



ANNALES

DE

L'INSTITUT FOURIER

B. Heinrich MATZAT

Frobenius modules and Galois representations

Tome 59, n° 7 (2009), p. 2805-2818.

http://aif.cedram.org/item?id=AIF_2009__59_7_2805_0

© Association des Annales de l'institut Fourier, 2009, tous droits réservés.

L'accès aux articles de la revue « Annales de l'institut Fourier » (<http://aif.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://aif.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

*Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>*

FROBENIUS MODULES AND GALOIS REPRESENTATIONS

by B. Heinrich MATZAT

ABSTRACT. — Frobenius modules are difference modules with respect to a Frobenius operator. Here we show that over non-archimedean complete differential fields Frobenius modules define differential modules with the same Picard-Vessiot ring and the same Galois group schemes up to extension by constants. Moreover, these Frobenius modules are classified by unramified Galois representations over the base field. This leads among others to the solution of the inverse differential Galois problem for p -adic differential equations with (strong) Frobenius structure over p -adic differential fields with algebraically closed residue field.

RÉSUMÉ. — Les modules de Frobenius sont des modules aux différences par rapport à un opérateur de Frobenius. Nous montrons ici que, sur des corps différentiels complets et non archimédiens, les modules de Frobenius définissent des modules différentiels ayant le même anneau de Picard-Vessiot, et quitte à étendre le corps des constantes, le même schéma en groupes de Galois. De plus, ces modules de Frobenius sont classifiés par des représentations galoisiennes non ramifiées sur le corps de base. Cela donne, entre autres, la solution du problème de Galois différentiel inverse pour les équations différentielles p -adiques avec une structure de Frobenius (forte), définies sur les corps différentiels p -adiques ayant un corps résiduel algébriquement clos.

0. Introduction

Frobenius modules encode many of the typical phenomena in positive characteristic. They enjoy a difference Galois theory with linear algebraic group schemes as partners similar to differential modules (see [13]). Here we study adic Frobenius modules in connection with their induced differential equations and Galois representations. This applies among others to ordinary Galois extensions, p -adic differential equations and t -motives.

Keywords: Frobenius modules, iterative differential modules, Galois representations, p -adic differential equations, inverse differential Galois theory.

Math. classification: 12H25, 12F12, 12H05, 12H10.

In the first chapter we introduce ordinary and relative Frobenius modules including p -adic and t -adic Frobenius modules. All these can be equipped with an iterative differential structure such that the corresponding Galois theories coincide up to base change. This has been proved in the preceding note [7] and is described here in a short and more unified way.

The second chapter is devoted to Frobenius modules over relative Frobenius rings which are complete with respect to their defining ideal. Following an idea in [12] these can be characterized by unramified Galois representations of the absolute Galois group of the base ring where in addition the image of the Galois representation is dense in the Galois group of the Frobenius module.

As an application we obtain the solution of the inverse Galois problem for Frobenius modules over complete base rings with separably algebraically closed residue field. In particular the inverse Galois problem for p -adic differential equations with strong Frobenius structure is solved.

1. Frobenius and Differential Modules

1.1. Let S be a commutative ring (always with a unit element) of prime characteristic $p > 0$. Then S is equipped with the p -power endomorphism $\phi : S \rightarrow S$, $a \mapsto a^p$, called Frobenius endomorphism. For this reason we call S together with the ordinary Frobenius action ϕ an *ordinary Frobenius ring* (S, ϕ) or an ordinary F-ring for short.

This notion can be generalized to an *F-ring* (S, ϕ) relative to some ideal $Q \trianglelefteq S$. This is a commutative ring S with an endomorphism ϕ with the property $\phi(Q) \subseteq Q$ such that the residue ring $\bar{S} := S/Q$ together with the induced endomorphism $\bar{\phi}$ is an ordinary Frobenius ring $(\bar{S}, \bar{\phi})$. Hence an ordinary F-ring is an F-ring relative to $Q = (0)$. In the following we denote by $S_l := \phi^l(S)$ the subring of S obtained as the image of ϕ^l and by $S^\phi := \{a \in S \mid \phi(a) = a\}$ the ring of invariants of S under ϕ . Obviously we have $S^\phi \subseteq \bigcap_{l \in \mathbb{N}} S_l$.

Basic examples are:

a. The polynomial ring $\mathbb{F}_p[s]$ over the prime field \mathbb{F}_p with the Frobenius endomorphism $\phi : s \mapsto s^p$ is an ordinary F-ring. Its ring of invariants $\mathbb{F}_p[s]^\phi$ equals \mathbb{F}_p .

b. The polynomial ring $\mathbb{Z}_p[s]$ over the ring of p -adic integers \mathbb{Z}_p with Frobenius endomorphism $\phi|_{\mathbb{Z}_p} = \text{id}$ and $\phi(s) = s^p$ is an F-ring relative to $Q = (p)$ with ring of invariants $\mathbb{Z}_p[s]^\phi = \mathbb{Z}_p$.

c. The polynomial ring $\mathbb{F}_p[t, s]$ in two variables over \mathbb{F}_p with $\phi(t) = t$ and $\phi(s) = s^p$ is an F-ring relative to $Q = (t)$ with ring of invariants $\mathbb{F}_p[t]$.

The rings $\mathbb{Z}_p[s]$ and $\mathbb{F}_p[t, s]$ are the ground rings in p -adic and t -adic analysis, respectively, including for example isocrystals in the p -adic and t -motives in the t -adic case.

