FROM FROBENIUS STRUCTURES TO DIFFERENTIAL EQUATIONS

B. H. Matzat

January 24, 2008

0 Introduction

Frobenius structures are omnipresent in arithmetic geometry. In this note we show that over suitable rings, Frobenius endomorphisms define differential structures and vice versa. This includes, for example, differential rings in positive characteristic and complete non-archimedean differential rings in characteristic zero. Further, in the global case, the existence of sufficiently many Frobenius rings is related to algebraicity properties. These results apply, for example, to t-motives as well as to p-adic and arithmetic differential equations.

In Chapter 1 Frobenius rings are defined as rings which modulo some prime ideal are equipped with an ordinary Frobenius endomorphism. (Rings with geometric Frobenius endomorphisms can be obtained from these "arithmetic" Frobenius rings by tensoring with rings with trivial Frobenius action). It is shown how Frobenius modules over such rings can be trivialised by some completion of the base ring (Thm. 1.7); in the case of an ordinary Frobenius module an algebraic extension is sufficient(Thm. 1.2).

Chapter 2 contains results in positive characteristic p. Here Frobenius modules and (iterative) differential modules are equivalent to certain projective systems. These can be used for transport of structures (Thm. 2.1 and Corollaries) and comparison of solution rings (Thm. 2.3). Chapter 3 is concerned with the p-adic case. Here again Frobenius structures define uniquely related differential structures (Thm. 3.1). The corresponding system of differential equations is obtained by a non-archimedean limit process (Cor. 3.2) and can be solved by solutions of the underlying Frobenius module (Thm. 3.3).

In Chapter 4 following [2] and [13] for differential and Frobenius modules, Galois group schemes are introduced. The related arithmetic Galois correspondence even takes care of inseparable extensions (corresponding to non-reduced group schemes). In the case of compatible differential and Frobenius structures the Galois group schemes are related by base change.

Finally in Chapter 5 differential rings and modules over Dedekind rings of algebraic numbers are studied. Here it is shown that differential modules provided with higher derivations lead to Picard-Vessiot extensions generated by Taylor series with coefficients in base ring (Cor. 5.2). This creates the possibility to compare these global PV-rings with the PV-rings of the reduced (iterative) differential modules in positive characteristic (Thm. 5.3). In particular, the existence of sufficiently many (congruence) Frobenius endomorphisms is equivalent to the algebraicity of the global PV-ring (Thm. 5.5).

1 Frobenius Modules and Frobenius Structures

1.1 A pair (S, ϕ) consisting of an integral domain S of characteristic $p > 0$ and an endomorphism $\phi \in \mathrm{End}(S)$ is called an *ordinary Frobenius ring* if there exists a prime power $q = p^d$ such that ϕ is the q-power endomorphism

$$\phi_q : S \to S, \quad a \mapsto a^q.$$

More generally a pair (S, ϕ) consisting of an integral domain of arbitrary characteristic and an endomorphism $\phi \in \mathrm{End}(S)$ is called a (lifted) *Frobenius ring (F-ring)* if S contains a ϕ-invariant prime ideal Q such that the residue ring $\overline{S} := S/Q$ equipped with the induced Frobenius endomorphism $\overline{\phi}$ is an ordinary Frobenius ring. Then Q is called a *characteristic prime ideal of* (S, ϕ) and ϕ the *Frobenius endomorphism of* S. For a Frobenius ring (S, ϕ) we obtain a family of *higher images* $S_l := \phi^l(S)$. These are Frobenius rings with the restricted Frobenius endomorphism $\phi_l := \phi|_{S_l}$. Further (S, ϕ) defines the *ring of Frobenius invariants* $S^\phi := \{a \in S \mid \phi(a) = a\}$.

In case the Frobenius endomorphism ϕ is an automorphism, (S, ϕ) becomes a difference ring with respect to ϕ. Such rings have been studied, for example, in [11]. Before introducing Frobenius modules let us discuss three examples:

1.1.1 Any integral domain S of characteristic $p > 0$ together with the p-power endomorphism ϕ_p is an ordinary Frobenius ring with characteristic prime ideal (0).

1.1.2 Let K be a perfect field containing $\mathbb{F}_p$with p-power endomorphism $\phi = \phi_p$. Then $S := K[s, t]$ with the Frobenius action $\phi|_K = \phi_p, \phi(s) = s, \phi(t) = t^p$ is a Frobenius ring with characteristic prime ideal (s). The higher images are $S_l = K[s, t^{p^l}]$ and the ring of invariants is given by $S^\phi = \mathbb{F}_p[s]$. Such rings occur as base rings of Anderson's t-modules and t-motives (see [15], Ch. 7.1).

1.1.3 Let W be the Witt ring over the algebraic closure $\mathbb{F}_p^{\mathrm{alg}}$ of $\mathbb{F}_p$ with the uniquely lifted Frobenius automorphism $\phi_W = \phi_p$. (This ring coincides with the completion of the ring of integers $\mathbb{Z}_p^{\mathrm{ur}}$ of the maximal unramified extension $\mathbb{Q}_p^{\mathrm{ur}}$ of the field of p-adic numbers $\mathbb{Q}_p$). Then $S := W[t]$ and $\phi : S \to S$ with $\phi|_W = \phi_W$ and $\phi(t) = t^p$ form a Frobenius ring with characteristic ideal (p). Its residue ring is the ordinary Frobenius ring $\mathbb{F}_p^{\mathrm{alg}}[t]$. The higher images are $S_l = W[t^{p^l}]$ and the invariant ring is $S^\phi = \mathbb{Z}_p$. The ring S and its completion with respect to the Gauß extension of the p-adic value play a fundamental role in the theory of p-adic differential equations (see [1] and [14]).

1.2 Let (S, ϕ) be a Frobenius ring as defined above. Then a pair (M, Φ) consisting of a free S-module M of finite rank m and an endomorphism $\Phi : M \to M$ is called a *Frobenius module over* S if Φ is ϕ-semilinear, i.e.,

$$\Phi(x+y)=\Phi(x)+\Phi(y) \quad \text{and} \quad \Phi(ax)=\phi(a)\Phi(x) \quad \text{for all} \quad x,y\in M \quad \text{and} \quad a\in S$$

and Φ maps a basis of M onto a basis of M. Similar to the case of rings we obtain a *family of higher images* $M_l := \Phi^l(M)$, where M_l is a Frobenius module over S_l.

For any extension ring $\widetilde{S}/S$ with extended Frobenius endomorphism $\widetilde{\phi}$ the module $M_{\widetilde{S}} := \widetilde{S}\otimes_S M$ becomes a Frobenius module over $\widetilde{S}$ with an extended Frobenius action $\widetilde{\Phi}$ in an obvious way. The solution space of M over such an extension ring $\widetilde{S}$ is defined by

$$\mathrm{Sol}^{\Phi}_{\widetilde{S}}(M) := (\widetilde{S}\otimes_S M)^{\widetilde{\Phi}} = \{x\in \widetilde{S}\otimes_S M \mid \widetilde{\Phi}(x)=x\}.$$

Obviously $\mathrm{Sol}^{\Phi}_{\widetilde{S}}(M)$ is an $\widetilde{S}^{\widetilde{\phi}}$-module. In case $\widetilde{S}^{\widetilde{\phi}}$ is a field, $\mathrm{Sol}^{\Phi}_{\widetilde{S}}(M)$ is free of rank at most m. The module M is called *trivial over* $\widetilde{S}$ if $\mathrm{Sol}^{\Phi}_{\widetilde{S}}(M)$ contains a basis of $\widetilde{S}\otimes_S M$. Then $(\widetilde{S},\widetilde{\phi})$ is called a *solution ring (or trivialization) of the Frobenius module* M.

From the definitions we immediately obtain

Proposition 1.1. *Let (S,ϕ) be a Frobenius ring and (M,Φ) a Frobenius module over S. Then $M^* := \bigcap_{l\in\mathbb{N}} M_l$ with $\Phi|_{M^*}$ is a Frobenius module over $S^* := \bigcap_{l\in\mathbb{N}} S_l$ with $\mathrm{Sol}^{\Phi}_{S^*}(M^*) = \mathrm{Sol}^{\Phi}_{S}(M)$.*

1.3 We now turn to Frobenius modules over ordinary Frobenius rings. In the case that the base ring is a field, we obtain

Theorem 1.2. *Let (S,ϕ) be an ordinary Frobenius field and (M,Φ) a Frobenius module over S. Then there exists a unique minimal solution ring R of M over S. The ring R is an ordinary Frobenius field with respect to the unique extension of ϕ onto R. Moreover the field extension R/S is a finite Galois extension.*

For the proof see [8], Prop. 5.4, or [6], Thm. 1.1. It follows that in the case of base rings a solution ring R of M can be found inside a finite Galois extension of $\mathrm{Quot}(S)$. In addition, Theorem 1.2 implies

Corollary 1.3. *Every Frobenius module over a separably algebraically closed ordinary Frobenius field is trivial.*

In order to make Theorem 1.2 more explicit, let $B := \{b_1,\ldots,b_m\}$ be a basis of M over S with $\Phi(b_j) = \sum_{i=1}^{m} b_i d_{ij}$. Then $D_B(\Phi) := (d_{ij})_{i,j=1}^m \in \mathrm{GL}_m(S)$ is a representing matrix of Φ. Further,

$$\Phi(x)=\Phi(B\boldsymbol{y})=\Phi(B)\phi(\boldsymbol{y})=BD_B(\Phi)\phi(\boldsymbol{y})$$

holds for $x=\sum_{j=1}^{m} b_j y_j = B\boldsymbol{y}\in M$. Thus $x=B\boldsymbol{y}$ is a solution of M if and only if $\Phi(B\boldsymbol{y})=B\boldsymbol{y}$, or $D_B(\Phi)\phi(\boldsymbol{y})=\boldsymbol{y}$, respectively. This is equivalent to the equation

$$\phi(\boldsymbol{y})=A\boldsymbol{y} \quad \text{with} \quad A=D_B(\Phi)^{-1}\in \mathrm{GL}_m(S).$$

Corollary 1.4. *Under the assumption of Theorem 1.2 there exists a matrix* $Y=(y_{ij})_{i,j=1}^m\in \mathrm{GL}_m(R)$ *with* $\phi_R(Y)=AY$, *and* R *is generated over* S *by the entries of* Y, *i.e.,* $R=S(y_{ij}\mid i,j=1,\ldots,m)$.

Such a matrix Y is called a *fundamental solution matrix* of (M,Φ). It is uniquely determined by M up to left multiplication with a base change matrix $C_1\in \mathrm{GL}_m(S)$ and right multiplication by a matrix $C_2\in\mathrm{GL}_m(R^\phi)$.

1.4 Another trivialization of Frobenius modules is useful in the p-adic and the t-motivic case. For this we first assume for simplicity that (S,ϕ) is a Frobenius ring whose characteristic ideal Q is a valuation ideal in $\mathrm{Quot}(S)$. Then we denote by (S_Q,ϕ) the completion of S with respect to Q and continuously extended Frobenius endomorphism. Let $(S_Q^{\mathrm{ur}},\phi^{\mathrm{ur}})$ be its integral closure inside the maximal unramified algebraic extension of $\mathrm{Quot}(S_Q)$ with the unique extension ϕ^{ur} of ϕ compatible with the ordinary Frobenius endomorphism of the residue ring $S_Q^{\mathrm{ur}}/(Q)$. Then $(\widehat{S_Q^{\mathrm{ur}}},\widehat{\phi})$ is the completion of S_Q^{ur} with respect to (Q) and with continuously extended Frobenius action. Thus Q generates a characteristic ideal (Q) not only in S but also in S_Q, S_Q^{ur}, and $\widehat{S_Q^{\mathrm{ur}}}$, and in addition this ideal remains a valuation ideal.

