞. (See 1.6).

1.7.1. PROPOSITION. *Every left $\mathcal{D}$-module M of finite dimension over K is a (finite) direct sum $\oplus_{F,m} I(F^m)^{e(F,m)}$. The numbers $e(F,m)$ are uniquely determined by M.*

Proof. The first statement follows from the classification of the indecomposable left $\mathcal{D}$-modules of finite dimension over K. The numbers $e(F, m)$ are uniquely determined by M since they can be computed in terms of the dimensions (over K) of the kernels of multiplication with F^i on M.

1.8. K SEPARABLY ALGEBRAICALLY CLOSED

For a separable algebraically closed field K one can be more explicit about differential modules over K. For a in the algebraic closure $\bar{K}$ of K one defines $v(a) \geqslant 1$ to be the smallest power of p such that $a^{v(a)} \in K^p$. The irreducible monic polynomials in $K^p[t]$ are the $t^{v(a)} - a^{v(a)}$. The left $\mathcal{D}$-module $M(a)$ corresponding to such a polynomial can be described as follows:

If $v(a) = 1$ then $M(a) = Ke$; $\partial e = be$ and $b \in K$ is any solution of the equation $b^{(p-1)} + b^p = a$. (See 1.4.2). The corresponding differential equation is $u' = -bu$.

If $v(a) > 1$ then $M(a)$ has a basis $e, \partial e, \ldots, \partial^{v(a)-1} e$ over K and $\partial^{v(a)} e = be$. The element $b \in K$ is any solution of the equation $b^{(p-1)} + b^p = a^{v(a)}$ (See 1.4.2). The corresponding differential equation is $u^{(v(a))} = -bu$.

The module $I(t^m)$ can be described as $K[t]/(t^m)e$ where $\partial e = c_m e$ is the image in $K[t]/(t^m)$ of $c_\infty := -z^{-1} \sum_{n \geqslant 0} (z^p t)^{p^n} \in K[[t]]$ and where the differentiation on $K[t]/(t^m)$ is defined as $(\sum a_n t^n)' = \sum a_n' t^n$ (compare with 1.6). More details about the modules $I(t^m)$ will be given in Sections 5 and 6.

The modules $M(a)$ and $I(t^m)$ generate the tensor category Diff_K. This is seen by the following formulas for tensor products.

1.8.1. EXAMPLES. For $a, b \in \bar{K}$ with $v(a) \geqslant v(b)$ one has

$$M(a) \otimes M(b) \cong (M(a+b) \otimes I(t^{v(a) - v(a+b)}))^{v(b)}.$$

For a with $v(a) = 1$ one has $M(a) \otimes I(t^m) \cong I((t-a)^m)$.

More general $M(a) \otimes I(t^m) \cong I((t^{v(a)} - a^{v(a)})^c)^d$, where $c = 1$ and $d = m$ if $m \leqslant v(a)$ and for $m > v(a)$ one has $c = m - v(a)$ and $d = v(a)$.

1.9. REMARK. In [K1] the *p-curvature* of a differential module over a field of characteristic $p > 0$ is defined. One can verify that in our setup the p-curvature of a left $\mathcal{D}$-module of finite dimension over K is the K-linear map $\partial^p \colon M \to M$. The p-curvature is zero if and only if M is a left $\mathcal{D}/(\partial^p) \cong M(p \times p, K^p)$ -module. From the classification above it follows that M is a "trivial" $\mathcal{D}$-module which means that M has a basis $\{e_1, \ldots, e_s\}$ over K with $\partial e_i = 0$ for every i.

2. An equivalence of categories

For Z-modules M_1, M_2 of finite dimension over K^p one defines the tensor product $M_1 \otimes M_2$ as follows: As a vector space over K^p the tensor product is equal to

$M_1 \otimes_{K^p} M_2$. The $Z = K^p[t]$ action on it is given by $t(m_1 \otimes m_2) = tm_1 \otimes m_2 + m_1 \otimes tm_2$.

In 1.7 we have seen that the classification of $\mathcal{D}$-modules (of finite dimension over K) and the classification of the Z-modules (of finite dimension over K^p) are very similar. One can make this more precise as follows.

2.1. PROPOSITION. *Assume that the field K is p-split (see 1.5.3). There exists an equivalence $\mathcal{F}$ of the category of $Z = K^p[t]$-modules of finite dimension over K^p, onto the category of left $\mathcal{D}$-modules of finite dimension over K. Moreover $\mathcal{F}$ is exact, K^p-linear and preserves tensor products.*

Proof. We start by defining the functor $\mathcal{F}$. Let $\hat{Z}$ denote the completion of Z with respect to the set of all non-zero ideals. Then $\hat{Z} = \prod_F \hat{Z}_F$ where the product taken over all monic irreducible polynomials $F \in Z$. The modules over Z of finite dimension over K^p coincide with $\hat{Z}$-modules of finite dimension over K^p. One writes $\hat{\mathcal{D}}$ for the projective limit of all $\mathcal{D}/(G)$ where $G \in Z$ runs in the set of monic polynomials. The left $\mathcal{D}$ modules of finite dimension over K coincide with the left $\hat{\mathcal{D}}$-modules of finite dimension over K. Consider a monic irreducible polynomial $F \in Z$. By 1.6 there exists a left $\hat{\mathcal{D}}$-module $\hat{Z}_F[z]e_\infty$ with the action of ∂ given by $\partial e_\infty = c_\infty e_\infty$. This module is denoted by $\hat{\mathcal{Q}}_F$. Let the left $\hat{\mathcal{D}}$-module $\mathcal{Q}$ be the product of all $\mathcal{Q}_F$. Then $\mathcal{Q} = \hat{Z}[z]e$ and the action of ∂ on $\mathcal{Q}$ is given by $\partial e = ce$ with a $c \in \hat{Z}[z]$ satisfying $c^{(p-1)} + c^p = t$ and where $t \in \hat{Z}$ denotes the image of ∂^p.

For every Z-module M of finite dimension over K^p, one regards M as a $\hat{Z}$-module and one defines a left $\hat{\mathcal{D}}$-module $\mathcal{F}(M) := M \otimes_{\hat{Z}} \mathcal{Q}$. This module has finite dimension and can also be considered as a left $\mathcal{D}$-module of finite dimension. For a morphism $\phi : M \to N$ of Z-modules of finite dimension, $\mathcal{F}(\phi) := \phi \otimes 1 : \mathcal{F}(M) \to \mathcal{F}(N)$. This defines the functor $\mathcal{F}$. It is clear that $\mathcal{F}$ is a K^p-linear exact functor. From the description of the indecomposables of the two categories it follows that $\mathcal{F}$ is bijective on (isomorphy classes of) objects. The map $\mathrm{Hom}(M_1, M_2) \to \mathrm{Hom}(\mathcal{F}M_1, \mathcal{F}M_2)$ is injective. By counting the dimensions of the two vector spaces over K^p one finds that the map is bijective.

The functor $\mathcal{F}$ can be written in a more convenient way, namely $\mathcal{F}M := M \otimes_{K^p} Ke$ with the obvious structure as $Z[z]$-module. Since $\mathcal{F}M$ has finite dimension as vector space over K it follows that $\mathcal{F}M$ is also a $\hat{Z}[z]$-module. The structure as left $\mathcal{D}$-module is defined by $\partial(m \otimes fe) = m \otimes f'e + c(m \otimes fe)$. For two Z-modules M_1, M_2 of finite dimension over K^p one defines a K-linear isomorphism

$$(\mathcal{F}M_1) \otimes_K (\mathcal{F}M_2) = (M_1 \otimes_{K^p} Ke) \otimes (M_2 \otimes_{K^p} Ke)$$

$$\to (M_1 \otimes_{K^p} M_2) \otimes_{K^p} Ke$$

$$= \mathcal{F}(M_1 \otimes_{K^p} M_2) \text{ by } (m_1 \otimes f_1 e) \otimes (m_2 \otimes f_2 e) \mapsto (m_1 \otimes m_2) \otimes f_1 f_2 e.$$

This is easily verified to be an isomorphism of left $\mathcal{D}$-modules.