In all our examples in addition we have a partial iterative derivation $\partial = \partial_s$ with respect to s (see [4], Ch. 1 or [7], Ch. 2.1 for the general definition) consisting of a family $\partial_s = (\partial_s^{(k)})_{k \in \mathbb{N}}$ of higher derivations $\partial_s^{(k)} : S \rightarrow S$ given by $\partial_s^{(k)}(s^l) = \binom{l}{k} s^{l-k}$, in particular by $\partial_s^{(p^l)}(s^{p^l}) = 1$. (In characteristic zero $\partial^{(k)}$ can be directly obtained from the powers of the ordinary derivation $\partial^{(1)}$ by the rule $\partial^{(k)} = \frac{1}{k!}(\partial^{(1)})^k$.)

It is obvious that $\partial_s^{(k)}(Q) \subseteq Q$ holds for $k \in \mathbb{N}$ and hence the iterative derivation ∂_s commutes with the reduction modulo Q . Moreover the Frobenius endomorphism ϕ and the iterative derivation ∂_s are related by $\partial_s^{(1)} \circ \phi(S) \subseteq Q$ and more generally for the higher derivations by $\partial_s^{(k)} \circ \phi^l(S) \subseteq Q^{l+1-d}$ for $d \leq l$ and $0 < k < p^d$.

An arbitrary Frobenius ring (S, ϕ) relative to some ideal Q together with a finite set of commuting iterative derivations $\Delta = \{\partial_1, \dots, \partial_n\}$ is called an *IDF-ring* (S, ϕ, Δ) if $\Delta(Q) \subseteq Q$ and the Frobenius action and the iterative derivations in Δ are related by the above *Frobenius compatibility*, i.e., by

$$\Delta_d \circ \phi^l(S) \subseteq Q^{l+1-d} \quad \text{for } d \leq l. \quad (1)$$

Here Δ_d consists of the set of all non trivial higher derivations $\partial_1^{(k_1)} \circ \dots \circ \partial_n^{(k_n)}$ in Δ of order $\sum_{i=1}^n k_i < p^d$ (and $\sum_{i=1}^n k_i \neq 0$). Obviously the basic examples are all IDF-rings with respect to $\Delta = \{\partial_s\}$. Moreover, the examples in positive characteristic fulfill the even stronger property $\Delta_d \circ \phi^l(S) = 0$ for $d \leq l$.

1.2. A Frobenius module is a difference module over a Frobenius ring. More precisely a *Frobenius module* (M, Φ) over an F-ring (S, ϕ) consists of a free S -module M of finite rank m and a ϕ -semilinear regular endomorphism $\Phi : M \rightarrow M$, i.e., Φ is additive with

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

and maps a basis of M to a basis of M . Obviously the images $M_l := \Phi^l(M)$ of an F-module M over S are F-modules over $S_l = \phi^l(S)$. Since M_{l+1} is

(1) In case the ideal $Q \leq S$ is not finitely generated in the formula Q should be replaced by the ideal Q_Δ generated by the transition elements $z_i \in Q$ defined by $\partial_i^{(1)} \circ \phi(a) = z_i \phi \circ \partial_i^{(1)}(a)$ for $a \in S$ (see [7], Ch. 3.1).

included in M_l , we get an S_{l+1} -linear embedding $\varphi_l : M_{l+1} \rightarrow M_l$. These define a projective system $(M_l, \varphi_l)_{l \in \mathbb{N}}$ of F-modules (M_l, Φ_l) over (S_l, ϕ_l) with $\Phi_l := \Phi|_{M_l}$ and $\phi_l := \phi|_{S_l}$.

For Φ with respect to a basis $B = \{b_1, \dots, b_m\}$ of M we find a representing matrix $D = D_B(\Phi) \in \text{GL}_m(S)$ by $\Phi(B) = B \cdot D$ (with the basis written as a row). The ϕ -semilinearity of Φ leads to $\Phi^l(B) = B \cdot D \cdots D_l$ where $D_l = \phi^l(D) \in \text{GL}_m(S_l)$ is the representing matrix of Φ_l on M_l .

For any extension F-ring $(\tilde{S}, \tilde{\phi})$ over (S, ϕ) the module $M_{\tilde{S}} := \tilde{S} \otimes_S M$ becomes a Frobenius module over \tilde{S} with an extended Frobenius action $\tilde{\Phi} := \tilde{\phi} \otimes \Phi$. Then the *solution space* of the F-module (M, Φ) over $(\tilde{S}, \tilde{\Phi})$ is defined by

$$\text{Sol}_{\tilde{S}}^{\tilde{\Phi}}(M) := \{x \in M_{\tilde{S}} \mid \tilde{\Phi}(x) = x\}.$$