Proposition 1.5. *Let* (S,ϕ) *be a Frobenius ring whose characteristic ideal* Q *is a valuation ideal and let* (M,Φ) *be a Frobenius module over* (S,ϕ). *Then* M *becomes trivial over* $(\widehat{S_Q^{\mathrm{ur}}},\widehat{\phi})$.

Proof. (compare [6], proof of Thm. 6.2). We first assume that $Q=(r)$ induces a discrete valuation. With respect to some basis B of M the Frobenius endomorphism Φ is represented by a matrix $D=D_B(\Phi)\in\mathrm{GL}_m(S)$ with inverse $A=D^{-1}$. The residue matrix $\overline{A}$ (mod r) belongs to $\mathrm{GL}_m(\overline{F})$, where $\overline{F}$ denotes the residue field $\overline{F}:=S/Q$. The surjectivity of the Lang isogeny $\pi:\mathrm{GL}_m(\overline{F}^{\mathrm{sep}})\to\mathrm{GL}_m(\overline{F}^{\mathrm{sep}})$ gives a matrix $\overline{D}_0\in\mathrm{GL}_m(\overline{F}^{\mathrm{sep}})$ with $\overline{A}=\overline{\phi}(\overline{D}_0)\overline{D}_0^{-1}$. In fact, the entries of $\overline{D}_0$ belong to some finite extension $\overline{F}_0/\overline{F}$. Thus there exists an unramified ring extension with lifted Frobenius endomorphism $(\widetilde{S}_0,\phi_{\widetilde{S}_0})$ of finite degree over (S,ϕ) and a matrix $D_0\in\mathrm{GL}_m(\widetilde{S}_0)$ such that

$$A=\phi_{\widetilde{S}_0}(D_0)(I+rG_0)D_0^{-1} \quad\text{with}\quad G_0\in\widetilde{S}_0^{m\times m}.$$

Now we want to refine the resulting congruence $A \equiv \phi_{\widetilde{S}_0}(D_0)D_0^{-1} \pmod{r}$ modulo higher powers of r. The next such approximation step with $D_1 = I + rH_1$ and $\phi(r) = er$ would lead to the congruence

$$\begin{aligned} I + rG_0 &\equiv \phi_{\widetilde{S}_1}(D_1)(I + r^2 G_1)D_1^{-1} \\ &\equiv (I + \phi_{\widetilde{S}_1}(rH_1))(I - rH_1) \\ &\equiv I + er\phi_{\widetilde{S}_1}(H_1) - rH_1 \pmod{r^2}. \end{aligned}$$

Since the reduced equation $\overline{G}_0 = \overline{e}\phi_{\overline{F}_1}(\overline{H}_1) - \overline{H}_1$ has a solution matrix $\overline{H}_1$ over a finite extension $\overline{F}_1/\overline{F}_0$ there exists an F-ring $(\widetilde{S}_1, \phi_{\widetilde{S}_1})$ unramified and of finite degree over $(\widetilde{S}_0, \phi_{\widetilde{S}_0})$ and a matrix $D_1 = I + rH_1 \in \mathrm{GL}_m(\widetilde{S}_1)$ such that

$$A = \phi_{\widetilde{S}_0}(D_0)\phi_{\widetilde{S}_1}(D_1)(I + r^2 G_1)D_1^{-1}D_0^{-1} \quad \text{with} \quad G_1 \in \widetilde{S}_1^{m \times m}.$$

Thus by induction we obtain a tower of unramified ring extensions $S \leq \widetilde{S}_0 \leq \widetilde{S}_1 \leq \cdots \leq \widetilde{S}_l$ inside $\widehat{S_Q^{\mathrm{ur}}}$ and matrices $D_l \in \mathrm{GL}_m(\widetilde{S}_l)$ such that

$$A \equiv \phi_{\widetilde{S}_0}(D_0) \cdots \phi_{\widetilde{S}_l}(D_l)D_l^{-1} \cdots D_0^{-1} \pmod{r^{l+1}}.$$

Since $D_l = I + r^l H_l \in \mathrm{GL}_m(\widehat{S_Q^{\mathrm{ur}}})$, the product $D_0 \cdots D_l$ converges in $\mathrm{GL}_m(\widehat{S_Q^{\mathrm{ur}}})$. Hence there exists a matrix $Y \in \mathrm{GL}_m(\widehat{S_Q^{\mathrm{ur}}})$ with $A = \phi(Y)Y^{-1}$, which by definition is a fundamental solution matrix of (M, Φ).

In the non-discrete case the proof can be completed by refining the approximation steps modulo $r \in Q$ above as in the proof of Hensel's Lemma for non-discrete valuations. $\square$

Obviously Proposition 1.5 implies

Corollary 1.6. *Let (S, ϕ) be a separably algebraically closed complete non-archimedean field with continuous Frobenius automorphism. Then every Frobenius module over S is trivial.*

Now let (S, ϕ) be an F-ring whose characteristic ideal Q contains a chain of prime ideals $Q \supsetneq Q_1 \supsetneq \cdots \supsetneq Q_h$ with $\phi(Q_i) \subseteq Q_i$ and $h = \mathrm{height}(Q)$. Then Proposition 1.5 and induction on h can be used to prove the existence of a minimal solution ring inside the completion $\widehat{S_Q^{\mathrm{ur}}}$ with respect to the prime ideal Q (see [3], Ch. 7). This is fulfilled, for example, in case Q has an ideal basis which is elementwise invariant under ϕ. Such a Frobenius ring will be called a *pure Frobenius ring* in the sequel.

Theorem 1.7. *Let (S, ϕ) be a pure Frobenius ring with characteristic ideal Q. Then every Frobenius module (M, Φ) over S has a minimal solution ring inside $\widehat{S_Q^{\mathrm{ur}}}$.*

1.5 The notion of a Frobenius module M over a Frobenius ring S can be weakened. For this we substitute the series of S_l-submodules M_l of M by a projective system$(M_l, \varphi_l)_{l\in\mathbb{N}}$ consisting of free S_l-modules of the same rank and S_{l+1}-linear embeddings $\varphi_l : M_{l+1} \to M_l$, such that $\varphi_l(M_l)$ contains an S_l-basis of M_l. Then a family $(\Phi_l)_{l\in\mathbb{N}}$ of ϕ_l-semilinear surjection maps $\Phi_l : M_l \to M_{l+1}$ or $(M_l, \Phi_l)_{l\in\mathbb{N}}$ respectively, is called a *Frobenius structure* on $M = M_0$. By using φ_l we can identify (M_l, Φ_l) with an S_l-submodule $\widetilde{M_l}$ of M with a Frobenius operator $\widetilde{\Phi}_l$ which in general is different from $\Phi|_{\widetilde{M_l}}$.

In case there exist $k, l \in \mathbb{N}$ such that $M_{k+l} \leq M_k$ with $\Phi_{k+l} = \Phi_k|_{M_{k+l}}$, the family Φ_l becomes periodic. Then the S_k-module M_k together with $\Phi_{k,l} := \Phi_{k+l-1} \circ \ldots \circ \Phi_k$ is a Frobenius module in the above sense. In this case the Frobenius structure is called a *strong Frobenius structure*, otherwise a *weak Frobenius structure* (compare [1], Ch. 4.8 or [14], Ch. 18.4). Thus any Frobenius module (M, Φ) defines a strong Frobenius structure and vice versa.

2 Differential Structures in Positive Characteristic

2.1 Let (S, ϕ) be an integral domain in characteristic $p > 0$ with an ordinary Frobenius endomorphism $\phi = \phi_q, q = p^d$, and higher Frobenius images $S_l = \phi^l(S)$ for $l \in \mathbb{N}$. A set of commuting iterative derivations (also called Hasse derivations) $\Delta = \{\partial_1^*, \ldots, \partial_n^*\}$ on S which consists of families of maps $\partial_i^* = (\partial_i^{(k)})_{k \in \mathbb{N}}$ from S to S with $\partial^{(0)} = \mathrm{id}$ and

$$\partial_i^{(k)}(a+b) = \partial_i^{(k)}(a) + \partial_i^{(k)}(b), \quad \partial_i^{(k)}(ab) = \sum_{j+l=k} \partial_i^{(j)}(a)\partial_i^{(l)}(b),$$

$$\partial_i^{(k)}\partial_i^{(l)} = \binom{k+l}{k} \partial_i^{(k+l)}$$

for all $a, b \in S, j, k, l \in \mathbb{N}$ and

$$\partial_j^{(k)}\partial_i^{(l)} = \partial_i^{(l)}\partial_j^{(k)} \quad \text{for} \quad i, j \in \{1, \ldots, n\} \quad \text{and all} \quad l, k \in \mathbb{N}$$

is called an *iterative differential structure on S (ID-structure).* Then (S, Δ) is called an *ID-ring* and the intersection

$$C_S := \bigcap_{0<k_1+\ldots+k_n \in \mathbb{N}} \ker(\partial_1^{(k_1)} \circ \cdots \circ \partial_n^{(k_n)}) = \bigcap_{k \in \mathbb{N}} \bigcap_{i=1}^{n} \ker(\partial_i^{(p^k)})$$

is the *ring of differential constants of* (S, Δ). The subsets

$$\Delta_l := \{\partial_i^{(p^k)} \mid k < l; \quad i = 1, \ldots, n\}$$

of Δ define a chain of subrings

$$T_l := \ker(\Delta_l) := \bigcap_{k<l} \bigcap_{i=1}^{n} \ker(\partial_i^{(p^k)})$$

of S with $\bigcap_{l \in \mathbb{N}} T_l = C_S$. The property that S is an ordinary F-ring with $\phi = \phi_q$, $q = p^d$, implies $\Delta_{dl} \circ \phi^l = 0$ or $T_{dl} \geq S_l$, respectively.

Now let S be a (lifted) F-ring with characteristic prime ideal Q and induced Frobenius endomorphism $\overline{\phi} = \overline{\phi}_q$ on S/Q with $q = p^d$. Then an ID-structure Δ on S with $\Delta(Q) \subseteq Q$ and the above property $\Delta_{dl} \circ \phi^l = 0$ is called *F-compatible* and (S, ϕ, Δ) is an *IDF-ring*. If, moreover,

$$T_{dl} = \ker(\Delta_{dl}) = \phi^l(S) = S_l,$$

then Δ is called *totally F-compatible* and S a *total IDF-ring*.

2.1.1 A basic example is the polynomial ring $S=\mathbb{F}_p^{\mathrm{alg}}[t_1,\ldots,t_n]$ in n variables over the algebraic closure $\mathbb{F}_p^{\mathrm{alg}}$ of $\mathbb{F}_p$ with the ordinary Frobenius action $\phi=\phi_p$. On S we have the set Δ of partial iterative derivatives $\partial_i^*=\partial_{t_i}^*$ given by

$$\partial_{t_i}^{(k)}(t_j^l)=\delta_{ij}\binom{l}{k}t_j^{l-k}.$$

Obviously Δ defines an ID-structure on S with $\ker(\Delta_l)=\mathbb{F}_p^{\mathrm{alg}}[t_1^{p^l},...,t_n^{p^l}]=\phi^l(S)$. Thus Δ is a totally F-compatible ID-structure and (S,ϕ,Δ) a total IDF-ring.

