Galois Groups and Fundamental Groups
MSRI Publications
Volume **41**, 2003

Constructive Differential Galois Theory

B. HEINRICH MATZAT AND MARIUS VAN DER PUT

Abstract. We survey some constructive aspects of differential Galois theory and indicate some analogies between ordinary Galois theory and differential Galois theory in characteristic zero and nonzero.

Contents

Introduction

Classical Theory

Modular Theory

References

INTRODUCTION

The aim of this article is to survey some constructive aspects of differential Galois theory and to indicate some analogies between ordinary Galois theory and differential Galois theory in characteristic zero and nonzero. We hope it may serve as an appetizer for people who work in ordinary Galois theory but are not familiar with the differential analogue.

In the first part we start with a constructive foundation of the Picard–Vessiot theory in characteristic zero mimicking Kronecker's construction of root fields.

This leads to a smallest differential field extension (with no new constants) containing a full system of solutions of a (system of) linear differential equation(s) with a linear algebraic group as differential Galois group. Then we explain the Galois correspondence between the intermediate differential fields of a Picard–Vessiot extension and the Zariski closed subgroups of the differential Galois group. On the way we deal with the question of solvability by elementary functions, comparable to the question of solvability by radicals in ordinary Galois theory. In Chapter 3 we describe the link between the differential Galois group and the monodromy group over the complex numbers generalizing the effective version of Riemann's existence theorem used in (ordinary) inverse Galois theory [MM]. Further we recall the solution of the inverse differential Galois problem over $\mathbb{C}$ in the case of monodromy groups (Riemann–Hilbert problem) given by Plemelj (1908) and its completion by Tretkoff and Tretkoff [TT] for differential Galois groups. Finally in Chapter 4 we outline the constructive solution of the inverse problem for connected groups over general algebraically closed fields of characteristic 0 recently given by Mitschi and Singer [MS].

In the second part we develop a Picard–Vessiot theory in positive characteristic. For this purpose ordinary derivations — these cause new constants in any nonalgebraic extension — are replaced by a family of higher derivations, called iterative derivations in the original paper of Hasse and Schmidt [HS]. They have already been used earlier by Okugawa [Oku] to outline a Picard–Vessiot theory in characteristic $p > 0$. Here we follow a new approach developed in [MP] based on the study of iterative differential modules (ID-modules) and corresponding projective systems. This allows us to construct (iterative) Picard–Vessiot extensions in the same formal way as in characteristic 0. We again obtain as ID-Galois groups reduced linear algebraic groups defined over the field of constants and we establish a Galois correspondence between the intermediate ID-fields of a Picard–Vessiot extension and the reduced closed subgroups of the corresponding ID-Galois group. In Chapter 7 we determine the structure of ID-modules and ID-Galois groups over local fields — these are trigonalizable extensions of connected solvable groups by finite local Galois groups — and solve the inverse problem for these groups. Finally in Chapter 8 we solve the inverse problem of differential Galois theory over global fields of positive characteristic and prove an analogue of the Abhyankar conjecture for differential Galois extensions.

The main sources (sometimes used without a reference) are the introductory texts of Magid [Mag] and the second author [Put2] for the classical part, for the modular part there are the research paper [MP] combined with the notes [Mat]. Different approaches for differential equations in positive characteristic have been developed, for example, by Katz [Kat2] and André [And].

Acknowledgement. The authors thank the Mathematical Science Research Institute in Berkeley (MSRI) for its hospitality and support during the research program Galois Groups and Fundamental Groups, and for giving us the opportunity to present most of the results given in this article in a series of lectures at the MSRI. Among other things, the solution of the inverse problem of ID-Galois theory for connected groups over global fields (Theorem 8.4) and the proof of the connected differential Abhyankar conjecture (Corollary 8.5) have been achieved during our stay in Berkeley.

CLASSICAL THEORY

1. Linear Differential Equations

1.1. Derivations. In this first section we collect some well-known facts on derivations and differential rings. The proofs can be found, for example, in [Jac], Chapter 8.15.

Let R be a commutative ring (always with unit element). A map $\partial : R \to R$ is called a *derivation* of R if

$$\partial(a+b) = \partial(a) + \partial(b) \quad \text{and} \quad \partial(a \cdot b) = \partial(a)b + a\partial(b)$$

for all $a, b \in R$. An element $c \in R$ with $\partial(c) = 0$ is a *differential constant.* The set of differential constants forms a ring denoted here by $C(R)$. Further a ring R together with a derivation ∂ of R is called a *differential ring* (D-ring) (R, ∂).

From the definition we immediately obtain the formulas

$$\partial\left(\frac{a}{b}\right) = \frac{1}{b^2}(\partial(a)b - a\partial(b)) \qquad \text{in case } b \in R^\times, \tag{1–1}$$

$$\partial^k(ab) = \sum_{i+j=k} \binom{k}{i} \partial^i(a)\partial^j(b) \tag{1–2}$$

for $a, b \in R$ and $i, j, k \in \mathbb{N}$.

Now let (R, ∂_R) and (S, ∂_S) be two D-rings. Then a ring homomorphism $\varphi \in \mathrm{Hom}(R, S)$ is called a *differential homomorphism* (D-homomorphism) if $\varphi \circ \partial_R = \partial_S \circ \varphi$. The set of all D-homomorphisms is denoted by $\mathrm{Hom}_{\mathrm{D}}(R, S)$. An ideal A of R with $\partial_R(A) \subseteq A$ is called a *differential ideal* (D-ideal). It can be shown that in case R is a Ritt algebra, i.e., $\mathbb{Q} \leq R$, the nil radical of any D-ideal again is a D-ideal. A corresponding statement does not hold anymore in positive characteristic (see [Kap], I.4).

If (R, ∂_R) is a D-ring and $S \subseteq R$ a multiplicatively closed subset with $0 \notin S$ we have a canonical map $\lambda_S : R \to S^{-1}R$ from R into the quotient ring $S^{-1}R$. Then by (1–1) there exists a uniquely determined derivation $\partial_{S^{-1}R}$ of $S^{-1}R$ such that $\partial_{S^{-1}R} \circ \lambda_S = \lambda_S \circ \partial_R$. In particular, if R is an integral domain, ∂_R can be extended uniquely to its quotient field $F = \mathrm{Quot}(R)$. A field F with derivation ∂_F is called a *differential field* (D-field).

Finally, let E/F be a finitely generated separable field extension of a D-field (F, ∂_F) with separating transcendence basis $x_1, \dots, x_r$. Then for all $y_1, \dots, y_r \in E$ there exists exactly one extension ∂_E of ∂_F on E with $\partial_E(x_i) = y_i$ for all i. In particular, an extension of ∂_F to a separably algebraic field extension E/F always exists and is unique.

1.2. Linear differential operators. From now on, (F, ∂_F) denotes a D-field of characteristic 0. Then $\ell := \sum_{k=0}^{n} a_k \partial^k$ with $a_k \in F$ and $a_n \neq 0$ is called a *linear differential operator* of degree $\deg(\ell) = n$ over F (D-operator) and $F[\partial]$ is the (noncommutative) *ring of linear differential operators* over F. Now let (E, ∂_E) be a D-field extension of F. Then an element $y \in E$ is called a *solution* of ℓ if y is a solution of the homogeneous linear differential equation

$$\ell(y) = \sum_{k=0}^{n} a_k \partial^k(y) = 0. \tag{1–3}$$

The set of all solutions of ℓ in E forms a vector space over the field of constants $C(E)$ of E and is named the *solution space* $V_E(\ell)$ *of* ℓ *in* E.

PROPOSITION 1.1. *Let* (F, ∂_F) *be a D-field of characteristic* 0 *and* $\ell \in F[\partial]$ *a D-operator. Then for all D-field extensions* $(E, \partial_E) \geq (F, \partial_F)$ *the solution space* $V_E(\ell)$ *of* ℓ *is a vector space over* $C(E)$ *with* $\dim_{C(E)}(V_E(\ell)) \leq \deg(\ell)$.

The proof of Proposition 1.1 relies on the fact that the *Wronskian determinant*

$$\mathrm{wr}(y_1, \dots, y_n) := \det(\partial^{i-1}(y_j))_{i,j=1}^{n} \tag{1–4}$$

of linearly independent elements $y_j \in E$ over $C(E)$ is different from zero (see [Mag], Theorem 2.9).

In the special case of equality in Proposition 1.1, $V_E(\ell)$ is called a *complete solution space*. The first fundamental question now concerns the existence of a D-field extension E/F such that $V_E(\ell)$ is a complete solution space. However, before answering this question we want to study some preliminary examples and to introduce a slightly more general setting.

For the examples let $F = \mathbb{C}(t)$ be the field of rational functions over the complex numbers $\mathbb{C}$ with derivation $\partial = \partial_t := d/dt$ and $E \geq F$ the field of analytic functions.

EXAMPLE 1.2.1. Take $\ell = \partial^1 - a \in F[\partial]$ with $a \in \mathbb{C}^\times$. Then $\ell(y) = 0$ if $\partial(y) = ay$. Therefore the solution space is given by $V_E(\ell) = \mathbb{C} \cdot \exp(at)$ and every nontrivial solution is transcendental over E.

EXAMPLE 1.2.2. In the case $\ell = \partial^1 - \frac{1}{nt}$ with $n \in \mathbb{N}$ any solution of ℓ in E belongs to $V_E(\ell) = \mathbb{C}\sqrt[n]{t}$ and therefore is algebraic over F.

EXAMPLE 1.2.3. A solution of the inhomogeneous differential equation $\partial(y) = f \in F^\times$ is also a solution of the degree 2 homogeneous differential equation $\ell(y) = \partial^2(y) - f^{-1}\partial(f)\partial(y) = 0$. The solution space of the latter consists of

$V_E(\ell) = \mathbb{C} \oplus \mathbb{C}g$ where $g = \int f dt$ denotes a solution of the inhomogeneous equation. This may be an element of F as for $f = 1$ or transcendental over F as for $f = \frac{1}{t}$.

These examples show that solutions and solution spaces of linear differential equations may algebraically behave very differently.

1.3. Systems of linear differential equations. Any solution $y \in E$ of $\ell \in F[\partial]$ leads to a solution $\mathbf{y} = (y, \partial^1(y), \ldots, \partial^{n-1}(y))^{\mathrm{tr}} \in E^n$ of the matrix differential equation

$$\partial(\mathbf{y}) = A_\ell \mathbf{y}, \quad \text{where } A_\ell = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & \cdots & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix} \in F^{n\times n},$$

and vice versa. Now we start with an arbitrary $A \in F^{n\times n}$ and define the *solution space* of A to be

$$V_E(A) := \{\mathbf{y} \in E^n \mid \partial(\mathbf{y}) = A\mathbf{y}\}.$$

This again is a vector space over the constant field of E of dimension less than or equal to n.

Two matrices A and $B \in F^{n\times n}$ are called *differentially equivalent*, or *D-equivalent*, if every solution $\mathbf{z} \in V_E(B)$ can be transformed into a solution $\mathbf{y} \in V_E(A)$ by a matrix $C \in \mathrm{GL}_n(F)$, i.e., if $V_E(A) = CV_E(B)$. The latter is equivalent to the matrix identity $B = C^{-1}AC - C^{-1}\partial(C)$.

Assume for a moment that $A \in F^{n\times n}$ admits a complete solution space over some D-field extension $E \geq F$, i.e., there exists a matrix $Y \in \mathrm{GL}_n(E)$ with $\partial_E(Y) = AY$. Such a matrix is called a *fundamental solution matrix* of the system of differential equations $\partial(\mathbf{y}) = A\mathbf{y}$ over E. If $Y, \tilde{Y} \in \mathrm{GL}_n(E)$ are two fundamental solution matrices for the same A, then it is easy to verify that these can only differ by a matrix $C \in \mathrm{GL}_n(C(E))$, i.e., $\tilde{Y} = YC$. Using this information, one obtains the following partial converse of the statement above.

PROPOSITION 1.2. *Let (F, ∂) be a nontrivial D-field of characteristic 0 and $A \in F^{n\times n}$. Assume that there exists a D-field extension E/F such that the matrix differential equation defined by A has a complete solution space over E. Then A is D-equivalent to a matrix $A_\ell \in F^{n\times n}$ defined by a linear differential operator $\ell \in F[\partial]$.*

A proof of Proposition 1.2 is presented in [Kat1]. In Section 2.1 we will see that the assumption on the existence of a fundamental solution matrix over some extension field is superfluous.

1.4. Differential modules. Another very common way to describe linear differential equations are differential modules. A *differential module* or D-module for short is a module M over a D-ring (R, ∂_R) together with a map $\partial_M : M \to M$ with the properties

$$\partial_M(\mathbf{x}+\mathbf{y}) = \partial_M(\mathbf{x}) + \partial_M(\mathbf{y}) \quad \text{and} \quad \partial_M(a\mathbf{x}) = \partial_R(a)\mathbf{x} + a\partial_M(\mathbf{x}) \tag{1–5}$$

for $\mathbf{x}, \mathbf{y} \in M$ and $a \in R$. The solution space of M is defined by

$$V(M) = \{\mathbf{x} \in M \mid \partial_M(\mathbf{x}) = 0\}.$$

M is called a *trivial D-module* if $M \cong V(M) \otimes_{C(R)} R$. In case (M, ∂_M) and (N, ∂_N) are two D-modules over R, an element $\varphi \in \mathrm{Hom}_R(M, N)$ is called a *differential homomorphism* (D-homomorphism) if $\varphi \circ \partial_M = \partial_N \circ \varphi$. Obviously the D-modules over R together with the D-homomorphisms form an abelian category denoted by $\mathbf{DMod}_R$.

Now assume that R is a D-field F with field of constants K. Then it is easy to verify that $\mathbf{DMod}_F$ with the tensor product over F becomes a tensor category over K. Here the tensor product $M \otimes_F N$ is provided with the derivation

$$\partial_{M\otimes N}(\mathbf{x} \otimes \mathbf{y}) = \partial_M(\mathbf{x}) \otimes \mathbf{y} + \mathbf{x} \otimes \partial_N(\mathbf{y}) \tag{1–6}$$

and the dual vector space $M^* = \mathrm{Hom}(M, F)$ with

$$(\partial_{M^*}(f))(\mathbf{x}) = \partial_F(f(\mathbf{x})) - f(\partial_M(\mathbf{x})) \tag{1–7}$$

for $\mathbf{x} \in M, \mathbf{y} \in N$ and $f \in M^*$. Then (F, ∂_F) is the unit element of $\mathbf{DMod}_F$ with $\mathrm{End}_{\mathbf{DMod}_F}(F, \partial_F) = K$. If in addition K is algebraically closed, $\mathbf{DMod}_F$ even forms a *Tannakian category* using the forgetful functor

$$\Omega : \mathbf{DMod}_F \to \mathbf{Vect}_F, \quad (M, \partial_M) \mapsto M$$

from the category $\mathbf{DMod}_F$ into the category of vector spaces over F (see [Del]). However, this will not be used in the sequel.

The link between D-modules and systems of linear differential equations is given in the following way. Let $M = \bigoplus_{i=1} \mathbf{b}_i F$ be a finite-dimensional D-module over F with basis $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$. Then by (1–5) the action of ∂ is uniquely determined by

$$\partial_M(\mathbf{b}_j) = \sum_{i=1}^{n} \mathbf{b}_i a_{ij} \quad \text{with } a_{ij} \in F. \tag{1–8}$$

Thus for $\sum_{i=1}^{n} \mathbf{b}_i y_i = B\mathbf{y} \in M$ with $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ and $\mathbf{y} = (y_1, \dots, y_n)^{\mathrm{tr}} \in F^n$ the two statements

$$B\mathbf{y} \in V(M) \quad \text{and } \partial_F(\mathbf{y}) = -A\mathbf{y}$$

where $A = (a_{ij}) \in F^{n\times n}$ are equivalent because of

$$\partial_M(B\mathbf{y}) = \partial_M(B)\mathbf{y} + B\partial_F(\mathbf{y}) = B(A\mathbf{y} + \partial_F(\mathbf{y})).$$

Therefore a D-module M with representing matrix $A \in F^{n\times n}$ of ∂_M leads to a system of linear differential equations over F with matrix $-A$. In particular, the solution space $V(M)$ of M coincides with $V(A)$ and thus is a vector space over K with $\dim_K(V(M)) \leq \dim_F(M)$.

2. Picard–Vessiot Extensions

2.1. Picard–Vessiot rings and fields. Now we are coming back to the questions raised in Section 1.2: For a linear differential equation $\partial(\mathbf{y}) = A\mathbf{y}$ over a D-field F of characteristic 0 with (algebraically closed) field of constants K, does there always exist a D-field E with $\dim_K(V(M \otimes_F E)) = \dim_E(M \otimes_F E)$? (The latter number equals $\dim_F(M)$.) For this purpose we define a *Picard–Vessiot ring* (PV-ring) R *for* A to be a differential ring $(R, \partial_R) \geq (F, \partial_F)$ with the following properties:

(2–1) R is a simple D-ring, i.e., R only contains trivial D-ideals.

(2–2) There exists a fundamental solution matrix over R, i.e., there exists a $Y \in \mathrm{GL}_n(R)$ such that $\partial_R(Y) = A \cdot Y$.

(2–3) R is generated over F by the coefficients y_{ij} of $Y = (y_{ij})_{i,j=1}^n$ and $\det(Y)^{-1}$.

It is easy to verify that a finitely generated simple D-ring is always an integral domain and that R and even $\mathrm{Quot}(R)$ do not contain new constants. The next proposition is basic for all that follows.