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

Now we are interested in the existence of a minimal solution ring of a Frobenius module which sometimes is called a *Picard-Vessiot ring* (*PV-ring*) or ring of periods of M etc. For this we assume that our F-ring (S, ϕ) is an integral domain - we call it an F-domain - relative to a valuation ideal $Q \triangleleft S$ of rank ≤ 1 . This means that by Chevalley's Extension Theorem (see [2], Thm. 3.1.1 or [1], Exerc. 11.2) Q defines a valuation on $\text{Quot}(S)$ of rank ≤ 1 . Then the completion S_Q of S with respect to Q is a Henselian integral domain with continuously extended Frobenius endomorphism ϕ . The integral closure of S_Q in the maximal unramified algebraic extension of $\text{Quot}(S_Q)$ is denoted by S_Q^{ur} . It is an F-ring with respect to the unique extension ϕ^{ur} of ϕ compatible with the ordinary Frobenius endomorphism of the residue ring $S_Q^{\text{ur}}/(Q)$. Thus the completion of S_Q^{ur} with respect to the ideal $(Q) \triangleleft S_Q^{\text{ur}}$ generated by Q with the continuously extended Frobenius endomorphism $\hat{\phi} = \hat{\phi}^{\text{ur}}$ again is a Henselian F-domain $(\hat{S}_Q^{\text{ur}}, \hat{\phi})$. (In case $Q = (0)$ the F-ring $(\hat{S}_Q^{\text{ur}}, \hat{\phi})$ simply consists of the separable algebraic closure S^{sep} of S with the ordinary Frobenius endomorphism ϕ).

The following theorem is proved in [7], Prop. 1.2 (see also [5], Prop. 8.3 and [10], Prop. 3.3.9 for special cases).

THEOREM 1.1. — *Let (S, ϕ) be an F-domain relative to a valuation ideal Q of rank at most one. Then every Frobenius module (M, Φ) over S has a Picard-Vessiot ring inside \hat{S}_Q^{ur} .*

In [10] the PV-ring in Theorem 1.1 is called a *rigid analytic trivialization* of M . It should be mentioned that in general a PV-ring of a difference module may have zero divisors (see [13], Example 1.6) and usually is not uniquely determined up to isomorphism (except when the base ring is an algebraically closed field).

1.3. For any Frobenius module (M, Φ) over an IDF-ring (S, ϕ, Δ) complete with respect to the defining ideal Q we can construct a unique Frobenius compatible differential structure ∇ on M . This means that $\nabla = \{\delta_1, \dots, \delta_n\}$ consists of commuting iterative derivations δ_i related to $\partial_i \in \Delta$ by the generalized Leibniz rule

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

The construction is based on the projective system $(M_l, \varphi_l)_{l \in \mathbb{N}}$ introduced in the last section. By Frobenius compatibility any basis $B_l = \{b_{l1}, \dots, b_{lm}\}$ of $M_l = \Phi^l(M)$ should satisfy

$$\nabla_d(B_l) \subseteq Q^{l-d+1}M. \quad (1)$$

Thus, using the embedding $\varphi_0 \circ \dots \circ \varphi_{l-1}(B_l) \subseteq M$ any element $x \in M$ can be written as a linear combination $x = \sum_{j=1}^m b_{lj}a_j$ with $a_j \in S$. By the Leibniz rule, Frobenius compatibility leads to

$$\delta_i^{(k)}(x) \equiv \sum_{j=1}^m b_{lj}\partial_i^{(k)}(a_j) \pmod{Q^{l-d+1}} \quad \text{for } k < p^d$$

which can be expressed by

$$\delta_i^{(k)}(x) \equiv \varphi_0 \circ \dots \circ \varphi_{l-1} \circ \partial_i^{(k)} \circ \varphi_{l-1}^{-1} \circ \dots \circ \varphi_0^{-1}(x) \pmod{Q^{l-d+1}} \quad \text{for } k < p^d.$$

(In this formula $\partial_i^{(k)}$ symbolizes that after transformation to a basis of M_l only the coefficients of x with respect to the new basis have to be differentiated.) By assumption the limit

$$\delta_i^{(k)}(x) := \lim_{l \rightarrow \infty} (\varphi_0 \circ \dots \circ \varphi_{l-1} \circ \partial_i^{(k)} \circ \varphi_{l-1}^{-1} \circ \dots \circ \varphi_0^{-1}(x))$$

exists and defines the higher derivation $\delta_i^{(k)}$ on M .

In case we have the stronger Frobenius compatibility $\Delta_d \circ \phi^l(S) = 0$ for $d \leq l$ mentioned at the end of Section 1.1, $\delta_i^{(k)}(x)$ can be defined without

(1) Compare footnote on p. 2

using limits by

$$\delta_i^{(k)}(x) := \varphi_0 \circ \dots \circ \varphi_{l-1} \circ \partial_i^{(k)} \circ \varphi_{l-1}^{-1} \circ \dots \circ \varphi_0^{-1}(x) \quad \text{for } k < p^l.$$

Thus in this case the assumption of completeness is superfluous.

For a solution $x = \sum_{j=1}^m b_j y_j$ of the Frobenius module M with coordinates y_j in some extension IDF-ring $(\tilde{S}, \tilde{\phi}, \tilde{\Delta})$ over S the formulas above translate into

$$\tilde{\partial}_i^{(k)}(\mathbf{y}) = A_i^{(k)} \mathbf{y}$$

with $\mathbf{y} = (y_1, \dots, y_m)^{tr}$ and

$$A_i^{(k)} = \lim_{l \rightarrow \infty} (\partial_i^{(k)}(D_0 \cdots D_{l-1})(D_0 \cdots D_{l-1})^{-1}).$$