2.1.2 The second example is the Frobenius ring $S=K[s,t]$ introduced in Example 1.1.2. Here the partial iterative derivation $\partial^*=\partial_t^*=(\partial_t^{(k)})_{k\in\mathbb{N}}$ defines an ID-structure $\Delta=\{\partial^*\}$ on S with $\ker(\Delta_l)=K[s,t^{p^l}]=\phi^l(S)$. Thus here again (S,ϕ,Δ) is a total IDF-ring.

2.2 Now we start with an ID-ring (S,Δ) with $\mathrm{char}(S)=p>0$ and ID-structure $\Delta=\{\partial_1^*,\ldots,\partial_n^*\}$. As before, let M denote a free S-module of rank $m<\infty$. Then a set $\Delta_M=\{\partial_{M,1}^*,\ldots,\partial_{M,n}^*\}$ of families of maps $\partial_{M,i}^*=(\partial_{M,i}^{(k)})_{k\in\mathbb{N}}$ is called an *iterative differential structure on M over Δ* (ID-structure over Δ), if $\partial_{M,i}^{(k)}:M\to M$ are commuting additive maps related to Δ by the mixed Leibniz rule

$$\partial_{M,i}^{(k)}(ax)=\sum_{j+l=k}\partial_i^{(j)}(a)\partial_{M,i}^{(l)}(x)\quad\text{for}\quad a\in S,x\in M,i=1,\ldots,n.$$

Then (M,Δ_M) is called an *iterative differential module over S* or an *ID-module* for short.

As in the case of rings the subsets

$$\Delta_{M,l}:=\{\partial_{M,i}^{(p^k)}\mid k<l;\quad i=1,\ldots,n\}$$

of Δ_M lead to a chain of T_l-submodules

$$\ker(\Delta_{M,l})=\bigcap_{k<l}\bigcap_{i=1}^{n}\ker(\partial_{M,i}^{(p^k)})$$

of M. These are ID-modules over T_l with respect to the shifted ID-structure

$$\Delta_M^{(l)}:=\{\partial_{M,i}^{(kp^l)}\mid k\in\mathbb{N};\quad i=1,\ldots,n\}.$$

Theorem 2.1. *Let (S,ϕ,Δ) be an IDF-ring of positive characteristic with $\Delta_{dl}\circ\phi^l=0$. Assume that M is a free S-module of rank m with (weak) Frobenius structure $(M_l,\Phi_l)_{l\in\mathbb{N}}$.*

(a) *There exists a unique ID-structure* Δ_M *over* Δ *on* M *such that*

$$\ker(\Delta_{M,dl}) \geq \widetilde{M_l} := \varphi_0 \circ \ldots \circ \varphi_{l-1}(M_l).$$

(b) *If* (S, ϕ, Δ) *is a total IDF-ring it holds the equality*

$$\ker(\Delta_{M,dl}) = \widetilde{M_l}.$$

Proof. Let $\widetilde{\varphi}_l : S \otimes_{S_{l+1}} \widetilde{M}_{l+1} \to S \otimes_{S_l} \widetilde{M_l}$ be the linear extension of the embedding $\widetilde{M}_{l+1} \to \widetilde{M_l}$. Since $\Delta_{M,dl}$ must annihilate any basis of $\widetilde{M_l}$, the image of $x \in M$ under $\partial_{M,i}^{(p^k)}$ for $k < l$ has to be defined by

$$\partial_{M,i}^{(p^k)}(x) = \widetilde{\varphi}_0 \circ \ldots \circ \widetilde{\varphi}_{l-1} \circ \partial_i^{(p^k)} \circ \widetilde{\varphi}_{l-1}^{-1} \circ \ldots \circ \widetilde{\varphi}_0^{-1}(x),$$

where $\partial_i^{(p^k)}$ only acts on the coefficients in S of the image of x in $S \otimes_{S_l} \widetilde{M_l}$. This leads to a unique ID-structure Δ_M on M with $\ker(\Delta_{M,dl}) \geq \widetilde{M_l}$. Here equality holds if and only if $S_l = T_{dl}$, i.e., if (S, ϕ, Δ) is a total IDF-ring.

□

If in Theorem 2.1 $(M_l, \Phi_l)_{l \in \mathbb{N}}$ defines a strong Frobenius structure, by Section 1.5 we are dealing with a Frobenius module (M, Φ) over S with $\Phi^l(M) = M_l = \widetilde{M_l}$. In case M has an ID-structure Δ_M compatible with Φ, i.e.,

$$\ker(\Delta_{M,dl}) \geq \Phi^l(M),$$

the triple (M, Φ, Δ_M) is called an *IDF-module* or an *ID-module with strong Frobenius structure*. If moreover $\ker(\Delta_{M,dl}) = \Phi^l(M)$, the IDF-module (M, Φ, Δ_M) is called a *total IDF-module*. This leads to

Corollary 2.2. *Let* (M, Φ) *be a Frobenius module over an IDF-ring* (S, ϕ, Δ)*.*

(a) *There exists a unique ID-structure* Δ_M *on* M *so that* (M, Φ, Δ_M) *is an IDF-module over* S*.*

(b) *In case* (S, ϕ, Δ) *is a total IDF-ring,* (M, Φ, Δ_M) *is a total IDF-module.*

If in Theorem 2.1 we start with an ID-module (M, Δ_M) such that any T_l-module $N_l := \ker(\Delta_{M,l})$ contains an S-basis B_l of M, we can easily detect a weak Frobenius structure $(M_l, \Phi_l)_{l \in \mathbb{N}}$ on M inducing Δ_M: we just have to define M_l as the free S_l-submodule over B_{dl} and $\Phi_l : M_l \to M_{l+1}$ as the ϕ_l-linear map sending B_{dl} onto $B_{d(l+1)}$. In case S is a total IDF-ring, i.e., $T_{dl} = S_l$, we obtain $N_{dl} = M_l$ and $(\Phi_l)_{l \in \mathbb{N}}$ is uniquely determined by the property $\Phi_l(N_{dl}) = N_{d(l+1)}$.

2.3 Now let (S,Δ) be an ID-ring with $\Delta=\{\partial_1^*,\ldots,\partial_n^*\}$ and let (M,Δ_M) be an ID-module over S with related ID-structure $\Delta_M=\{\partial_{M,1}^*,\ldots,\partial_{M,n}^*\}$. Then any extension of ID-rings $(\widetilde{S},\widetilde{\Delta})$ with $\widetilde{\Delta}=\{\widetilde{\partial}_1^*,\ldots,\widetilde{\partial}_n^*\}$ and $\widetilde{\partial}_i^*|_{S_i}=\partial_i^*$ leads to an extended ID-module $(M_{\widetilde{S}},\widetilde{\Delta}_M)$ with $M_{\widetilde{S}}:=\widetilde{S}\otimes_S M$ and an extended ID-structure $\widetilde{\Delta}_M=\{\widetilde{\partial}_{M,1}^*,\ldots,\widetilde{\partial}_{M,n}^*\}$ over $\widetilde{\Delta}$. Then we define the *solution space* of M over $\widetilde{S}$ to be

$$\mathrm{Sol}_{\widetilde{S}}^{\Delta}(M):=\bigcap_{l\in\mathbb{N}}\bigcap_{i=1}^{n}\ker(\widetilde{\partial}_{M,i}^{(p^l)}).$$

Obviously $\mathrm{Sol}_{\widetilde{S}}^{\Delta}(M)$ is a $C_{\widetilde{S}}$-module of rank at most m. In case the rank equals m, M is called *trivial over* $\widetilde{S}$ and $\widetilde{S}$ is called a *solution ring* of the ID-module M.

Next we want to compare the solution spaces of an IDF-module (M,Φ,Δ_M) with respect to the Frobenius structure and the ID-structure. The result is

Theorem 2.3. *Let (S,ϕ,Δ) be a pure IDF-ring of positive characteristic and let (M,Φ,Δ_M) be an IDF-module over S of finite rank.*
(a) *Let (R,ϕ_R) be a minimal solution ring of (M,Φ), then there exists a differential structure Δ_R on R so that (R,Δ_R) is a solution ring of (M,Δ_M) and the solution spaces are related by*

$$\mathrm{Sol}_R^{\Delta}(M)=C_R\otimes_{R^\phi}\mathrm{Sol}_R^{\Phi}(M)\quad\textit{and}\quad\mathrm{Sol}_R^{\Phi}(M)=\mathrm{Sol}_R^{\Delta}(M)^{\widetilde{\Phi}}$$

where $\widetilde{\Phi}$ is the canonical extension of Φ onto $\mathbb{R}\otimes_S M$.
(b) *Set $\widetilde{S}:=C_R\otimes_{C_S}S$ with trivially extended ID-structure $\widetilde{\Delta}$. Then (R,Δ_R) is a minimal solution ring of the ID-module $(M_{\widetilde{S}},\widetilde{\Delta}_M)$ over $(\widetilde{S},\widetilde{\Delta})$.*
(c) *The ring of constants C_R is a minimal solution ring of a Frobenius module of finite rank over C_S. In particular C_R over C_S is finite separable if C_S is an ordinary Frobenius ring.*

Proof. Let $U:=S[\mathrm{GL}_m]$ be the coordinate ring of GL_m over S, i.e., $U:=S[x_{ij},\det(x_{ij})^{-1}]_{i,j=1}^m$. We define an action of Φ and Δ_M on the matrix of indeterminates $X:=(x_{ij})_{i,j=1}^m$ by

$$\phi_U(X):=AX\quad\text{and}\quad\partial_{U,i}^{(p^l)}(X)=A_i^{(p^l)}X.$$

Here A equals $D_B(\Phi)^{-1}$ for some basis B of M over S and $A_i^{(p^l)}$ can be computed by recursion from the formulas

$$\partial_{\widetilde{M},i}^{(k)}(BX)=\sum_{j=0}^{k}\partial_{M,i}^{(k-j)}(B)\partial_{U,i}^{(j)}(X)=0.$$

Then (U, ϕ_U, Δ_U) becomes an IDF-ring over S. By Theorem 1.7 there exists an S-linear map $\theta : U \to \widehat{S_Q^{\mathrm{ur}}}$ onto a minimal solution ring of (M, Φ) inside $\widehat{S_Q^{\mathrm{ur}}}$. Hence $\ker(\theta)$ is a maximal ϕ_U-invariant prime ideal $P \trianglelefteq U$ with $P \cap S = (0)$. From $\Delta_{U,1}(P) \subseteq \Delta_{U,1}(S\phi_U(P)) \subseteq S\phi_U(P) \subseteq P$ follows by induction $\Delta_U(P) \subseteq P$. Thus $R := U/P$ is a minimal solution ring of M with respect to the induced Frobenius structure ϕ_R and a solution ring with respect to the induced ID-structure Δ_R with the common fundamental matrix $Y := X \pmod{P}$. Obviously any minimal solution ring R of (M, Φ) with some fundamental solution matrix Y can be obtained in this way by defining P as the kernel of the S-homomorphism $U \to R, X \mapsto Y$. This proves (a) with the obvious extension $\widetilde{\Phi}$ of Φ onto $R \otimes_S M$.

