Séminaires & Congrès

COLLECTION SMF

MONODROMY OF FROBENIUS MODULES

B. H. Matzat

THÉORIES DE GALOIS GÉOMÉTRIQUE ET DIFFÉRENTIELLE

Numéro 27 D. Bertrand, P. Boalch, J.-M. Couveignes, P. Dèbes, éds.

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Séminaires & Congrès
27, 2012, p. 169–180

MONODROMY OF FROBENIUS MODULES

by

B. H. Matzat

Abstract. — Monodromy groups of Frobenius modules and differential modules with Frobenius structure over p-adic and t-adic rings of Laurent series are studied. Using Galois representations in many cases, at least the connected inverse problem could be solved affirmatively.

***Résumé* (Monodromie des modules de Frobenius).** — Nous étudions les groupes de monodromie des modules de Frobenius et des modules différentiels munis d'une structure de Frobenius sur les anneaux p-adiques et t-adiques. Les représentations galoisiennes permettent dans bien des cas de résoudre au moins le problème inverse connexe.

Introduction

This note is a continuation of [5] and presents a further application of Galois representations for Frobenius modules and related differential modules in characteristic zero as well as in positive characteristic (by the use of iterative differential Galois theory developed in [6], [7]).

It is shown that the monodromy group $\mathcal{G}$ of a Frobenius module over a p-adic or t-adic ring of integral Laurent series S has a reduced connected component $\mathcal{G}^\circ$ whose quotient $\mathcal{G}/\mathcal{G}^\circ$ appears as Galois group over the residue field $\overline{S}$. Moreover it is proved that at least all reduced connected linear algebraic groups (defined over the ring of Frobenius invariants S^ϕ) and all finite Galois groups over $\overline{S}$ appear as such monodromy groups, solving the connected and the discrete inverse problem. By transport of structures the same holds for (iterative) differential modules with strong Frobenius structure over S.

In the analytic case, over the base ring $S^\dagger$ of overconvergent Laurent series the results differ considerably in characteristic $p > 0$ and in characteristic zero. Since in positive characteristic every Frobenius module over $S^\dagger$ automatically has a compatible iterative differential structure, the results over S and $S^\dagger$ coincide. In contrast, in characteristic zero the lack of completeness of $S^\dagger$ imposes strong obstructions on the existence of compatible Frobenius and differential structures. This is proved by the

result of N. Tsuzuki [15] that the monodromy group of a differential module with strong Frobenius structure over $S^\dagger$ is finite. Thus here the inverse problem only for finite groups could be solved.

At the very end Tsuzuki's monodromy theorem is interpreted as an algebraicity criterion for differential modules over rings of integral overconvergent Laurent series comparable with the one presented in [4] for integral global iterative differential modules.

1. Monodromy of Ordinary Frobenius Modules

1.1. — Let S be an integral domain of characteristic $p > 0$. Then S is equipped with the ordinary Frobenius endomorphism $\phi : S \to S, a \mapsto a^p$. For this reason we call S together with ϕ an *ordinary Frobenius ring* (S, ϕ) or an F-ring for short.

This notion is generalized to a *Frobenius ring* (S, ϕ) *relative to some prime ideal* $Q \trianglelefteq S$. This is an integral domain S with an endomorphism ϕ having the property $\phi(Q) \subseteq Q$, such that the residue ring $\overline{S} := S/Q$ together with the induced endomorphism $\overline{\phi}$ is an ordinary F-ring $(\overline{S}, \overline{\phi})$ (see [5] for a further generalization). Hence an ordinary F-ring is an F-ring relative to the prime ideal $Q = (0)$. 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.