2.2. REMARKS. (1) Proposition 2.1 can also be derived from the Morita equivalence since the existence of the $\hat{\mathcal{D}}$-module $\mathcal{Q} = \hat{Z}[z]e$ implies that $\hat{\mathcal{D}} \cong M(p \times p, \hat{Z})$.

(2) If K is not split then one can still define a functor $\mathcal{F}$ from the category of Z-modules of finite dimension over K^p to Diff_K. This functor is exact, K^p-linear and is bijective on (isomorphy classes of) objects. However, $\mathcal{F}$ is not bijective on morphisms and $\mathcal{F}$ does not preserve tensor products.

(3) In the remainder of this section we study the tensor category of the modules over the polynomial ring $L[t]$ which have finite dimension as vector spaces over L.

2.3. CATEGORIES OF $L[t]$-MODULES

Let L be any field and let $L[t]$ denote the polynomial ring over L. We want to describe the category $F\mathrm{Mod}_{L[t]}$ of all $L[t]$-modules of finite dimension over L in more detail. For the terminology of Tannakian categories we refer to [DM]. The tensor product of two modules M and N is defined as $M \otimes_L N$ with the structure of $L[t]$-module given by $t(m \otimes n) = tm \otimes n + m \otimes tn$. The identity object $\mathbf{1}$ is $L[t]/(t)$. The internal Hom is given as $\underline{\mathrm{Hom}}(M, N) = \mathrm{Hom}_L(M, N)$ with the $L[t]$-module structure given by $(tl)(m) = l(tm) - t(l(m))$ for $l \in \mathrm{Hom}_L(M, N)$ and $m \in M$. It is easily verified that $F\mathrm{Mod}_{L[t]}$ is a rigid abelian L-linear tensor category. It is moreover a neutral Tannakian category over L since there is an obvious fibre functor $\omega\colon F\mathrm{Mod}_{L[t]} \to \mathrm{Vect}_L$ given as $\omega(M) = M$ as vector space over L.

Let G_L denote the affine group scheme over L which represents the functor $\mathcal{G} := \mathrm{Aut}^{\otimes}(\omega)$. The functor $\mathrm{End}^{\otimes}(\omega)$ is represented by the Lie-algebra of G_L. We consider the following cases:

(1) *L is algebraically closed and has characteristic 0.* The irreducible modules are $\{L[t]/(t-a)\}_{a \in L}$ and the indecomposable modules are

$$\{L[t]/(t-a)^n\}_{a \in L, n \geqslant 1} = \{L[t]/(t-a) \otimes L[t]/t^n\}_{a \in L, n \geqslant 1}.$$

Let R be any L-algebra and let $\lambda \in \mathcal{G}(R)$. The action of λ on $R \otimes L[t]/(t-a)$ is multiplication by an element $h(a) \in R^*$. Using that $L[t]/(t-a) \otimes L[t]/(t-b) = L[t]/(t-(a+b))$ one finds that $a \mapsto h(a)$ is a homomorphism of $L \to R^*$. The action of λ on all $L[t]/t^k$ induces an action on the inductive limit $L[t^{-1}]$ of all $L[t]/t^k$. The action of t on $L[t^{-1}]$ is defined as $t.1 = 0$ and $t.t^{-n} = t^{-n+1}$ for $n > 0$. The action of λ on $R \otimes L[t^{-1}]$ is multiplication by a certain power series $E(t) = 1 + r_1 t + r_2 t^2 + \cdots \in R[[t]]$. The action of t on $L[t^{-1}] \otimes L[t^{-1}]$ is the multiplication by $t \otimes 1 + 1 \otimes t$. Hence $L[t^{-1} \otimes 1] \subset L[t^{-1}] \otimes L[t^{-1}]$ is isomorphic to $L[t^{-1}]$. The action of λ on $R \otimes L[t^{-1}] \otimes L[t^{-1}]$ is the multiplication by $E(t \otimes 1)E(1 \otimes t)$. It follows that $E(t \otimes 1)E(1 \otimes t) = E(t \otimes 1 + 1 \otimes t)$. Since the field L has characteristic 0 and has $E(t) = \exp(rt)$ for a certain $r \in R$. Hence $\mathcal{G}(R) = \mathbf{G}_{a,L}(R) \times \mathrm{Hom}(L, R^*)$, where $\mathbf{G}_{a,L}$ denotes the additive group over L. One can write the additive group L as the direct limit of its finitely generated free subgroups Λ over $\mathbf{Z}$. Each $R \mapsto \mathrm{Hom}(\Lambda, R^*)$ is represented by a torus over L and so $R \mapsto \mathrm{Hom}(L, R^*)$ is represented by a projective limit of tori over L. This describes G_L as affine group scheme over L.

In the same way one can see that $\mathrm{End}^{\otimes}(\omega)(R)$ is isomorphic to $\mathrm{Hom}(L, R) \times R$.

For an object $M \in F\,\mathrm{Mod}_{L[t]}$ one defines $\{\{M\}\}$ as the full subcategory of $F\,\mathrm{Mod}_{L[t]}$ whose objects are the subquotients of some $M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*$. This is also a neutral Tannakian category. As above one sees finds that the group scheme G_M over L associated to $\{\{M\}\}$ can be described as follows:

Let Λ denote the subgroup of L generated by the eigenvalues of the action of t on M. The torus part T_M of G_M is the torus over L with character group Λ. If the action of t on M is semi-simple then $G_M = T_M$. If the action of t on M is not semi-simple then $G_M = T_M \times \mathbf{G}_{a,L}$.

(2) *L is algebraically closed and has characteristic $p > 0$.* The calculation of $\mathcal{G}(R)$ is similar to the case above with as exception the calculation of $E(t)$. The functional equation $E(t_1)E(t_2) = E(t_1 + t_2)$ for $E(t) \in 1 + tR[[t]]$ implies that $E(t)^p = 1$. Hence $E(t) = 1 + b_1 t + b_2 t^2 + \cdots$ with all $b_i^p = 0$. One can write E uniquely as a product $\prod_{n \geqslant 1} \exp(c_i t^i)$ with all $c_i^p = 0$. The terms with i equal to a power of p satisfy the functional equation. We want to show that only those terms occur in E. Let m be the smallest integer with $c_m \neq 0$ and m not a power of p. After removing the terms $\exp(c_i t^i)$ with $i < m$ we may suppose that $\exp(c_m t^m)$ is the first term in the expression for E. Now $c_m(t_1 + t_2)^m$ contains a term $t_1^a t_2^b$ with $a + b = m; a \neq 0 \neq b$. Also $\exp(c_m(t_1 + t_2)^m)$ contains such a term. This term can not be cancelled in $\prod_{i \geqslant m} \exp(c_i(t_1 + t_2)^i)$. Hence $E(t_1 + t_2)$ can not be equal to $E(t_1)E(t_2)$. This shows that $E(t) = \exp(r_0 t)\exp(r_1 t^p)\exp(r_2 t^{p^2}) \cdots$ where all $r_n \in R$ satisfy $r_n^p = 0$. Therefore $\mathcal{G}(R) = \mathrm{Hom}(L, R^*) \times \{r \in R \mid r^p = 0\}^{\mathbf{N}}$.