The ring (R, Δ_R) is an ID-ring over $(\widetilde{S}, \widetilde{\Delta})$ without new constants generated by the fundamental matrix $Y \in \mathrm{GL}_m(R)$ of $(M_{\widetilde{S}}, \widetilde{\Delta}_M)$. Thus by the characterization of iterative Picard-Vessiot rings in [5], Prop. 4.8 (see also [9], Thm. 6.10), R is a simple ID-ring over $\widetilde{S}$ and hence a minimal solution ring for $(M_{\widetilde{S}}, \widetilde{\Delta}_M)$ over $\widetilde{S}$ by definition.

For the proof of (c) we observe that R is generated over S by finitely many solutions of Frobenius polynomials, called Frobenius-finite elements over S. It follows that all elements of R are Frobenius-finite over S and the elements of C_R are Frobenius-finite over C_S. Since C_R is finitely generated over C_S, C_R is a solution ring of a Frobenius module over C_S of finite rank. Thus in case C_S is an ordinary F-ring, C_R over C_S is finite by Theorem 1.2. □

A minimal solution ring of an ID-module (M, Δ) over S without new constants is called an *iterative Picard-Vessiot ring* or an *IPV-ring* for short. With this notion we obtain

Corollary 2.4. *Let (M, Φ) be a Frobenius module over a pure IDF-ring (S, ϕ, Δ) with separably algebraically closed ring of constants C_S. Let Δ_M be the ID-structure of M related to Φ according to Theorem 2.1. Then a minimal solution ring of (M, Φ) is an IPV-extension of M over S with respect to Δ_M.*

This corollary covers Theorem 3.2 of [6]. Another special case follows from Theorem 1.7:

Corollary 2.5. *Let (M, Φ) be a Frobenius module over a pure IDF-ring (S, ϕ, Δ) of positive characteristic with characteristic ideal Q. Assume that the ring of differential constants C_S of S is complete with respect to $Q \cap C_S$ and that its residue field is separably algebraically closed. Then a minimal solution ring of (M, Φ) is an IPV-extension of M over S with respect to the unique ID-structure of M related to Φ.*

This corollary applies, for example, to Frobenius rings (S, ϕ) of type $S = K[[s]][t]$ over an algebraically closed field K with ordinary Frobenius action $\phi = \phi_p$ and with $\phi(s) = s, \phi(t) = t^p$. Then the characteristic ideal Q of S equals (s) and $C_S = K[[s]]$ is complete with respect to (s).

3 Differential Equations in Characteristic Zero

3.1 In this chapter we study Frobenius modules in characteristic zero. It is well known that the p-power Frobenius endomorphism $\overline{\phi}_p$ of $\mathbb{F}_p^{\mathrm{alg}}/\mathbb{F}_p$ has a unique lift ϕ_p to $\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p$ where $\mathbb{Q}_p^{\mathrm{ur}}$ denotes the maximal unramified algebraic extension of $\mathbb{Q}_p$. Therefore its ring of integers $(\mathbb{Z}_p^{\mathrm{ur}}, \phi_p)$ and the completion $W := \widehat{\mathbb{Z}}_p^{\mathrm{ur}} = \mathbb{W}(\mathbb{F}_p^{\mathrm{alg}})$ with the continuous extension $\widehat{\phi}_p$ of ϕ_p are Frobenius rings with characteristic ideal (p), compare Example 1.1.3. Moreover, by Proposition 1.5 every Frobenius module over W is trivial.

Now let (S, ϕ) be an arbitrary Frobenius ring in characteristic zero with characteristic ideal Q. A set of commuting derivations $\Delta = \{\partial_1, \ldots, \partial_n\}$ in S with $\partial_i(Q) \subseteq Q$ for $i = 1, \ldots, n$ is called a *differential structure on* S and (S, Δ) a *D-ring* (compatible with Q). Every finitely generated ideal $Q_0 \subseteq Q$ defines a series of *congruence constant rings*

$$T_l := \{a \in S \mid \partial(a) \in Q_0^l \quad \text{for} \quad \partial \in \Delta\}.$$

If (S, Δ) is a D-ring with the property that all higher derivations $\partial_i^{(k)} := \frac{1}{k!}\partial_i^k$ for $k \in \mathbb{N}$ and $i = 1, \ldots, n$ are maps from S to itself with $\partial_i^{(k)}(Q) \subseteq Q$, (S, Δ) is called an *iterative differential ring* or *ID-ring* for short (compatible with Q).

In case the D-structure Δ on S and the Frobenius endomorphism are related by formulas of type

$$\partial_i \circ \phi = z_i \phi \circ \partial_i \quad \text{with} \quad z_i \in Q \quad \text{for} \quad i = 1, \ldots, n,$$

the triple (S, ϕ, Δ) is called an *(iterative) differential ring with Frobenius structure* or a *DF-ring (IDF-ring)* and $\{z_i \mid i = 1, \ldots, n\}$ is called the set of *transition elements* for (ϕ, Δ). If $z_i \in Q_0^d$ for some d and all i, the formula $\partial_i \circ \phi = z_i \phi \circ \partial_i$ imply $S_l \leq T_{dl}$ in analogy to Section 2.1. Moreover the residue ring $\overline{S} := S/Q$ with the induced Frobenius action $\overline{\phi}$ and the induced iterative differential structure becomes an IDF-ring in positive characteristic with ordinary Frobenius action as discussed in the last chapter.

As an example we consider the Frobenius ring $(S, \phi) = (W[t_1, \ldots, t_n], \phi)$ from Example 1.1.3 with $W = \widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ and $\phi(t_i) = t_i^p$. With the differential structure $\Delta = \{\partial_1, \ldots, \partial_n\}$ consisting of the partial derivations $\partial_i : t_j \mapsto \delta_{ij}$, S becomes an IDF-ring with $z_i = pt_i^{p-1}$. The residue ring $\overline{S} = S/(p)$ equals the IDF-ring $\mathbb{F}_p^{\mathrm{alg}}[t_1, \ldots, t_n]$ with the partial iterative derivations $\partial_i^* = \partial_{t_i}^*$ already discussed in Example 2.1.1.

3.2 Now let (S, Δ) be an integral domain in characteristic zero with differential structure $\Delta = \{\partial_1, \ldots, \partial_n\}$. Assume M is a free S-module of finite rank m. Then a set $\Delta_M = \{\partial_{M,1}, \ldots, \partial_{M,n}\}$ of additive maps $\partial_{M,i} : M \to M$ related to Δ by

$$\partial_{M,i}(ax) = \partial_i(a)x + a\partial_{M,i}(x) \quad \text{for} \quad a \in S, x \in M$$

defines a *D-structure on M over S*. In case (S,Δ) is an ID-ring and $\partial_{M,i}^{(k)} := \frac{1}{k!}\partial_{M,i}^k$ are maps from M to itself, Δ_M is called an *ID-structure* and (M,Δ_M) is called an *ID-module* over S.

For Frobenius rings (S,ϕ), we define a *Frobenius module* (M,Φ) over S and a Frobenius structure $(M_l,\Phi_l)_{l\in\mathbb{N}}$ in the same way as in Section 1.2 or Section 1.5, respectively. Next we want to show that as in the case of positive characteristic, for a module over an IDF-ring any weak Frobenius structure $(M_l,\Phi_l)_{l\in\mathbb{N}}$ on M defines a unique ID-structure Δ_M on M compatible with $(\Phi_l)_{l\in\mathbb{N}}$. But here for simplicity we assume $M_l \leq M$, i. e., we identify $\widetilde{M_l} = \varphi_0 \circ \cdots \circ \varphi_{l-1}(M_l)$ with M_l.

Theorem 3.1. *Let (S,ϕ,Δ) be an IDF-ring with $\mathrm{char}(S) = 0$ which is complete with respect to Q. Let $Q_\Delta \trianglelefteq S$ be the ideal generated by the transition elements $z_i \in Q$ of $\partial_i \in \Delta$. Then for a free S-module M of finite rank the following holds:*

(a) *Assume M has a weak Frobenius structure $(M_l,\Phi_l)_{l\in\mathbb{N}}$ with $M_l \leq M$. Then there exists a unique differential structure $\Delta_M = \{\partial_{M,1}\ldots,\partial_{M,n}\}$ on M with*

$$\partial_{M,i}(M_l) \equiv 0 \pmod{Q_\Delta^l M} \quad \textit{for} \quad i = 1,\ldots,n.$$

(b) *In case M has a strong Frobenius structure Φ, i.e., (M,Φ) is a Frobenius module over S, Δ_M and Φ are related by*

$$\partial_{M,i} \circ \Phi = z_i \Phi \circ \partial_{M,i} \quad \textit{for} \quad i = 1,\ldots,n.$$

Proof of Thm. 3.1 (a). (compare [6], Thm. 7.2, for the univariate case): According to our assumption the weak Frobenius structure $(M_l,\Phi_l)_{l\in\mathbb{N}}$ defines a projective system $(M_l,\varphi_l)_{l\in\mathbb{N}}$ of S_l-submodules of M with S_{l+1}-linear embeddings $\varphi_l : M_{l+1} \to M_l$. Chosen bases $B_l = \{b_{l,1},\ldots,b_{l,m}\}$ of M_l are related by $B_lD_l = B_{l+1}$ with base change matrices $D_l \in \mathrm{GL}_m(S_l)$ called representing matrices of Φ_l. Moreover, the embeddings φ_l can be uniquely extended to S-linear isomorphisms $\widetilde{\varphi}_l : S \otimes_{S_{l+1}} M_{l+1} \to S \otimes_{S_l} M_l$. Then the congruences in (a) are equivalent to

$$\partial_{M,i}(x) \equiv \widetilde{\varphi}_0 \circ \cdots \circ \widetilde{\varphi}_{l-1} \circ \partial_i \circ \widetilde{\varphi}_{l-1}^{-1} \circ \cdots \circ \widetilde{\varphi}_0^{-1}(x) \pmod{Q_\Delta^l M}$$

with the derivation ∂_i acting on the coefficients of x only (with respect to the basis B_l). In view of the congruences above for $x = B\boldsymbol{y} = \sum_{i=1}^m b_iy_i$ we define

$$\delta_{i,l}(x) := BD_0\cdots D_{l-1}\partial_i(D_{l-1}^{-1}\cdots D_0^{-1}\boldsymbol{y}) \in M.$$

From $D_l^{-1} \in \mathrm{GL}_m(S_l)$ we obtain $\partial_i(D_l^{-1}) \equiv 0 \pmod{Q_\Delta^l}$. Hence the coefficients of $\delta_{i,l}(x)$ converge in S and

$$\partial_{M,i}(x) := \lim_{l\to\infty}(\delta_{i,l}(x)) \in M$$

is well defined. It is easy to verify that the $\partial_{M,i} : M \to M$ are additive with $\partial_{M,i}(ax) = \partial_i(a)x + a\partial_{M,i}(x)$ for $a \in S, x \in M$. Therefore the $\partial_{M,i}$ are derivations on M related to ∂_i with $\partial_{M,i}(M_l) \equiv 0 \pmod{Q_\Delta^l M}$ and are uniquely determined by this property. $\square$