Proposition 2.1. *Let (F, ∂_F) be a D-field with algebraically closed field of constants K of characteristic* 0 *and $A \in F^{n\times n}$. Then for the differential equation $\partial(\mathbf{y}) = A\mathbf{y}$ there exists a Picard–Vessiot ring (R, ∂_R) over F and it is unique up to D-isomorphism.*

The construction of R is similar to Kronecker's construction of root fields in the case of polynomial equations. Let $X = (x_{ij})_{i,j=1}^n$ be a matrix with over F algebraically independent elements x_{ij}. Then by Section 1.1 we can extend ∂_F uniquely to $F[x_{ij}]_{i,j=1}^n$ by $\partial_U(X) = A \cdot X$, i.e., $\partial_U(x_{ij}) = \sum_{k=1} a_{ik}x_{kj}$, and to $U := F[\mathrm{GL}_n] = F[x_{ij}, \det(x_{ij})^{-1}]_{i,j=1}^n$. Then (U, ∂_U) is a D-ring over F. By Zorn's Lemma there exists a maximal D-ideal $P \trianglelefteq U$. The quotient $R := U/P$ is a simple D-ring containing a fundamental solution matrix $Y := \kappa_P(X)$, where κ_P denotes the canonical map $\kappa_P : U \to R = U/P$. Obviously, R is generated over F by the coefficients y_{ij} of Y and by $\det(Y)^{-1}$ such that by definition R is a Picard–Vessiot ring. It finally remains to be checked that two PV-rings belonging to the same matrix A are D-isomorphic. This can be done by elementary computations (see [Put2], Proposition 3.4).

The quotient field $E := \mathrm{Quot}(R)$ of a PV-ring is called a *Picard–Vessiot field* for A. It can be characterized without using R.

Proposition 2.2. *Let F and $A \in F^{n\times n}$ be as in Proposition* 2.1 *and let $(E,\partial_E) \geq (F,\partial_F)$ be a D-field extension. Then E/F is a Picard–Vessiot extension for A if and only if*

(a) *the constant fields of E and F coincide,*
(b) *there exists a $Y \in \mathrm{GL}_n(E)$ with $\partial_E(Y) = A\cdot Y$,*
(c) *E is generated over F by the coefficients y_{ij} of Y.*

A proof is given in [Put2], Proposition 3.5. These characterizing properties correspond to the classical definition of PV-fields (compare [Kap], III.11 and [Mag], Definition 3.2).

2.2. The differential Galois group. As before, let R be a PV-ring and $E = \mathrm{Quot}(R)$ a PV-field over a D-field F of characteristic 0 with algebraically closed field of constants. Then an automorphism γ of R/F or E/F, respectively, is called a *differential automorphism* (D-automorphism) if $\partial\circ\gamma = \gamma\circ\partial$. The group of all D-automorphisms is called the *differential Galois group* (D-Galois group) of R/F or E/F, respectively, and is denoted by $\mathrm{Gal}_{\mathrm{D}}(R/F) = \mathrm{Gal}_{\mathrm{D}}(E/F)$.

Since $\mathrm{Gal}_{\mathrm{D}}(E/F)$ acts faithfully on the solution space $V_E(A)$, it is a subgroup of $\mathrm{GL}_n(K)$. It can be characterized in the following way.

Proposition 2.3. *Let F be a D-field of characteristic* 0 *with algebraically closed field of constants and let R/F be a PV-ring for $A \in F^{n\times n}$ with fundamental solution matrix $Y = (y_{ij}) \in \mathrm{GL}_n(R)$. Then*

$$\mathrm{Gal}_{\mathrm{D}}(R/F) = \{C \in \mathrm{GL}_n(K) \mid q(Y\cdot C) = 0 \quad \textit{for all } q \in P\}$$

where P denotes the annulator ideal

$$P = \{q \in F[\mathrm{GL}_n] \mid q(y_{ij}) = 0\}.$$

A proof can be found for example in [Mag], Corollary 4.10. Since P is finitely generated, $\mathrm{Gal}_{\mathrm{D}}(R/F)$ consists of the K-rational points of a Zariski closed subgroup of $\mathrm{GL}_n(K)$ ([Eis], Section 15.10.1) and therefore of a reduced linear algebraic group $\mathcal{G}$ over K. This already proves the first part of the next proposition.

Proposition 2.4. *Let F be a D-field of characteristic* 0 *with algebraically closed field of constants K and E/F a PV-extension. Then there exists a reduced linear algebraic group $\mathcal{G}$ over K with $\mathrm{Gal}_{\mathrm{D}}(E/F) \cong \mathcal{G}(K)$. In addition the fixed field $E^{\mathcal{G}(K)}$ coincides with F.*

The last statement follows from the fact that for each $z \in E\backslash F$ a $\gamma \in \mathrm{Gal}_{\mathrm{D}}(E/F)$ can be constructed that moves z (see [Put2], Proposition 3.6). Now we return to our examples in Section 1.2. Again (F,∂) denotes the D-field $(\mathbb{C}(t),\partial_t)$.

Example 2.2.1. Let $\ell = \partial - a \in F[\partial]$ with $a \in \mathbb{C}^\times$. Then by Example 1.2.1 the PV-field for ℓ is given by $E = F(y)$ and $V_E(\ell) = \mathbb{C}y$ for $y = \exp(at)$. The D-Galois group $\mathrm{Gal}_{\mathrm{D}}(E/F)$ equals $\mathbb{G}_m(\mathbb{C}) = \mathrm{GL}_1(\mathbb{C})$ since any $c \in \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$ defines a D-automorphism because of $\partial(cy) = c\partial(y)$.

Example 2.2.2. In the case $\ell = \partial - \frac{1}{nt}$ we obtain $E = F(y)$ for $y = \sqrt[n]{t}$ and $\mathrm{Gal}_{\mathrm{D}}(E/F) = C_n$ is the cyclic group of order n.

Example 2.2.3. For $\ell = \partial^2 + \frac{1}{t}\partial$ the PV-field E is $F(y)$ with $y = \log(t)$ and $V_E(\ell) = \mathbb{C} \oplus \mathbb{C}y$. Because of $(\gamma \circ \partial)(y) = \frac{1}{t} = \partial(y)$, for any $\gamma \in \mathrm{Gal}_{\mathrm{D}}(E/F)$ there exists a $c \in \mathbb{C}$ with $\gamma(y) = y + c$. This proves $\mathrm{Gal}_{\mathrm{D}}(E/F) = \mathbb{G}_a(\mathbb{C}) = \mathbb{C}$.

2.3. Torsors and Kolchin's Theorem. In order to prove a Galois correspondence between the intermediate D-fields of a PV-extension E/F and the Zariski closed subgroups of $\mathrm{Gal}_{\mathrm{D}}(E/F) = \mathcal{G}(K)$ we need a structural theorem due to Kolchin which shows that after a finite field extension $\tilde{F}/F$ a defining PV-ring R inside E becomes isomorphic to the coordinate ring of $\mathcal{G}_{\tilde{F}} = \mathcal{G} \times_K \tilde{F}$, i.e., $R \otimes_F \tilde{F} \cong \tilde{F}[\mathcal{G}_F]$. This is a consequence of the fact that the affine scheme $\mathcal{X} = \mathrm{Spec}(R)$ over F is a *$\mathcal{G}_F$-torsor* or a *principal homogeneous space for $\mathcal{G}_F$*, respectively. This means that $\mathcal{G}_F$ acts on $\mathcal{X}$ via

$$\Gamma : \mathcal{X} \times_F \mathcal{G}_F \to \mathcal{X}, \quad (x, g) \mapsto x \cdot g \tag{2–4}$$

and in addition

$$\mathrm{Id} \times \Gamma : \mathcal{X} \times_F \mathcal{G}_F \to \mathcal{X} \times_F \mathcal{X}, \quad (x, g) \mapsto (x, x \cdot g) \tag{2–5}$$

is an isomorphism of affine schemes over F (see [Put2], Section 6.2). Such a torsor $\mathcal{X}$ is called a *trivial $\mathcal{G}_F$-torsor* if $\mathcal{X} \cong \mathcal{G}_F$ where the action is given by the multiplication. The latter is equivalent to $\mathcal{X}(F) \neq \varnothing$ where as usual $\mathcal{X}(F)$ denotes the set of F-rational points of $\mathcal{X}$.

Theorem 2.5 (D-Torsor Theorem). *Let F be a D-field of characteristic 0 with algebraically closed field of constants, $A \in F^{n \times n}$ and R a PV-ring for A over F. Further let $\mathcal{G}$ denote the reduced linear algebraic group over K with $\mathcal{G}(K) = \mathrm{Gal}_{\mathrm{D}}(R/F)$ and $\mathcal{G}_F := \mathcal{G} \times_K F$. Then $\mathrm{Spec}(R)$ is a $\mathcal{G}_F$-torsor.*

For the proof see for example [Put2], Section 6.2. Since the $\mathcal{G}_F$-torsor $\mathrm{Spec}(R)$ becomes trivial after a finite field extension $\tilde{F}/F$, the following version of Kolchin's theorem is an immediate consequence of the D-Torsor Theorem.

Corollary 2.6 (Kolchin). *With the same assumptions as in Theorem 2.5, and setting $\mathcal{X} := \mathrm{Spec}(R)$:*

(a) *There exists a finite field extension $\tilde{F}/F$ with $\mathcal{X} \times_F \tilde{F} \cong \mathcal{G}_F \times_F \tilde{F}$.*
(b) *$\mathcal{X}$ is smooth and connected over F.*
(c) *The degree of transcendence of $\mathrm{Quot}(R)/F$ equals $\dim(\mathcal{G})$ (over K).*

2.4. The differential Galois correspondence. Now we are ready to explain the differential Galois correspondence. This can be stated as follows:

Theorem 2.7 (D-Galois Correspondence). *Let F be a D-field of characteristic 0 with algebraically closed field of constants K, $A \in F^{n \times n}$ and E a PV-extension for A. Denote by $\mathcal{G}$ the reduced linear algebraic group over K with $\mathcal{G}(K) = \mathrm{Gal}_{\mathrm{D}}(E/F)$. Then:*

(a) *There exists an anti-isomorphism between the lattices*

$$\mathfrak{H} := \{\mathcal{H}(K) \mid \mathcal{H}(K) \leq \mathcal{G}(K) \textit{ closed}\} \textit{ and } \mathfrak{L} := \{L \mid F \leq L \leq E \textit{ D-field}\}$$

given by

$$\Psi : \mathfrak{H} \to \mathfrak{L},\ \mathcal{H}(K) \mapsto E^{\mathcal{H}(K)} \textit{ and } \Psi^{-1} : \mathfrak{L} \to \mathfrak{H},\ L \mapsto \mathrm{Gal}_{\mathrm{D}}(E/L).$$

(b) *If thereby $\mathcal{H}(K)$ is a normal subgroup, then $L := E^{\mathcal{H}(K)}$ is a PV-extension of F with* $\mathrm{Gal}_{\mathrm{D}}(L/F) \cong \mathcal{G}(K)/\mathcal{H}(K)$.

(c) *Denote by $\mathcal{G}^0$ the identity component of $\mathcal{G}$ and $F^0 := E^{\mathcal{G}^0(K)}$. Then F^0/F is a finite Galois extension with Galois group* $\mathrm{Gal}_{\mathrm{D}}(F^0/F) \cong \mathcal{G}(K)/\mathcal{G}^0(K)$.

Besides Proposition 2.4, for (a) we have to use that for all Zariski closed subgroups $\mathcal{H} \lneq \mathcal{G}$ the fixed field $E^{\mathcal{H}(K)}$ is different from F. For the proof of this fact as well as for the proof of (b) Kolchin's theorem has to be used (compare [Put2], Section 6.3).

As an application, we obtain a result comparable to the classical solution of polynomial equations by radicals. To this end we define a PV-extension E/F to be a *Liouvillean extension* if it contains a tower of intermediate D-fields

$$F = F_0 \leq F_1 \leq \ldots \leq F_n = E \quad \text{with } F_i = F_{i-1}(y_i)$$

and $\frac{\partial(y_i)}{y_i} \in F_{i-1}$ or $\partial(y_i) \in F_{i-1}$ or y_i is algebraic over F_{i-1}. Further a linear algebraic group $\mathcal{G}$ is called *virtually solvable* or solvable-by-finite if the connected component $\mathcal{G}^0$ is a solvable group. Since in this case the composition factors of $\mathcal{G}^0$ are isomorphic either to $\mathbb{G}_m$ or to $\mathbb{G}_a$ and D-Galois extensions of this type can be generated by solutions of $\partial(y) = fy$ or $\partial(y) = f$ with $f \in F$ we find from Theorem 2.7:

Corollary 2.8. *A PV-extension E/F is Liouvillean if and only if its D-Galois group is virtually solvable.*

For a more complete proof and further applications concerning integration in finite terms see for example [Mag], Chapter 6. As in the polynomial case, linear differential equations with non (virtually) solvable Galois groups exist. We want to verify this statement with the Airy equation. For this purpose we first explain an analogue of the square-discriminant criterion in ordinary Galois theory which is useful to reduce D-Galois group considerations to unimodular groups.

Proposition 2.9. *Let F be a D-field of characteristic* 0 *with algebraically closed field of constants K, $\ell = \sum_{k=0}^{n} a_k \partial^k \in F[\partial]$ a monic differential operator and E/F a PV-extension defined by ℓ or A_ℓ, respectively. Then the linear differential equation over F*

$$\partial(w) + a_{n-1}w = 0 \tag{2–6}$$

has a solution w in E with the properties

(a) *$F(w)/F$ is a PV-extension with* $\mathrm{Gal}_{\mathrm{D}}(F(w)/F) \leq \mathbb{G}_m(K)$,

(b) $\mathrm{Gal}_{\mathrm{D}}(E/F(w)) \cong \mathrm{Gal}_{\mathrm{D}}(E/F) \cap \mathrm{SL}_n(K)$.

For the proof let $\{y_1, \dots, y_n\}$ denote a K-basis of $V_E(\ell)$. Then any $y \in V_E(\ell)$ satisifies

$$\ell(y) = \mathrm{wr}(y_1, \dots, y_n, y) \cdot \mathrm{wr}(y_1, \dots, y_n)^{-1}. \tag{2–7}$$

In particular, for the first derivative of the Wronskian determinant $w := \mathrm{wr}(y_1, \dots, y_n)$ we obtain equation (2–6). Now any $\gamma \in \mathrm{Gal}_{\mathrm{D}}(E/F)$ acts on the fundamental solution matrix $Y = (\partial^{i-1}(y_j))_{i,j=1}^n$ of E/F via $\gamma(Y) = YC_\gamma$ with $C_\gamma \in \mathrm{GL}_n(K)$ and on w via $\gamma(w) = w \det(C_\gamma)$. Hence w is left invariant by γ if and only if $\det(C_\gamma) = 1$.

With the help of Proposition 2.9 we are able to compute the Galois group of the Airy equation.

Example 2.4.1. By Corollary 3.2 below the *Airy equation* $\partial^2(y) = ty$ has no algebraic solution over the D-field $(F, \partial_F) = (\mathbb{C}(t), \partial_t)$. Hence by Proposition 2.9 its Galois group $G = \mathcal{G}(\mathbb{C})$ is a connected closed subgroup of $\mathrm{SL}_2(\mathbb{C})$. In case $G \neq \mathrm{SL}_2(\mathbb{C})$ the linear algebraic group $\mathcal{G}$ would be reducible and $V_E(\ell)$ would contain a G-invariant line $\mathbb{C}y$. But then $z := \partial(y)y^{-1}$ would be invariant under G and therefore belong to F. Obviously no element z of $F = \mathbb{C}(t)$ satisifies

$$\partial(z) = \partial^2(y)y^{-1} - \partial(y)^2 y^{-2} = t - z^2.$$

as can be seen from the reduced expression of z as a quotient of polynomials.

2.5. Characterization of PV-rings and PV-fields. The theorem of Kolchin allows us to characterize the PV-ring R inside $\mathrm{Quot}(R)$.

Proposition 2.10. *Let F be a D-field of characteristic 0 with algebraically closed field of constants K and R a PV-ring over F with quotient field E and Galois group $G := \mathrm{Gal}_{\mathrm{D}}(R/F) = \mathcal{G}(K)$. Then for $z \in E$ are equivalent*:

(a) $z \in R$, *(b)* $\dim_K(K\langle Gz\rangle) < \infty$, *(c)* $\dim_F(F\langle \partial^k(z)\rangle_{k\in\mathbb{N}}) < \infty$.

Here $K\langle Gz\rangle$ denotes the K-vector space generated by the G-orbit of z and $F\langle \partial^k(z)\rangle_{k\in\mathbb{N}}$ is the F-vector space generated by all derivatives $\partial^k(z)$ of z. The critical step is the one from (a) to (b). By the D-Torsor Theorem we may, after a finite extension, assume $R = F[\mathcal{G}]$. Then the result follows from the fact that the action of $\mathcal{G}(F)$ on $F[\mathcal{G}]$ is locally finite, i.e., $F[\mathcal{G}]$ is a union of finite-dimensional G-stable subspaces ([Spr], Proposition 2.3.6).

It is quite natural to call an element $z \in E$ with property (c) in Proposition 2.10 *differentially finite* (D-finite). For such an element there exists, by definition, a nonconstant linear differential operator $\ell_z \in F[\partial]$ monic of minimum degree with $\ell_z(z) = 0$. We call ℓ_z a *minimal differential operator of z*. Given a basis $z_1, \dots, z_n$ of $K\langle Gz\rangle$, it can be constructed by

$$\ell_z(y) = \frac{\mathrm{wr}(z_1, \dots, z_n, y)}{\mathrm{wr}(z_1, \dots, z_n)}, \tag{2–8}$$

where wr denotes the Wronskian determinant defined in (1–4). In this notation, Proposition 2.10 tells us that the PV-ring R is characterized inside a PV-field $E = \mathrm{Quot}(R)$ as the ring of D-finite elements. In the particular case of finite D-extensions E/F the PV-ring R coincides with E. Another implication of Proposition 2.10 is the following characterization of PV-fields.

Theorem 2.11. *Let $F \leq E$ be D-fields of characteristic* 0 *with algebraically closed field of constants. Then E is a PV-extension of F if and only if*

(a) *E/F is finitely generated by D-finite elements*,
(b) *E and F share the same field of constants K*,
(c) *for all D-finite $z \in E$ yields $\dim_K(V_E(\ell_z)) = \deg(\ell_z)$, where $\ell_z \in F[\partial]$ is the minimal D-operator of z.*

An elementary proof is presented for example in [Put2], Proposition 6.11.