As in the case of rings a Frobenius module (M, Φ) over an IDF-ring (S, ϕ, Δ) with differential structure ∇ related to Φ by Frobenius compatibility

$$\nabla_d \circ \Phi^l(M) \subseteq Q^{l-d+1}M \quad \text{for } d \leq l$$

is called an *IDF-module* (M, Φ, ∇) . On such modules, in addition to the Picard-Vessiot theory for difference modules we have a Picard-Vessiot theory for differential modules. One may ask how the corresponding Picard-Vessiot extensions and solution spaces are related. This is answered in the following theorem proved in [7], Thm. 2.2 and Thm. 3.2:

THEOREM 1.2. — *Let (S, ϕ, Δ) be an IDF-domain relative to a rank one valuation ideal Q and let (M, Φ, ∇) 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 such that (R, Δ_R) is a solution ring of (M, ∇) , and the solution spaces are related by*

$$\text{Sol}_R^\nabla(M) = C_R \otimes_{R^\phi} \text{Sol}_R^\Phi(M) \quad \text{and} \quad \text{Sol}_R^\Phi(M) = \text{Sol}_R^\nabla(M)^{\tilde{\Phi}},$$

where C_R is the ring of differential constants of R and $\tilde{\Phi}$ denotes the canonical extension of Φ to $R \otimes_S M$.

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

(c) *The ring 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 $(\widehat{C_S})_Q^{\text{ur}}$ of C_S with respect to $Q \cap C_S$.*

In particular, if $C_R = C_S$, the Picard-Vessiot ring R of (M, Φ) coincides with the Picard-Vessiot ring of (M, ∇) . This is the case for example if C_S is separably algebraically closed or if C_S is complete with respect to $Q \cap C_S$ with separably algebraically closed residue ring (see [7], Cor. 2.2, 2.3 and 3.2).

1.4. Now we want to compare the Galois groups or the Galois group schemes, respectively, of an IDF-module (M, Φ, ∇) over S with respect to the Frobenius structure Φ and the differential structure ∇ . For simplicity we assume that the Picard-Vessiot ring R of (M, Φ) over S coincides with the one of (M, ∇) . By Theorem 1.2 this is equivalent to assuming that R does not contain new differential constants.

Over an F-field (S, ϕ) with field of invariants $L := S^\phi$ the Galois group scheme is defined as a functor from the category of L -algebras to the category of groups

$$\underline{\text{Aut}}^\Phi(R/S) : L\text{-Alg} \rightarrow \text{Groups}, A \mapsto \text{Aut}^\Phi(R \otimes_L A/S \otimes_L A)$$

which over L is represented by the L -algebra $(R \otimes_S R)^{\phi_R \otimes \phi_R}$. The corresponding affine group scheme over L is called *Frobenius Galois group scheme* and is denoted by $\mathcal{G}^\Phi = \underline{\text{Gal}}^\Phi(R/S)$ (compare [10], Ch. 4 in case ϕ is an automorphism or [7], Ch. 4.3). In the same manner with Φ substituted by ∇ and S^ϕ substituted by the field of differential constants C_S in S one defines the *differential Galois group scheme* $\mathcal{G}^\nabla = \underline{\text{Gal}}^\nabla(R/S)$ over C_S .

In [7], Thm. 4.2 it is observed that under the above assumptions both Galois group schemes are simply related by base change.

COROLLARY 1.3. — *Let (M, Φ, ∇) be an IDF-module over the quotient field S of a Frobenius ring relative to a valuation ideal Q of rank at most one. Assume that the ring of differential constants C_R of a minimal Frobenius solution ring R of M equals C_S . Then for the Galois group schemes $\mathcal{G}_{S^\phi}^\Phi = \underline{\text{Gal}}^\Phi(R/S)$ and $\mathcal{G}_{C_S}^\nabla = \underline{\text{Gal}}^\nabla(R/S)$, one has*

$$\mathcal{G}_{C_S}^\nabla = \text{Spec}(C_S) \times_{S^\phi} \mathcal{G}_{S^\phi}^\Phi.$$

Moreover, both Galois group schemes lead to a Galois correspondence between the closed subgroup schemes and IDF-intermediate fields of $\text{Quot}(R)/S$. This could also be derived from the fact that both the category of Φ - and of ∇ -modules over S are equivalent neutral Tannakian categories with fiber functors given by the respective solution spaces of M inside the rigid analytic trivialization R of (M, Φ) or (M, ∇) respectively (see [10], Thm. 3.3.15 and [9], Ch. 11 respectively).

In the examples of this note the group of rational points

$$\text{Gal}^\Phi(R/S) := \mathcal{G}_{S^\phi}^\Phi(S^\phi) \quad \text{and} \quad \text{Gal}^\nabla(R/S) := \mathcal{G}_{C_S}^\nabla(C_S)$$

of the Galois group schemes $\underline{\text{Gal}}^\Phi(R/S) = \mathcal{G}_{S^\phi}^\Phi$ respectively $\underline{\text{Gal}}^\nabla(R/S) = \mathcal{G}_{C_S}^\nabla$ are Zariski dense. This implies that S is the subring of R fixed by either one of $\text{Gal}^\Phi(R/S)$ or $\text{Gal}^\nabla(R/S)$. Thus $\text{Gal}^\Phi(R/S)$ becomes the Φ -Galois group and $\text{Gal}^\nabla(R/S)$ the differential Galois group of R/S (compare [5], Ch. 9.2). Moreover, the group schemes $\underline{\text{Gal}}^\Phi(R/S)$ and $\underline{\text{Gal}}^\nabla(R/S)$ are uniquely determined by these Galois groups. Thus here for simplicity we can work with the Frobenius and differential Galois groups themselves instead of the underlying group schemes.