Before proving (b) we derive explicit formulas for the matrices defining $\partial_{M,i}$ with respect to some basis B of M. As above, let $B_l = BD_0 \cdots D_{l-1}$ be an S_l-basis of M_l. Then any $x = B\boldsymbol{y} \in M$ with $\boldsymbol{y} \in S^m$ can be written as $x = B_l \boldsymbol{y}_l$ where $\boldsymbol{y}_l = (D_0 \cdots D_{l-1})^{-1}\boldsymbol{y}$. Now $x = B\boldsymbol{y}$ belongs to $\mathrm{Sol}_{\widetilde{S}}^{\widetilde{\Delta}}(M)$ for some extension D-ring $(\widetilde{S}, \widetilde{\Delta})$ if and only if $\widetilde{\partial}_i(\boldsymbol{y}_l) \equiv 0 \pmod{Q_\Delta^l}$ for $i = 1, \ldots, n$ and all $l \in \mathbb{N}$. The last congruences are equivalent to

$$\widetilde{\partial}_i(\boldsymbol{y}) = \widetilde{\partial}_i(D_0 \cdots D_{l-1}\boldsymbol{y}_l) \equiv \partial_i(D_0 \cdots D_{l-1})\boldsymbol{y}_l = A_{i,l}\boldsymbol{y} \pmod{Q_\Delta^l}$$

with $A_{i,l} := \partial_i(D_0 \cdots D_{l-1})(D_0 \cdots D_{l-1})^{-1}$. Since $A_{i,l} \equiv A_{i,l-1} \pmod{Q_\Delta^l}$, the limits

$$A_i := \lim_{l\to\infty}(A_{i,l}) \in S^{m\times m}$$

exist, and the congruences in Theorem 3.1(a) are equivalent to the system of linear differential equations

$$\partial_i(\boldsymbol{y}) = A_i\boldsymbol{y} \quad \text{for} \quad i = 1, \ldots, n.$$

Corollary 3.2. *Let M be an S-module with weak Frobenius structure $(M_l, \Phi_l)_{l\in\mathbb{N}}$ with $M_l \le M$ as in Theorem 3.1(a). Let D_l be the representing matrices of Φ_l with respect to bases B_l of M_l. Then the differential structure Δ_M on M related to $(\Phi_l)_{l\in\mathbb{N}}$ is given by*

$$\partial_{M,i}(B) = -B \cdot A_i \ \text{ with } \ A_i = \lim_{l\to\infty}(\partial_i(D_0 \cdots D_l)(D_0 \cdots D_l)^{-1}) \ \text{ and } \ B = B_0.$$

Proof of Thm. 3.1 (b). (compare [6], Cor. 7.5): For this part of Theorem 3.1 we have $D_l = \phi^l(D_0)$. Then the definition of $A_{i,l}$ leads to the identities

$$\begin{aligned} A_{i,l}D_0 &= \partial_i(D_0 \cdots D_l)(D_0 \cdots D_l)^{-1}D_0 \\ &= \partial_i(D_0) + D_0\partial_i(\phi(D_0 \cdots D_{l-1}))\phi(D_0 \cdots D_{l-1})^{-1} \\ &= \partial_i(D_0) + z_i D_0 \phi(A_{i,l-1}) \end{aligned}$$

and thus to

$$A_i D_0 = \partial_i(D_0) + z_i D_0 \phi(A_i).$$

But then for the basis B of M we obtain

$$\partial_{M,i}(\Phi(B)) = \partial_{M,i}(BD_0) = -BA_iD_0 + B\partial_i(D_0)$$

$$= -z_i B D_0 \phi(A_i) = z_i \Phi(-BA_i) = z_i \Phi(\partial_{M,i}(B)).$$

$\square$

Theorem 3.1 applies for example to the rings in rigid analytic geometry. The most basic example is the ring $S = W\langle t_1, \dots, t_n\rangle$ of restricted power series (the Tate ring) over the ring $W = \widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ which is complete with respect to the Gauß extension of the p-adic value (or the corresponding valuation ring in $\mathrm{Quot}(S)$, respectively). Here the Frobenius endomorphism ϕ is given by $\phi|_W = \phi_p$ and $\phi(t_i) = t_i^p$, and the differential structure $\Delta = \{\partial_1, \dots, \partial_n\}$ by the partial derivations $\partial_i = \frac{d}{dt_i}$.

3.3 In view of Theorem 3.1(b) even over a general IDF-ring (S, ϕ, Δ) a Frobenius module (M, Φ) with differential structure Δ_M is called an *IDF-module* if Δ_M and Φ are related by the formulas

$$\partial_{M,i} \circ \Phi = z_i \Phi \circ \partial_{M,i}$$

with the transition elements z_i coming from S. In the next theorem we want to clarify how in this case the solution rings with respect to Φ and Δ_M are related.

Theorem 3.3. *Let (S, ϕ, Δ) be a pure IDF-ring with* $\mathrm{char}(S) = 0$ *and (M, Φ, Δ_M) an IDF-module over S.*

(a) *Let (R, ϕ_R) be a minimal solution ring of (M, Φ). Then there exist a differential structure Δ_R on R so that (R, Δ_R) is a solution ring of (M, Δ_M), and the solution spaces are related by*

$$\mathrm{Sol}_R^{\Delta}(M) = C_R \otimes_{R^\phi} \mathrm{Sol}_R^{\Phi}(M) \quad \textit{and} \quad \mathrm{Sol}_R^{\Phi}(M) = \mathrm{Sol}_R^{\Delta}(M)^{\widetilde{\Phi}}$$

where $\widetilde{\Phi}$ denotes the canonical extension of Φ onto $R \otimes_S M$.

(b) *Set $\widetilde{S} := C_R \otimes_{C_S} S$ with trivially extended D-structure $\widetilde{\Delta}$. Then R is a Picard-Vessiot ring of the D-module $(M_{\widetilde{S}}, \widetilde{\Delta}_M)$ over $(\widetilde{S}, \widetilde{\Delta})$.*

(c) *The ring of constants C_R is a minimal solution ring of a Frobenius module of finite rank over C_S. In particular, the ring C_R is contained in the completion of the maximal unramified extension $(\widehat{C_S})_Q^{\mathrm{ur}}$ of C_S with respect to $Q \cap C_S$.*

Proof. The proof is almost identical to the proof of Theorem 2.3. For (a) we only have to recognize that by Corollary 3.2 any fundamental solution matrix Y of (M, Φ) additionally is a fundamental solution matrix of (M, Δ_M). Then part (b) and the first part of (c) follow with the same arguments. Finally, the second part of (c) is an application of Theorem 1.7. $\square$

Corollary 3.4. *Let (S, ϕ, Δ) be a pure IDF-ring with* $\mathrm{char}(S) = 0$ *and characteristic ideal Q. Assume the ring of differential constants C_S of S is complete with respect to $Q \cap C_S$ and the residue field $C_S/(Q \cap C_S)$ is separably algebraically closed. Then for any IDF-module (M, Φ, Δ_M) over S the following holds: R is a minimal solution ring of (M, Φ) over S if and only if R is a PV-extension for (M, Δ_M) over S, and the solution spaces are related by the formulas given in Theorem 3.3(a).*

The proof follows immediately from Theorem 3.3, since our assumptions imply $C_S = (\widehat{C}_S)^{\mathrm{ur}}_Q$. Among the rings S with this property are, for example, the polynomial ring $W[t_1, \ldots, t_n]$ and the ring of restricted power series $W\langle t_1, \ldots, t_n\rangle$ over the Witt ring $W = \mathbb{W}(\mathbb{F}_p^{\mathrm{alg}}) = \widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ or over the ring of integers in the p-adic universe $\mathbb{C}_p$ with the obvious IDF-structures.

4 Galois Groups and Picard-Vessiot Theory

4.1 We start again with a Frobenius module (M, Φ) of rank m over a pure Frobenius ring (S, ϕ) of arbitrary characteristic. For simplicity in this chapter we substitute S by its field of fractions $F := \mathrm{Quot}(S)$. By Theorem 1.7 there exists a minimal solution ring (R, ϕ_R) of M over F without zero divisors and with ring of invariants $R^\phi = F^\phi$. The *Frobenius automorphism group* of R/F is defined by

$$\mathrm{Aut}^\Phi(R/F) = \{\gamma \in \mathrm{Aut}(R/F) \mid \phi_R \circ \gamma = \gamma \circ \phi_R\}.$$

Obviously any element $\gamma \in \mathrm{Aut}^\Phi(R/F)$ acts on the F^ϕ-vector space $\mathrm{Sol}_R^\Phi(M)$ by an F^ϕ-linear transformation. Thus we obtain a faithful representation of $\mathrm{Aut}^\Phi(R/F)$ into $\mathrm{GL}_m(F^\phi)$. This explains the first part of the next proposition, the second part follows from Theorem 1.2 and ordinary Galois theory.

Proposition 4.1. *Let (M, Φ) be a Frobenius module over a pure Frobenius field (F, ϕ) with minimal solution ring (R, ϕ_R). Then the following holds:*

(a) *The group $G := \mathrm{Aut}^\Phi(R/F)$ is a subgroup of $\mathrm{GL}_m(F^\phi)$.*

(b) *If F is an ordinary Frobenius field, the ring of G-invariants R^G equals F.*

Now let (M, Δ_M) be a D-module (or an ID-module, respectively,) over a differential field (F, Δ) of arbitrary characteristic with field of constants C_F. Then by differential Galois theory we obtain a minimal solution ring (R, Δ_R), which may not be unique in case C_F is not algebraically closed. But in any case, the ring of constants C_R of R is at most a finite extension of C_F. In many cases there even exists a solution ring R with $C_R = C_F$, for example if F has a C_F-valued place regular for M (compare Section 5.2). Then we define the *differential automorphism group* by

$$\mathrm{Aut}^\Delta(R/F) = \{\gamma \in \mathrm{Aut}(R/F) \mid \partial \circ \gamma = \gamma \circ \partial \quad \text{for all} \quad \partial \in \Delta_R\}.$$

Again $\mathrm{Aut}^\Delta(R/F)$ acts on the solution space $\mathrm{Sol}_R^\Delta(M)$ which now is a vector space over C_R. This shows the first part of

Proposition 4.2. *Let (M, Δ_M) be a D-module (ID-module in the case of positive characteristic) over a differential field (F, Δ) with minimal solution ring (R, Δ_R).*

(a) *The group $G := \mathrm{Aut}^\Delta(R/F)$ is a subgroup of $\mathrm{GL}_m(C_R)$.*

(b) *If C_F is an algebraically closed field and R is separabel over F, then R^G equals F.*

Here part (b) follows from Picard-Vessiot theory in characteristic zero (see for example [12], Thm. 1.27) or characteristic $p > 0$, respectively (see [8], Thm. 3.5 or [5], Thm. 3.10). It remains to study what happens in case C_F is not algebraically closed and how for IDF-modules the groups Aut^Δ and Aut^Φ are related.

4.2 The first step to establish a reasonable Galois correspondence between R/F and $G = \mathrm{Aut}^\Delta(R, F)$ must be to prove $R^G = F$. For this we assume that the field of constants C_R of R coincides with C_F which can be achieved by a finite extension. Then R/F becomes a Picard-Vessiot ring with field of differential constants $K := C_R = C_F$. In this situation T. Dyckerhoff [2] proposed to introduce a functor from the category of K-algebras to the category of groups

$$\underline{\mathrm{Aut}}^\Delta(R/F) : \text{K-Alg} \to \text{Groups},\ B \mapsto \mathrm{Aut}^\Delta(R \otimes_K B/F \otimes_K B)$$

which sends a K-algebra B to the group of differential automorphisms $\mathrm{Aut}^\Delta(R \otimes_K B/F \otimes_K B)$ where the differential structure on R (or F, respectively,) is trivially extended to the tensor product. The following proposition has been proved by T. Dyckerhoff in characteristic zero ([2], Thm. 1.26) and A. Röscheisen in positive characteristic ([13], Prop. 10.9).