3. Monodromy and the Riemann–Hilbert Problem

3.1. Regular and singular points. Let $F = K(\mathcal{C})$ be the function field of a smooth projective curve $\mathcal{C}$ over an algebraically closed field K of characteristic zero with a nontrivial derivation ∂_F. Then $C(F) = K$. Further for $x \in \mathcal{C}$ the completion of F with respect to the valuation defined by x is denoted by F_x. It is isomorphic to the field of Laurent series $K((t))$ where $t \in F$ denotes a local parameter at x. Now let E/F be a PV-extension defined by $A \in F^{n\times n}$. Then a point $x \in \mathcal{C}$ is called a *regular point for E/F* if A is D-equivalent to a matrix over F_x without poles, i.e., there exists a matrix $B \in \mathrm{GL}_n(F_x)$ such that

$$B^{-1}AB - B^{-1}\partial(B) \in K[\![t]\!]^{n\times n}. \tag{3–1}$$

This property can also be characterized by having a fundamental solution matrix over $F_x = K((t))$:

Proposition 3.1. *Let $F = K(\mathcal{C})$ as above and $A \in F^{n\times n}$. Then $x \in \mathcal{C}$ is a regular point for the PV-extension E/F defined by A if and only if the D-equation $\partial(\mathbf{y}) = A\mathbf{y}$ possesses a fundamental solution matrix $Y \in \mathrm{GL}_n(F_x)$.*

This result immediately implies

Corollary 3.2. *Let E/F be as in Proposition* 3.1 *with $\mathrm{Gal}_{\mathrm{D}}(E/F) = \mathcal{G}(K)$ and let L be the fixed field of $\mathcal{G}^0(K)$. Then the finite Galois extension L/F is unramified in all regular points $x \in \mathcal{C}$ for E/F.*

In the particular case $\mathcal{C} = \mathbb{P}^1$ (projective line), the Galois group of a PV-extension E/F with at most one non regular point is connected. This applies, for example, to the Airy equation $\partial^2(y) = ty$ in Example 2.4.1 since all finite points are regular.

Non regular points $x \in \mathcal{C}$ for E/F are called *singular points* and the set of all singular points is called the *singular locus* $\mathcal{S}_{E/F}$ of E/F. A point $x \in \mathcal{S}_{E/F}$ is called *tamely (weakly, regular) singular* if there exists a $B \in \mathrm{GL}_n(F_x)$ such that

$$B^{-1}AB - B^{-1}\partial(B) \in \frac{1}{t}K[\![t]\!]^{n\times n}, \tag{3–2}$$

otherwise it is a *wild (strong, singular) singularity*. For tame singularities, an even stronger characterization can be given.

Proposition 3.3. *Let $F = K(\mathcal{C})$ as above, $A \in F^{n\times n}$ and E/F a PV-extension defined by A. Then $x \in \mathcal{C}$ is tamely singular if and only if there exists a $B \in \mathrm{GL}_n(F_x)$ and a constant matrix $D \in K^{n\times n}$ such that $B^{-1}AB - B^{-1}\partial(B) = \frac{1}{t}D$.*

For a sketch of proof see for example [Put2], Exercise 7.

For later use we add a characterization of regular and tamely singular points in the language of D-modules which immediately follows from the definitions (3–1) and (3–2) above.

Corollary 3.4. *Let (M, ∂) be a D-module over $F = K(\mathcal{C})$, $x \in \mathcal{C}$, $M_x := M \otimes_F F_x$ and let $t \in F$ be a local parameter for x such that $F_x = K((t))$.*

(a) *A point $x \in \mathcal{C}$ is regular if and only if M_x contains a ∂-invariant $K[\![t]\!]$-lattice.*
(b) *$x \in \mathcal{C}$ is tamely singular if and only if M_x contains a δ-invariant $K[\![t]\!]$-lattice where $\delta := t\partial$.*

3.2. The monodromy group. In the case of $K = \mathbb{C}$ the matrix B in Proposition 3.3 can be chosen to have coefficients in the subfield $F_x^{conv} \leq F_x = K((t))$ of convergent Laurent series (see [Put2], Exercise 7 or [For], § 11.12). This allows us to analyze the local behaviour.

Theorem 3.5. *Let $F = \mathbb{C}(\mathcal{C})$, $A \in F^{n\times n}$ and E/F a PV-extension for A. Assume $x \in \mathcal{C}$ is a tame singularity and denote by t a local parameter at x.*

(a) *Then $\partial(\mathbf{y}) = A\mathbf{y}$ possesses a local fundamental solution matrix of the form $Y = B\exp(C\log(t))$ with $B \in \mathrm{GL}_n(F_x^{\mathrm{conv}})$ and $C \in \mathbb{C}^{n\times n}$.*
(b) *Via analytic continuation along a loop σ around x we obtain $\sigma(Y) = Y \cdot M_\sigma$ with $M_\sigma = \exp(2\pi i C)$.*

For a proof see for example [For], § 11. The matrix $M_\sigma \in \mathrm{GL}_n(\mathbb{C})$ is called a *local monodromy matrix* and is determined inside $\mathrm{GL}_n(\mathbb{C})$ only up to conjugation.

In order to simplify the notation we now restrict ourselves to the projective line $\mathcal{C} = \mathbb{P}^1(\mathbb{C})$. Then $F = \mathbb{C}(\mathbb{P}^1) = \mathbb{C}(t)$ is the field of rational functions over $\mathbb{C}$. Let $\mathcal{S} \subseteq \mathbb{P}^1(\mathbb{C})$ be a nonempty set of cardinality $\sharp\mathcal{S} = s < \infty$ and let $\mathcal{U} := \mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}$. Then the *fundamental group of $\mathcal{U}$* with respect to a base point $x_0 \in \mathcal{U}$ is known to be

$$\pi_1(\mathcal{U}; x_0) = \langle \sigma_1, \ldots, \sigma_s \mid \sigma_1 \cdots \sigma_s = 1\rangle \tag{3–3}$$

where the σ_i are loops starting from x_0 counterclockwise around the points $x_i \in \mathcal{S}$ (compare [Ful], Chapter 19).

Applying Theorem 3.5 and analytic continuation we obtain a homomorphism (the monodromy map)

$$\mu : \pi_1(\mathcal{U}; x_0) \to \mathrm{GL}_n(\mathbb{C}), \quad \sigma \mapsto M_\sigma \tag{3–4}$$

where the image is called the *monodromy group* $\mathrm{Mon}(E/F)$ of E/F. Again $\mathrm{Mon}(E/F)$ is only determined up to conjugacy inside $\mathrm{GL}_n(\mathbb{C})$.

Since $M_\sigma \in \mathrm{GL}_n(\mathbb{C})$ acts on the solution space $V_E(A)$ spanned by the columns of Y it induces an automorphism γ_σ of E/F compatible with the differentiation on E. Consequently

$$\gamma : \mathrm{Mon}(E/F) \to \mathrm{Gal}_{\mathrm{D}}(E/F), \;\; M_\sigma \mapsto \gamma_\sigma \tag{3–5}$$

defines a homomorphism from $\mathrm{Mon}(E/F)$ to the D-Galois group of E/F, which in fact is a monomorphism. This already gives the first part of the next theorem.

THEOREM 3.6. (a) *Let $F = \mathbb{C}(t)$ and E/F be a PV-extension. Then* $\mathrm{Mon}(E/F)$ *is* (*isomorphic to*) *a subgroup of* $\mathrm{Gal}_{\mathrm{D}}(E/F)$.

(b) *If in addition the singular locus $\mathcal{S}_{E/F}$ is tame*, *then* $\mathrm{Mon}(E/F)$ *is Zariski dense in* $\mathrm{Gal}_{\mathrm{D}}(E/F)$.

The proof of (b) relies on the fact that systems of linear differential equations with only tame singularities by Propositions 3.1 and 3.3 only admit locally meromorphic solutions and that meromorphic functions on $\mathbb{P}^1(\mathbb{C})$ (fixed by $\mathrm{Mon}(E/F)$) are rational ([For], Corollary 2.9).

In Example 2.4.1 of the Airy equation $\partial^2(y) = ty$ we have $\mathcal{S}_{E/F} = \{\infty\}$. Therefore $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}) = \pi_1(\mathbb{A}^1(\mathbb{C})) = 1$ and $\mathrm{Mon}(E/F)$ is trivial. But $\mathrm{Gal}_{\mathrm{D}}(E/F) = \mathrm{SL}_2(\mathbb{C})$, hence ∞ is a wild singularity.

3.3. The Riemann–Hilbert Problem. We have seen that in the case of a tame singular locus the D-Galois group coincides with the Zariski closure of the monodromy group. Therefore it is a fundamental question if every homomorphic image of $\pi_1(\mathcal{U}; x_0)$ already appears as the monodromy group of a linear system of differential equations possibly even with only tame singularities. This problem is named the *Riemann–Hilbert problem* for tame (regular) systems and is number 21 among the famous Hilbert problems. A positive solution has already been presented by Plemelj (1908) in the following form.

THEOREM 3.7 (PLEMELJ). *For any finite set $\mathcal{S} = \{x_1, \dots, x_s\} \subseteq \mathbb{P}^1(\mathbb{C})$ and any set of matrices $M_i \in \mathrm{GL}_n(\mathbb{C})$ with $\prod_{i=1}^s M_i = 1$ there exists a tamely singular system of linear D-equations $\partial(\mathbf{y}) = A\mathbf{y}$ over $\mathbb{C}(t)$ with monodromy matrices $M_i = M_{\sigma_i}$ around x_i.*

This theorem can be seen as a differential analogue and generalization of the algebraic version of Riemann's existence theorem (see for example [Voe], Theorem 2.13). A modern proof is given in [AB], Theorem 3.2.1. It relies on the theorem of Birkhoff and Grothendieck on the triviality of complex holomorphic vector bundles. A simplified version for noncompact Riemann surfaces, for example $\mathbb{A}^1(\mathbb{C})$, can be found in [For], § 30 and § 31. Here is an easy consequence of Theorem 3.7:

COROLLARY 3.8. *Every finitely generated subgroup $G \leq \mathrm{GL}_n(\mathbb{C})$ can be realized as the monodromy group of a system of homogeneous linear differential equations over $\mathbb{C}(t)$ with tame singular locus.*

3.4. The inverse problem over the complex numbers. The solution of the Riemann–Hilbert problem is also the main ingredient for the solution of the inverse D-Galois problem over $\mathbb{C}(t)$. Namely by Theorem 3.6 it is enough to observe that all linear algebraic groups over $\mathbb{C}$ have finitely generated dense subgroups. This final step of the solution of the inverse problem was settled by Tretkoff and Tretkoff only in 1979.

PROPOSITION 3.9. *Any Zariski closed subgroup of $\mathrm{GL}_n(\mathbb{C})$ possesses finitely generated dense subgroups.*

For the proof see [TT], Proposition 1. Together with Theorem 3.7, Proposition 3.9 solves the inverse D-Galois problem over $\mathbb{C}(t)$ even with tame singularities.

THEOREM 3.10. *Every linear algebraic group over $\mathbb{C}$ can be realized as a differential Galois group over $\mathbb{C}(t)$ with tame singular locus.*

Unfortunately the above general solution of the inverse D-Galois problem over $\mathbb{C}$ relies on nonconstructive topological and cohomological considerations. In contrast to the case of finite groups it does not even carry over to algebraically closed fields of constants different from $\mathbb{C}$ due to the lack of a D-analogue of Grothendieck's Specialization Theorem.

For connected groups the situation looks more pleasant. There is a new constructive solution of the inverse D-Galois problem due to Mitschi and Singer which is valid for all D-fields with algebraically closed field of constants of characteristic 0. This will be outlined in the next section.

Before that, however, we want to indicate a theorem of Ramis concerning realizations with restricted singular locus.

THEOREM 3.11 (RAMIS). *A linear algebraic group over $\mathbb{C}$ can be realized as a differential Galois group over $\mathbb{C}(t)$ with at most one singular point if and only if it is generated by its maximal tori.*

More generally a linear algebraic group $\mathcal{G}(\mathbb{C})$ over $\mathbb{C}$ can be realized as a D-Galois group over $\mathbb{C}(t)$ with singular locus inside $\mathcal{S}$ if and only if the same is true for the quotient by its maximal closed normal subgroup generated by tori. A proof is elaborated in [Ram].

4. The Constructive Inverse Problem

4.1. The logarithmic derivative. As before, let (F, ∂_F) be an arbitrary D-field of characteristic 0 with algebraically closed field of constants K. Then the F-algebra

$$D := F[X]/(X)^2 = F + Fe, \quad \text{where } e^2 = 0,$$

is called the *algebra of dual numbers over F*. It has the advantage that the map

$$\delta : F \to D, \quad a \mapsto a + \partial_F(a)e$$

defined by the non-multiplicative derivation ∂_F is a K-homomorphism. For a linear algebraic group $\mathcal{G} \le \mathrm{GL}_{n,F}$ over F the *Lie algebra* of $\mathcal{G}$ can be defined to be the F-vector space

$$\mathrm{Lie}_F(\mathcal{G}) := \{A \in F^{n\times n} \mid 1 + eA \in \mathcal{G}(F[e])\}$$

provided with the *Lie bracket*

$$[\cdot,\cdot] : \mathrm{Lie}_F(\mathcal{G}) \times \mathrm{Lie}_F(\mathcal{G}) \to \mathrm{Lie}_F(\mathcal{G}), \quad (A, B) \mapsto [A, B] := AB - BA.$$

It can be shown that in fact the Lie algebra as defined above is isomorphic to the tangent space of $\mathcal{G}$ at the unit point and therefore only depends on $\mathcal{G}$ and not on the chosen embedding $\mathcal{G} \le \mathrm{GL}_{n,F}$.

Proposition 4.1. *Let $\mathcal{G} \le \mathrm{GL}_{n,F}$ be a linear algebraic group defined over a D-field F of characteristic* 0 *with derivation ∂_F and with algebraically closed field of constants. Then*

$$\lambda : \mathcal{G}(F) \to \mathrm{Lie}_F(\mathcal{G}), \quad A \mapsto \partial_F(A)A^{-1}$$

is a map from $\mathcal{G}(F)$ to the Lie algebra of $\mathcal{G}$ over F. It has the property

$$\lambda(A \cdot B) = \lambda(A) + A\lambda(B)A^{-1}.$$

The proof of Proposition 4.1 is immediate (compare [Kov], Section 1). The map λ is usually called the *logarithmic derivative.* One of its nice features also stated in [Kov] is that it gives an upper bound for the D-Galois group.

Proposition 4.2. *Let (F, ∂_F) be a D-field as above with field of constants K, $\mathcal{G}$ a linear algebraic group over K and $A \in \mathrm{Lie}_F(\mathcal{G})$. Then the D-Galois group of a PV-extension E/F defined by $\partial(\mathbf{y}) = A\mathbf{y}$ is isomorphic to a subgroup of $\mathcal{G}(K)$.*

For the proof we only have to observe that $A \in \mathrm{Lie}_F(\mathcal{G})$ implies that the defining ideal $I \trianglelefteq F[\mathrm{GL}_n]$ of $\mathcal{G}_F$ is a D-ideal. Hence the maximal D-ideal $P \trianglelefteq F[\mathrm{GL}_n]$ defining the PV-ring $R \le E$ contains a conjugate of I. By Proposition 2.3 this already entails the assertion.

In the case where the field F in question has *cohomological dimension* $\mathrm{cd}(F) \le 1$ there is a partial converse of Proposition 4.2. This relies on the famous Theorem of Springer and Steinberg ([Ser], III, § 2.3). Among the fields with this property are, for example, all fields of transcendence degree 1 over an algebraically closed field (Theorem of Tsen, [Ser], II, § 3.3).

Theorem 4.3 (Springer and Steinberg). *Let F be a perfect field with* $\mathrm{cd}(F) \leq 1$. *Then for every connected linear algebraic group $\mathcal{G}$ over F*

$$H^1(G_F, \mathcal{G}(F^{\mathrm{alg}})) = 0 \quad \textit{where} \quad G_F = \mathrm{Gal}(F^{\mathrm{alg}}/F).$$

Here F^{alg} denotes the algebraic closure of F and hence G_F the absolute Galois group of F. Now let F be a D-field with $\mathrm{cd}(F) \leq 1$ and with algebraically closed field of constants K. Since $H^1(G_F, \mathcal{G}(F^{\mathrm{alg}}))$ classifies the $\mathcal{G}_F$-torsors, with the assumptions of Theorem 4.3 all $\mathcal{G}_F$-torsors are trivial. Hence by the D-Torsor Theorem 2.5 then any PV-ring R over F with connected D-Galois group $\mathcal{G}(K)$ is isomorphic to the coordinate ring $F[\mathcal{G}]$ of $\mathcal{G}$. Another consequence of Theorem 4.3 of Springer and Steinberg is the following converse of Proposition 4.2 (see for example [Put2], Theorem 4.4).

Corollary 4.4. *Let (F, ∂_F) be a D-field of characteristic* 0 *with algebraically closed field of constants K and* $\mathrm{cd}(F) \leq 1$, *$\mathcal{H} \leq \mathrm{GL}_{n,K}$ a connected closed subgroup, $A \in \mathrm{Lie}_F(\mathcal{H}) \subseteq F^{n\times n}$ and E/F a PV-extension defined by A with connected Galois group* $\mathrm{Gal}(E/F) = \mathcal{G}(K)$. *Then there exists a $B \in \mathcal{H}(F)$ such that*

$$B^{-1}AB - B^{-1}\partial_F(B) \in \mathrm{Lie}_F(\mathcal{G}).$$

In this case E/F can be generated by a differential equation $\partial(\mathbf{y}) = A\mathbf{y}$ with $A \in \mathrm{Lie}_F(\mathcal{G})$. D-Galois extensions of this specific type are called *effective PV-extensions* in this article. Obviously the existence of effective PV-extensions is restricted to connected groups.