2. Q -adic Frobenius Modules and Galois Representations

2.1. In this chapter we assume that (S, ϕ) is a Frobenius domain relative to a valuation ideal Q of rank equal or less than 1 defining a discrete (or trivial) valuation v_Q on S . We further assume that $S = S_Q$ is complete with respect to v_Q . Such a domain in the following is called a Q -adic F -ring. It is called a q -adic F -ring, if Q is generated by a ϕ -invariant element q . Obviously Q -adic F -rings are Henselian with respect to the valuation induced by Q .

Basis examples are:

a. The polynomial ring $\mathbb{F}_p[s_1, \dots, s_n]$ in n variables over the prime field \mathbb{F}_p with Frobenius endomorphism ϕ defined by $\phi(s_i) = s_i^p$ for $i = 1, \dots, n$ is an ordinary F -ring. Thus $\mathbb{F}_p[s_1, \dots, s_n]$ is a Q -adic F -ring relative to $Q = (0)$ with the trivial valuation v_Q .

b. The ring of analytic elements $\mathbb{Z}_p\langle\langle s_1, \dots, s_n \rangle\rangle$ over \mathbb{Z}_p with Frobenius endomorphism given by $\phi(s_i) = s_i^p$ is a Q -adic F -ring relative to $Q = (p)$. It can be obtained from the polynomial ring $\mathbb{Z}_p[s_1, \dots, s_n]$ by completion with respect to the Gauß extension of the p -adic valuation on \mathbb{Z}_p .

c. The ring of analytic elements $\mathbb{F}_p[[t]]\langle\langle s_1, \dots, s_n \rangle\rangle$ over $\mathbb{F}_p[[t]]$ with Frobenius endomorphism defined by $\phi(t) = t$ and $\phi(s_i) = s_i^p$ is a Q -adic F -ring relative to $Q = (t)$. It is the completion of $\mathbb{F}_p[[t]][s_1, \dots, s_n]$ with respect to the Gauß extension of the t -adic valuation on $\mathbb{F}_p[[t]]$.

All these examples in addition are IDF-rings (S, ϕ, Δ) with respect to the set of iterative partial derivations $\Delta = \{\partial_{s_1}, \dots, \partial_{s_n}\}$ and thus are Q -adic IDF-rings.

First we assume $Q = (0)$. Then by Theorem 1.1, M has a Picard-Vessiot ring R inside S^{sep} . If we suppose that $S = \text{Quot}(S)$ is a field, R/S becomes

a finite F-field extension which in fact is an ordinary finite Galois extension (see [5], Thm. 1.1 or [8], Prop. 5.4(2)).

PROPOSITION 2.1. — *Let (S, ϕ) be an ordinary F-field.*

(a) *Let (M, Φ) be an F-module over (S, ϕ) . Then the Picard-Vessiot ring R of M over S is a finite Galois extension which is unique inside S^{sep} .*

(b) *For every finite Galois extension R/S there exists a Frobenius module (M, Φ) over S with Picard-Vessiot ring R .*

Part (a) can be made explicit by choosing a basis $B = \{b_1, \dots, b_m\}$ of M . Then Φ is given by a representing matrix $D = D_B(\Phi) \in \text{GL}_m(S)$ and $\mathbf{y} = (y_1, \dots, y_m)^{tr} \in \text{Sol}^\Phi(M)$ is equivalent to the matrix equation

$$D \cdot \mathbf{y}^p = D_B(\Phi) \cdot \phi(\mathbf{y}) = \mathbf{y}.$$

This defines a system of algebraic equations over S with the identity matrix as Jacobian matrix. Thus, by the Theorem of Bézout it has p^m different solutions forming an m -dimensional \mathbb{F}_p -vector space. In case S is not finite, $\text{Sol}_R^\Phi(M)$ contains a Φ -cyclic element and R/S is generated by the roots of an additive separable polynomial of degree p^m (see [5], Thm. 2.1 and Cor. 2.2). The latter can be computed from the matrix equation by using Buchberger’s algorithm.

For (b) let $y \in R$ be a primitive element with minimal polynomial $f_y(T) \in S[T]$. The roots of $f_y(T)$ in R span a finite dimensional \mathbb{F}_p -vector space V , with $\dim(V) = m$ say. Then the polynomial

$$g(T) := \prod_{v \in V} (T - v) = \sum_{i=0}^m a_i T^{p^i}$$

is an additive polynomial whose companion matrix

$$C = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & \cdots & \cdots & \cdots & -a_{m-1} \end{pmatrix}$$

given by $\mathbf{y}^p = C\mathbf{y}$ defines an m -dimensional Frobenius module (M, Φ) over S with Picard-Vessiot ring R (compare [5], Section 2.1).

2.2. In the case $Q \neq (0)$ we have a non trivial discrete rank 1 valuation v_Q on S . Since $S = S_Q$ is Henselian with respect to v_Q the Galois group Γ_S^{ur} of the maximal unramified field extension of $\text{Quot}(S)$ is isomorphic to the absolute Galois group $\Gamma_{\bar{S}}$ of the quotient field $\text{Quot}(\bar{S})$ of the residue ring

$\bar{S} = S/Q$ (see for example [2], Thm. 5.2.7). This fact can be used to provide a Q -adic F -module (M, Φ) of dimension m with a Galois representation $\rho_M : \Gamma_S^{\text{ur}} \rightarrow \text{GL}_m(S)$ and vice versa. The precise statement is formulated in the next Theorem 2.2. Special cases already go back to van der Put [12] in the p -adic and Stalder [11] in the t -adic case.