We will now describe the group scheme G_L representing $\mathcal{G}$. Let $\{x_i\}_{i \in I}$ denote a basis of L over $\mathbf{F}_p$. Consider the affine group scheme $H = \mathrm{Spec}(A)$ over L where

$$A = L[X_i, X_i^{-1}, Y_n \mid i \in I, n \in \mathbf{N}] \text{ with comultiplication given by}$$

$$X_i \mapsto X_i \otimes X_i \quad \text{and} \quad Y_n \mapsto Y_n \otimes 1 + 1 \otimes Y_n.$$

The relative Frobenius $\mathrm{Fr} : H \to H = H^{(p)}$ is the L-algebra endomorphism of A given by $X_i \mapsto X_i^p$; $Y_n \mapsto Y_n^p$. One defines G_L as the kernel of $\mathrm{Fr} : H \to H$. It is clear that G_L represents the functor $\mathcal{G}$. The affine ring of G_L is $L[x_i, y_n \mid i \in I, n \in \mathbf{N}]$ where the relations are given by $x_i^p = 1$; $y_n^p = 0$.

A similar calculation shows that $\mathrm{End}^{\otimes}(\omega)(R)$ is equal to $\mathrm{Hom}_{\mathbf{F}_p}(L, R) \oplus R^{\mathbf{N}}$.

The method above yields also the following: For an object $M \in F\,\mathrm{Mod}_{L[t]}$ the affine algebraic group associated to the neutral Tannakian category $\{\{M\}\}$ is a product of a finite number of copies of $\mu_{p,L}$ and $\alpha_{p,L}$. The p-Lie algebra of this group is the p-Lie subalgebra of $\mathrm{End}_L(M)$ over L generated by the actions of t.

(3) L *any field.* Let $\bar{L}$ denote an algebraic closure of L. The affine group scheme G_L associated to $F\,\mathrm{Mod}_{L[t]}$ has the property that $G_L(R) \to G_{\bar{L}}(R)$ is an isomorphism for every $\bar{L}$-algebra R. This implies that $G_L \otimes \bar{L}$ is isomorphic to $G_{\bar{L}}$.

The group G_N of an object $N \in F\,\mathrm{Mod}_{L[t]}$ satisfies $G_N \otimes \bar{L} \cong G_{\bar{L}\otimes N}$ as well. If the field L has characteristic $p > 0$, then (as we know already) $\mathrm{Lie}(G_N) \otimes_L \bar{L} = \mathrm{Lie}(G_{\bar{L}\otimes_L N})$ is generated by the actions of $t, t^p, t^{p^2}, \ldots,$ on $\bar{L} \otimes_L N$. Hence $\mathrm{Lie}(G_N)$ is also the (commutative) p-Lie algebra over L generated by the action of t on N.

3. Differential Galois groups

3.1. Groups of height one

In this subsection we recall definitions and theorems of [DG]. Let L be a field of characteristic $p > 0$. Let G be a linear algebraic group over L and let $\mathrm{Fr}\colon G \to G^{(p)}$ denote the relative Frobenius. The kernel H of Fr is called a *group of height one*. This can also be stated as follows: a linear algebraic group H over L has height one if $H = \ker(\mathrm{Fr}\colon H \to H^{(p)})$. We note that $\mu_{p,L} := \ker(\mathrm{Fr}\colon \mathbf{G}_{m,L} \to \mathbf{G}_{m,L})$ and $\alpha_{p,L} := \ker(\mathrm{Fr}\colon \mathbf{G}_{a,L} \to \mathbf{G}_{a,L})$ are groups of height one.

The differential Galois group $D\mathrm{Gal}(M)$ of a differential module over K turns out to be a commutative group of height one over K^p and its p-Lie algebra is the p-Lie-subalgebra of $\mathrm{End}_{K^p}(M)$ generated by the action of the curvature $t = \partial^p$ on M. According to [DG], Proposition (4.1) on p. 282, the map: $H \mapsto \mathrm{Lie}(H)$, from groups of height 1 over L to p-Lie algebras over L, is an equivalence of categories. Hence the action of t determines the differential Galois group.

In order to be more concrete we will give the construction (following [DG]) of the commutative height one group G over L which has as p-Lie algebra the p-Lie algebra generated by a linear map t on a finite dimensional vector space M over L. Let k be the dimension of this p-Lie algebra. There is a relation $t^{p^k} = a_0 t + a_1 t^p + \cdots + a_{k-1} t^{p^{k-1}}$. One considers the ring $L[x] = L[X]/(X^{p^k} - a_{k-1}X^{p^{k-1}} - \cdots - a_0 X)$ and the homomorphisms of L-algebras

$$\Delta\colon L[x] \to L[x] \otimes_L L[x];$$

$$\epsilon : L[x] \to L \quad \text{given by} \quad \Delta(x) = x \otimes x \quad \text{and} \quad \epsilon(x) = 0.$$

For any L-algebra R (commutative and with identity element) one defines $\mathcal{G}(R)$ to be the group of elements $f \in (R \otimes_L L[x])^*$ satisfying $\Delta(f) = f \otimes f$ and $\epsilon f = 1$. The functor $R \mapsto \mathcal{G}(R)$ is represented by a group scheme G over L.

This group scheme is the commutative group of height one with the prescribed p-Lie-algebra.

We note that the group G_N of part (3) of 2.3 is a commutative group of height one and that its commutative p-Lie algebra is generated by the action of t on N.

3.2. NEUTRAL TANNAKIAN CATEGORIES

Diff_K denotes, as before, the category of the differential modules over the field K, i.e. the left $\mathcal{D}$-modules which are finite dimensional over K. Let M be a differential module M over K. The tensor subcategory of Diff_K generated by M, i.e. the full subcategory with as objects the subquotients of any $M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*$, is given the notation $\{\{M\}\}$. The category $\{\{M\}\}$ is a neutral Tannakian category if there exists a fibre functor $\omega : \{\{M\}\} \to \mathrm{Vect}_{K^p}$. In this situation the affine group scheme representing the functor $\mathrm{Aut}^{\otimes}(\omega)$ is called *the differential Galois group of M and is denoted by $D\mathrm{Gal}(M)$.*

3.2.1. REMARK. In [A1, A2] one considers for a differential module M the fibre functor $\omega_1 : \{\{M\}\} \to \mathrm{Vect}_K$ given by $\omega_1(N) = N$. The differential Galois group of [A1, A2] is defined as the affine group scheme representing $\mathrm{Aut}^{\otimes}(\omega_1)$. Suppose that $\{\{M\}\}$ is a neutral Tannakian category with fibre functor $\omega : \{\{M\}\} \to \mathrm{Vect}_{K^p}$. Then one can show that $K \otimes_{K^p} \omega \cong \omega_1$. In particular the affine group scheme occurring in [A1, A2] is isomorphic to $D\mathrm{Gal}(M) \otimes_{K^p} K$. It has been shown by Y. André that his differential Galois group is a commutative group of height one over K and that its p-Lie algebra is generated over K by the p-curvature $t = \partial^p$.

3.2.2. THEOREM. *Let M be a differential module over K. Assume that for every monic irreducible $F \in Z$ appearing in the decomposition 1.7.1 of M the algebra $\mathcal{D}/(F)$ is isomorphic to $M(p \times p, Z/(F))$. Then:*

(1) *$\{\{M\}\}$ is a neutral Tannakian category.*

(2) *The differential Galois group $D\mathrm{Gal}(M)$ of M is a commutative group of height one over K^p.*

(3) *The p-Lie algebra of $D\mathrm{Gal}(M)$ is the p-Lie algebra over K^p in $\mathrm{End}_{K^p}(M)$ generated by the action of $t = \partial^p$ on M.*

Proof. (1) Let Diff^*_K be the full subcategory of Diff_K consisting of the modules $M = \oplus I(F^m)^{e(F,m)}$ such that $e(F,m) = 0$ if $\mathcal{D}/(F)$ is a skew field. We will show that Diff^*_K is closed under subquotients, duals and tensor products. The statement about subquotients is trivial. The dual of $I(F^m)$ is $I(G^m)$ with $G = \pm F(-t) \in Z = K^p[t]$. The obvious K^p-isomorphism between fields $Z/(F)$ and $Z/(G)$ extends to an isomorphism of the K^p-algebras $\mathcal{D}/(F)$ and $\mathcal{D}/(G)$. This proves the statement for duals.