4.2. Chevalley modules. Before tackling the inverse problem for connected groups, we have to recall some basic notions and general structure theorems for linear algebraic groups $\mathcal{G}$. The maximal connected solvable normal subgroup of $\mathcal{G}$ is called the *radical of* $\mathcal{G}$ and its maximal connected unipotent normal subgroup the *unipotent radical of* $\mathcal{G}$. These are denoted by $\mathcal{R}(\mathcal{G})$ and $\mathcal{U}(\mathcal{G})$, respectively. Further $\mathcal{G}$ is called *semisimple* if $\mathcal{R}(\mathcal{G}) = 1$ and *reductive* if $\mathcal{U}(\mathcal{G}) = 1$. For a connected linear algebraic group we have the following structure theorem (see [Bor], IV, 11.22 and [Spr], Proposition 7.3.1 and 8.1.6).

Theorem 4.5. *Let $\mathcal{G}$ be a connected linear algebraic group over an algebraically closed field K of characteristic* 0.

(a) *Then $\mathcal{G}$ is isomorphic to a semidirect product $\mathcal{U} \rtimes \mathcal{P}$ of its unipotent radical $\mathcal{U} = \mathcal{U}(\mathcal{G})$ and a maximal reductive subgroup $\mathcal{P} \leq \mathcal{G}$ (Levi complement).*

(b) *The group $\mathcal{P}$ is the product $\mathcal{T} \cdot \mathcal{H}$ of a torus $\mathcal{T} = \mathcal{R}(\mathcal{P}) \cong \mathbb{G}_m^r$ and the connected semisimple group $\mathcal{H} = (\mathcal{P}, \mathcal{P})$. More precisely, there exists a finite subgroup $H = \mathcal{H} \cap \mathcal{T}$ such that $\mathcal{P} \cong (\mathcal{T} \times \mathcal{H})/H$.*

This already suggests a strategy for solving the inverse problem for connected groups. The first step would be to realize tori and semisimple groups and the second to solve embedding problems with unipotent kernel. For the realization of connected semisimple groups we need some strengthening of the following theorem of Chevalley.

Theorem 4.6 (Chevalley). *Let $\mathcal{G}$ be a linear algebraic group over K. Then for all closed subgroups $\mathcal{H} \leq \mathcal{G}$ there exist a K-vector space V, a linear representation $\varrho_{\mathcal{H}} : \mathcal{G} \to \mathrm{GL}(V)$ and a one-dimensional subspace $W \leq V$ such that*

$$\mathcal{H}(K) = \{h \in \varrho_{\mathcal{H}}(\mathcal{G}) \mid h(W) \subseteq W\}.$$

For the proof see [Spr], Theorem 5.5.3. From this theorem it is fairly easy to deduce the following statement ([MS], Lemma 3.1).

Corollary 4.7. *Let $\mathcal{G}$ be a connected semisimple linear algebraic group over an algebraically closed field K of characteristic* 0*. Then there exist a K-vector space V and a faithful linear representation $\varrho : \mathcal{G} \to \mathrm{GL}(V)$ with the following properties*:

(a) *V contains no one-dimensional $\varrho(\mathcal{G})$-submodule.*
(b) *Any connected closed subgroup $\mathcal{H}$ of $\mathcal{G}$ leaves a one-dimensional subspace of V invariant.*

Such a module is called a *Chevalley module for $\mathcal{G}$* in [MS]. Obviously the natural 2-dimensional representation of $\mathrm{SL}_2(K)$ already defines a Chevalley module for this group. In general, Chevalley modules are obtained by composing representations of the type of Theorem 4.6 and therefore are not of this simple structure.

4.3. Realization of connected reductive groups. The key lemma for the realization of semi-simple groups as differential Galois groups over $F = K(t)$ is the following.

Proposition 4.8. *Let $F = K(t)$ be a field of rational functions over an algebraically closed field K of characteristic* 0, *$\mathcal{G}$ be a semisimple linear algebraic group over K with Chevalley module V and without loss of generality $\mathcal{G} \leq \mathrm{GL}(V)$. Let $A := A_0 + tA_1 \in \mathrm{Lie}_F(\mathcal{G})$ with constant matrices $A_0, A_1 \in \mathrm{Lie}_K(\mathcal{G})$, and E/F a PV-extension for A. Then $\mathrm{Gal}_{\mathrm{D}}(E/F)$ is a proper subgroup of $\mathcal{G}(K)$ if and only if there exists a vector $w \in V \otimes_K K[t]$ and a polynomial $f \in K[t]$ of degree at most* 1 *with*

$$(A - \partial)w = fw.$$

Obviously by Proposition 4.2 the group $\mathrm{Gal}_{\mathrm{D}}(E/F)$ is isomorphic to a subgroup $\mathcal{H}(K)$ of $\mathcal{G}(K)$. In case $\mathcal{H}(K) \neq \mathcal{G}(K)$ by Corollary 4.4 there exists a $B \in \mathcal{G}(F)$ such that $\tilde{A} := B^{-1}AB - B^{-1}\partial(B) \in \mathrm{Lie}_F(\mathcal{H})$. Since V is a Chevalley module there exists in addition a $v \in V, v \neq 0$, such that $\tilde{A}v \in Fv$. But then for $w := Bv$ one obtains $(A - \partial)w = fw \in Fw$ with $\deg(f) \leq 1$.

Hence, one only has to find constant matrices A_0 and A_1 such that $(A-\partial)w = fw$ has no solution. For the construction of such matrices we need the root space decomposition of $\mathfrak{L} := \mathrm{Lie}_K(\mathcal{G})$. This is given by

$$\mathfrak{L} = \mathfrak{L}_0 \oplus \Bigl(\bigoplus_{\alpha} \mathfrak{L}_\alpha\Bigr)$$

where $\mathfrak{L}_0$ denotes the Cartan subalgebra and the one-dimensional spaces $\mathfrak{L}_\alpha = KX_\alpha$ are the eigenspaces for the adjoint action of $\mathfrak{L}_0$ on $\mathcal{G}$ corresponding to the non-zero roots $\alpha \in \mathfrak{L}_0^*$, i.e., $\alpha : \mathfrak{L}_0 \to K$. More precisely the adjoint action of $\mathfrak{L}_0$ on $\mathfrak{L}_0$ is trivial, and for any root $\alpha \neq 0$ one has $[C, X_\alpha] = \alpha(C)X_\alpha$ for all $C \in \mathfrak{L}_0$.

The action of $\mathfrak{L}_0$ on the Chevalley module V produces a similar decomposition $V = \bigoplus_\beta V_\beta$ into eigenspaces for a collection of linear maps $\beta \in \mathfrak{L}_0^*$. These are called the weights of V.

Now we choose

$$A_0 := \sum_{\alpha\neq 0} X_\alpha. \tag{4–0}$$

In order to fulfill the assumptions of Proposition 4.8, for A_1 we choose an element in $\mathfrak{L}_0$ satisfying the following conditions:

(4–1) The $\alpha(A_1)$ are non-zero and distinct for the non-zero roots α of $\mathfrak{L}$.
(4–2) The $\beta(A_1)$ are non-zero and distinct for the non-zero weights of V.
(4–3) The linear operator

$$\sum_{\alpha\neq 0} \frac{-1}{\alpha(A_1)} X_{-\alpha} X_\alpha$$

does not have positive integers as eigenvalues.

Obviously the set of $A_1 \in \mathfrak{L}_0$ satisfying (4–1) and (4–2) is Zariski dense. Condition (4–3) can be fulfilled using a suitable multiple of A_1. Now Mitschi and Singer have proved the following result in [MS]:

PROPOSITION 4.9. *With matrices A_0 and A_1 satisfying* (4–0) *to* (4–3), *the PV-extension E/F in Proposition* 4.8 *generated by $A = A_0 + tA_1$ has the differential Galois group $\mathcal{G}(K)$.*

In particular, any connected semi-simple linear algebraic group can be realized effectively as a differential Galois group over $F = K(t)$. The next step is the realization of tori $\mathcal{T} = \mathbb{G}_m(K)^r$, $r \in \mathbb{N}$, as differential Galois groups over F. This follows from the next result:

PROPOSITION 4.10. *Let $F = K(t)$ as in Proposition* 4.8 *and $c_1, \dots, c_r \in K$ linearly independent over $\mathbb{Q}$. Then the PV-extension E/F generated by $A = \mathrm{diag}(c_1, \dots, c_r) \in \mathrm{Lie}_K(\mathbb{G}_m^r)$ has the differential Galois group $\mathbb{G}_m^r(K)$.*

Obviously by Proposition 4.2 and Corollary 3.2 $\mathrm{Gal}_{\mathrm{D}}(E/F)$ is a connected subgroup of $\mathbb{G}_m^r(K)$. Hence the result follows from the fact that the solutions $y_j = \exp(c_j t)$ of $\partial(y) = c_j y$ are algebraically independent over F for $j = 1, \dots, r$.

Since any connected reductive group is a quotient of a direct product of a connected semi-simple group and a torus by a finite group, from Proposition 4.9 and 4.10 we immediately obtain

Theorem 4.11. *Every connected reductive linear algebraic group over an algebraically closed field K of characteristic 0 can be realized effectively as differential Galois group over $F = K(t)$.*

4.4. Embedding problems with unipotent kernel. In order to solve the inverse problem of differential Galois theory for arbitrary connected groups over $F = K(t)$ by Theorem 4.11 it remains to solve differential embedding problems with unipotent kernel.

Here a differential embedding problem is defined in the following way. Let L/F be a PV-extension with D-Galois group $\mathrm{Gal}_{\mathrm{D}}(L/F) \cong \mathcal{H}(K)$ and let

$$1 \to \mathcal{A}(K) \to \mathcal{G}(K) \overset{\beta}{\to} \mathcal{H}(K) \to 1 \tag{4–4}$$

be an exact sequence of linear algebraic groups (in characteristic zero). Then the corresponding *differential embedding problem* (D-embedding problem), denoted by $\mathcal{E}(\alpha, \beta)$, asks for the existence of a PV-extension E/F with $E \geq L$ and a monomorphism γ which maps $\mathrm{Gal}_{\mathrm{D}}(E/F)$ onto a closed subgroup of $\mathcal{G}(K)$ such that the diagram

$$\begin{tikzcd}
 & & \mathrm{Gal}(E/F) \arrow[r, dotted, "\mathrm{res}"] \arrow[d, dotted, "\gamma"'] & \mathrm{Gal}(L/F) \arrow[d, "\cong"', "\alpha"] & \\
1 \arrow[r] & \mathcal{A}(K) \arrow[r] & \mathcal{G}(K) \arrow[r, "\beta"] & \mathcal{H}(K) \arrow[r] & 1
\end{tikzcd} \tag{4–5}$$

commutes. The kernel $\mathcal{A}(K)$ is also called the *kernel of* $\mathcal{E}(\alpha, \beta)$ and the monomorphism γ a *solution* of $\mathcal{E}(\alpha, \beta)$. We say γ is a *proper* solution if γ is an epimorphism. Further the D-embedding problem is called a *split embedding problem* if the exact sequence splits (i.e., $\mathcal{G}(K)$ as an algebraic group is a semidirect product of $\mathcal{A}(K)$ with $\mathcal{H}(K)$) and a *Frattini embedding problem* if $\mathcal{G}$ is the only closed supplement of $\mathcal{A}$ in $\mathcal{G}$ (i.e., any $\mathcal{U} \leq \mathcal{G}$ which satisfies $\mathcal{A}\mathcal{U} = \mathcal{G}$ already equals $\mathcal{G}$). Finally we say the embedding problem is an *effective embedding problem*, if L/F is an effective PV-extension (according to Section 4.1).

The unipotent radical $\mathcal{U}$ of a linear algebraic group $\mathcal{G}$ possesses a closed complement $\mathcal{H}$ which is a reductive linear algebraic group (Levi complement). Thus $(\mathcal{G}/\mathcal{U})(K) \cong \mathcal{H}(K)$ already can be realized effectively as D-Galois group over F. Hence to realize $\mathcal{G}(K)$ as D-Galois group it suffices to solve an effective split embedding problem with unipotent kernel $\mathcal{U}(K)$. Dividing by the commutator subgroup $\mathcal{U}'(K)$ of $\mathcal{U}(K)$ this embedding problem decomposes into an effective split embedding problem with abelian unipotent kernel

$$1 \to \mathcal{U}(K)/\mathcal{U}'(K) \to \mathcal{G}(K)/\mathcal{U}'(K) \to \mathcal{H}(K) \to 1 \tag{4–6}$$

and a Frattini embedding problem belonging to

$$1 \to \mathcal{U}'(K) \to \mathcal{G}(K) \to \mathcal{G}(K)/\mathcal{U}'(K) \to 1. \tag{4–7}$$

For the first of these embedding problems we can use a recent result of Oberlies ([Obe], Proposition 2.4) based on a theorem of Ostrowski.

Proposition 4.12. *Every effective split D-embedding problem with* (*minimal*) *unipotent abelian kernel has an effective proper solution over* $K(t)$, *where* K *is algebraically closed of characteristic* 0.

Here the assumption of minimality can be neglected by direct decomposition of the kernel (compare [Obe], Reduction). The solvability of the second embedding problem already goes back to Kovacic ([Kov], Proposition 11). In our terminology it can be stated in the following way.

Proposition 4.13. *Every effective Frattini D-embedding problem has an effective proper solution over* $K(t)$, *where* K *is algebraically closed of characteristic* 0.

For a sketch of the proof, denote $d\beta : \mathrm{Lie}_F(\mathcal{G}) \to \mathrm{Lie}_F(\mathcal{H})$ the surjective Lie algebra map induced by $\beta : \mathcal{G} \to \mathcal{H}$ and $A \in \mathrm{Lie}_F(\mathcal{H})$ a matrix defining an effective PV-extension L/F with isomorphism $\alpha : \mathrm{Gal}(L/F) \to \mathcal{H}(K)$. Then any inverse image $B \in \mathrm{Lie}_F(\mathcal{G})$ of A by $d\beta$, i.e., $d\beta(B) = A$, defines a PV-extension E/F with $\mathrm{Gal}_{\mathrm{D}}(E/F) \leq \mathcal{G}(K)$ by Proposition 4.2 and $E \geq L$. Hence by the Frattini property there exists an isomorphism $\gamma : \mathrm{Gal}_{\mathrm{D}}(E/F) \to \mathcal{G}(K)$ with in addition $\alpha \circ \mathrm{res} = \beta \circ \gamma$, i.e., γ is an effective proper solution of $\mathcal{E}(\alpha, \beta)$.

Combining Proposition 4.12 and 4.13 above with Theorem 4.11 we get a constructive solution of the inverse problem for connected groups (see [MS]).

Theorem 4.14 (Mitschi–Singer). *Every connected linear algebraic group over an algebraically closed field* K *of characteristic* 0 *can be realized effectively as differential Galois group over* $F = K(t)$.

A nonconstructive variant of proof had already been presented in [Sin].

Added in Proof. A solution of the inverse problem in differential Galois theory over $K(t)$ for nonconnected groups has recently been obtained by J. Hartmann in her thesis [Har].

MODULAR THEORY

5. Iterative Differential Modules and Equations

5.1. Iterative derivations. When trying to set up a differential Galois theory in positive characteristic, one is confronted with the problem that the usual differentiation, extended to transcendental extensions of a differential field, automatically causes new constants. This problem can be overcome using iterative derivations (also called higher derivations of infinite rank in [Jac], 8.15). These were introduced for the first time by H. Hasse and F. K. Schmidt [HS].

As before, let R be a commutative ring. A family $\partial^* = (\partial^{(k)})_{k\in\mathbb{N}}$ of maps $\partial^{(k)} : R \to R$ with $\partial^{(0)} = \mathrm{id}_R$ is called an *iterative derivation of* R if

$$\partial^{(k)}(a+b) = \partial^{(k)}(a) + \partial^{(k)}(b), \qquad \partial^{(k)}(a\cdot b) = \sum_{i+j=k} \partial^{(i)}(a)\partial^{(j)}(b),$$
$$\partial^{(i)} \circ \partial^{(j)} = \binom{i+j}{j}\partial^{(i+j)} \tag{5–1}$$

for all $a, b \in R$ and $i, j, k \in \mathbb{N}$. (Observe the modified product rule!) The pair (R, ∂^*) is then called an *iterative differential ring* or ID-ring for short. An element $c \in R$ is a *differential constant* if $\partial^{(k)}(c) = 0$ for all $k > 0$. Again the set of all differential constants forms a ring denoted by $C(R)$.

In case (R, ∂) is a differential ring containing $\mathbb{Q}$, i.e., a Ritt algebra, the maps $\partial^{(k)} = \frac{1}{k!}\partial^k$ define an iterative derivation on R. (This observation has also led to the name divided powers.) In the case of positive characteristic p, the last condition in (5–1) implies $(\partial^{(1)})^p = 0$, i.e., iterative derivations always have *trivial p-curvature.*

The following example shows that in positive characteristic extensions of iterative derivations to transcendental extensions may maintain the constant rings in contrast to ordinary derivations. For this purpose let $F = K(t)$ be a field of rational functions. Then $\partial^{(k)}(t^n) = \binom{n}{k}t^{n-k}$ defines an iterative derivation on F denoted by ∂_t^*. Thus with the iterative derivation ∂_t^*, the ring of differential constants remains K in any characteristic.