THEOREM 2.2. — *Let (S, ϕ) be a q -adic Frobenius ring.*

(a) *Let (M, Φ) be an F -module over (S, ϕ) with rigid analytic trivialization R/S and Galois group $\text{Gal}^\Phi(R/S) \leq \text{GL}_m(S^\phi)$. Then M defines an unramified continuous Galois representation*

$$\rho_M : \Gamma_S^{\text{ur}} \rightarrow \text{GL}_m(S^\phi) \quad \text{with} \quad \rho_M(\Gamma_S^{\text{ur}}) \leq \text{Gal}^\Phi(R/S)$$

Zariski dense.

(b) *For every unramified continuous Galois representation $\rho : \Gamma_S^{\text{ur}} \rightarrow \text{GL}_m(S^\phi)$ there exists a Frobenius module (M, Φ) over S with rigid analytic trivialization R/S such that $\rho_M = \rho$.*

For the proof of Theorem 2.2(a) we basically follow the construction in [5], Section 6.3. Let R/S be a rigid analytic trivialization of a Frobenius module (M, Φ) over $S = S_Q$ generated by $D = D_B(\Phi) \in \text{GL}_m(S)$. Then there exists a linear algebraic group \mathcal{G} over S^ϕ such that $\text{Gal}^\Phi(R/S) = \mathcal{G}(S^\phi)$. Moreover, R over S is generated by the entries of a fundamental solution matrix $Y = (y_{ij})_{i,j=1}^m \in \text{GL}_m(R)$ and its inverse. Reduction modulo Q of R/S and Y produces an ordinary Galois extension \bar{R}_1/\bar{S} over $\bar{S} = S/Q$ generated by the reduced fundamental solution matrix $\bar{Y}_1 \in \text{GL}_m(\bar{R}_1)$ with $\bar{D}^{-1} = \phi(\bar{Y}_1)\bar{Y}_1^{-1}$. By [2], Thm. 5.2.7 there exists a unique F -ring (R_1, ϕ_1) unramified and of finite degree over (S, ϕ) with residue ring \bar{R}_1 and a matrix $Y_1 \in \text{GL}_m(R_1)$ such that

$$D^{-1} = \phi_1(Y_1)(I + qD_1)Y_1^{-1} \quad \text{with} \quad D_1 \in R_1^{m \times m}$$

and $\bar{Y}_1 = \bar{Y}$.

Now we refine the resulting congruence $D^{-1} \equiv \phi(Y_1)Y_1^{-1} \pmod{q}$ modulo higher powers of q . The next such approximation step with $Y_2 = I + qZ_2$ leads to the congruences

$$\begin{aligned} I + qD_1 &\equiv \phi(Y_2)(1 + q^2D_2)Y_2^{-1} \equiv (I + \phi(qZ_2))(I - qZ_2) \\ &\equiv I + q\phi(Z_2) - qZ_2 \pmod{q^2}. \end{aligned}$$

The reduced equation $\bar{D}_1 = \phi(\bar{Z}_2) - \bar{Z}_2$ is of Artin-Schreier type and has a solution matrix \bar{Z}_2 over a finite extension \bar{R}_2/\bar{R}_1 . Hence there exist a Frobenius ring (R_2, ϕ_2) with residue ring \bar{R}_2 unramified and of finite degree

over (R_1, ϕ_1) and a matrix $Y_2 = 1 + qZ_2 \in \text{GL}_m(R_2)$ compatible with the initial values of Y modulo q^2 such that

$$D^{-1} = \phi_1(Y_1)\phi_2(Y_2)(I + q^2D_2)Y_2^{-1}Y_1^{-1} \quad \text{with} \quad D_2 \in R_2^{m \times m}.$$

Thus by induction we obtain a tower of unramified Frobenius ring extension $(S, \phi) \leq (R_1, \phi_1) \leq \dots \leq (R_k, \phi_k)$ and matrices $Y_k \in \text{GL}_m(R_k)$ with the property

$$D^{-1} \equiv \phi_1(Y_1) \cdots \phi_k(Y_k)Y_k^{-1} \cdots Y_1^{-1} \pmod{q^k}.$$

By construction the rings R_k are the minimal unramified algebraic ring extensions of S which contain a full system of congruence solutions modulo Q^k of the Frobenius equation $D \cdot \phi_k(\mathbf{y}) = \mathbf{y}$. These form a free $(S/Q^k)^\phi$ -module Λ_k . Since any monomorphism over S of $\text{Quot}(R_k)$ into $\text{Quot}(S^{\text{sep}})$ permutes Λ_k the extensions R_k/S even are Galois ring extensions with some finite Galois group G_k .

The union $R_\infty := \bigcup_{k=1}^\infty R_k$ with the unique Frobenius endomorphism ϕ_∞ defined by $\phi_\infty|_{R_k} = \phi_k$ is an F-ring with profinite Galois group $G_\infty := \text{Gal}(R_\infty/S)$. Thus the completion $(\widehat{R}_\infty, \widehat{\phi}_\infty)$ of R_∞ with respect to v_Q again is an F-ring with continuously extended Frobenius endomorphism $\widehat{\phi}_\infty$. Because of $Y_k = I + q^{k-1}Z_k \in \text{GL}_m(R_k)$ the product $\prod_{k=1}^l Y_k$ converges in $\text{GL}_m(\widehat{R}_\infty)$ to a fundamental solution matrix $\widehat{Y} = \prod_{k=1}^\infty Y_k$ of M .