Proposition 4.3. *For a Picard-Vessiot ring R/F, the group functor $\underline{\mathrm{Aut}}^\Delta(R/F)$ is represented by the K-algebra of differential constants in $R \otimes_F R$.*

Thus $\underline{\mathrm{Aut}}^\Delta(R/F)$ is an affine group scheme over K which will be called the *differential Galois group scheme* $\mathrm{Gal}^\Delta(R/F)$ of R/F. Obviously the group $\mathrm{Aut}^\Delta(R/F)$ introduced in the last subsection coincides with the group of K-rational points of $\mathcal{G}_K = \mathrm{Gal}^\Delta(R/F)$. As in the classical case, Proposition 4.3 leads to a torsor theorem with $\mathcal{G}_F := \mathrm{Spec}(F) \times_K \mathcal{G}_K$:

Corollary 4.4. *Let R/F be a Picard-Vessiot ring. Then* $\mathrm{Spec}(R)$ *is a $\mathcal{G}_F$-torsor over* $\mathrm{Spec}(F)$.

For the differential Galois group scheme $\mathcal{G} = \mathrm{Gal}^\Delta(R/F)$ the *ring of (functorial) invariants* $A^{\mathcal{G}}$ of a K-algebra A is defined by the set of all $a \in A$ such that for all K-algebras B the element $a \otimes 1 \in A \otimes_K B$ is invariant under $\mathcal{G}(B)$. It is then immediate that $R^{\mathcal{G}} = F$. Now let $L :=$ Quot (A) be the localization of A by all non zero divisors. Then an element $\frac{a}{b} \in L$ is called *invariant under* $\mathcal{G}$ if for all K-algebras B and all $\beta \in \mathcal{G}(B)$

$$\beta(a \otimes 1) \cdot (b \otimes 1) = (a \otimes 1) \cdot \beta(b \otimes 1) \in L \otimes_K B.$$

The ring of invariants of L is denoted by $L^{\mathcal{G}}$. With these notations we obtain

Theorem 4.5. *Let (F, Δ) be a differential field in arbitrary characteristic with field of constants K, and let R/F be a Picard-Vessot ring with differential Galois group scheme $\mathcal{G} = \mathrm{Gal}^\Delta(R/F)$ and field of fractions E. Then:*

(a) *There exists a Galois correspondence between the lattice of closed K-subgroup schemes $\mathcal{H}$ of $\mathcal{G}$ and the lattice of intermediate differential fields L of E/F given by*

$$\mathcal{H} \mapsto E^{\mathcal{H}} \quad \textit{and} \quad L \mapsto \mathrm{Gal}^\Delta(RL/L).$$

(b) *If $\mathcal{H} \trianglelefteq \mathcal{G}$ is a normal K-subgroup scheme, then $E^{\mathcal{H}} = \mathrm{Quot}(R^{\mathcal{H}})$ and $R^{\mathcal{H}}$ is a Picard-Vessiot ring over F with differential Galois group scheme $\mathcal{G}/\mathcal{H}$.*

(c) *The K-subgroup scheme $\mathcal{H}$ is reduced if and only if E is separable over $E^{\mathcal{H}}$.*

The proof for Theorem 4.5 in characteristic zero is given by Dyckerhoff ([2], Thm. 1.37) and in positive characteristic by Röscheisen ([13],Thm. 11.4). The Galois correspondence above translates into a Galois correspondence with the groups of K-rational points $\mathcal{H}(K)$ instead of $\mathcal{H}$ as in the classical case, if and only if for all closed K-subgroup schemes $\mathcal{H}$ of $\mathcal{G}, \mathcal{H}$ is reduced and the group $\mathcal{H}(K)$ is dense in $\mathcal{H}(K^{\mathrm{alg}})$, where K^{alg} denotes an algebraic closure of K.

4.3 It is obviously possible to develop a completely similar theory for the Frobenius automorphism groups. Then one obtains a *Frobenius Galois group scheme* $\mathcal{G}^{\Phi} := \mathrm{Gal}^{\Phi}(R/F)$ over the field F^{ϕ} represented by $(R \otimes_F R)^{\phi_R \otimes \phi_R}$, and R becomes a $\mathcal{G}^{\Phi}_F$-torsor of $\mathcal{G}^{\Phi}$ over $\mathrm{Spec}(F)$, at least if F is the field of fractions of a pure Frobenius ring. These facts have been worked out by Papanikolas ([10], Thm. 4.2.11) in the case where ϕ is an automorphism of F, but the results remain true for Frobenius endomorphisms, too. Here we do not want to follow this direction further. Instead we want to compare the Galois group schemes $\mathrm{Gal}^{\Delta}(R/F)$ and $\mathrm{Gal}^{\Phi}(R/F)$ in the case of a common minimal solution ring.

In characteristic zero any D-field F is an ID-field and any D-module over F is an ID-module. Hence we may assume without loss of generality that (M, Φ, Δ_M) is an IDF-module over a field of fractions of an IDF-ring in arbitrary characteristic. Then by Theorem 2.3 and Theorem 3.3 a necessary and sufficient condition for the existence of a common minimal solution ring R for the ID- and the F-structure is $C_F = C_R$. This implies that the minimal solution ring of M with respect to Φ is a Picard-Vessiot extension over F with respect to Δ_M. This is true for example under the assumption of Corollary 2.4, Corollary 2.5 or Corollary 3.4, respectively. Then $\mathrm{Spec}(R)$ at the same time is a $\mathcal{G}^{\Delta}_F$-torsor for $\mathcal{G}^{\Delta} = \mathrm{Gal}^{\Delta}(R/F)$ and a $\mathcal{G}^{\Phi}_F$-torsor for $\mathcal{G}^{\Phi} = \mathrm{Gal}^{\Phi}(R/F)$. This implies

Theorem 4.6. *Let (M, Φ, Δ_M) be an IDF-module over a pure IDF-field (F, ϕ, Δ) in arbitrary characteristic. Assume that the ring of differential constants C_R of a minimal Frobenius solution ring R of M equals C_F. Then for the Galois group schemes $\mathcal{G}^{\Phi}_{F^{\phi}} = \mathrm{Gal}^{\Phi}(R/F)$ and $\mathcal{G}^{\Delta}_K = \mathrm{Gal}^{\Delta}(R/F)$,*

$$\mathcal{G}^{\Delta}_K = \mathrm{Spec}(K) \times_{F^{\phi}} \mathcal{G}^{\Phi}_{F^{\phi}}.$$

Thus in the case of Theorem 4.6 the Galois group schemes are the same up to a base change with K (compare [6], Prop. 9.2, for a p-adic version involving the respective groups of rational points.)

4.4 We close this chapter with two examples. In both cases we take the field $F = \mathbb{F}_p^{\mathrm{alg}}((s))(t)$ as base ring S. F has a Frobenius endomorphism ϕ defined by $\phi|_{\mathbb{F}_p^{\mathrm{alg}}} = \phi_p, \phi(s) = s$ and $\phi(t) = t^p$ and a compatible differential structure given by $\Delta = \{\partial^*\}$ with the iterative derivation $\partial^* = \partial_t^*$ on t (compare Examples 1.1.2 and 2.1.2). Thus (F, ϕ, Δ) is the field of fractions of a pure IDF-ring with field of differential constants $C_F = \mathbb{F}_p^{\mathrm{alg}}((s))$ and field of Frobenius invariants $F^\phi = \mathbb{F}_p((s))$. We will now show that over F in contrast to ordinary Frobenius rings infinite groups like $\mathbb{G}_m$ or $\mathbb{G}_a$ occur as Galois groups of IDF-modules.

4.4.1 Let M be the 1-dimensional F-module $M = bF$ with basis $B = \{b\}$. It becomes a Frobenius module over F by setting $\Phi(b) = b(1 + at)$ with $a \in F^\phi$. Then the solution ring R of (M, Φ) is generated over F by an element $y \in R$ with $\phi_R(y) = (1 + at)^{-1}y$. This leads to the solution space

$$\mathrm{Sol}_R^\Phi(M) = yF^\phi \quad \text{with} \quad y = \prod_{l\in\mathbb{N}}(1 + at^{p^l}).$$

In case $a \in \mathbb{F}_p$ the power series y is solution of a Frobenius module over the ordinary Frobenius ring $\mathbb{F}_p(t)$. Thus y is algebraic over $\mathbb{F}_p(t)$ by Theorem 1.2 and the identity $\phi(y) = y^p = (1+at)^{-1}y$ leads to $y = (1+at)^{-1/(p-1)}$. If $a \notin \mathbb{F}_p, y$ has infinitely many zeros in $\mathbb{F}_p((s))^{\mathrm{alg}}$ and is thus transcendental over F.

By Theorem 2.1 the Frobenius structure Φ of M is related to a differential structure $\Delta_M = \{\partial_M^*\}$. A solution $B\boldsymbol{y}$ of (M, Δ_M) fulfills $\partial_M^{(p^l)}(B\boldsymbol{y}) = 0$ for all $l \in \mathbb{N}$. Defining $D_l := \phi^l(D_B(\Phi)), B_{l+1} := BD_0 \cdots D_l, \boldsymbol{y}_{l+1} := (D_0 \cdots D_l)^{-1}\boldsymbol{y}$, this statement becomes equivalent to $0 = \partial_M^{(p^l)}(B\boldsymbol{y}) = \partial_M^{(p^l)}(B_{l+1}\boldsymbol{y}_{l+1}) = B_{l+1}\partial_R^{(p^l)}(\boldsymbol{y}_{l+1})$ and hence to

$$\partial_R^{(p^l)}(\boldsymbol{y}) = \partial_R^{(p^l)}(D_0 \cdots D_l\boldsymbol{y}_{l+1}) = \partial_F^{(p^l)}(D_0 \cdots D_l)\boldsymbol{y}_{l+1} = A^{(p^l)}\boldsymbol{y}$$

for all $l \in \mathbb{N}$ where

$$A^{(p^l)} = \partial_F^{(p^l)}(D_0 \cdots D_l)(D_0 \cdots D_l)^{-1}.$$

In our example we compute $A^{(p^l)} = (1 + at^{p^l})^{-1}$. This allows to verify directly that y as above additionally solves the differential equations of the ID-module (M, Δ_M). The Galois group scheme of (M, Φ) or (M, Δ_M), respectively, is a subgroup scheme of $\mathbb{G}_m$ over $\mathbb{F}_p((s))$ (or $\mathbb{F}_p^{\mathrm{alg}}((s))$, respectively). By the considerations above we obtain the full group $\mathbb{G}_m$ as Galois group for exactly those $a \in F^\phi$ not belonging to $\mathbb{F}_p$.