Iterative derivations can also be characterized by the behaviour of their Taylor series. An *iterative Taylor series* of $a \in R$ is defined by

$$\mathbf{T}_a(T) := \sum_{k\in\mathbb{N}} \partial^{(k)}(a)T^k \tag{5–2}$$

with the higher derivations $\partial^{(k)}$ instead of ∂^k. The following result was found by F. K. Schmidt ([HS], Satz 3):

Proposition 5.1. *A commutative ring R together with a family of maps $\partial^{(k)}$: $R \to R$ for $k \in \mathbb{N}$ is an ID-ring if and only if*

(a) *the Taylor map* $\mathbf{T} : R \to R[\![T]\!]$, $a \mapsto \mathbf{T}_a(T)$ *is a ring homomorphism with* $I \circ \mathbf{T} = \mathrm{id}_R$ *for* $I : R[\![T]\!] \to R$, $\Theta(T) \mapsto \Theta(0)$,

(b) *the extended map*

$$\tilde{\mathbf{T}} : R[\![T]\!] rightarrow R[\![T]\!],\ \sum_{i\in\mathbb{N}} a_i T^i \mapsto \sum_{i\in\mathbb{N}}\sum_{j\in\mathbb{N}} \partial^{(j)}(a_i) T^{i+j}$$

is a ring homomorphism with $\partial_T^{(k)} \circ \tilde{\mathbf{T}} = \tilde{\mathbf{T}} \circ \partial^{(k)}$.

Using iterative Taylor series it is easy to extend an iterative derivation ∂_R^* of R to quotient rings $S^{-1}R$ by expanding $\mathbf{T}_{a/b}(T) := \mathbf{T}_a(T)/\mathbf{T}_b(T)$. Obviously this extension is unique. In particular, an iterative derivation of an integral domain R uniquely extends to its quotient field $F = \mathrm{Quot}(R)$ ([HS], Satz 5). For separable field extensions, the following result is given in [HS], Satz 6 and Satz 7.

PROPOSITION 5.2. *Let* (F, ∂_F^*) *be an ID-field and* E/F *a finitely generated separable field extension. Then* ∂_F^* *extends to an iterative derivation* ∂_E^* *of* E. *In case* E/F *is finite this extension is unique.*

COROLLARY 5.3. *The ring of differential constants* K *of an ID-field* (F, ∂^*) *is a field which is separably algebraically closed in* F.

5.2. The Wronskian determinant. In positive characteristic the Wronskian determinant as defined in the classical case may vanish even if the functions involved are linearly independent. Fortunately the iterative Taylor series preserve linear independency.

PROPOSITION 5.4. *Let* (F, ∂_F^*) *be an ID-field with field of constants* K. *Then for elements* $x_1, \dots, x_n \in F$ *linearly independent over* K *the iterative Taylor series* $\mathbf{T}_{x_1}, \dots, \mathbf{T}_{x_n}$ *are linearly independent over* F.

The proof can be found in [Sch]. From this result one obtains the existence of elements $d_i \in \mathbb{N}$ with $\det(\partial^{(d_i)}(x_j))_{i,j=1}^n \neq 0$. The set $D = \{d_1, \dots, d_n\}$ of natural numbers, which are the smallest (in lexicographical order) with this property is called the *set of derivation orders* of $x_1, \dots, x_n$. The corresponding determinant

$$\mathrm{wr}_D(x_1, \dots, x_n) := \det(\partial^{(d_i)}(x_j))_{i,j=1}^n \tag{5–3}$$

is called the *Wronskian determinant* of $x_1, \dots, x_n$. Obviously the set of derivation orders only depends on the K-module spanned by the x_j. With this modified Wronskian determinant we now obtain the following result familiar from characteristic zero.

COROLLARY 5.5. *Let* (F, ∂_F^*) *be an ID-field with field of constants* K. *Then elements* $x_1, \dots, x_n \in F$ *with set of derivation orders* D *are linearly independent over* K *if and only if* $\mathrm{wr}_D(x_1, \dots, x_n) \neq 0$.

In characteristic 0 the set of derivation orders always coincides with $\{0, \dots, n-1\}$ which is closed by $\leq$. On the contrary, in characteristic $p > 0$ each subset $D \subseteq \mathbb{N}$

which is closed by the relation $\leq_p$ may appear as a set of derivation orders. Here $k \leq_p l$ stands for the property that all coefficients of the p-expansion of k are less than or equal to the corresponding coefficients of l. This can be verified for example with $(F, \partial_F^*) = (K(t), \partial_t^*)$ and $\{x_1, \ldots, x_n\} = \{t^{d_1}, \ldots, t^{d_n}\}$ for $D = \{d_1, \ldots, d_n\}$. In particular, in characteristic $p \geq n$ the set of derivation orders is always the same as in the classical case.

5.3. Iterative differential modules. In positive characteristic it is more suitable to define differential equations by introducing differential modules first (compare Section 1.4). For this purpose let (R, ∂_R^*) be an ID-ring with ring of constants S and M be an R-module. A family $\partial_M^* = (\partial_M^{(k)})_{k \in \mathbb{N}}$ of maps $\partial_M^{(k)} : M \to M$ with $\partial_M^{(0)} = \mathrm{id}_M$ satisfying

$$\partial_M^{(k)}(\mathbf{x} + \mathbf{y}) = \partial_M^{(k)}(\mathbf{x}) + \partial_M^{(k)}(\mathbf{y}), \qquad \partial_M^{(k)}(a \cdot \mathbf{x}) = \sum_{i+j=k} \partial_R^{(i)}(a) \partial_M^{(j)}(\mathbf{x}),$$

$$\text{and} \quad \partial_M^{(i)} \circ \partial_M^{(j)} = \binom{i+j}{i} \partial_M^{(i+j)}$$

for all $a \in R$, $\mathbf{x}$, $\mathbf{y} \in M$ and $i, j, k \in \mathbb{N}$ is called an *iterative derivation on* M, and (M, ∂_M^*) is called an *iterative differential module* or ID-module for short. The S-module

$$V(M) = \bigcap_{k>0} \mathrm{Ker}(\partial_M^{(k)})$$

is called the *solution space of* M. Further M is called a *trivial ID-module* if $M \cong V(M) \otimes_S R$.

Given ID-modules (M, ∂_M^*) and (N, ∂_N^*) over R, an element $\varphi \in \mathrm{Hom}_R(M, N)$ is called an *iterative differential homomorphism* (ID-homomorphism) if $\varphi \circ \partial_M^{(k)} = \partial_N^{(k)} \circ \varphi$ for all $k \in \mathbb{N}$. The *category of ID-modules over* R with ID-homomorphisms as morphisms is denoted by $\mathbf{IDMod}_R$.

It is easy to check that in case R is a field F, i.e., (F, ∂_F^*) is an ID-field, $\mathbf{IDMod}_F$ is an abelian category. It becomes a tensor category over the field of constants K using the tensor product $M \otimes_F N$ with the iterative derivation

$$\partial_{M \otimes N}^{(k)}(\mathbf{x} \otimes \mathbf{y}) = \sum_{i+j=k} \partial_M^{(i)}(\mathbf{x}) \otimes \partial_N^{(j)}(\mathbf{y}) \tag{5–4}$$

and the dual $M^* = \mathrm{Hom}_F(M, F)$ with

$$\partial_{M^*}^{(k)}(f) = \sum_{i+j=k} (-1)^j \partial_F^{(i)} \circ f \circ \partial_M^{(j)} \tag{5–5}$$

for all $\mathbf{x} \in M$, $\mathbf{y} \in N$, $f \in M^*$ and $i, j, k \in \mathbb{N}$. Then (F, ∂_F^*) is the unit element of $\mathbf{IDMod}_F$ with $\mathrm{End}_{\mathbf{IDMod}_F}(F, \partial_F^*) = K$. If in addition K is algebraically closed then $\mathbf{IDMod}_F$ together with the forgetful functor

$$\Omega : \mathbf{IDMod}_F \to \mathbf{Vect}_F, \qquad (M, \partial_M^*) \mapsto M$$

is even a *Tannakian category.* As in the classical case we will not make use of this property in the sequel.

From Corollary 5.5 we immediately obtain the following formal analogue of Proposition 1.1.

PROPOSITION 5.6. *Let (F, ∂_F^*) be an ID-field with constant field K and $M \in$ $\mathbf{IDMod}_F$ an ID-module over F. Then for the solution space $V(M)$ of M we have*

$$\dim_K(V(M)) \leq \dim_F(M).$$

5.4. Projective systems. ID-modules over fields of positive characteristic can be described by projective systems of vector spaces. To explain this connection, let (M, ∂_M^*) be an ID-module over an ID-field (F, ∂_F^*) of characteristic $p > 0$. Then

$$M_l := \bigcap_{j<l} \operatorname{Ker}(\partial_M^{(p^j)}) \tag{5–6}$$

is a vector space over the field $F_l := \bigcap_{j<l} \operatorname{Ker}(\partial_F^{(p^j)})$. Indeed, M_l is even an ID-module over F_l with respect to the iterative derivations $(\partial_M^{(kp^l)})_{k\in\mathbb{N}}$ and $(\partial_F^{(kp^l)})_{k\in\mathbb{N}}$, respectively. Further the embedding $\varphi_l : M_{l+1} \to M_l$ is an F_{l+1}-linear map and defines a projective system $(M_l, \varphi_l)_{l\in\mathbb{N}}$. Moreover each φ_l can be extended uniquely to an isomorphism $\tilde{\varphi}_l : M_{l+1} \otimes_{F_{l+1}} F_l \to M_l$. In order to prove $\dim_{F_{l+1}}(M_{l+1}) = \dim_{F_l}(M_l)$ for the last statement one has to use the triviality of the p-curvature $(\partial_M^{(p^l)})^p = 0$ on M_l (compare [Mat], Proposition 2.7). In fact ID-modules are characterized by the above properties.

THEOREM 5.7. *Let (F, ∂_F^*) be an ID-field of characteristic $p > 0$. Then the category $\mathbf{IDProj}_F$ of projective systems $(N_l, \psi_l)_{l\in\mathbb{N}}$ over F with the properties*

(a) *N_l is an F_l-vector space of finite dimension and ψ_l is F_{l+1}-linear,*
(b) *each ψ_l extends to an isomorphism $\tilde{\psi}_l : N_{l+1} \otimes_{F_{l+1}} F_l \to N_l$*

is equivalent to the category $\mathbf{IDMod}_F$.

This equivalence is even compatible with the structure of Tannakian categories. The critical point in the proof is the definition of an iterative derivation on $M := N_0$. Defining $M_l := (\psi_0 \circ \cdots \circ \psi_{l-1})(N_l)$ we get $M_l \subseteq M_{l-1} \subseteq \ldots \subseteq M$. By property (b) an F_l-basis $B_l = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ of M_l also is an F-basis of M. So for all $\mathbf{x} \in M$ we can find coefficients $a_i \in F$ such that $\mathbf{x} = \sum_{i=1}^n \mathbf{b}_i a_i = B_l \cdot \mathbf{a}$ for $\mathbf{a} = (a_1, \ldots, a_n)^{\mathrm{tr}}$. Since by induction $B_l \subseteq M_l \subseteq \bigcap_{k<p^l} \operatorname{Ker}(\partial_M^{(k)})$, for all $k < p^l$ we can define

$$\partial_M^{(k)}(\mathbf{x}) = \sum_{i=1}^n \mathbf{b}_i \partial_F^{(k)}(a_i) = B_l \partial_F^{(k)}(\mathbf{a}). \tag{5–7}$$

Obviously this definition is independent of the choice of the bases B_l of M_l. The above step in the proof leads to the following formula for the iterative derivation which is basic for the introduction of iterative differential equations.

COROLLARY 5.8. *Let (M, ∂_M^*) be an ID-module over an ID-field (F, ∂_F^*) of characteristic $p > 0$ with corresponding projective system $(M_l, \varphi_l)_{l\in\mathbb{N}}$. Then*

$$\partial_M^{(k)} = \tilde{\varphi}_0 \circ \cdots \circ \tilde{\varphi}_l \circ \partial_F^{(k)} \circ \tilde{\varphi}_l{}^{-1} \circ \cdots \circ \tilde{\varphi}_0{}^{-1} \qquad \text{for all } k < p^{l+1}.$$

5.5. Iterative differential equations. As before, M denotes an ID-module over an ID-field F of characteristic $p > 0$ with projective system $(M_l, \varphi_l)_{l\in\mathbb{N}}$. Let $B_l = \{\mathbf{b}_{l1}, \dots, \mathbf{b}_{ln}\}$ be a basis of M_l and D_l the representing matrix of φ_l with respect to B_{l+1} and B_l, i.e., $B_{l+1} = B_l D_l$ for $B_l = (\mathbf{b}_{l1}, \dots, \mathbf{b}_{ln})$ etc. Then Corollary 5.8 leads to the formula

$$\partial_M^{(k)}(B_0) = B_0 D_0 \cdots D_l \partial_F^{(k)}(D_l^{-1} \cdots D_0^{-1}) \quad \text{for } k < p^{l+1} \tag{5–8}$$

because of $B_0 = B_{l+1} D_l^{-1} \cdots D_0^{-1}$ and $\partial_M^{(k)}(B_0) = B_{l+1}\partial_M^{(k)}(D_l^{-1} \cdots D_0^{-1})$. From (5–8) we get the following characterization of the solution space of an ID-module.

PROPOSITION 5.9. *Assume the characteristic is $p > 0$. Let (M, ∂_M^*) be an ID-module over an ID-field (F, ∂_F^*) with corresponding projective system $(M_l, \varphi_l)_{l\in\mathbb{N}}$, basis $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ of M, and $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$. Then for $\mathbf{y} = (y_1, \dots, y_n)^{\mathrm{tr}} \in F^n$, the following statements are equivalent*:

(a) $B\mathbf{y} = \sum_{i=1}^n \mathbf{b}_i y_i \in V(M) = \bigcap_{l\in\mathbb{N}} M_l$,
(b) $\mathbf{y}_l := D_{l-1}^{-1} \cdots D_0^{-1}\mathbf{y} \in F_l^n$ *for all* $l \in \mathbb{N}$,
(c) $\partial_F^{(p^l)}(\mathbf{y}_l) = A_l^\circ \mathbf{y}_l$ *for all* $l \in \mathbb{N}$ *where* $A_l^\circ = \partial_F^{(p^l)}(D_l)D_l^{-1}$,
(d) $\partial_F^{(p^l)}(\mathbf{y}) = A_l\mathbf{y}$ *for all* $l \in \mathbb{N}$ *where* $A_l = \partial_F^{(p^l)}(D_0 \cdots D_l)(D_0 \cdots D_l)^{-1}$.

Here the equivalence of (a) and (b) directly follows from the definition of M_l and (5–8). The equivalence with (c) and (d) is derived from

$$\partial_F^{(p^l)}(\mathbf{y}_l) = \partial_F^{(p^l)}(D_l\mathbf{y}_{l+1}) = \partial_F^{(p^l)}(D_l)\mathbf{y}_{l+1} = \partial_F^{(p^l)}(D_l)D_l^{-1}\mathbf{y}_l$$

and the corresponding equation for $\mathbf{y} = D_0 \cdots D_l \mathbf{y}_{l+1}$.

The families of higher differential equations in Proposition 5.9, (c) and (d) associated to the ID-module M are called an *iterative differential equation* (IDE) (in its relative and its absolute version, respectively). In terms of the logarithmic derivative associated to $\partial_F^{(p^l)}$

$$\lambda_l : \mathrm{GL}_n(F) \to F^{n\times n} = \mathrm{Lie}(\mathrm{GL}_n(F)), \quad D \mapsto \partial_F^{(p^l)}(D)D^{-1} \tag{5–9}$$

these read as

$$\begin{aligned} \partial_F^{(p^l)}(\mathbf{y}_l) &= \lambda_l(D_l)\mathbf{y}_l \quad \text{with} \quad \lambda_l(D_l) \in F_l^{n\times n}, \\ \partial_F^{(p^l)}(\mathbf{y}) &= \lambda_l(D_0 \cdots D_l)\mathbf{y} \quad \text{with} \quad \lambda_l(D_0 \cdots D_l) \in F^{n\times n}. \end{aligned} \tag{5–10}$$

We close the section with two typical examples:

EXAMPLE 5.5.1. Let $(F, \partial_F^*) = (K(t), \partial_t^*)$ be an ID-field of characteristic $p > 0$ and $M = Fb$ a one-dimensional vector space over F. Suppose $D_l = (t^{a_l p^l}) \in \mathrm{GL}_1(F_l)$. Then $A_l = \partial_F^{(p^l)}(D_0 \cdots D_l)(D_0 \cdots D_l)^{-1} = (a_l t^{-p^l})$ and the corresponding IDE is given by

$$\partial^{(p^l)}(y) = a_l t^{-p^l} y \quad \text{for} \quad l \in \mathbb{N}.$$

EXAMPLE 5.5.2. Let again $(F, \partial_F^*) = (K(t), \partial_t^*)$ with $\mathrm{char}(F) = p > 0$ and let $M = Fb_1 \oplus Fb_2$. For $D_l = \begin{pmatrix} 1 & a_l t^{p^l} \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(F_l)$ we obtain $A_l = \lambda_l(D_0 \cdots D_l) = \begin{pmatrix} 0 & a_l \\ 0 & 0 \end{pmatrix}$. Therefore the corresponding IDE simply is

$$\partial^{(p^l)}(\mathbf{y}) = \begin{pmatrix} 0 & a_l \\ 0 & 0 \end{pmatrix} \mathbf{y} \quad \text{where} \quad \mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

6. Iterative Picard–Vessiot Theory

6.1. Iterative PV-rings and fields. Surprisingly Picard–Vessiot rings and fields in positive characteristic can formally be defined in the same way as in characteristic zero. Let (F, ∂_F^*) be an ID-field of characteristic $p > 0$ with algebraically closed field of constants K and

$$\partial^{(p^l)}(\mathbf{y}) = A_l \mathbf{y} \quad \text{with } A_l \in F^{n \times n} \text{ for } l \in \mathbb{N} \tag{6–1}$$

an IDE over F as defined in the second line of (5–10). Let (R, ∂_R^*) be an ID-ring with $R \geq F$ and ∂_R^* extending ∂_F^*. Then $Y \in \mathrm{GL}_n(R)$ is called a *fundamental solution matrix* for the IDE (6–1) if $\partial_R^{(p^l)}(Y) = A_l Y$ for all $l \in \mathbb{N}$. The ring R is called an *iterative Picard–Vessiot ring* (IPV-ring) if it satisfies the following conditions:

(6–2) R is a simple ID-ring, i.e., R contains no nontrivial ID-ideals,
(6–3) there exists a $Y \in \mathrm{GL}_n(R)$ with $\partial_R^{(p^l)}(Y) = A_l Y$ for all $l \in \mathbb{N}$,
(6–4) R over F is generated by the coefficients of Y and $\det(Y)^{-1}$.