By construction \widehat{Y} has the same initial values as Y and thus is equal to Y . Hence $(\widehat{R}_\infty, \widehat{\phi}_\infty)$ is a trivialization of (M, Φ) containing (R, ϕ_R) up to ϕ -isomorphisms over S . The group of continuously extended automorphisms of R_∞/S acts faithfully on the solution space $\text{Sol}_{\widehat{R}_\infty}^\Phi(M) = \text{Sol}_R^\Phi(M) = \bigoplus_{j=1}^m y_{j1}S^\phi$. This defines an embedding of G_∞ into $\text{GL}_m(S^\phi)$.

Since the elements of G_∞ commute with the Frobenius endomorphism of R_∞ or \widehat{R}_∞ respectively, G_∞ is isomorphic to an abstract subgroup of $\text{Gal}^\Phi(R/S)$. By $R^{G_\infty} \leq \widehat{R}^{G_\infty} = R_\infty^{G_\infty} = S$, the group G_∞ is Zariski dense in $\text{Gal}^\Phi(R/S)$. We thus obtain the postulated Galois representation ρ_M by combining the restriction $\Gamma_S^{\text{ur}} \rightarrow \text{Gal}(R_\infty/S)$ and the above embedding $\text{Gal}(R_\infty/S) \hookrightarrow \text{Gal}^\Phi(R/S) = \mathcal{G}(S^\phi)$. This finishes the proof of Theorem 2.2(a).

We now turn to the proof of Theorem 2.2(b). Let

$$\rho : \Gamma_S^{\text{ur}} \rightarrow \text{GL}(\Lambda) \quad \text{with} \quad \Lambda = \bigoplus_{i=1}^m e_i S^\phi$$

be a continuous Q -adic Galois representation of Γ_S^{ur} on a free S^ϕ -module Λ of rank m . Let S^{ur} be the integral closure of S in the maximal unramified field extension $\text{Quot}(S)^{\text{ur}}/\text{Quot}(S)$. Then $V := \Lambda \otimes_{S^\phi} S^{\text{ur}}$ is a free S^{ur} -module of rank m . On V we have an action of Γ_S^{ur} by composing ρ on Λ and the natural action of Γ_S^{ur} on S^{ur} as well as a Frobenius action given by $\Phi|_\Lambda = \text{id}$ and $\Phi|_{S^{\text{ur}}} = \phi^{\text{ur}}$. Here ϕ^{ur} denotes the unique lift of the ordinary Frobenius endomorphism of the residue ring extension. Then on V the actions of Γ_S^{ur} and Φ commute.

Now let M be the S -module of Γ_S^{ur} -invariant elements of V . Then M is a free module over S of rank m by the profinite version of the Lemma of Speiser (see [3], Ch. III, Prop. 3.10). Moreover for any $x \in M$ also the image $\Phi(x)$ is Γ_S^{ur} -invariant and thus belongs to M . Hence the restriction of Φ to M defines a Frobenius action on M . Since M contains a basis of V as S^{ur} -module, this action is regular and defines a Frobenius module (M, Φ) over S .

Let R/S be a rigid analytic trivialization of M . Then Λ can be identified with $\text{Sol}_R^\Phi(M)$ as S^ϕ -module and we obtain the basis $E = \{e_1, \dots, e_m\}$ of Λ from a basis $B = \{b_1, \dots, b_m\}$ of M by transformation with a fundamental solution matrix $Y \in \text{GL}_m(R)$ of R , i.e., by $E = B \cdot Y$. Going through the proof of part (a) we see that ρ as well as ρ_M essentially are determined by the kernel $\text{Gal}(S^{\text{ur}}/R_\infty)$ and are fixed by the choice of Y . This proves Theorem 2.2(b).

2.3. Theorem 2.2 can be used to attack inverse Galois problems for Frobenius modules and related differential modules over q -adic F -rings. A special nice situation arises in the case that $\bar{S} = S/Q$ is a field and $\Gamma_S^{\text{ur}} = \Gamma_{\bar{S}}$ is a free profinite group. By a theorem of Harbater and Pop the latter is true if \bar{S} is a function field of one variable over a separably algebraically closed field of constants. Then $\Gamma_{\bar{S}}$ is a free profinite group of rank equal to the cardinality of \bar{S} (see [3], Ch. V, Thm. 2.10 and Remark). Basic examples fulfilling this assumption are the rings of analytic elements over the p -adic Witt ring $\mathbb{W}(\bar{\mathbb{F}}_p) = \widehat{\mathbb{Z}}_p^{\text{ur}}$ or over the t -adic ring $\bar{\mathbb{F}}_p[[t]]$ localized outside (p) or (t) respectively. Here \bar{S} is equal to $\bar{\mathbb{F}}_p(s)$ in each case. The general result is

THEOREM 2.3. — *Let (S, ϕ) be a q -adic F -ring relative to a maximal ideal Q . Assume that the maximal unramified fundamental group Γ_S^{ur} of S is a free profinite group of infinite rank. Then for every reduced linear algebraic group \mathcal{G} defined over S^ϕ there exists a Frobenius module (M, Φ)*

over S and a rigid analytic trivialization R of M such that $\text{Gal}^\Phi(R/S) \cong \mathcal{G}(S^\phi)$.