It suffices to show that $I(F_1), I(F_2) \in \mathrm{Diff}^*_K$, with F_1, F_2 monic irreducible elements of Z, implies that $I(F_1) \otimes_K I(F_2) \in \mathrm{Diff}^*_K$. Write $I(F_i) = Z/(F_i)[z]e_i$

for $i = 1, 2$. The tensor product $I(F_1) \otimes_K I(F_2)$ can be identified as $K[t]$-module with $(Z/(F_1) \otimes_{K^p} Z/(F_2))[z]e_1 \otimes e_2$. Let $G_1, \ldots, G_s$ denote the monic irreducible divisors of the annihilator of $Z/(F_1) \otimes_{K^p} Z/(F_2)$. Then $Z/(F_1) \otimes_{K^p} Z/(F_2)$ has a unique direct sum decomposition $\oplus M_i$ where the annihilator of each M_i is a power of G_i. Further $I(F_1) \otimes_K I(F_2)$ decomposes as $\mathcal{D}$-module as $\oplus(M_i \otimes_{K^p} K)e_1 \otimes e_2$. The dimension of $I(G_i)$ as vector space over K is equal to $\epsilon_i \dim_{K^p}(Z/(G_i)$ where $\epsilon_i = p$ if $\mathcal{D}/(G_i)$ is a skew field and $\epsilon_i = 1$ in the other case. Using that $(M_i \otimes_{K^p} K)e_1 \otimes e_2$ has a filtration by direct sums of $I(G_i)$ one finds that all ϵ_i are 1. This proves the statement for tensor products.

Let $F\,\mathrm{Mod}^*_{K^p[t]}$ be the full subcategory of $F\,\mathrm{Mod}_{K^p[t]}$ consisting of the finite dimensional $K^p[t]$-modules M such that for every irreducible factor F of the annihilator of M the algebra $\mathcal{D}/(F)$ is not a skew field. The reasoning above also proves that $F\,\mathrm{Mod}^*_{K^p[t]}$ is closed under subquotients, duals and tensor products. The method of 2.1 yields an equivalence of categories $\mathcal{F}^* : F\,\mathrm{Mod}^*_{K^p[t]} \to \mathrm{Diff}^*_K$ which preserves tensor products. Then Diff^*_K is a neutral Tannakian category with fibre functor

$$\omega\colon \mathrm{Diff}^*_K \overset{(\mathcal{F}^*)^{-1}}{\to} F\,\mathrm{Mod}^*_{K^p[t]} \overset{\omega_2}{\to} \mathrm{Vect}_{K^p},$$

where ω_2 is the restriction of the obvious fibre functor of 2.3. The restriction of ω to $\{\{M\}\}$ is a fibre functor for the last category. This shows that $\{\{M\}\}$ is a neutral Tannakian category.

(2) and (3) follow from 3.1 and 2.3 part (3) and from the following observation: If $M = \mathcal{F}^*(N)$ then the p-Lie subalgebra of $\mathrm{End}_{K^p}(N)$ generated by t coincides with the p-Lie algebra in $\mathrm{End}_{K^p}(M)$ generated by t.

3.2.3. REMARKS. (a) If the field K is p-split then 2.1 shows that Diff_K is a neutral Tannakian category. If K is not p-split then there is an obvious fibre functor $\omega_1 \colon \mathrm{Diff}_K \to \mathrm{Vect}_K$ with $\omega_1(M) = M$ as vector space over K. This is not enough for proving that Diff_K is a neutral Tannakian category. I have not been able to verify the possibility that P. Deligne's work (see [D], 6.20) implies that Diff_K is a neutral Tannakian category.

(b) For any differential module M over K there exists a finite separable extension L of K such that the differential module $L \otimes_K M$ over L satisfies the condition of 3.2.2. Hence $D\mathrm{Gal}(L \otimes_K M)$ and its Lie-algebra are well defined.

(c) Assume that for a differential module M over K the category $\{\{M\}\}$ is a neutral Tannakian category. Then the p-Lie algebra of $D\mathrm{Gal}(M)$ is isomorphic to the p-Lie algebra $\mathcal{L}$ over K^p in $\mathrm{End}_{K^p}(M)$ is generated by the action of t on M. We indicate a proof of this.

Let $\tau : \{\{M\}\} \to \mathrm{Vect}_{K^p}$ denote a fibre functor. The p-Lie algebra $\mathrm{Lie}(D\mathrm{Gal}(M))$ of $D\mathrm{Gal}(M)$ represents $\mathrm{End}^{\otimes}(\tau)$. It suffices to produce an element $\tilde{t}$ in $\mathrm{End}^{\otimes}(\tau)(K^p)$ such that after a finite separable field extension L of K this element $\tilde{t}$ generates the p-Lie algebra $\mathrm{End}^{\otimes}(\tau)(L^p)$ over L^p and such that $\tilde{t} \mapsto t$ gives the required isomorphism $\mathrm{End}^{\otimes}(\tau)(L^p) \cong \mathcal{L} \otimes_{K^p} L^p$. The separable field extension is chosen such that $L \otimes_K M$ satisfies the condition of 3.2.2. The construction of $\tilde{t}$ goes as follows: For every $N \in \{\{M\}\}$ one defines $t_N := \tau(N \xrightarrow{t} N)\colon \tau(N) \to \tau(N)$. The family $\{t_N\}$ is by definition an element of $\mathrm{End}^{\otimes}(\tau)(K^p) = \mathrm{Lie}(D\mathrm{Gal}(M))$. This is the element $\tilde{t}$.

4. Picard-Vessiot theory

For a differential field K of characteristic 0, with algebraically closed field of constants, a quick proof of the existence of a Picard-Vessiot field goes as follows: Let the differential module M corresponds with the differential equation in matrix notation $y' = Ay$, where A is a $n \times n$-matrix with coefficients in K. On the K-algebra $B := K[X_{a,b}; 1 \leqslant a, b \leqslant n]$ one defines an extension of the differentiation of K by $(X'_{a,b}) = A(X_{a,b})$. One takes an ideal $\underline{p}$ of B which is maximal among the ideals which are invariant under differentiation and do not contain $\det(X_{a,b})$. The ideal $\underline{p}$ turns out to be a prime ideal and the field of fractions of $B/\underline{p}$ can be shown to have no new constants. Therefore this field of fractions is a Picard-Vessiot field for M. Sometimes one prefers to work with the ring $B/\underline{p}$ instead of a Picard-Vessiot field.

For a field K of characteristic $p > 0$ one can try to copy this construction. The ideal $\underline{p}$ (with the same notation as above) is almost never a radical ideal. Consider the following example: Suppose that the equation $y' = ay$ with $a \in K^*$ has only the trivial solution 0 in K. Then $B = K[X]$ and $X' = aX$. The ideal $\underline{p} = (X^p - 1)$ is maximal among the ideals which are invariant under differentiation. The differential extension $B/\underline{p}$ has the same set of constants as K, namely K^p. The image y of X in $B/\underline{p}$ is an invertible element and satisfies $y' = ay$. This motivates the following definition:

Definition of a minimal Picard-Vessiot ring

Let a differential equation $u' = Au$ over a field K as above be given, where A is a $n \times n$-matrix with coefficients in K. A commutative K-algebra R with a unit element is called a *minimal Picard-Vessiot ring for the differential equation* if:

(1) R has a differentiation (also called $'$) extending the differentiation of K.