Again it is easy to verify that a finitely generated simple ID-ring is an integral domain with no new constants. The quotient field of R is called an *iterative Picard–Vessiot field* (IPV-field).

PROPOSITION 6.1. *Let (F, ∂_F^*) be an ID-field of characteristic $p > 0$ with algebraically closed field of constants K. Then for every IDE $\partial^{(p^l)}(\mathbf{y}) = A_l \mathbf{y}$ over F there exists an iterative Picard–Vessiot ring which is unique up to an iterative differential isomorphism.*

By Section 5.5 the matrices A_l have the form $A_l = \lambda_l(D_0 \cdots D_l)$ with $D_l = D(\varphi_l)$. Then $U := F[\mathrm{GL}_n] = F[x_{ij}, \det(x_{ij})^{-1}]_{i,j=1}^n$ can be given the structure of an ID-ring in the following way: First we define ∂_U^* on the vector space $F\langle x_{ij}\rangle_{i,j=1}^n$ simply by

$$\partial_U^{(p^l)}(\mathbf{x}_j) = A_l\mathbf{x}_j \quad \text{for } \mathbf{x}_j = (x_{1j},\dots,x_{nj})^{\mathrm{tr}}. \tag{6–5}$$

This corresponds to the projective system (N_l,ψ_l) where $N_l = F_l(X_l)$ denotes the F_l-vector space generated by the coefficients of $X_l = D_{l-1}^{-1}\cdots D_0^{-1}X$ and ψ_l the F_{l+1}-linear map defined by $\psi_l : N_{l+1} \to N_l$, $X_{l+1} \mapsto D_lX_{l+1} = X_l$. Then by the product rule ∂_U^* uniquely extends to an iterative derivation on the polynomial ring $F[x_{ij}]_{i,j=1}^n$ and finally on $F[\mathrm{GL}_n]$. Now we can proceed as in the classical case: Factoring U by a maximal ID-ideal P we obtain an IPV-ring R with fundamental solution matrix $Y = \kappa_P(X)$ which turns out to be uniquely determined by A_l up to ID-isomorphism ([MP], Lemma 3.4).

Again the IPV-field $E = \mathrm{Quot}(R)$ can be described without referring to R (see [Mat], Proposition 4.8).

Proposition 6.2. *Let (F,∂_F^*) be an ID-field of characteristic $p>0$ with algebraically closed field of constants and $A_l = \lambda_l(D_0\cdots D_l) \in F^{n\times n}$. Then an ID-field $(E,\partial_E^*) \ge (F,\partial_F^*)$ is an IPV-field for $(A_l)_{l\in\mathbb{N}}$ if and only if*

(a) *E does not contain new constants*,
(b) *there exists an $Y \in \mathrm{GL}_n(E)$ with $\partial_E^{(p^l)}(Y) = A_lY$ for all $l \in \mathbb{N}$*,
(c) *E is generated over F by the coefficients of Y.*

Obviously Proposition 6.2 immediately implies the following minimality property for the solution space of the underlying ID-module M.

Corollary 6.3. *The IPV-extension E/F in Proposition 6.2 is a minimal field extension of F such that $\dim_K(V_E(M)) = \dim_F M$ where $V_E(M) = V(M\otimes_F E)$.*

6.2. The ID-Galois group. An automorphism of an IPV-extension R/F or E/F is called an *iterative differential automorphism* (ID-automorphism) if it commutes with $\partial^{(k)}$ for all $k \in \mathbb{N}$. Correspondingly the group of all ID-automorphisms of R/F (or E/F) is called the *iterative differential Galois group* (ID-Galois group) of R/F or E/F and is denoted by $\mathrm{Gal}_{\mathrm{ID}}(R/F) = \mathrm{Gal}_{\mathrm{ID}}(E/F)$. This again is a maximal subgroup of $\mathrm{GL}_n(K)$ respecting the maximal ID-ideal P of $F[\mathrm{GL}_n]$ used for the construction of R (compare Proposition 2.3). With similar arguments as in the classical case we can deduce ([Mat], Theorem 3.10):

Proposition 6.4. *Let F be an ID-field of characteristic $p>0$ with algebraically closed field of constants K and E/F an IPV-extension. Then there exists a reduced linear algebraic group $\mathcal{G}$ defined over K such that $\mathrm{Gal}_{\mathrm{ID}}(E/F) \cong \mathcal{G}(K)$. Moreover the fixed field of $\mathcal{G}(K)$ equals F.*

From the preceding proposition it follows immediately that an IPV-extension E/F with finite ID-Galois group is an ordinary finite Galois extension. On the other hand a finite Galois extension E/F of an ID-field (F, ∂_F^*) is even an IPV-extension since ∂_F^* uniquely extends to E and since every $\gamma \in \mathrm{Gal}(E/F)$ is an ID-automorphism. To complete the proof we can use the following characterization of IPV-extensions ([Mat], Proposition 3.11).

Proposition 6.5. *Let $E \geq F$ be ID-fields of characteristic $p > 0$ over an algebraically closed field of constants. Then E/F is an IPV-extension if and only if*

(a) *there exists a finite-dimensional F-vector space $V \subseteq E$ with $E = F(V)$ and*
(b) *a group G of ID-automorphisms of E acting on V with $E^G = F$.*

Corollary 6.6. *Finite Galois extensions of ID-fields of characteristic $p > 0$ with algebraically closed field of constants are IPV-extensions and vice versa.*

We now return to our examples in Section 5.5 where $(F, \partial_F^*) = (K(t), \partial_t^*)$.

Example 6.2.1. Let $D_l = (t^{a_l p^l})$ as in Example 5.5.1 with corresponding IDE $\partial^{(p^l)}(y) = a_l t^{-p^l} y$ and IPV-extension E/F. Then for all $y \in V_E(M)$ and $\gamma \in \mathrm{Gal}_{\mathrm{ID}}(E/F)$

$$\partial_E^{(p^l)}\left(\frac{\gamma(y)}{y}\right) = \partial_E^{(p^l)}\left(\frac{\gamma(y_{l+1})}{y_{l+1}}\right) = 0 \quad \text{for} \quad y_{l+1} = D_l^{-1} \cdots D_0^{-1} y$$

such that $\gamma(y) = cy$ with $c \in K^\times$, i.e., $\mathrm{Gal}_{\mathrm{ID}}(E/F)$ is a subgroup of $\mathbb{G}_m(K)$. A formal solution of the IDE is given by $y = \prod_{l \in \mathbb{N}} t^{a_l p^l} = t^{\sum_{l \in \mathbb{N}} a_l p^l}$. This represents an algebraic function if and only if the p-adic integer $\alpha := \sum_{l \in \mathbb{N}} a_l p^l$ belongs to $\mathbb{Q}$, i.e., $\alpha = \frac{a}{n}$ with a, n coprime. Then $\mathrm{Gal}_{\mathrm{ID}}(E/F)$ is cyclic of order n, otherwise $\mathrm{Gal}(E/F) = \mathbb{G}_m(K) = K^\times$.

Example 6.2.2. From Example 5.5.2 we know that the IDE for

$$D_l = \begin{pmatrix} 1 & a_l p^l \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(F)$$

is given by

$$\partial^{(p^l)}(\mathbf{y}) = A_l \mathbf{y}, \quad \text{where } A_l = \begin{pmatrix} 0 & a_l \\ 0 & 0 \end{pmatrix} \text{ and } \mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Obviously $y_2 \in K$. Then the IPV-extension is generated by y_1, i.e., $E = F(y_1)$. For $\gamma \in \mathrm{Gal}_{\mathrm{ID}}(E/F)$ and $y_1 \in V_E(M)$ we have $\partial_E^{(p^l)}(\gamma(y_1) - y_1) = 0$ such that $\gamma(y_1) = y_1 + c$ with $c \in K$ and $\mathrm{Gal}_{\mathrm{ID}}(E/F) \leq \mathbb{G}_a(K)$. A formal solution of the IDE is given by $y_1 = \left(\sum_{l \in \mathbb{N}} a_l t^{p^l}\right) y_2$ with $y_2 \in K$. This function is separably algebraic over F if and only if the sequence $(a_l)_{l \in \mathbb{N}}$ becomes periodic. Then the ID-Galois group is a finite elementary abelian p-group, otherwise $\mathrm{Gal}_{\mathrm{ID}}(E/F) \cong \mathbb{G}_a(K)$.

6.3. Kolchin's Theorem and the Galois correspondence. Now we are ready to explain the ID-Galois correspondence. Again it relies substantially on Kolchin's theorem based on the following ID-torsor theorem.

THEOREM 6.7 (ID-TORSOR THEOREM). *Let F be an ID-field of characteristic $p > 0$ with algebraically closed field of constants K, R an IPV-ring over F for some IDE with* $\mathrm{Gal}_{\mathrm{ID}}(R/F) \cong \mathcal{G}(K)$ *and* $\mathcal{G}_F := \mathcal{G} \times_K F$. *Then* $\mathrm{Spec}(R)$ *is a* $\mathcal{G}_F$*-torsor.*

Here the proof given in [Put2], Section 6.2, in the classical case completely carries over by replacing all statements used for D-structures by the corresponding statements for ID-structures ([Mat], Theorem 4.4). Then Kolchin's theorem as stated in Corollary 2.6 is a formal consequence of it. As another consequence we get the ID-Galois correspondence in the following form ([MP], Theorem 3.5).

THEOREM 6.8 (ID-GALOIS CORRESPONDENCE). *Let F be an ID-field of characteristic $p > 0$ with algebraically closed field of constants K and E/F an IPV-extension of some IDE with* $\mathrm{Gal}_{\mathrm{ID}}(E/F) \cong \mathcal{G}(K)$. *Then*:

(a) *There exists an anti-isomorphism between the lattices*

$$\mathfrak{H} = \{\mathcal{H}(K) \mid \mathcal{H}(K) \leq \mathcal{G}(K) \textit{ reduced closed}\} \textit{ and } \mathfrak{L} = \{L \mid F \leq L \leq E \textit{ ID-field}\}$$

given by

$$\Psi : \mathfrak{H} \to \mathfrak{L},\ \mathcal{H} \mapsto E^{\mathcal{H}(K)} \textit{ and } \Psi^{-1} : \mathfrak{L} \to \mathfrak{H},\ L \mapsto \mathrm{Gal}_{\mathrm{ID}}(E/L).$$

(b) *If thereby $\mathcal{H}(K)$ is a normal subgroup then $L := E^{\mathcal{H}(K)}$ is an IPV-extension of F with* $\mathrm{Gal}_{\mathrm{ID}}(L/F) \cong \mathcal{G}(K)/\mathcal{H}(K)$.

The statement on finite ID-Galois extensions corresponding to Theorem 2.7(c) is already contained in Corollary 6.6.

6.4. Characterization of IPV-rings and fields. It remains to carry over the characterization theorems for PV-rings and PV-fields. Obviously the definition of a D-finite element has to be adjusted. Let E/F be an IPV-extension. Then $z \in E$ is called *iterative differentially finite over F* (ID-finite) if

$$\dim_F(W_E(z)) < \infty, \quad \text{where } W_E(z) := F\langle \partial_E^{(k)}(z)\rangle_{k\in\mathbb{N}}, \tag{6–6}$$

with the iterative derivation ∂_E^* of E. Then Proposition 2.10 translates into

PROPOSITION 6.9. *Let F be an ID-field of characteristic $p > 0$ with algebraically closed field of constants, R/F an IPV-ring and $E =$* $\mathrm{Quot}(R)$ *with* $G := \mathrm{Gal}_{\mathrm{ID}}(E/F)$. *Then for $z \in E$ the following conditions are equivalent*:

$$(a)\ \ z \in R, \qquad (b)\ \ \dim_K(K\langle Gz\rangle) < \infty, \qquad (c)\ \ \dim_F(W_E(z)) < \infty.$$

In the classical case the proof relies on the use of the minimal D-operator of z defined using the Wronskian $\mathrm{wr}(z_1,\dots,z_r)$ of a base of $K\langle Gz\rangle$. In positive characteristic this has to be replaced by a family of higher D-operators

$$\ell^{(k)}(y) := \frac{\mathrm{wr}_D^{(k)}(z_1,\dots,z_r,y)}{\mathrm{wr}_D(z_1,\dots,z_r)},$$

where the classical Wronskian determinant is replaced by the F. K. Schmidt Wronskian wr_D defined in (5–3) with set of derivation orders $D=\{d_1,\dots,d_r\}$ and where $\mathrm{wr}_D^{(k)}$ denotes the Wronskian with derivation orders $d_1,\dots,d_r$ and k. Then $K\langle Gz\rangle$ can be characterized as the K-vector space of solutions of $(\ell^{(k)})_{k\in\mathbb{N}}$ in E, which is denoted by $V_E(z)$. Using this we finally get the following characterization of IPV-fields analogous to Theorem 2.11.

THEOREM 6.10. *Let $E \geq F$ be ID-fields of characteristic $p>0$ with algebraically closed field of constants. Then E is an IPV-extension of F if and only if*

(a) *E/F is finitely generated by ID-finite elements*,
(b) *E and F share the same field of constants K*,
(c) *for any ID-finite element $z\in E$, $\dim_F(W_E(z)) = \dim_K(V_E(z))$.*

Complete proofs of Proposition 6.9 and Theorem 6.10 are presented in [Mat], Section 4.3.

7. Local Iterative Differential Modules

7.1. Tamely singular ID-modules. For the definition of regular and tamely singular ID-modules we use an ID-analogue of Corollary 3.4.

Let $F=K((t))$ be the field of power series over an algebraically closed field K of characteristic $p>0$ with $\partial_F^* = \partial_t^*$ and M an ID-module over F with iterative derivation ∂_M^*. Then the members $\partial_M^{(k)}$ of the family ∂_M^* generate a commutative K-algebra denoted by

$$\mathcal{D}_M := K[\partial_M^{(k)} | k\in\mathbb{N}]. \tag{7–1}$$

Corresponding to Corollary 3.4 (a) we call M a *regular local ID-module* if and only if M contains a $\mathcal{D}_M$-invariant $K[[t]]$-lattice (of full rank).

In order to obtain an analogous definition for tamely singular local ID-modules as in Corollary 3.4 we have to replace $\partial^{(k)}$ by $\delta^{(k)} := t^k\partial^{(k)}$.

PROPOSITION 7.1. *Let K be an algebraically closed field of characteristic $p>0$, $F=K((t))$ with $\partial_F^*=\partial_t^*$ and M an ID-module over F. Then*

$$\mathcal{D}_M^0 := K[\delta_M^{(k)} | k\in\mathbb{N}] \quad \textit{with } \delta_M^{(k)} := t^k\partial_M^{(k)}$$

is a commutative K-algebra with the additional property

$$(\delta^{(k)})^p = \delta^{(k)} \quad \textit{for } k\in\mathbb{N}.$$

Here the amazing second property immediately follows from

$$(\delta^{(k)})^p(t^n) = \binom{n}{k}^p t^n = \binom{n}{k} t^n = \delta^{(k)}(t^n).$$

According to Corollary 3.4(b) a local ID-module M is called a *tamely singular ID-module* if it contains a $\mathcal{D}_M^0$-invariant $K[\![t]\!]$-lattice. Obviously any regular local ID-module is tamely singular. Moreover, all one-dimensional local ID-modules are tamely singular by Example 5.5.1.

In case $\mathcal{D}_M^0$ acts on a finite-dimensional K-vector space V by Proposition 7.1 the $\delta^{(k)}$ are commuting diagonalizable endomorphisms. Hence V possesses a basis of common eigenvectors for $\mathcal{D}_M^0$. This already explains the first part of

Corollary 7.2. *Let V be a K-vector space of dimension $n \in \mathbb{N}$ which is a $\mathcal{D}_M^0$-algebra. Then the following hold*:

(a) *There exists a direct sum decomposition $V = \bigoplus_{i=1}^n V_i$ where each V_i is $\mathcal{D}_M^0$-stable of dimension* 1.

(b) *For each $V_i = K\mathbf{v}_i$ there exists an $\alpha_i \in \mathbb{Z}_p$ such that*

$$\delta_M^{(p^l)}(\mathbf{v}_i) = -\overline{\binom{\alpha_i}{p^l}}\mathbf{v}_i$$

where "$^-$" denotes the residue in $\mathbb{F}_p$.

Here the second statement follows from the fact that by the rule $(\delta_M^{(p^l)})^p = \delta_M^{(p^l)}$ the elements $a_{il} \in K$ with $\delta_M^{(p^l)}(\mathbf{v}_i) = -a_{il}\mathbf{v}_i$ belong to $\mathbb{F}_p$. Hence $\alpha_i := \sum_{l\in\mathbb{N}} a_{il}p^l \in \mathbb{Z}_p$ has the desired property. By abuse of language we call $V = \bigoplus_{i=1}^n V_i$ an *eigenspace decomposition* and $\alpha_i \in \mathbb{Z}_p$ *eigenvalues* of the whole family $\delta_M^* = (\delta_M^{(k)})_{k\in\mathbb{N}}$.