4.4.2 Now we start with a 2-dimensional Frobenius module M over F with basis $B = \{b_1, b_2\}$ and Frobenius action given by $\Phi(b_1) = b_1, \Phi(b_2) = atb_1 + b_2$ with $a \in C_F$. Then a solution ring R of (M, Φ) is generated by $y_i \in R$ with

$$\phi_R \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & -at \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Thus y_2 belongs to $R^\phi = F^\phi$ and can be chosen to be $y_2 = 1$. The other solution $y := y_1$ fulfills $\phi(y) = y - at$. This gives

$$\mathrm{Sol}_R^\Phi(M) = yF^\phi + F^\phi \quad \text{with} \quad y = \sum_{l\in\mathbb{N}} \phi^l(a)t^{p^l}.$$

In case $a \in \mathbb{F}_q((s))$ for some power q of p, the sequence $\phi^l(a)$ becomes periodic and y is algebraic over F. Conversely, assume that y is algebraic over F. Then there exists a nontrivial equation of the form

$$\sum_{i=0}^n g_i y^{p^i} = 0 \quad \text{with} \quad g_i \in F$$

of minimal degree. Using $\partial^{(p^l)}$ for l large enough, we find

$$\sum_{i=0}^n g_i \phi^{l-i}(a) = 0.$$

Taking a shortest such linear recursion for the $\phi^l(a)$ we can conclude $g_i \in F^\phi$. This implies that the F^ϕ-vector space generated by the $\phi^l(a)$ is finite dimensional and thus the sequence $(\phi^l(a))_{l\in\mathbb{N}}$ is periodic. In all other cases, for example for

$$a = \sum_{i\in\mathbb{N}} c_i s^i \in \mathbb{F}_p^{\mathrm{alg}}((s)) \quad \text{with} \quad c_i \in \mathbb{F}_{p^{i+1}} \setminus \mathbb{F}_{p^i},$$

y is transcendental over F.

The ID-structure Δ_M related to Φ can be computed with the formulas derived in the previous example. Thus the differential equations for y_1, y_2 are given by

$$\partial_R^{(p^l)} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = A^{(p^l)} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \quad \text{with} \quad A^{(p^l)} = \begin{pmatrix} 0 & \phi^l(a) \\ 0 & 0 \end{pmatrix}.$$

The Galois group schemes $\mathrm{Gal}^\Phi(R/F)$ and $\mathrm{Gal}^\Delta(R/F)$ are subgroup schemes of the additive group $\mathbb{G}_a$ over F^ϕ or C_F, respectively, and we obtain the full group $\mathbb{G}_a$ if and only if $(\phi^l(a))_{l\in\mathbb{N}}$ is not periodic.

5 Global Frobenius Modules and the Grothendieck Conjecture

5.1 In this last chapter we study differential modules over differential rings which have infinitely many Frobenius endomorphisms. In order to construct such rings we start with a number field K (of finite degree over $\mathbb{Q}$) with set of non-archimedean valuations (places) $\mathbb{P}_K$. Let $\mathbb{P}'_K$ be a cofinite subset of $\mathbb{P}_K$ and $\mathcal{O}_\mathfrak{p}$ the valuation ring of $\mathfrak{p} \in \mathbb{P}'_K$. Then a Dedekind ring of type

$$\mathcal{O}'_K := \bigcap_{\mathfrak{p} \in \mathbb{P}'_K} \mathcal{O}_\mathfrak{p} \subseteq K$$

is called a *global ring* or an *order* in K. The valuations $\mathfrak{p} \in \mathbb{P}'_K$ can be extended uniquely onto the rational function field $K(\boldsymbol{t}) := K(t_1, \ldots, t_n)$ by setting $|t_i|_\mathfrak{p} = 1$ (Gauß extension) and further to every finite extension $F/K(\boldsymbol{t})$. The set of all valuations obtained in this way is denoted by $\mathbb{P}'_F := \{\mathfrak{P} \in \mathbb{P}_F \mid \mathfrak{P}|_{\mathcal{O}'_K} \in \mathbb{P}'_K\}$ and is called the *set of $\boldsymbol{t}$-extensions of* $\mathbb{P}'_K$. Then obviously

$$\mathcal{O}'_F := \bigcap_{\mathfrak{P} \in \mathbb{P}'_F} \mathcal{O}_\mathfrak{P} \subseteq F$$

is again a Dedekind ring.
The field $K(\boldsymbol{t})$ has a natural differential structure $\Delta = \{\partial_1, \ldots, \partial_n\}$ given by the partial derivations $\partial_i = \frac{d}{dt_i}$. These extend uniquely to F and define a differential structure Δ_F on F. In the following a ring $\mathcal{O}'_F$ as above is called a *global differential ring* (global D-ring) if

$$\partial(\mathcal{O}'_F) \subseteq \mathcal{O}'_F \quad \text{and} \quad \partial(\mathfrak{P}) \subseteq \mathfrak{P} \quad \text{for all} \quad \partial \in \Delta_F, \quad \mathfrak{P} \in \mathbb{P}'_F.$$

Further, $(\mathcal{O}'_F, \Delta_F)$ is called a *global iterative differential ring* (global ID-ring) if the inclusions above additionally hold for the higher derivations $\partial_i^{(k)} := \frac{1}{k!}\partial_i^k$ (compare Section 3.1). Obviously in any algebraic function field of several variables F over a number field K there exist many global ID-rings which can be obtained from any given $\mathcal{O}'_F$ by localizing at most at the places $\mathfrak{P} \in \mathbb{P}'_F$ ramified in $F/K(\boldsymbol{t})$ (see [7], Prop. 1.1).
For the present, let $K/\mathbb{Q}$ and $F/K(\boldsymbol{t})$ be Galois extensions. Then the global ID-rings $(\mathcal{O}'_F, \Delta_F)$ have Frobenius structures for all $\mathfrak{P} \in \mathbb{P}'_F$. These can be obtained by first lifting the Frobenius endomorphisms ϕ_p of the residue field extension $\mathcal{O}'_K/\mathfrak{p}$ over $\mathbb{F}_p = \mathbb{Z}/(p)$ to an automorphism $\phi_\mathfrak{p}$ of $\mathcal{O}'_K$ over $\mathbb{Z}_{(p)}$. Then $\phi_\mathfrak{p}$ can be extended to an endomorphism of $K(\boldsymbol{t})$ by setting, for example, $\phi_\mathfrak{p}(t_i) = t_i^p$. Since $F/K(\boldsymbol{t})$ is assumed to be a Galois extension, $\phi_\mathfrak{p}$ extends further to an endomorphism $\phi_\mathfrak{P}$ of $\mathcal{O}'_F$ (unique up to automorphisms of $F/K(\boldsymbol{t})$). Then $(\mathcal{O}'_F, (\phi_\mathfrak{P})_{\mathfrak{P} \in \mathbb{P}'_F}, \Delta_F)$ is called a *global ID-ring with Frobenius structure* or a *global IDF-ring*. This notion fits with the definitions used in earlier chapters, since the residue ring of $\mathcal{O}'_F$ modulo the

characteristic ideal $Q = \mathfrak{P}$ is an ordinary Frobenius ring for every $\mathfrak{P} \in \mathbb{P}'_F$. In case $K/\mathbb{Q}$ or $F/K(\boldsymbol{t})$ is not a Galois extension, $\phi_{\mathfrak{P}}(\mathcal{O}'_F)$ may be a subring of an isomorphic global ID-ring $\widetilde{\mathcal{O}}'_{\widetilde{F}}$. But then a power of $\phi_{\mathfrak{P}}$ maps $\mathcal{O}'_F$ to $\mathcal{O}'_F$ and thus defines a Frobenius endomorphism on $\mathcal{O}'_F$.

5.2 A *global differential module* (global D-module) (M, Δ_M) over a global D- or ID-ring $(\mathcal{O}'_F, \Delta_F)$ with $\Delta_F = \{\partial_1, \ldots, \partial_n\}$ is a free $\mathcal{O}'_F$-module with differential structure $\Delta_M = \{\partial_{M,1}, \ldots, \partial_{M,n}\}$ related to Δ_F by

$$\partial_{M,i}(ax) = \partial_i(a)x + a\partial_{M,i}(x) \quad \text{for} \quad a \in \mathcal{O}'_F, \quad x \in M.$$

The pair (M, Δ_M) is called a *global iterative differential module* (global ID-module) if in addition $\partial^{(k)}_{M,i}(M) \subseteq M$ holds for all higher derivations $\partial^{(k)}_{M,i} := \frac{1}{k!}\partial^k_{M,i}$. Next we want to construct and study Picard-Vessiot rings for global ID-modules.

In order to avoid new constants from now on we assume that K is algebraically closed in F and $\mathcal{O}'_F/\mathcal{O}'_K$ has a regular rational place $\wp$, i.e., the corresponding local ring $(\mathcal{O}'_F)_\wp$ is regular. Then the completion $\widehat{F}_\wp$ of F with respect to $\wp$ is the field of fractions $K((\boldsymbol{u})) := K((u_1, \ldots, u_n))$ of the ring of power series $K[[\boldsymbol{u}]] := K[[u_1, \ldots, u_n]]$, where the u_i are local parameters at $\wp$ of the form $u_i = t_i - c_i$ with $c_i \in \mathcal{O}'_K$ or $u_i = t_i^{-1}$. This defines an embedding

$$\tau_\wp : \mathcal{O}'_\wp \to K[[\boldsymbol{u}]], \quad a \mapsto \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} (\partial_1^{(k_1)} \circ \cdots \circ \partial_n^{(k_n)}(a))(\wp)u_1^{k_1} \cdots u_n^{k_n}$$

which extends uniquely to a differential monomorphism $\tau_\wp : \mathcal{O}'_F \to K((\boldsymbol{u}))$ over $\mathcal{O}'_K$ called *Taylor homomorphism*. Now we assume that $\wp$ in addition is a regular point for M. This means that $K^{\mathrm{alg}} \otimes_{\mathcal{O}'_K} M$ contains a Δ_M-invariant $K^{\mathrm{alg}}[[\boldsymbol{u}]]$-lattice. Then M becomes trivial over $K((\boldsymbol{u}))$. Obviously any global D-module over a global D-ring $\mathcal{O}'_F$ inside a rational function field $F = K(\boldsymbol{t})$ has infinitely many such regular points $\wp$ which are regular for M.