(2) The ring of constants of R is equal to K^p.

(3) There is a fundamental matrix $(U_{i,j})$ with coefficients in R for $u' = Au$.

(4) R is minimal with respect to (3), i.e. if a differential ring $\tilde{R}$, with $K \subset \tilde{R} \subset R$, satisfies (3) then $\tilde{R} = R$.

Another possible analogue of the construction in characteristic 0 would be to consider an ideal $\underline{p}$ of B, which is maximal among the set of *prime* ideals of B which are invariant under differentiation and do not contain $\det(X_{a,b})$. Here is an example: Suppose that the equation $y' = ay$ with $a \in K^*$ has only the trivial solution 0 in K. Then $B = K[X]$ and $X' = aX$. In 6.1 part (1), one proves that: The only prime ideal invariant under differentiation is (0). The field of fractions

$L := K(X)$ contains a non-zero solution of the equation and the field of constants of L is as small as possible, namely L^p. This motivates the following definition.

Definition of a Picard-Vessiot field

Let A be an $n \times n$-matrix with coefficients in K. The field $L \supset K$ is *a Picard-Vessiot field for the equation* $u' = Au$ if

(1) L has a differentiation $'$ extending $'$ on K.

(2) The field of constants of L is L^p.

(3) There is a fundamental matrix with coefficients in L.

(4) L is minimal in the sense that any differential subfield M of L, containing K and satisfying (2) and (3), must be equal to L.

We do not have a direct proof that suitable differential ideals $\underline{p}$ of $B := K[X_{a,b}; 1 \leqslant a, b \leqslant n]$ lead to a minimal Picard-Vessiot ring and a Picard-Vessiot field. The difficulty is to controle the set of constants. The classification of differential modules over K, or more precisely over the separable algebraic closure of K, is the tool for producing minimal Picard-Vessiot rings and Picard-Vessiot fields.

5. Minimal Picard-Vessiot rings

Let a differential equation in matrix form $u' = Au$ over the field K be given. From the definition it follows that a minimal Picard-Vessiot ring R is a quotient of the ring $\tilde{R}(\Lambda) = K[x_{i,j}; 1 \leqslant i, j \leqslant n]$ defined by the relations $x_{i,j}^p = \lambda_{i,j}^p$ where $\Lambda = (\lambda_{i,j})$ is an invertible matrix with coefficients in K and where the differentiation is given by $(x'_{i,j}) = A(x_{i,j})$. The kernel of the surjective morphism $\tilde{R}(\Lambda) \to R$ is a ∂-ideal I. The ring $\tilde{R}(\Lambda)$ is a local Artinian ring. Let $\underline{m}$ denote its maximal ideal. The residue field of $\tilde{R}(\Lambda)$ is K. It follows that R is also a local Artinian ring with residue field K. The ideal

$$J := \{a \in \underline{m} |\ a^{(i)} \in \underline{m} \text{ for all } i\}$$

is the unique maximal ∂-ideal of $\tilde{R}(\Lambda)$. The natural candidate for R is then $R(\Lambda) := \tilde{R}(\Lambda)/J$.

5.1. EXAMPLES. (1) We consider the equation $u' = au$ with $a \in K$ such that the equation has only the trivial solution 0 in K. Then Λ is a 1×1-matrix with entry λ. Write $R(\lambda) := R(\Lambda)$. The ideal J turns out to be 0 and so $R(\lambda) = K[x]$ with $x' = ax$ and $x^p = \lambda^p$. One easily verifies that $R(\lambda)$ has the required properties (1)-(4). However the ∂-rings $R(\lambda_1)$ and $R(\lambda_2)$ are isomorphic if and only if $\lambda_1 = \lambda_2\mu$ for some $\mu \in K^p$. Hence we find non-isomorphic minimal Picard-Vessiot rings.

(2) Consider the equation $u' = a$ with $a \in K$. Suppose that the equation has no solution in K. The construction above gives a $R(\lambda) := R(\Lambda)$ of the form $R = K[x]$ with $x' = a$ and $x^p = \lambda^p \in K^p$. It is easy to show that $R(\lambda)$ is indeed a

minimal Picard-Vessiot ring. Further $R(\lambda_1)$ and $R(\lambda_2)$ are isomorphic if and only if $\lambda_1 - \lambda_2 \in K^p$. Again we find non-isomorphic minimal Picard-Vessiot rings.

(3) In general the ring of constants of $R(\Lambda)$ is not K^p. We give an example of this. Suppose that the equation $u' = au$ has a solution $b \in K^*$. The ideals in the differential ring $K[x]$, defined by $x^p = \lambda^p$ and $x' = ax$, are $(x-\lambda)^i$ for $i = 0, \ldots, p-1$. The derivative of $(x-\lambda)^i$ is $i(ax-\lambda')(x-\lambda)^{i-1}$. One concludes that $K[x]$ has only (0) as ∂-invariant ideal if $\lambda \neq cb$ for all $c \in (K^p)^*$. For such a λ one has $(\frac{x}{b})' = 0$ and so $K[x]$ has new constants.

5.2. THEOREM. *Suppose that a minimal Picard-Vessiot ring R exists for the differential module M over K. Then $\{\{M\}\}$ is a neutral Tannakian category. Moreover the group of the K-linear automorphisms of R commuting with $'$, considered as a group scheme over K^p, coincides with $D\mathrm{Gal}(M)$.*

Proof. As before $\{\{M\}\}$ denotes the tensor subcategory of Diff_K generated by M. Let $\tau\colon \{\{M\}\} \to \mathrm{Vect}_{K^p}$ be the functor given by $\tau(N) = \ker(\partial, R\otimes_K N)$ for $N \in \{\{M\}\}$. The definition of R implies that the canonical map $R \otimes_{K^p} \tau(N) \to R \otimes_K N$ is an isomorphism of R-modules. One knows that R is a local ring with maximal ideal $\underline{m}$ and that $R/\underline{m} = K$. By taking the tensor product over R with $K = R/\underline{m}$ one finds an isomorphism $K \otimes_{K^p} \tau(N) \to N$. Hence $K \otimes_{K^p} \tau \cong \omega_1'$, where ω_1' is the restriction to $\{\{M\}\}$ of the trivial fibre functor $\omega_1\colon \mathrm{Diff}_K \to \mathrm{Vect}_K$. This implies that τ is a fibre functor and that $\{\{M\}\}$ is a neutral Tannakian category.

The differential Galois group of M represents $\mathrm{Aut}^{\otimes}(\tau)$ and its p-Lie algebra is $\mathrm{End}^{\otimes}(\tau)(K^p)$. As remarked in 3.2.3 part (c), $\mathrm{End}^{\otimes}(\tau)(K^p)$ is generated by a certain element $\tilde{t}$ and is isomorphic with the p-Lie algebra generated by the action of t on M.

Let $\mathrm{Aut}(R/K,\ ')$ denote the group scheme of the K-linear automorphisms of R which commute with the derivation $'$ on R. Let $\mathrm{Der}(R/K,\ ')$ denote the p-Lie algebra of the derivations of R over K which commute with $'$. It is easily seen that $\mathrm{Der}(R/K,\ ')$ is the p-Lie algebra of $\mathrm{Aut}(R/K,\ ')$. There are canonical morphisms $\mathrm{Aut}(R/K,\ ') \to \mathrm{Aut}^{\otimes}(\tau)$ and $\mathrm{Der}(R/K,\ ') \xrightarrow{\alpha} \mathrm{End}^{\otimes}(\tau)(K^p)$. It suffices to show that α is an isomorphism.