Using an induction process the eigenspace decomposition in Corollary 7.2 can be lifted to tamely singular ID-modules over $F = K((t))$. The result is the following ([MP], Proposition 6.1)

Theorem 7.3. *Let K be an algebraically closed field of characteristic $p > 0$, $F = K((t))$ be an ID-field with $\partial_F^* = \partial_t^*$ and let M be a tamely singular local ID-module over F of dimension n.*

(a) *There exist $\alpha_i \in \mathbb{Z}_p$ and a decomposition $M = \bigoplus_{i=1}^n M_i$ of M into a direct sum of one-dimensional ID-submodules $M_i = F\mathbf{b}_i$ with*

$$\delta_M^{(p^l)}(\mathbf{b}_i) = -\overline{\binom{\alpha_i}{p^l}}\mathbf{b}_i.$$

(b) *The ID-Galois group of the corresponding IPV-ring R/F is the maximal closed subgroup of $\mathbb{G}_m(K)^n$ preserving the $\mathbb{Z}$-relations between the eigenvalues*

α_i, *i.e.*,

$$\mathrm{Gal}(R/F) = \{(c_1, \dots, c_n) \in (K^\times)^n | \prod_{i=1}^n c_i^{d_i} = 1 \text{ if } \sum_{i=1}^n d_i\alpha_i \in \mathbb{Z}, d_i \in \mathbb{Z}\}.$$

In particular, if the α_i are $\mathbb{Z}$-linearly independent $\mathrm{Gal}(R/F)$ is the full group $\mathbb{G}_m(K)^n$. Here part (b) relies on the fact that algebraic relations over F between solutions y_i of M_i are of the simple form $\prod_{i=1}^n y_i^{d_i} = t^{d_0}$ with $d_i \in \mathbb{Z}$.

From Theorem 7.3 we further obtain the following characterization of regular and tamely singular local ID-modules by their ID-Galois groups.

Corollary 7.4. *Let (F, ∂_F^*), M and R be as in Theorem* 7.3.

(a) *M is tamely singular if and only if* $\mathrm{Gal}_{\mathrm{ID}}(R/F)$ *is diagonalizable.*
(b) *M is regular if and only if* $\mathrm{Gal}_{\mathrm{ID}}(R/F)$ *is trivial.*

Part (a) follows directly from Theorem 7.3, thanks to the fact that all one-dimensional local ID-modules are tamely singular. Then (b) follows from (a) by observing that in the regular case all eigenvalues equal zero.

7.2. The structure of local ID-modules. By Theorem 7.3 one-dimensional ID-modules M over $F = K((t))$ are determined by their eigenvalues $\alpha \in \mathbb{Z}_p$, and any $\alpha \in \mathbb{Z}$ leads to the trivial ID-module. To be more precise, the isomorphism class of a one-dimensional ID-module is characterized by the congruence class $\bar{\alpha}$ of its eigenvalue α modulo $\mathbb{Z}$. Using tensor products, the set of isomorphism classes $\mathbf{IDMod}_F^1$ of ID-modules of dimension 1 becomes a group $(\mathbf{IDMod}_F^1, \otimes)$ where in the parameter space $\mathbb{Z}_p/\mathbb{Z}$ the group law translates into the addition. This proves

Proposition 7.5. *Let $F = K((t))$ be an ID-field with $\partial_F^* = \partial_t^*$ over an algebraically closed field K of characteristic $p > 0$. Then*

$$(\mathbf{IDMod}_F^1, \otimes) \cong (\mathbb{Z}_p/\mathbb{Z}, +).$$

If the dimension of a local ID-module M is greater than 1 then inside M we can always find a nontrivial tamely singular ID-submodule and thus by Theorem 7.3 a nontrivial one-dimensional ID-submodule. Hence by induction on the dimension of M we obtain the first half of the following

Theorem 7.6. *Let $F = K((t))$ be an ID-field over an algebraically closed field K of characteristic $p > 0$ with $\partial_F^* = \partial_t^*$, M an ID-module over F and R an IPV-ring for M. Then*:

(a) *M is a repeated extension of one-dimensional ID-modules.*
(b) $\mathrm{Gal}(R/F) = \mathcal{G}(K)$ *is trigonalizable and there exists and exact sequence of finite groups*

$$1 \to P \to \mathcal{G}(K)/\mathcal{G}^0(K) \to Z \to 1$$

where P is a p-group and Z is a cyclic group of order prime to p.

The first assertion in (b) is a direct consequence of (a) since $\mathcal{G}(K)$ can be embedded into the standard Borel subgroup $\mathcal{B}_n(K)$, and the exact sequence for $\mathcal{G}/\mathcal{G}^0$ follows from Hilbert theory. A complete proof can be found in [MP], Proposition 6.3 and Corollary 6.4.

7.3. The connected local inverse problem. The question remains if every linear algebraic group with the two properties in Theorem 7.6 (b) appears as ID-Galois group over F. Before giving the solution in the connected case we have to explain the meaning of effectivity in the context of IPV-extensions. It is based on the following analogue of Proposition 4.2:

Proposition 7.7. *Let F be an ID-field of characteristic $p > 0$ with algebraically closed field of constants K and $\mathcal{G}$ a reduced connected linear algebraic group over K. Let M be an ID-module over F with associated projective system $(M_l, \varphi_l)_{l\in\mathbb{N}}$ and representing matrices D_l (with respect to suitable bases of M_l). Assume that $D_l \in \mathcal{G}(F_l)$; then for the corresponding IPV-extension E/F we have $\mathrm{Gal}_{\mathrm{ID}}(E/F) \leq \mathcal{G}(K)$.*

As in the classical case the proof relies on the fact that the defining ideal $I \trianglelefteq F[\mathrm{GL}_n]$ of $\mathcal{G}_F$ is an ID-ideal with respect to the iterative derivation on $F[\mathrm{GL}_n]$ given by $A_l = \lambda_l(D_0 \cdots D_l)$ according to Section 6.1 (see [MP], Proposition 5.3, or [Mat], Theorem 5.1).

In the case of equality $\mathrm{Gal}_{\mathrm{ID}}(E/F) = \mathcal{G}(K)$ the field extension E/F in Proposition 7.7 is called an *effective IPV-extension*. This further leads to the notion of an *effective embedding problem* as defined in Section 4.4 etc. In case the field F has cohomological dimension $\mathrm{cd}(F) \leq 1$ it follows from the Theorem 4.3 of Springer and Steinberg that all IPV-extensions E/F with connected Galois group are effective. More precisely in analogy to Corollary 4.4 we obtain ([Mat], Thm 5.9)

Corollary 7.8. *Let F be an ID-field of characteristic $p > 0$ with $\mathrm{cd}(F) \leq 1$ and with algebraically closed field of constants K, $\mathcal{H} \leq \mathrm{GL}_{n,K}$ a reduced connected closed subgroup and M an ID-module over F with projective system $(M_l, \varphi_l)_{l\in\mathbb{N}}$ and $D_l \in \mathcal{H}(F_l)$. Assume the ID-Galois group $\mathcal{G}(K)$ of M is connected. Then there exist $C_l \in \mathcal{H}(F_l)$ such that $C_l D_l C_{l+1}^{-1} \in \mathcal{G}(F_l)$.*

Now we come back to the inverse problem. In the case of connected groups this problem restricts to the realization of reduced connected solvable linear algebraic groups over K. Such a group $\mathcal{G}$ is a semidirect product $\mathcal{U} \rtimes \mathcal{T}$ of a unipotent normal subgroup $\mathcal{U}$ and a torus $\mathcal{T}$. According to Proposition 7.5 $\mathcal{T}(K)$ can effectively be realized as ID-Galois group over $F = K((t))$ by a direct sum of one-dimensional ID-modules $M = \bigoplus_{i=1}^{r} M_i$ with eigenvalues $\alpha_i \in \mathbb{Z}_p$ linearly independent over $\mathbb{Z}$. Since any connected solvable group with nontrivial unipotent radical possesses a normal subgroup $\mathcal{A}$ isomorphic to $\mathbb{G}_a$ ([Spr], Lemma 6.3.6) it remains to solve effective embedding problems with kernel $\mathbb{G}_a$.

In analogy to Proposition 4.12 and 4.13 we obtain in positive characteristic:

PROPOSITION 7.9. *Every effective split ID-embedding problem with kernel $\mathbb{G}_a$ has an effective proper solution over F, where $F = K(t)$ or $F = K((t))$ and K is algebraically closed of characteristic $p > 0$.*

PROPOSITION 7.10. *Every effective Frattini ID-embedding problem has an effective proper solution over F, where $F = K(t)$ or $F = K((t))$ and K is algebraically closed of characteristic $p > 0$.*

The next theorem is an immediate consequence of these two propositions.

THEOREM 7.11. *Let K be an algebraically closed field of characteristic $p > 0$. Then for every reduced connected solvable linear algebraic group $\mathcal{G}$ over K there exists an effective IPV-extension $E/K((t))$ with ID-Galois group $\mathcal{G}(K)$.*

7.4. The nonconnected local inverse problem. In order to solve the general inverse problem we still have to solve embedding problems with connected kernel and finite cokernel. With the following theorem of Borel–Serre [BoS] and Platonov (see [Weh], Lemma 10.10) this problem can be reduced to the solution of split embedding problems.

THEOREM 7.12. *Let $\mathcal{G}$ be a linear algebraic group over an algebraically closed field K. Then the connected component $\mathcal{G}^0$ of $\mathcal{G}$ possesses a finite supplement.*

In the case of potential local ID-Galois groups we can prove in addition that the finite supplement H can be chosen to be of the form $H = P \rtimes Z$ with P and Z as in Theorem 7.6(b) ([Mat], Proposition 8.4). From the inverse problem of ordinary Galois theory over $K((t))$ we know that finite groups of this type appear as Galois groups and hence as ID-Galois groups over $F := K((t))$ (compare [Bo$^+$], 14.2). Therefore there exists an IPV-extension L/F with $\mathrm{Gal}_{\mathrm{ID}}(L/F) \cong H$.

Now we want to realize the semidirect product $\mathcal{G}^0(K) \rtimes H$ with the obvious action of H on $\mathcal{G}^0(K)$ as an ID-Galois group over F. This leads to the following split embedding problem $\mathcal{E}(\alpha, \beta)$ with homomorphic regular section σ.

$$\begin{tikzcd}
& & \mathrm{Gal}(E/F) \arrow[r, dotted, "\mathrm{res}"] \arrow[d, dotted, "\gamma"'] & \mathrm{Gal}(L/F) \arrow[d, "\alpha", "\cong"'] & \\
1 \arrow[r] & \mathcal{G}^0(K) \arrow[r] & \mathcal{G}^0(K) \rtimes H \arrow[r, shift left, "\beta"] & H \arrow[l, shift left, "\sigma"] \arrow[r] & 1
\end{tikzcd} \qquad (7\text{–}2)$$

In other words, we have to find an IPV-extension E/L with connected Galois group $\mathrm{Gal}_{\mathrm{ID}}(E/L) \cong \mathcal{G}^0(K)$ such that E/F is an IPV-extension and in addition $\mathrm{Gal}_{\mathrm{ID}}(E/F) \cong \mathcal{G}^0(K) \rtimes H$ (via an isomorphism γ with $\alpha \circ \mathrm{res} = \beta \circ \gamma$). This problem can be attacked by the following criterion proved in [Mat], Theorem 8.2:

PROPOSITION 7.13. *Let $\mathcal{G} \cong \mathcal{G}^0 \rtimes H$ be a linear algebraic group defined over an algebraically closed field K of characteristic $p > 0$ with regular homomorphic* *section $\sigma : H \to \mathcal{G}(K)$. Further, let F be an ID-field with field of constants K and* $\mathrm{cd}(F) \leq 1$.

(a) *Let L/F be a finite Galois extension with Galois group isomorphic to H via α. Let*

$$\chi := \sigma \circ \alpha : \mathrm{Gal}(L/F) \to \sigma(H) \leq \mathcal{G}(K), \quad \eta \mapsto C_\eta$$

be the composite isomorphism. Then for all $l \in \mathbb{N}$ there exist elements $Z_l \in \mathrm{GL}_n(L_l)$ satisfying $\eta(Z_l) = Z_l C_\eta$ for all $\eta \in H \cong \mathrm{Gal}(L/F)$. Moreover, $L = F(Z)$ with $Z := Z_0$.

(b) *Let E/L be an IPV-extension with Galois group isomorphic to $\mathcal{G}^0(K)$ via an isomorphism*

$$\gamma_L : \mathrm{Gal}(E/L) \to \mathcal{G}^0(K) \trianglelefteq \mathcal{G}(K), \quad \varepsilon \mapsto C_\varepsilon.$$

Then there exist elements $Y_l \in \mathcal{G}^0(E_l)$ satisfying $\varepsilon(Y_l) = Y_l C_\varepsilon$ for all $\varepsilon \in \mathrm{Gal}(E/L)$ and $D_l \in \mathcal{G}^0(L_l)$ such that $Y_{l+1} = D_l^{-1} Y_l$. Moreover, $E = L(Y)$ with $Y := Y_0$.

(c) *Suppose in addition that the following equivariance condition is satisfied*:

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

Then E/F is an IPV-extension with ID-Galois group isomorphic to $\mathcal{G}(K)$ and fundamental solution matrix ZY. Further, the isomorphism γ_L in (*b*) *can be extended to an isomorphism*

$$\gamma : \mathrm{Gal}_{\mathrm{ID}}(E/F) \to \mathcal{G}(K) \quad \textit{with } \mathrm{res} \circ \alpha = \beta \circ \gamma.$$

In order to solve the embedding problem $\mathcal{E}(\alpha, \beta)$ above we thus have to construct an ID-module M over L having a system of representing matrices $D_l \in \mathcal{G}^0(L_l)$ as defined in Section 5.5 fulfilling the equivariance condition in (c). The latter can be transformed into $D_l = C_\eta \eta(D_l) C_\eta^{-1}$, i.e., D_l belongs to the group of F-rational points of the L/F-form $\mathcal{G}_\chi^0$ of $\mathcal{G}^0$ with the twisted Galois action given by

$$\eta * D = C_\eta \eta(D) C_\eta^{-1} = \chi(\eta)\eta(D)\chi(\eta^{-1}) \tag{7–3}$$

(compare [Spr], 12.3.7). This is the key observation for the proof of

Proposition 7.14. *For a potential local Galois group $\mathcal{G}(K)$* (*as described in Theorem* 7.6) *the derived split ID-embedding problem $\mathcal{E}(\alpha, \beta)$ given by* (7–2) *has a proper solution.*

For the proof we first show that the L/F-form $\mathcal{G}_\chi^0$ of $\mathcal{G}^0$ is F-split ([Mat], proof of Proposition 8.3). Then the proof of Theorem 7.11 can be recycled to realize $\mathcal{G}^0(K)$ as an ID-Galois group over L with matrices $D_l \in \mathcal{G}_\chi^0(F)$. Applying Proposition 7.13 yields the result.

The next theorem now follows almost immediately from Proposition 7.14:

THEOREM 7.15. *Let K be an algebraically closed field of characteristic $p > 0$. Then every trigonalizable reduced linear algebraic group $\mathcal{G}$ over K with $\mathcal{G}/\mathcal{G}^0 \cong P \rtimes Z$ and P, Z as in Theorem* 7.6 *is the ID-Galois group of some IPV-extension $E/K((t))$.*

Let $\mathcal{G}$ be as in Theorem 7.15. Then $\mathcal{G}$ has a finite supplement H of type $P \rtimes Z$. As remarked above, H can be realized as ID-Galois group of a finite extension L/F. By Proposition 7.14 we can solve the split embedding problem $\mathcal{E}(\alpha, \beta)$ for $\mathcal{G}^0(K) \rtimes H$ by $\gamma : \mathrm{Gal}(E/F) \xrightarrow{\cong} \mathcal{G}^0(K) \rtimes H$. Using the regular (morphic) homomorphism

$$\psi : \mathcal{G}^0(K) \rtimes H \to \mathcal{G}(K), \quad (D, C) \mapsto D \cdot C \tag{7–4}$$

the fixed field $\tilde{E} := E^{\mathrm{Ker}(\psi\circ\gamma)}$ of $\psi \circ \gamma$ defines an IPV-extension $\tilde{E}/F$ with $\mathrm{Gal}_{\mathrm{ID}}(\tilde{E}/F) \cong \mathcal{G}(K)$.

8. Global Iterative Differential Modules

8.1. The singular locus. In this chapter let F/K be an algebraic function field of one variable over an algebraically closed field K of characteristic $p > 0$, i.e., the function field $F = K(\mathcal{C})$ of a smooth projective curve $\mathcal{C}$ over K. Let M be an ID-module over F with projective system (M_l, φ_l) and E/F a corresponding IPV-extension. Then a point $x \in \mathcal{C}$ is called a *regular point of* M (or of E/F respectively) if there exists a local parameter t for x, an open neighborhood $\mathcal{V} \subseteq \mathcal{C}$ of x and a $\partial^*_{M,t}$-stable $\mathcal{O}(\mathcal{V})$-lattice $\Lambda \subseteq M$, where

$$\partial^{(p^l)}_{M,t} = \tilde{\varphi}_0 \circ \cdots \circ \tilde{\varphi}_l \circ \partial^{(p^l)}_t \circ \tilde{\varphi}_l^{-1} \circ \cdots \circ \tilde{\varphi}_0^{-1} \tag{8–1}$$

according to Corollary 5.8. The points which are not regular are called *singular points* and the set $\mathcal{S}_M \subseteq \mathcal{C}$ of singular points of M is referred to as the *singular locus of* M. The iterative chain rule guarantees that the notion of a regular point does not depend on the choice of the local parameter t.

The following proposition is immediate and connects the regularity of points with the regularity of local ID-modules introduced in the last chapter.

PROPOSITION 8.1. *Let $F = K(\mathcal{C})$ be a function field over an algebraically closed field K of characteristic $p > 0$ and $x \in \mathcal{C}$ be a regular point of an ID-module M over F. Then $F_x \otimes_F M$ is a regular local ID-module over the completion F_x of F at x.*

Unfortunately this local property of regular points cannot be used for the definition as the following example shows. Let $\mathcal{C} = \mathbb{P}^1(K)$ be the projective line and $F = K(t)$ its field of rational functions with $\partial^*_F = \partial^*_t$. Further, let M be a one-dimensional ID-module over F with $D_l = (t - a_l)^{p^l} \in \mathbb{G}_m(F_l)$ for pairwise distinct a_l. Then we obtain an IDE by

$$\partial^{(p^l)}_F(y_l) = \lambda_l(D_l) y_l = (t - a_l)^{-p^l} y_l$$

which has the symbolic solution $y = \prod_{l\in\mathbb{N}}(t-a_l)^{p^l}$. The differential Galois group lies inside $\mathbb{G}_m(K)$ and is in fact the full multiplicative group by the considerations made in Section 6.2. Obviously every point $x \in \mathbb{P}^1(K)\backslash\mathcal{S}$ with $\mathcal{S} = \{a_l | \ l \in \mathbb{N}\}$ is regular. For $x \in \mathcal{S}$, we can assume without loss of generality that $x = a_0$. Then $F_x = K((t-a_0))$ and thus y again defines an element in M_x. Consequently, M_x is regular for all $x \in \mathbb{P}^1(K)$. In particular, all local ID-Galois groups are trivial, and $\mathrm{Gal}_{\mathrm{ID}}(E/F)$ is not generated by the Galois groups of the localized modules.