Basic examples are:

a. The polynomial ring $\mathbb{F}_p[s]$ and the ring of power series $\mathbb{F}_p[[s]]$ over the prime field $\mathbb{F}_p$ with the Frobenius endomorphism $\phi(s) = s^p$ are ordinary F-rings. Their rings of invariants $\mathbb{F}_p[s]^\phi$ and $\mathbb{F}_p[[s]]^\phi$ are equal to $\mathbb{F}_p$.

b. The polynomial ring $\mathbb{Z}_p[s]$ and the ring of power series $\mathbb{Z}_p[[s]]$ over the ring of p-adic integers with the Frobenius endomorphism ϕ given by $\phi|_{\mathbb{Z}_p} = \mathrm{id}$ and $\phi(s) = s^p$ are F-rings relative to $Q = (p)$ with ring of invariants $\mathbb{Z}_p[s]^\phi = \mathbb{Z}_p[[s]]^\phi = \mathbb{Z}_p$.

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

The relative Frobenius rings $\mathbb{Z}_p$, $\mathbb{F}_p[t]$ etc. are equipped with a valuation v_Q defined by $Q = (p)$ or $Q = (t)$, respectively. The Gauß extensions of these valuations onto $\mathbb{Z}_p[s]$, $\mathbb{Z}_p[[s]]$, $\mathbb{F}_p[t, s]$ etc. are discrete rank one valuations which again will be denoted by v_Q. Then the completions of $\mathbb{Z}_p[s]$ and $\mathbb{F}_p[[t]][s]$ with respect to v_Q are the *rings of analytic elements* $\mathbb{Z}_p\{s\}$ over $\mathbb{Z}_p$ or $\mathbb{F}_p[[t]]\{s\}$ over $\mathbb{F}_p[[t]]$, respectively. These are the ground rings in p-adic and t-adic analysis. In the following an F-ring (S, ϕ) relative to a valuation ideal Q defining a valuation v_Q of rank at most one which is complete with respect to v_Q is called a *Q-adic F-ring*.

For the investigation of the monodromy we need substitutes for the fields of power series which are complete under v_Q. Let (K, ϕ) be the quotient field of a Q-adic

F-ring like the field of p-adic numbers $\mathbb{Q}_p = \mathrm{Quot}(\mathbb{Z}_p)$ or the field of power series $\mathbb{F}_p((t)) = \mathrm{Quot}(\mathbb{F}_p[[t]])$ and let $\mathcal{O}_K$ be its ring of integers with respect to v_Q. Then

$$\mathcal{O}_K\{\{s\}\} := \{\sum_{k\in\mathbb{Z}} a_k s^k \mid a_k \in \mathcal{O}_K\,,\ \lim_{k\to-\infty} |a_k|_Q = 0\}$$

is an integral domain which is complete with respect to the Gauß extension of v_Q. The Frobenius action ϕ on K can be extended to $\mathcal{O}_K\{\{s\}\}$ by $\phi(s) = s^p$. This makes $(\mathcal{O}_K\{\{s\}\}, \phi)$ to an F-ring relative to Q. The quotient field

$$K\{\{s\}\} := \mathrm{Quot}(\mathcal{O}_K\{\{s\}\})$$

with the uniquely extended valuation v_Q is called the field of (formal) *Q-adic Laurent series* over K and $\mathcal{O}_K\{\{s\}\}$ its subring of *integral Q-adic Laurent series*. The field $K\{\{s\}\}$ is complete with respect to v_Q and contains the field of analytic elements $K\{s\}$. Let $\overline{K} := \mathcal{O}_K/Q$ be the residue field of K. Then the residue field of $O_K\{\{s\}\}$ modulo (Q) is the field $\overline{K}((s))$ of power series over $\overline{K}$. (Here (Q) denotes the ideal generated by $Q \trianglelefteq \mathcal{O}_K$ in $\mathcal{O}_K\{\{s\}\}$.) Thus $K\{\{s\}\}$ is a perfect analogue of $K((s))$ in the Q-adic case. Moreover inside $S = K\{\{s\}\}$ we will find the ring $\mathcal{E}_S^\dagger$ of bounded Laurent series convergent on a thin annulus of outer radius one (see Section 3.3).