We will describe the map α explicitly. The description of the map $\mathrm{Aut}(R/K,\ ') \to \mathrm{Aut}^{\otimes}(\tau)$ is similar. Let $d \in \mathrm{Der}(R/K,\ ')$. For any $N \in \{\{M\}\}$ one defines $d_N\colon R\otimes_K N \to R\otimes_K N$ by $d_N(r\otimes n) = d(r)\otimes n$. This commutes with the action of ∂ on $R\otimes_K N$. Therefore $\tau(N)$ is invariant under d_N and we also write d_N for the restriction of d_N to $\tau(N)$. The family $\{d_N\}_N$ is (by definition) an element of $\mathrm{End}^{\otimes}(\tau)(K^p)$. One defines α by $\alpha(d) = \{d_N\}_N$.

We apply the definition of α to the derivation d of R/K given by $r \mapsto r^{(p)}$. The formula $\partial^p(r\otimes n) = r^{(p)}\otimes n + r\otimes tn$ implies that d_N acts on $\tau(N)$ as $-\tau(t)$. Hence $\alpha(d) = -\tilde{t}$ (in the notation of 3.2.3 part (c)) and α is surjective.

The proof ends by showing that the map α is injective.

Let $e \in \mathrm{Der}(R/K, ')$ satisfy $\alpha(e) = 0$. One has $R \otimes_K M = R \otimes_{K^p} \tau(M)$. Choose a basis $v_1, \dots, v_d$ of $\tau(M)$ over K^p and a basis $m_1, \dots, m_d$ of M over K. Write $v_i = \sum_j r_{ji} m_j$. Then R is generated over K by the r_{ji}. By assumption $e(v_i) = 0$ for all i. Then $e(r_{ji}) = 0$ for all i, j. Hence the map e is 0 on R and $e = 0$.

5.3. THEOREM. *Let M be a differential module over K. There exists a finite separable extension K_1 of K such that the differential module $K_1 \otimes M$ over K_1 has a minimal Picard-Vessiot ring.*

The proof will be given in Section 6, since it uses the same tools as the construction of Picard-Vessiot fields.

5.4. REMARK. The theorems seem to give a satisfactory theory of minimal Picard-Vessiot rings. However, the non-uniqueness of a minimal Picard-Vessiot ring remains an unpleasant feature. Can one sharpen the definition of minimal Picard-Vessiot ring in order to obtain uniqueness?

6.5. Picard-Vessiot fields in characteristic p

Assume that L is a Picard-Vessiot field for the differential equation $u' = Au$ over K. The definition implies that L contains the field of fractions of some $B/\underline{p}$ where

(1) $B = K[X_{a,b}; 1 \leqslant a, b \leqslant n]$ with differentiation given by $(X'_{a,b}) = A(X_{a,b})$.

(2) $\underline{p}$ is a ∂-ideal which is prime and does not contain the determinant of $(X_{a,b})$.

This is used in the following examples.

6.1. EXAMPLES. (1) Consider the equation $u' = au$ with $a \in K^*$ such that there are no solutions in K^*. The ∂-ring $K[X]$ with differentiation given by $X' = aX$ contains no prime ideal ($\neq 0$) which is invariant under $'$.

Indeed, suppose that the prime ideal generated by the polynomial $f = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n$ is invariant under differentiation. Then $f' = naf$. Comparing coefficients one finds first $a_0' = naa_0$. By assumption n is divisible by p and as a consequence $a_0 \in K^p$. For $1 \leqslant i < n$ one has an equation $a_i' + iaa_i = 0$. For i not divisible by p one must have $a_i = 0$ and for i divisible by p one finds $a_i \in K^p$. The conclusion "$f = g^p$ for some $g \in K[X]$" contradicts that (f) is a prime ideal. Hence $L \supset K(X)$.

We will verify that the constants of $K(X)$ are $K^p(X^p)$. Let $f = \sum_{i=0}^{p-1} f_i X^i$ be an element with all $f_i \in K(X^p)$ and $f' = 0$. One has $f' = \sum_{i=0}^{p-1}(f_i' + iaf_i)X^i$ and so all $f_i' + iaf_i = 0$. For $i \neq 0$ there exists a j with $ij = 1 \in \mathbf{F}_p$. One sees that $(f_i^j)' = af_i^j$. If $f_i^j \in K(X^p)$ is not zero then one finds also a non zero $g \in K[X^p]$ satisfying $g' = ag$. Any non zero coefficient c of g satisfies again $c' = ac$. This is in contradiction with the assumption. Hence $f_i = 0$ for $i \neq 0$. Further $f_0' = 0$ implies that $f_0 \in K^p(X^p)$.

We conclude that $K(X)$ is a Picard-Vessiot field for the equation. The minimality property of L implies that $L = K(X)$. In other words the field $K(X)$ with $X' = aX$ is the unique Picard-Vessiot field for $u' = au$. An obvious calculation shows that the group of ∂-automorphisms of $K(X)/K$ is the multiplicative group $\mathbf{G}_m(K^p)$.

(2) Assume that the equation $y' = a$ has no solution in K. A calculation similar to the one above shows that the unique Picard-Vessiot field for the equation is $L = K(X)$ with $X' = a$. The group of ∂-automorphisms of $K(X)/K$ is $\mathbf{G}_a(K^p)$.

6.2. THEOREM. *Suppose that the field K is separably algebraically closed and that $[K : K^p] = p$. Then every differential module M over K has a unique Picard-Vessiot field.*

Proof. We will use the classification of the differential modules over K for the construction of a Picard-Vessiot field.

(1) By section 2, $M = \mathcal{F}(N) = N \otimes_{K^p} Ke$ and M is determined by the action of t on N. The action of t on N is given by the eigenvalues of t on N and by multiplicities. Since M is as a vector space over K^p a direct sum of p copies of N, we might as well consider the action of t on M as a vector space over K^p. Let Λ be the $\mathbf{F}_p$-linear subspace of the algebraic closure $\bar{K}$ of K, generated by the eigenvalues of t on M, considered as a K^p-linear map on M. This space Λ has a filtration by the subspaces $\Lambda_i := \{a \in \Lambda | v(a) \leqslant p^i\}$. We take a basis $c_1, \dots, c_r$ of Λ such that $v(c_1) \leqslant v(c_2) \leqslant \cdots \leqslant v(c_r)$ and such that each subspace Λ_i is generated by the c_j with $v(c_j) \leqslant p^i$. The tensor subcategory $\{\{M\}\}$ of Diff_K generated by M is also generated by the $M(c_i)$ and $I(t^m)$ for a certain m. In terms of equations, the Picard-Vessiot field L that we want to construct must have L^p as set of constants and must be minimal such that the equations: $u^{(v(c_i))} = b_i u$ with $b_i \in K$ such that $b_i^{(p-1)} + b_i^p = -c_i^{v(c_i)}$ and $u^{(m)} = 0$ for a suitable $m \geqslant 1$ have a full set of solutions in L.

(2) For $m = 0$ we conclude by 1.8.1 that all $v(c_i) = 1$. Then L must contain the field of fractions of a quotient of $K[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}]$ with respect to a prime ideal with is invariant under differentiation. The differentiation on $K[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}]$ is given by $X_i' = b_i X_i$ for all i. One calculates that the only prime ideal, invariant under differentiation, is (0). A further calculation shows that the field of constants of $K(X_1, \dots, X_r)$ is $K^p(X_1^p, \dots, X_r^p)$. Hence $L = K(X_1, \dots, X_r)$. This proves existence and uniqueness of the Picard-Vessiot field in this case.