The group $\mathcal{G}(S^\phi)$ embedded in some $\text{GL}_m(S^\phi)$ has a series of principal congruence subgroups \mathcal{G}_k modulo Q^k with finite quotients $G_k := \mathcal{G}(S^\phi)/\mathcal{G}_k$. By the freeness of $\Gamma_{\bar{S}}$ for the projective system of these groups G_k with the natural epimorphisms there exists a tower of Galois field extensions \bar{R}_k/\bar{S} with Galois groups $\text{Gal}(\bar{R}_k/\bar{S}) \cong G_k$. The corresponding unramified lifts R_k/S are Galois ring extensions with the same Galois groups. Hence the union $R_\infty := \bigcup_{k \in \mathbb{N}} R_k$ is a profinite Galois ring extension with group $G_\infty = \varprojlim (G_k)$ embedded in $\text{GL}_m(S^\phi)$ and Zariski closure isomorphic to $\mathcal{G}(S^\phi)$. Thus by Theorem 2.2 the induced Galois representation

$$\rho : \Gamma_S^{\text{ur}} \rightarrow \text{GL}_m(S^\phi)$$

with image G_∞ defines a Frobenius module (M, Φ) over S with Galois group $\mathcal{G}(S^\phi)$. This ends the proof of Theorem 2.3.

Our examples namely the localized rings of analytic elements $S = \widehat{\mathbb{Z}}_p^{\text{ur}} \langle \langle s \rangle \rangle_{(p)}$ and $\overline{\mathbb{F}}_p[[t]] \langle \langle s \rangle \rangle_{(t)}$ in addition are IDF-rings with respect to the iterative derivation $\partial = \partial_s$ on s . Thus by Theorem 1.2 Frobenius modules (M, Φ) over (S, ϕ, Δ) with $\Delta = \{\partial\}$ automatically are IDF-modules (M, Φ, ∇) . They are determined by (iterative) p -adic or t -adic differential equations with a compatible Frobenius structure. For this in p -adic analysis these are called (iterative) differential modules with strong Frobenius structure (compare [7], Ch. 2.2). Hence the observation above leads to the solution of the inverse Galois problem for q -adic ID-modules with strong Frobenius structure:

COROLLARY 2.4. — *Let (S, ϕ, Δ) be a q -adic IDF-ring relative to a maximal ideal Q with ring of differential constants C_S . Assume the unramified fundamental group Γ_S^{ur} of S is a free profinite group of infinite rank. Then for every reduced linear algebraic group \mathcal{G} defined over S^ϕ there exists an ID-module with strong Frobenius structure (M, Φ, ∇) over S and a rigid analytic trivialization R of M such that $\text{Gal}^\nabla(R/S) = \mathcal{G}(C_S)$.*

In the p -adic case the last result supplements an older result contained in [6]. There in Theorem 8 the corresponding inverse Galois problem for integral p -adic differential equations without strong Frobenius structure has been solved.

Acknowledgements. I thank M. Dettweiler, J. Hartmann and A. Maurischat for helpful comments and discussions on the topics of the paper.

BIBLIOGRAPHY

- [1] D. EISENBUD, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry, xvi+785 pages.
- [2] A. J. ENGLER & A. PRESTEL, *Valued fields*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005, x+205 pages.
- [3] G. MALLE & B. H. MATZAT, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999, xvi+436 pages.
- [4] B. H. MATZAT, “Differential Galois Theory in Positive Characteristic”, Preprint 35, IWR, 2001.
- [5] ———, “Frobenius modules and Galois groups”, in *Galois theory and modular forms*, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, p. 233-267.
- [6] ———, “Integral p -adic differential modules”, in *Groupes de Galois arithmétiques et différentiels*, Sémin. Congr., vol. 13, Soc. Math. France, Paris, 2006, p. 263-292.
- [7] ———, “From Frobenius structures to differential equations”, in *DART II Proceedings*, World Scientific Publisher, 2009.
- [8] B. H. MATZAT & M. VAN DER PUT, “Iterative differential equations and the Abhyankar conjecture”, *J. Reine Angew. Math.* **557** (2003), p. 1-52.
- [9] A. MAURISCHAT, “Galois theory for iterative connections and nonreduced Galois groups”, Trans. AMS, to appear.
- [10] M. A. PAPANIKOLAS, “Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms”, *Invent. Math.* **171** (2008), no. 1, p. 123-174.
- [11] N. R. STALDER, “Algebraic Monodromy Groups of A-Motives”, PhD Thesis, ETH Zürich, 2007.
- [12] M. VAN DER PUT, “Bounded p -adic differential equations”, in *Circumspice, Various Papers in and around Mathematics in Honor of Arnoud van Rooij*, Kath. Univ. Nijmegen, 2001.
- [13] M. VAN DER PUT & M. F. SINGER, *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666, Springer-Verlag, Berlin, 1997, viii+180 pages.

Manuscrit reçu le 25 février 2009,
révisé le 7 juillet 2009,
accepté le 25 août 2009.

B. Heinrich MATZAT
University of Heidelberg
Interdisciplinary Center for Scientific Computing
Im Neuheimer Feld 368
69120 Heidelberg (Germany)
matzat@iwr.uni-heidelberg.de