Theorem 5.1. *Let (M, Δ_M) be a global (iterative) D-module of rank m over a global (iterative) D-ring $(\mathcal{O}'_F, \Delta_F)$ with ring of differential constants $\mathcal{O}'_K$. Assume $\mathcal{O}'_F$ has a regular rational place $\wp$ over $\mathcal{O}'_K$ regular for M.*

(a) *There exists a Picard-Vessiot ring (R, Δ_R) inside $\widehat{F}_\wp$ for M over $\mathcal{O}'_F$ with fundamental solution matrix $Y \in \mathrm{GL}_m(R)$ which satisfies $Y(\wp) \in \mathrm{GL}_m(\mathcal{O}'_K)$. In the iterative case Δ_R is an iterative differential structure.*

(b) *The property $Y(\wp) \in \mathrm{GL}_m(\mathcal{O}'_K)$ determines (R, Δ_R) uniquely up to (iterative) differential isomorphism.*

Proof. In the univariate case Theorem 5.1 is proved in [7], Thm. 2.1. The main point is the extension of the Taylor homomorphism $\tau_\wp$ to $U := \mathcal{O}'_F[\mathrm{GL}_m] = \mathcal{O}'_F[x_{ij}, \det(x_{ij})^{-1}]^m_{i,j=1}$. Let $A_i \in (\mathcal{O}'_F)^{m\times m}$ be the matrix representing the derivation $\partial_{M,i}$ with respect to some fixed basis B of M, i.e., $\partial_{M,i}(B) = -BA_i$. Then U becomes a D-ring by setting $\partial_{U,i}(X) := A_iX$ for $X = (x_{ij})_{i,j=1}^m$. We now choose a matrix $X(\wp) = (x_{ij}(\wp))_{i,j=1}^m \in \mathrm{GL}_m(\mathcal{O}'_K)$ of initial values at $\wp$, for example $x_{ij}(\wp) = \delta_{ij}$. Then from $A_i(\wp) \in (\mathcal{O}'_K)^{m\times m}$ and $A_i^{(k)}(\wp) \in K^{m\times m}$ for the matrices $A_i^{(k)}$ representing $\partial_{M,i}^{(k)}$ we obtain $(\partial_{U,1}^{(k_1)} \circ \cdots \circ \partial_{U,n}^{(k_n)}(X))(\wp) \in K^{m\times m}$ for all i, k_j by recursion. This leads to an extension

$$\tau_\wp : U \to K((\boldsymbol{u})),\ x_{ij} \mapsto \sum_{(k_1,\dots,k_n)\in\mathbb{N}^n} (\partial_{U,1}^{(k_1)} \circ \cdots \circ \partial_{U,n}^{(k_n)}(x_{ij}))(\wp) u_1^{k_1} \cdots u_n^{k_n}$$

of the Taylor homomorphism on U depending on $X(\wp)$. By construction, $\tau_\wp$ is a differential homomorphism whose image in $K((\boldsymbol{u}))$ is a simple D-ring over $\tau_\wp(\mathcal{O}'_F)$ generated by $\tau_\wp(x_{ij})$ and $\tau_\wp(\det(X)^{-1})$. Thus the kernel of $\tau_\wp$ is a maximal differential ideal $P \trianglelefteq U$ with $P \cap \mathcal{O}'_F = (0)$. Hence $R := U/P$ is a Picard-Vessiot ring of M over $\mathcal{O}'_F$ with fundamental solution matrix $Y := X \pmod{P}$. The Taylor homomorphism $\tau_\wp$ factors through R, thus we obtain a further injective Taylor map

$$\tau_\wp : R \to K((\boldsymbol{u})), y_{ij} \mapsto \sum_{(k_1,\dots,k_n)\in\mathbb{N}^n} (\partial_{R,1}^{(k_1)}) \circ \cdots \circ \partial_{R,n}^{(k_n)}(y_{ij}))(\wp) u_1^{k_1} \dots u_n^{k_n}.$$

Now $\tau_\wp(C_R) \subseteq K$ implies $C_R \cong \tau_\wp(C_R) = \mathcal{O}'_K$, proving (a).
The uniqueness in (b) follows as in the classical case: Let R and $\widetilde{R}$ be two PV-extensions for M over $\mathcal{O}'_F$ with fundamental solution matrices $Y, \widetilde{Y}$ and $Y(\wp), \widetilde{Y}(\wp) \in \mathrm{GL}_m(\mathcal{O}'_K)$. Then by general PV-theory there exists a matrix $C \in \mathrm{GL}_m(K^{\mathrm{alg}})$ such that $\widetilde{Y} = YC$. Specialization modulo $\wp$ leads to $\widetilde{Y}(\wp) = Y(\wp)C$ showing $C \in \mathrm{GL}_m(\mathcal{O}'_K)$. □

Corollary 5.2. *If in Theorem 5.1 (M, Δ_M) is a global ID-module over a global ID-ring, the solution space $\mathrm{Sol}_R^\Delta(M)$ has the property*

$$\tau_\wp(\mathrm{Sol}_R^\Delta(M)) \subseteq \mathcal{O}'_K[[\boldsymbol{u}]],$$

i.e., $\mathrm{Sol}_R^\Delta(M)$ has a basis consisting of Taylor series whose coefficients are integral for almost all primes $\mathfrak{p} \in \mathbb{P}_K$.

This follows immediately from Theorem 5.1 since in this case aside from $A_i(\wp)$ all matrices $A_i^{(k)}(\wp)$ belong to $(\mathcal{O}'_K)^{m\times m}$.

5.3 By Corollary 5.2 Picard-Vessiot rings (R, Δ_R) of global ID-modules (M, Δ_M) can be reduced modulo $\mathfrak{P}$ for almost all $\mathfrak{P} \in \mathbb{P}'_F$. On the other hand, the ID-module M itself can also be reduced to an ID-module $(M_\mathfrak{P}, \Delta_{M_\mathfrak{P}})$ over $\mathcal{F}_\mathfrak{P} := \mathcal{O}'_F/\mathfrak{P}$ by reducing the ID-structure Δ_M modulo $\mathfrak{P}$. Then general iterative differential Galois theory proves the existence of a Picard-Vessiot ring for $M_\mathfrak{P}$ after a finite extension of constants ([8], Lemma 3.2). If, moreover, there exists a regular rational place in

$\mathcal{F}_{\mathfrak{P}}$ regular for $M_{\mathfrak{P}}$, a Picard-Vessiot ring $R_{\mathfrak{P}}$ for $M_{\mathfrak{P}}$ over $\mathcal{F}_{\mathfrak{P}}$ can be constructed without new constants (compare the characteristic zero case). The next theorem shows that for almost all $\mathfrak{P} \in \mathbb{P}'_F$, the reduced PV-ring $R \pmod{\mathfrak{P}}$ and the iterative PV-ring $R_{\mathfrak{P}}$ for $M_{\mathfrak{P}}$ coincide.

Theorem 5.3. *Let (M, Δ_M) be a global ID-module over a global ID-ring $(\mathcal{O}'_F, \Delta_F)$ with a regular rational place $\wp$ in $\mathcal{O}'_F/\mathcal{O}'_K$ regular for M. For $\mathfrak{P} \in \mathbb{P}'_F$, let $(M_{\mathfrak{P}}, \Delta_{M_{\mathfrak{P}}})$ be the reduced ID-module over $\mathcal{F}_{\mathfrak{P}}$. Assume the reduced place $\overline{\wp}$ is regular for $M_{\mathfrak{P}}$. Then the rings $R \pmod{\mathfrak{P}}$ and $R_{\mathfrak{P}}$ are isomorphic as ID-rings.*

Proof. For the proof we observe that the reduced PV-ring $\overline{R} := R (\mathrm{mod}\ \mathfrak{P})$ (of Taylor series) with fundamental solution matrix $\overline{Y} := Y (\mathrm{mod}\ \mathfrak{P})$ is a solution ring for $M_{\mathfrak{P}}$ without new constants . But then by [5], Prop. 4.8, $\overline{R}$ is an iterative PV-ring for $M_{\mathfrak{P}}$ over $\mathcal{F}_{\mathfrak{P}}$ which is unique up to ID-isomorphism over $\mathcal{F}_{\mathfrak{P}}$. $\square$

Grothendieck's Generic Flatness Lemma (see [3], Cor. 14.5) shows that the dimensions of $R \pmod{\mathfrak{P}}$ and $R_{\mathfrak{P}}$ are related by the formula

$$\dim(R_{\mathfrak{P}}) = \dim(R) - 1 \quad \text{for almost all} \quad \mathfrak{P} \in \mathbb{P}'_F$$

(compare [7], Cor. 3.2). This leads to

Corollary 5.4. *Under the assumptions of Theorem 5.3 the Picard-Vessiot ring R of M is algebraic over $\mathcal{O}'_F$ if and only if for almost all $\mathfrak{P} \in \mathbb{P}'_F$ the Picard-Vessiot ring $R_{\mathfrak{P}}$ of the reduced ID-module $M_{\mathfrak{P}}$ is algebraic over $\mathcal{F}_{\mathfrak{P}}$.*

The property that $R_{\mathfrak{P}}/\mathcal{F}_{\mathfrak{P}}$ is algebraic is guaranteed by the existence of a global strong Frobenius structure $(\Phi_{\mathfrak{P}})_{\mathfrak{P} \in \mathbb{P}'_F}$ for M. Such a Frobenius structure exists for example for all ID-modules which generate Galois ring extensions $\widetilde{\mathcal{O}}'_{\widetilde{F}}/\mathcal{O}'_F$ inside ordinary finite Galois extensions $\widetilde{F}/F$. This finally leads to

Theorem 5.5. *Let (M, Δ_M) be a global ID-module over a global IDF-ring $(\mathcal{O}'_F, (\phi_{\mathfrak{P}})_{\mathfrak{P} \in \mathbb{P}'_F}, \Delta_F)$ with strong Frobenius structure $\Phi_{\mathfrak{P}}$ for almost all $\mathfrak{P} \in \mathbb{P}'_F$. Assume there exists a regular rational place in $\mathcal{O}'_F$ regular for M. Then the Picard-Vessiot ring R of M is algebraic over $\mathcal{O}'_F$.*

Of course, for the conclusion in Theorem 5.5 that $R/\mathcal{O}'_F$ is algebraic, the existence of a p-adic Frobenius structure or a congruence Frobenius structure would be enough. On the other hand, the existence of an ID-structure $\Delta_M = \{\partial_1, \ldots, \partial_n\}$ implies the triviality of the p-curvature $\Delta_M^p = \{\partial_1^p, \ldots, \partial_n^p\}$ for almost all primes p modulo $\mathfrak{P} \in \mathbb{P}'_F$ with $(p) \subseteq \mathfrak{P}$. Thus Grothendieck's p-Curvature Conjecture predicts that all ID-modules M over global ID-rings $\mathcal{O}'_F$ are algebraic. By the considerations above this statement is equivalent to the existence of a global strong Frobenius structure for M.

Acknowledgements. I thank J. Hartmann and A. Röscheisen for helpful comments and discussions on the topics of the paper.

BIBLIOGRAPHY

[1] G. Christol: *Modules différentiels et équations différentielles p-adiques.* Queen's Papers in Pure and Applied Mathematics **66** (1983).

[2] T. Dyckerhoff: Picard-Vessiot extensions over number fields. Diplomarbeit, Univ. Heidelberg 2005.

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

[4] F. Heiderich: Picard-Vessiot-Theorie für lineare partielle Differentialgleichungen. Diplomarbeit, Univ. Heidelberg 2007.

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

[6] B. H. Matzat: Frobenius modules and Galois groups. In: K. Hashimoto et al. (Eds.): *Galois Theory and Modular Forms*. Kluwer, Dordrecht 2003, pp. 233-268.

[7] B. H. Matzat: Differential equations and finite groups. Journal of Algebra **300** (2006), 673-686.

[8] B. H. Matzat, M. van der Put: Iterative differential equations and the Abhyankar conjecture. J. reine angew. Math. **257** (2003), pp. 1-52.

[9] B. H. Matzat, M. van der Put: Constructive differential Galois theory. In: L. Schneps (Ed.): *Galois Groups and Fundamental Groups*. Cambridge Univ. Press 2003, pp. 425-467.

[10] M. A. Papanikolas: Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms. Invent. math. (2007)

[11] M. van der Put, M. F. Singer: *Galois Theory of Difference Equations*. Springer-Verlag, Berlin 1997.

[12] M. van der Put, M. F. Singer: *Galois Theory of Linear Differential Equations*. Springer-Verlag, Berlin 2003.

[13] A. Röscheisen: Galois theory for iterative connections and non-reduced Galois groups. Preprint 2007. Available at http://arxiv.org/abs//0712.3748 .

[14] P. Robba, G. Christol: *Equations différentielles p-adiques*. Hermann, Paris 1994.

[15] D. S. Thakur: *Function Field Arithmetic*. World Scientific, New Jersey 2004.