(3) Consider now the indecomposable modules $I(t^m)$. The module $I(t)$ has K as its Picard-Vessiot field. It is convenient to consider the projective limit of all $I(t^m)$. This is $K[[t]]e$ with ∂ operating by $\partial(fe) = (f' + cf)e$ where f' for an $f = \sum a_n t^n \in K[[t]]$ is defined as $\sum a_n' t^n$ and where $c = -z^{-1} \sum_{n \geqslant 0} (z^p t)^{p^n}$ (see

1.6.1). By construction $K[[t]]e/(t^m)$ is isomorphic to $I(t^m)$. Suppose that there is a field extension L of K such that:

(a) L has a differentiation $'$ extending the differentiation of K.
(b) $\{r \in L | \; r' = 0\} = L^p$.
(c) There is a $f = 1 + s_1 t + s_2 t^2 + \cdots \in L[[t]]$ with $f' + cf = 0$.
(d) L is minimal with respect to (a), (b) and (c).
(e) The subfield L_m generated over K by $s_1, \ldots, s_{m-1}$ has as field of constants L^p_m.

The kernel of ∂ on $L[[t]]e$ is then $L^p[[t]]fe$. For every $m \geqslant 1$ the kernel of ∂ on $L[[t]]e/(t^m)$ is equal to $L^p[[t]]fe/(t^m)$. This has the correct dimension over L^p. Hence the subfield L_m of L is a Picard-Vessiot field for $I(t^m)$. Further L is the union of the L_m.

As a tool for finding f we use the Artin-Hasse exponent E. For any ring R of characteristic p we consider $W(R)$ the group of Witt vectors over R and the Artin-Hasse exponent $E \colon W(R) \to R[[t]]^*$. For a Witt vector $(r_0, r_1, r_2, \ldots)$ one has

$$E(r_0, r_1, r_2, \ldots) = F(r_0 t) F(r_1 t^p) F(r_2 t^{p^2}) \cdots$$

where $F(T) = \prod_{(n,p)=1} (1 - T^n)^{\mu(n)/n} \in \mathbf{F}_p[[T]]$. See [DG] p.617 for more details. Suppose that $B \supset K$ is an extension of differential rings and that the $r_i \in B$. Using this formula for E one shows that

$$E(r_0, r_1, \ldots)' = E(r_0, r_1, \ldots) (\sum_{k \geqslant 0} (\sum_{i+j=k} r_i' r_i^{p^j - 1}) T^{p^k}).$$

Consider the ring $A = K[A_0, A_1, \ldots]$ with a differentiation $'$ extending the one of K and defined recursively by the formulas

$$\sum_{i+j=k} A_i' (A_i)^{p^j - 1} = -z^{p^{k+1} - 1} \quad \text{for all } k \geqslant 0.$$

Then $f := E(A_0, A_1, \ldots)$ satisfies $\frac{f'}{f} = -c$. Suppose that we have shown:
(f) The ring A has no $'$-invariant prime ideals.
(g) The ring A has as constants A^p.

The two statements imply that the field of fractions L of A satisfies (a)–(e) and that L_m is the unique Picard-Vessiot field for $I(t^m)$.

We will prove (f) and (g) for $K[A_0, \ldots, A_n]$ by induction on n. The case $n = 0$ is in fact done in 6.1 part (2). We will use the formula $A_{n-1}^{(p^n)} = 1$ and that the differentiation $r \mapsto r^{(p^{n+1})}$ is zero on $K[A_0, \ldots, A_{n-1}]$.

The proof of (f): Let $f \in K[A_0, \ldots, A_n]$ belong to a $'$-invariant prime ideal $\underline{p}$ of $K[A_0, \ldots, A_n]$. By induction $\underline{p} \cap K[A_0, \ldots, A_{n-1}] = 0$. Write $f = \sum c_i A_n^i$ with $c_i \in K[A_0, \ldots, A_{n-1}]$. We may assume that the degree of f in A_n is minimal. Define the derivation d by $d(a) = a^{(p^{n+1})}$. Then $d(f) = 0$ and so $f \in K[A_0, \dots, A_{n-1}][A_n^p]$. Then $f' = 0$ by minimality. Induction shows that all $c_i \in (K[A_0, \dots, A_{n-1}])^p$. Hence f is a pth power of an element which also belongs to $\underline{p}$. This contradicts the minimality of the degree of f.

The proof of (g): Suppose now that $f = \sum c_i A_n^i \in K[A_0, \dots, A_n]$ satisfies $f' = 0$. Then also $f^{(p^{n+1})} = 0$ and so $f \in K[A_0, \dots, A_{n-1}][A_n^p]$. Then $f' = 0$ implies that all $c_i' = 0$. By induction all $c_i \in (K[A_0, \dots, A_{n-1}])^p$. This shows $f \in (K[A_0, \dots, A_n])^p$.

The conclusion of (3) is that $K(A_0, \dots, A_n)$ is the unique Picard-Vessiot field for $I(t^m)$ if $p^{n+1} < m \leqslant p^{n+2}$.

(4) In the general case where $\Lambda \neq 0$ and with any $m \geqslant 1$, one finds that any Picard-Vessiot field L must contain the field of fractions of a quotient of the differential ring $K[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}, A_0, \dots, A_n]$. The differentiation is given by the formula above for the A_m' and by $X_i' = f_i X_i$ where $f_i \in K[A_0, \dots, A_n]$ are (and can be!) chosen such that $X_i^{(v(c_i))} = b_i X_i$. Again one can see that this differential ring has no invariant prime ideals $\neq (0)$ and that the constants of its field of fractions N is N^p. By minimality N is the unique Picard-Vessiot field for M.

6.3. COROLLARY. *Let M be a differential module over the field K then there exists a finite separable extension K_1 of K such that the differential module $K_1 \otimes M$ over K_1 has a unique Picard-Vessiot field.*

Proof. K_{sep} will denote the separable algebraic closure of K. The differential module $K_{\text{sep}} \otimes M$ over K_{sep} has a unique Picard-Vessiot field L. This field is the field of fractions of a differential ring $K_{\text{sep}}[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}, A_0, \dots, A_n]$. Let $K_1 \subset K_{\text{sep}}$ be a finite extension of K such that the formulas for the derivatives of the $X_1, \dots, X_r, A_0, \dots, A_n$ have their coefficients in K_1. The ring $B := K_1[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}, A_0, \dots, A_n]$ is a differential ring. Using 6.2 one finds that any element $f \in B$ with $f' = 0$ lies in B^p. The field of fractions L_1 of B is therefore a Picard-Vessiot field for $K_1 \otimes M$ over K_1.

Let L_2 be another Picard-Vessiot field for $K_1 \otimes M$ over K_1. Then the compositum $K_{\text{sep}} L_2$ is a Picard-Vessiot field for $K_{\text{sep}} \otimes M$ over K_{sep}. Using 6.2 we may identify $K_{\text{sep}} L_2$ with L. Hence L_2 is a subfield of L. This subfield must contains the field of fractions of a quotient of $K_1[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}, A_0, \dots, A_n]$ by some prime ideal which is invariant under differentiation. We know that the only possible prime ideal is (0). Hence L_2 contains the field of fractions L_1 of $K_1[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}, A_0, \dots, A_n]$. By minimality one has $L_2 = L_1$.

6.4. THE PROOF OF 5.3. *Let M be a differential module over K. There exists a finite separable extension K_1 of K such that the differential module $K_1 \otimes M$ over K_1 has a minimal Picard-Vessiot ring.*

Proof. We will start by working over the separable algebraic closure K_{sep} of K. In the proof of 6.2 we have constructed a differential ring

$$K_{\text{sep}}[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}, A_0, \dots, A_n].$$

The ideal generated by $X_1^p - 1, \dots, X_r^p - 1, A_0^p, \dots, A_n^p$ is invariant under differentiation. The factor ring is denoted by $R := K_{\text{sep}}[x_1, \dots, x_r, a_0, \dots, a_n]$. We claim that this is a minimal Picard-Vessiot ring for $K_{\text{sep}} \otimes M$ over K_{sep}.