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 $\Phi : M \to M$, i.e., Φ is additive with

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

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 included in M_l, we get an S_{l+1}-linear embedding $\rho_l : M_{l+1} \to M_l$. These define a projective system $(M_l, \rho_l)_{l\in\mathbb{N}}$ 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 $B = \{b_1, \ldots, b_m\}$ of M we find a representing matrix $D = D_B(\Phi) \in \mathrm{GL}_m(S)$ 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 $D_l = \phi^l(D) \in \mathrm{GL}_m(S_{l-1})$ is the representing matrix of Φ_l on M_l.

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

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

Obviously $\mathrm{Sol}_{\widetilde{S}}^{\Phi}(M)$ is an $\widetilde{S}^{\widetilde{\phi}}$-module. In case $\widetilde{S}^{\widetilde{\phi}}$ is a field, $\mathrm{Sol}_{\widetilde{S}}^{\Phi}(M)$ is free of rank at most m. The F-module (M, Φ) is called *trivial over* $\widetilde{S}$ if $\mathrm{Sol}_{\widetilde{S}}^{\Phi}(M)$ contains a basis of $M_{\widetilde{S}}$. Then $(\widetilde{S}, \widetilde{\phi})$ 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 a *ring of periods* of M etc. For this we assume that our F-ring (S,ϕ) is an F-ring relative to a valuation ideal Q defining a valuation v_Q of rank at most one. Then the completion S_Q of S with respect to v_Q is a Q-adic F-ring with continuously extended Frobenius endomorphism ϕ. The integral closure of S_Q in the maximal unramified algebraic extension of $\mathrm{Quot}(S_Q)$ 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 $S_Q^{\mathrm{ur}}/(Q)$. Thus the completion of S_Q^{ur} with respect to the ideal $(Q) \trianglelefteq S_Q^{\mathrm{ur}}$ generated by Q with the continuously extended Frobenius endomorphism $\widehat{\phi} = \widehat{\phi}^{\mathrm{ur}}$ again is a Q-adic F-ring $(\widehat{S}_Q^{\mathrm{ur}}, \widehat{\phi})$. (In case $Q = (0)$ the F-ring $(\widehat{S}_Q^{\mathrm{ur}}, \widehat{\phi})$ simply consists of the separable algebraic closure S^{sep} of S with the ordinary Frobenius endomorphism ϕ).

The following theorem is proved in [4], Prop. 1.2 (see also [3], Prop. 8.3 and [10], Prop. 3.3.9 for special cases).

Theorem 1. — *Let (S,ϕ) be an integral F-ring 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 $\widehat{S}_Q^{\mathrm{ur}}$.*

In [10] the PV-ring in Theorem 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 [12], Example 1.6) and usually is not uniquely determined up to isomorphism (except when the base ring is an algebraically closed field).

1.3. — Now let (M,Φ) be a Frobenius module over an ordinary F-ring (S,ϕ) (relative to $Q = (0)$). Such an F-module is called here an *ordinary Frobenius module*. Then by Theorem 1, M has a Picard-Vessiot ring R inside S^{sep}. If we suppose $S = \mathrm{Quot}(S)$ is a field, R/S becomes a finite F-field extension which in fact is an ordinary Galois extension with some finite Galois group G (see [3], Thm. 1.1, or [5], Prop. 2.1). In the case S is a function field of one variable over some F-field K, the monodromy groups of R/S are given by decomposition groups $G_{\mathfrak{P}}$ of the ramified places $\mathfrak{P}/\mathfrak{p}$ in R/S. This implies the following result:

Proposition 2. — *Let (M,ϕ) be an ordinary Frobenius module over a function field of one variable S with algebraically closed field of constants K. Let R/S be the Picard-Vessiot extension defined by M with group G and let $\mathfrak{P}/\mathfrak{p}$ be a ramified place in R/S. Then the monodromy group $G_{\mathfrak{P}}$ of $\mathfrak{P}/\mathfrak{p}$ is a split extension of a finite p-group P with a finite cyclic group C_n of order n prime to p:*

$$1 \to P \to G_{\mathfrak{P}} \rightleftarrows C_n \to 1.$$