8.2. Realization of connected groups. As explained in Section 7.3, a solvable connected group $\mathcal{G} = \mathcal{U} \rtimes \mathcal{T}$ can be realized over $F = K(t)$ starting from an effective realization of $\mathcal{T}(K)$ over F by solving effective embedding problems with kernel $\mathbb{G}_a(K)$. As in the local case $\mathcal{T}(K)$ can be realized effectively by a direct sum of one-dimensional ID-modules over F with p-adic eigenvalues linearly independent over $\mathbb{Z}$. Hence from Propositions 7.9 and 7.10 we obtain also in the global case:

PROPOSITION 8.2. *For every reduced connected solvable linear algebraic group $\mathcal{G}$ over an algebraically closed field K of characteristic $p > 0$ the group of K-rational points $\mathcal{G}(K)$ can be realized effectively as ID-Galois group over $K(t)$.*

In the nonsolvable case first we have to find a substitute for Propositions 4.8 and 4.9 in the classical case. This is given by

PROPOSITION 8.3. *Let $\mathcal{G}$ be a reduced connected linear algebraic group over an algebraically closed field K of characteristic $p > 0$, let $\mathcal{A}$ be either $\mathbb{G}_a$ or $\mathbb{G}_m$ and set $S_l = K[t^{p^l}]$ or $S_l = K[t^{p^l}, t^{-p^l}]$, respectively. Suppose M is an ID-module over $F = K(t)$ with projective system $(M_l, \varphi_l)_{l\in\mathbb{N}}$ and representing matrices D_l of φ_l (with respect to a given basis of M_l). Assume further the following properties are satisfied:*

(a) *For all $l \in \mathbb{N}$ there exist $\gamma_l \in \mathrm{Mor}(\mathcal{A}, \mathcal{G})$ such that $D_l = \gamma_l(t^{p^l}) \in \mathcal{G}(S_l)$ and $\gamma_l(1_{\mathcal{A}(K)}) = 1_{\mathcal{G}(K)}$.*
(b) *For all $m \in \mathbb{N}$ the set $\{\gamma_l(\mathcal{A}(K)) | \ l \geq m\}$ generates $\mathcal{G}(K)$ as an algebraic group.*
(c) *There exists a number $d \in \mathbb{N}$ such that the degree of γ_l is bounded by d for all $l \in \mathbb{N}$.*
(d) *If $l_0 < l_1 < \ldots$ is the sequence of natural numbers l_i for which $\gamma_{l_i} \neq 1$, then $\lim_{i\to\infty}(l_{i+1} - l_i) = \infty$.*

Then the IPV-field E for M is effective over F with $\mathrm{Gal}_{\mathrm{ID}}(E/F) \cong \mathcal{G}(K)$.

Here in (c) the degree $\deg(\gamma_l)$ is defined as the maximum of the degrees of the numerator and the denominator of the reduced expression of γ_l (with respect to t^{p^l}). The proof of Proposition 8.3 is rather technical and can not be reproduced in this survey (compare [MP], Lemma 7.4, and [Mat], Theorem 7.14). But observe that the gap condition (d) mimicking the condition for Liouvillean transcendental numbers excludes all nonconnected subgroups.

As a consequence of Proposition 8.3 we obtain the solution of the connected inverse problem.

THEOREM 8.4. *Let $F = K(t)$ be an ID-field over an algebraically closed field K of characteristic $p > 0$ with $\partial_F^* = \partial_t^*$ and $\mathcal{G}$ be a reduced connected linear algebraic group over K. Then $\mathcal{G}(K)$ can effectively be realized as an ID-Galois group over F.*

For the proof one observes first that a maximal unipotent subgroup $\mathcal{U}(K)$ of $\mathcal{G}(K)$ can be realized via some $M \in \mathbf{IDMod}_F$ with projective system (M_l, φ_l) satisfying conditions (a) to (c) of Proposition 8.3. A suitable choice of the sequences (a_l) appearing in Example 6.2.2 for the chief factors $\mathcal{A}_i(K)$ of $\mathcal{U}(K)$ of type $\mathbb{G}_a(K)$ also guarantees property (d). (Take for example $a_{i,l} \in \mathbb{F}_p$ and $\alpha_i = \sum_{l \in \mathbb{N}} a_{i,l} p^l \in \mathbb{Z}_p$ algebraic independent over $\mathbb{Q}$). In the general case let $\mathcal{T}(K)$ be a maximal torus of $\mathcal{G}(K)$. Then $\mathcal{G}(K)$ is generated as an algebraic group by a finite number of conjugates of $\mathcal{U}(K)$ and $\mathcal{T}(K)$. By Proposition 8.2 $\mathcal{T}(K)$ has an effective realization via some $N \in \mathbf{IDMod}_F$ with projective system (N_l, ψ_l) satisfying conditions (a) to (d) in Proposition 8.3. Combining different conjugates of φ_l and ψ_l we obtain an ID-module $\tilde{M}$ which again satisfies the four conditions. Hence the corresponding IPV-field E is effective with $\mathrm{Gal}(E/F) \cong \mathcal{G}(K)$. Because of $D(\varphi_l) \in \mathcal{G}(K[t^{p^l}])$ and $D(\psi_l) \in \mathcal{G}(K[t^{p^l}, t^{-p^l}])$ from the proof we obtain in addition:

COROLLARY 8.5. *If $\mathcal{G}(K)$ in Theorem* 8.4 *above is generated by unipotent subgroups, it can be realized with at most one singular point at ∞. In the general case, $\mathcal{G}(K)$ can be realized with singular points at most in* $\{0, \infty\}$.

8.3. Realization of nonconnected groups. In order to solve the nonconnected inverse problem we need a version of Proposition 8.3 which not only works over $F = K(t)$, but also over finite Galois extensions of F.

PROPOSITION 8.6. *Let K be an algebraically closed field of characteristic $p > 0$ and let $L = K(s,t)$ be a finite Galois extension of $F = K(t)$ with $\partial_F^* = \partial_t^*$. Let $\mathcal{C}$ be an affine model of L/K defined by $f(s,t) = 0$ such that $\mathfrak{o} = (0,0) \in \mathcal{C}$ is a regular point. Then $L_l = L^{p^l} = K(s^{p^l}, t^{p^l})$ has an affine model $\mathcal{C}_l$ defined by some $f_l(s^{p^l}, t^{p^l}) = 0$. Let $\mathcal{G}$ be a reduced connected linear algebraic group over K and let $\mathcal{G}_\chi$ be an L/F-form of $\mathcal{G}$ defined by a regular homomorphic section $\chi : H := \mathrm{Gal}(L/F) \to \mathcal{G} \rtimes H$ as in* (7–3) *with $\mathcal{G}_\chi(F_l) \le \mathcal{G}(L_l)$. Let M be an ID-module over L with projective system $(M_l, \varphi_l)_{l \in \mathbb{N}}$ and representing matrices D_l. Suppose the following properties are satisfied*:

(a) *For all $l \in \mathbb{N}$ there exists a rational map $\gamma_l : \mathcal{C}_l \to \mathcal{G}_\chi$ such that $D_l = \gamma_l(s^{p^l}, t^{p^l}) \in \mathcal{G}_\chi(F_l)$ and $\gamma_l(\mathfrak{o}) = 1_{\mathcal{G}(K)}$.*

(b) *For all $m \in \mathbb{N}$ the algebraic group over L generated by $\{\gamma_l(\mathcal{C}_l) \mid l \ge m\}$ contains $\mathcal{G}(K)$.*

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

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

Then M defines an effective IPV-extension E/L with $\mathrm{Gal}_{\mathrm{ID}}(E/L) \cong \mathcal{G}(K)$.

Here in (c) the degree $\deg(\gamma_l)$ denotes the maximum of the degrees of the numerator and the denominator of the divisors of the matrix entries of D_l in L_l (compare to Proposition 8.3). From Proposition 8.6 we can derive

PROPOSITION 8.7. *Let K be an algebraically closed field of characteristic $p > 0$. Then every ID-embedding problem over $K(t)$ with connected kernel and finite cokernel has a proper solution.*

By the Theorem 7.12 of Borel–Serre and Platonov the problem can be reduced to a split ID-embedding problem of the same type. Hence, thanks to Proposition 7.13, we only need to find a sequence of matrices $D_l \in \mathcal{G}_\chi^0(F_l)$ which satisfy the conditions of Proposition 8.6. The group $\mathcal{G}_\chi^0$ is generated as an algebraic group by finitely many F-split unipotent subgroups and F-tori (essentially from [Spr], Corollary 13.3.10). For any such unipotent subgroup the matrices needed may be found as in the proof of Theorem 8.4. By [Tit], III, Proposition 1.6.4 a single element suffices to generate a dense subgroup of an F-torus, and such an element may be normed to satisfy condition (a) in Proposition 8.6. Finally, we splice these matrices together into a sequence satisfying the gap condition (d) in Proposition 8.6. Then we obtain an effective IPV-extension E/L with $\mathrm{Gal}_{\mathrm{ID}}(E/L) \cong \mathcal{G}^0(K)$ by Proposition 8.6 and $\mathrm{Gal}_{\mathrm{ID}}(E/F) \cong \mathcal{G}(K)$ by Proposition 7.13. Obviously Proposition 8.7 implies the solution of the nonconnected inverse problem.

THEOREM 8.8. *Let $\mathcal{G}$ be a reduced linear algebraic group over an algebraically closed field K of characteristic $p > 0$. Then $\mathcal{G}(K)$ appears as an ID-Galois group of an IPV-extension $E/K(t)$ with $\partial^*_{K(t)} = \partial^*_t$.*

8.4. The differential Abhyankar conjecture. In Corollary 8.5 we have seen that reduced connected linear algebraic groups which are generated by their closed unipotent subgroups can be realized as ID-Galois groups over $F = K(t)$ with at most one singular point. This statement resembles the Abhyankar conjecture stated in [Abh] and proved by Raynaud [Ray]: Every finite group which is generated by its p-Sylow groups can be realized as a Galois group over $F = K(t)$ unramified outside $\{\infty\}$. Such groups are usually called *quasi-p groups.*

In order to reduce an ID-embedding problem with connected unipotently generated kernel and finite quasi-p cokernel to split embedding problems of the same type we have to use the following variant of Theorem 7.12 ([Mat], Proposition 8.12).

Proposition 8.9. *Let $\mathcal{G}$ be a unipotently generated linear algebraic group over an algebraically closed field K of characteristic $p > 0$. Then $\mathcal{G}^0(K)$ has a finite supplement which is a quasi-p group.*

Next we have to adapt Proposition 8.6.

Proposition 8.10. *If the Galois extension L/F in Proposition* 8.6 *is unramified outside $\{\infty\}$ and $\mathcal{G}_\chi$ is a connected unipotent F-split group, the IPV-extension E/L can be constructed unramified outside the places of L above $\{\infty\}$.*

With these preparations we are able to prove the following differential analogue of the Abhyankar conjecture in the nonconnected case.

Theorem 8.11. *Let K be an algebraically closed field of characteristic $p > 0$ and let $F = K(t)$ an ID-field with $\partial_F^* = \partial_t^*$. Let $\mathcal{G}$ be a unipotently generated reduced linear algebraic group defined over K. Then $\mathcal{G}(K)$ can be realized as an ID-Galois group over F with at most one singularity.*

By Proposition 8.9 the connected component $\mathcal{G}^0(K)$ has a finite supplement H in $\mathcal{G}(K)$ which is a quasi-p group. Hence it suffices to consider the corresponding split ID-embedding problem. By the classical Abhyankar conjecture proved by Raynaud [Ray] there exists a finite Galois extension L/F with $\mathrm{Gal}(L/F) = H$ which is unramified outside $\{\infty\}$. The composite $\chi : \mathrm{Gal}(L/F) \tilde{\to} H \hookrightarrow \mathcal{G}(K)$ defines a twisted form $\mathcal{G}_\chi^0$ of $\mathcal{G}^0$ as used in Proposition 8.6. It can be shown that $\mathcal{G}_\chi^0$ is F-quasi-split and contains a maximal closed F-split unipotent subgroup $\mathcal{U}$ ([Mat], proof of Theorem 8.14). Since $\mathcal{G}_\chi^0(F)$ is dense in $\mathcal{G}_\chi^0(L) = \mathcal{G}^0(L)$, the group $\mathcal{G}_\chi^0$ is generated by finitely many $\mathcal{G}_\chi^0(F)$-conjugates of $\mathcal{U}$. Thanks to Proposition 8.10 these conjugates may be generated as algebraic groups over L by equivariant matrices with singular locus above $\{\infty\}$. Using Proposition 7.13 (c), these matrices may be combined into a sequence which realizes $\mathcal{G}(K)$ as ID-Galois group over F with singular locus inside $\{\infty\}$.

At the end we want to call the reader's attention to the parallelism between the differential Abhyankar conjecture in characteristic $p > 0$ as presented in Theorem 8.11 and the Theorem 3.11 of Ramis. It generalizes one of the Ramis–Raynaud analogies between finite Galois extensions in characteristic $p > 0$ and PV-extensions in characteristic 0. More specific links, particularly those concerning tame and wild ramifications and singularities respectively, are collected in the Ramis–Raynaud dictionary presented in the Bourbaki lecture notes [Put1].

References

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

[And] André, Y.: Différentielles non commutatives et théorie de Galois différentielle et aux différences. Ann. Sci. ENS **34** (2001), 685–739.

[AB] Anosov, D. V.; Bolibruch, A. A.: *The Riemann–Hilbert Problem.* Vieweg, Braunschweig 1994.

[Bor] Borel, A.: *Linear Algebraic Groups.* Springer, New York 1991.

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

[Bo$^+$] Bost, J.-B. et al.: *Courbes Semi-stables et Groupe Fondamental en Géometrie Algébrique.* Birkhäuser, Boston 2000.

[Del] Deligne, P.: Catégories Tannakiennes. In *The Grothendieck Festschrift. Volume* II, p. 111–195. Birkhäuser, Boston 1990.

[Eis] Eisenbud, D.: *Commutative Algebra with a View Toward Algebraic Geometry.* Springer, New York 1995.

[For] Forster, O.: *Riemannsche Flächen.* Springer, Berlin etc. 1977.

[Ful] Fulton, W.: *Algebraic Topology.* Springer, New York 1995.

[Har] Hartmann, J.: *On the Inverse Problem in Differential Galois Theory.* Thesis, Heidelberg 2002.

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

[Jac] Jacobson, N.: *Basic Algebra II.* Freeman, New York 1980.

[Kap] Kaplansky, I.: *An Introduction to Differential Algebra.* Hermann, Paris 1976.

[Kat1] Katz, N.: A simple algorithm for cyclic vectors. Amer. J Math. **109** (1987), 65–70.

[Kat2] Katz, N.: *Exponential Sums and Differential Equations.* Princeton Univ. Press, Princeton 1990.

[Kov] Kovacic, J. J.: The inverse problem in the Galois theory of differential equations. Annals of Math. **89** (1969), 583–608.

[Mag] Magid, A.: *Lectures on Differential Galois Theory*, AMS, Providence 1997.

[MM] Malle, G.; Matzat, B. H.: *Inverse Galois Theory.* Springer, Berlin 1999.

[Mat] Matzat, B. H.: *Differential Galois Theory in Positive Characteristic.* IWR-Preprint 2001-35.

[MP] Matzat, B. H.; Put, M. van der: Iterative differential equations and the Abhyankar conjecture. J. reine angew. Math. (to appear).

[MS] Mitschi, C.; Singer, M. F.: Connected linear groups as differential Galois groups. J. Algebra **184** (1996), 333–361.

[Obe] Oberlies, T.: Connected embedding problems. Preprint, Heidelberg 2001.

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

[Put1] Put, M. van der: Recent work on differential Galois theory. Astérisque **252** (1998), 341–367.

[Put2] Put, M. van der: Galois theory of differential equations, algebraic groups and Lie algebras. J. Symb. Comput. **28** (1999), 441–472.

[Ram] Ramis, J.-P.: About the inverse problem in differential Galois theory: The differential Abhyankar conjecture. In B. L. J. Braaksma et al.: *The Stokes Phenomenon and Hilbert's 16th Problem*, p. 261–278, World Scientific, Singapore 1996.

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

[Sch] Schmidt, F. K.: Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern. Math. Zeitschr. **45** (1939), 62–74.

[Ser] Serre, J.-P.: *Galois Cohomology*, Springer, Berlin 1997.

[Sin] Singer, M.: Moduli of linear differential equations on the Riemann sphere with fixed Galois groups. Pacific J. Math. **106** (1993), 343–395.

[Spr] Springer, T. A.: *Linear Algebraic Groups*, Birkhäuser, Boston 1998.

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

[TT] Tretkoff, C.; Tretkoff, M.: Solution of the inverse problem of differential Galois theory in the classical case. Amer. J. Math. **101** (1979), 1327–1332.

[Voe] Völklein, H.: *Groups as Galois Groups*, Cambridge University Press 1996.

[Weh] Wehrfritz, B. A. F.: *Infinite Linear Groups*. Springer, Berlin 1973.

B. Heinrich Matzat
IWR
University of Heidelberg
Im Neuenheimer Feld 368
D-69120 Heidelberg
Germany
matzat@iwr.uni-heidelberg.de

Marius van der Put
Department of Mathematics
University of Groningen
P.O. Box 800
NL-9700 AV Groningen
The Netherlands
mvdput@math.rug.nl