Define the derivation d on R by $d(r) = r^{(p^m)}$ with m sufficiently big. Then d is 0 on $K_{\text{sep}}[a_0, \dots, a_n]$ and $d(x_i) = \beta_i x_i$ for certain elements $\beta_i \in K_{\text{sep}}^p$. The choice of the basis of Λ (see the proof of 6.2) implies that the β_i are linearly independent over $\mathbf{F}_p$. Apply d to an element $\sum c(\underline{n}) x_1^{n_1} \cdots x_r^{n_r} \in R$ with $c(\underline{n}) \in K_{\text{sep}}[a_0, \cdots a_n]$ and all $0 \leqslant n_i \leqslant p-1$. If the result is 0 then all $c(\underline{n})$ are 0 for $\underline{n} \neq \underline{0}$. Hence $K_{\text{sep}}[a_0, \dots, a_n]$ is the kernel of d. In order to find the constants of $K_{\text{sep}}[a_0, \dots, a_n]$ we apply the derivation $d_n \colon r \mapsto r^{(p^{n+1})}$ to this ring. The kernel is $K_{\text{sep}}[a_0, \dots, a_{n-1}]$ since $d_n(a_i) = 0$ for $i = 0, \dots, n-1$ and $d_n(a_n) = 1$. By induction on n one finds that K_{sep}^p is the set of constants of $K_{\text{sep}}[a_0, \dots, a_n]$. Hence R is a minimal Picard-Vessiot ring for M.

Let $K_1 \subset K_{\text{sep}}$ be a finite extension of K such that the formulas for the derivatives of the $X_1, \dots, X_r, A_0, \dots, A_n$ have their coefficients in K_1. It is easily seen that $K_1[x_1, \dots, x_r, a_0, \dots, a_n]$ is a minimal Picard-Vessiot ring for $K_1 \otimes M$ over K_1.

6.5. Derivations and automorphisms of PV-fields

Assume that L is the Picard-Vessiot field of the differential module M over K. Let $\text{Der}(L/K, {}')$ denote the p-Lie algebra over L^p of the derivations of L over K commuting with $'$. Then d defined by $d(a) = a^{(p)}$ is an element of $\text{Der}(L/K, {}')$. It is an exercise to show that d generates $\text{Der}(L/K, {}')$ as p-Lie algebra over L^p. This means that $\text{Der}(L/K, {}')$ has the expected structure of commutative p-Lie algebra over L^p generated by the p-curvature.

The group $\text{Aut}(L/K, {}')$, of all K-automorphisms of L commuting with $'$, is in general a rather complicated object. As an example we give some calculations for $L = K(A_0, \dots, A_n)$, the Picard-Vessiot field of the equation $u^{(m)} = 0$ with $p^{n+1} < m \leqslant p^{n+2}$.

W_n denotes the group of Witt vectors of length n. Let σ be an ∂-automorphism of L over K. The action of σ is determined by the action on $E(A_0, \dots, A_n) \in L[t]/(t^m)$. Clearly

$$\sigma E(A_0, \dots, A_n) = E(\sigma A_0, \dots, \sigma A_n) = E(A_0, \dots, A_n).E(y_0, \dots, y_n)$$

for a certain elements $y_i \in L$. Since σ commutes with $'$ one concludes that $E(y_0, \dots, y_n)' = 0$ and all $y_i \in L^p$. With $\oplus$ denoting the addition in W_n one has

$$(\sigma A_0, \dots, \sigma A_n) = (A_0, \dots, A_n) \oplus (y_0, \dots, y_n).$$

Hence we can see $\text{Aut}(L/K, {}')$ as a subgroup of $W_n(L^p)$. The set of the σ's with all $y_i \in K^p$ is clearly a subgroup of $\text{Aut}(L/K, {}')$ isomorphic to $W_n(K^p)$. Therefore

$W_n(K^p) \subset \mathrm{Aut}(L/K,\ ') \subset W_n(L^p)$. If $n \geqslant 1$ then $W_n(K^p) \neq \mathrm{Aut}(L/K,\ ') \neq W_n(L^p)$.

Indeed, take $n = 1$ and $L = K(A_0, A_1)$. Any $\sigma \in \mathrm{Aut}(L/K,\ ')$ must have the form

$$\sigma A_0 = A_0 + y_0 \quad \text{and}$$

$$\sigma A_1 = A_1 - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} A_0^i y_0^{p-i} + y_1 \quad \text{with} \quad y_0, y_1 \in L^p.$$

For given $y_0, y_1 \in L^p$, the σ given by the formulas above is an endomorphism of L/K commuting with $'$. The choice $y_0 = A_0^p$ and $y_1 = 0$ gives an endomorphism which has no inverse. Any choice $y_0 \in K^p$ and $y_1 \in L^p$ leads to an automorphism. Thus $W_1(K^p) \neq \mathrm{Aut}(L/K,\ ') \neq W_1(L^p)$.

6.6. REMARKS. (1) It is likely that existence and uniqueness of a Picard-Vessiot field for a differential module M over K hold without going to a finite separable extension of K. Similarly, the existence of a minimal Picard-Vessiot ring for M is likely to hold over K instead over a finite separable extension of K.

(2) *Other fields of characteristic p.*

Let K be a field of characteristic p such that $[K : K^p] = p^r$. The universal differential module $K \xrightarrow{d} \Omega_K$ is a vector space over K of dimension r. One can consider certain partial differential equations over K, namely K-modules M with an integrable connection $\nabla\colon M \to \Omega_K \otimes_K M$. The classification of such modules and the corresponding differential Galois theory is quite analogous to the case $r = 1$ that we have studied in detail.

Another interesting possibility is to consider differential equations over a differential field K satisfying $[K : K^p] < \infty$ and with field of constants K^p. For fields of that type it can be shown that $\mathcal{D}$ is a finite module over its center.

References

[A] Amitzur, S. A.: Division algebras. A survey, *Comtemporary Mathematics*, Volume 13 (1982) 3–26.

[A1] André, Y.: Quatre descriptions des groupes de Galois différentielles, Séminaire d'algèbre de Paris 86/87, *Lect. Notes in Math.* 1296 (1987).

[A2] André, Y.: Notes sur la théorie de Galois différentielles, preprint IHES/M/89/49, (1989).

[B] Blanchard, A.: Les corps non commutatifs, *Collection Sup 9*, Presses Universitaires de France, (1972).

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

[DG] Demazure, M., Gabriel, P.: *Groupes algébriques 1*, North Holland, Amsterdam, (1970).

[DM] Deligne, P., Milne, J.: Tannakian categories, *Lect. Notes in Math.* 900, (1982) 101–228.

[J] Jacobson, N.: p-algebras of exponent p, *Bull. Am. Math. Soc.* 43 (1937) 667–670.

[K1] Katz, N.: A conjecture in the arithmetic theory of differential equations, *Bull. Soc. Mat. France.* 110 (1982) 203–239.

[K2] Katz, N.: On the calculations of some differential Galois groups, *Invent. Math.* 87 (1987) 13–61.

[R] Renault, G.: Algèbre non commutative, *Collection "Varia Mathematica"*, Gauthiers-Villars, (1975).

[S1] Serre, J-P.: Cohomologie Galoisienne, *Lect. Notes in Math.* 5 (1973).

[S2] Serre, J-P.: Corps locaux, Hermann, Paris, (1968).