ON P-ADIC MONODROMY

Stienstra, Jan; Put, Marius van der; Marel, Bert van der

Published in:
Mathematische zeitschrift

Publication date:
1991

Math. Z. 208, 309–325 (1991)

Mathematische
Zeitschrift

On p-adic monodromy

Jan Stienstra[1], **Marius van der Put**[2], **and Bert van der Marel***
[1] Mathematisch Instituut der Rijksuniversiteit te Utrecht, Postbus 80010, 3508 TA Utrecht, The Netherlands
[2] Mathematisch Instituut der Rijksuniversiteit te Groningen, Postbus 800, 9700 AV Groningen, The Netherlands

Received March 21, 1990; in final form February 1, 1991

1 Introduction

Every scheme X carries a sheaf $\underline{\mathscr{W}\mathcal{O}_X}$ of generalized Witt vectors. In §2 we study the cohomology groups $\mathrm{H}^m(X, \underline{\mathscr{W}\mathcal{O}_X})$ under the reasonable hypothesis (2.4). Implicitly this is a study of the formal groups of Artin and Mazur [1], but for our purpose there is no need to make these formal groups more explicit. In §3 we consider after base changing X/A to a p-adic situation $X \otimes R/R$ the cohomology of the sheaf of p-typical Witt vectors $\mathrm{H}^m(X \otimes R, \mathscr{W}\mathcal{O}_{X \otimes R})$. The crucial, and fairly restrictive, hypothesis in this section requires that the Frobenius operator F_p acts bijectively on the fibers $\mathrm{H}^m(X_s, \mathscr{W}\mathcal{O}_{X_s})$ at the geometric points s of $\mathrm{Spec}(R/pR)$. We show that after further base changing to $R^{\text{ét}}$, the p-adic completion of an infinite étale extension of the ring R, the $\mathscr{W}(R^{\text{ét}})$-module $\mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathcal{O}_{X \otimes R^{\text{ét}}})$ has a basis $\underline{\xi}$ consisting of elements which are fixed by F_p. Let $\Lambda := \ker(F_p - 1)$. Then Λ is a free $\mathbb{Z}_p$-module with basis $\underline{\xi}$. Projection of Witt vectors onto their first coordinate induces an injection of Λ into $\mathrm{H}^m(X, \mathcal{O}_X) \otimes R^{\text{ét}}$ and in fact

$$\Lambda \otimes_{\mathbb{Z}_p} R^{\text{ét}} \simeq \mathrm{H}^m(X, \mathcal{O}_X) \otimes_A R^{\text{ét}} .$$

In terms of the basis $\underline{\xi}$ of Λ and an A-basis $\underline{\omega}$ of $\mathrm{H}^m(X, \mathcal{O}_X)$ this isomorphism is described by an invertible matrix C with entries in $R^{\text{ét}}$: $\underline{\xi} = C\underline{\omega}$.

In §4 we discuss the interpretation of Λ as the fiber at $\mathrm{Spec}\,\Omega$ of a p-adic étale locally constant sheaf on $\mathrm{Spec}(R/pR)$; here Ω is an algebraically closed field containing R/pR. Thus the algebraic fundamental group $\pi_1 := \pi_1(\mathrm{Spec}(R/pR), \Omega)$ acts on Λ. We call this representation $\mathscr{M}$: $\pi_1 \to \mathrm{Aut}_{\mathbb{Z}_p}(\Lambda)$ the *p-adic monodromy representation*. With respect to the basis $\underline{\xi}$ one finds $\mathscr{M}(\tau)\underline{\xi} = C^{\tau}C^{-1}\underline{\xi}$ for $\tau \in \pi_1$.

This result is not new. Much of it goes back to Dwork's pioneering work on the variation of the zeta function in a family of hypersurfaces; see [5, 13, 14]. Many related results and generalizations have appeared in the literature; e.g. [15, 4, 7, 10] (this list is far from complete, but any list of references on this subject would

* Supported by the Dutch Organization for Scientific Research (NWO)

probably be incomplete; a complication in reading the literature is the variety of formulations and techniques). Nevertheless we want to present our modest attempt to understand something of this material and demonstrate in §5 how the approach via Witt vector cohomology leads to a method for explicitly computing the p-adic monodromy group in non-trivial examples of hypergeometric curves.

The cohomology of the sheaf of Witt vectors gives the slope < 1 part of crystalline cohomology [1, 11]. Under the hypothesis of §3 it gives precisely the slope 0 part: the *unit root subcrystal* [13]. For curves there is still the complementary slope 1 part, which escapes our methods. Accordingly Λ gives only one half of the p-adic solution space of the hypergeometric differential equations. More precisely the group of $\mathbf{n}$-th roots of unity acts on the hypergeometric curve $y^{\mathbf{n}} = x^{\mathbf{a}}(x-1)^{\mathbf{b}}(x-\lambda)^{\mathbf{c}}$ and splits its H^1_{DR} into isotypical pieces, each of which corresponds to one hypergeometric differential equation. In general these isotypical pieces are mixed by Frobenius and for Λ we are dealing with a system of related hypergeometric differential equations. Nonetheless, Λ gives only one half of the solution space. It would be very interesting to also understand the other half and then compare p-adic and classical monodromy.

2 Generalized Witt vector cohomology

2.1 Every scheme X carries a sheaf $\underline{\mathscr{W}\mathcal{O}_X}$ of generalized Witt vectors [3, 9]. The underlying sheaf of additive groups for $\underline{\mathscr{W}\mathcal{O}_X}$ is the sheaf of multiplicative groups $1 + t\mathcal{O}_X[[t]]$. The sheaf of generalized Witt vectors of length n is $\underline{\mathscr{W}_n\mathcal{O}_X} := \underline{\mathscr{W}\mathcal{O}_X}/\mathrm{Fil}_n\underline{\mathscr{W}\mathcal{O}_X}$ with $\mathrm{Fil}_n\underline{\mathscr{W}\mathcal{O}_X} := 1 + t^{n+1}\mathcal{O}_X[[t]]$.

If a is a section of $\mathcal{O}_X$ we write $\underline{\underline{a}}$ for the power series of $(1-at)^{-1}$ viewed as a section of $\underline{\mathscr{W}\mathcal{O}_X}$. For $n \in \mathbb{N}$ the substitution $t \mapsto t^n$ induces an endomorphism V_n of $\underline{\mathscr{W}\mathcal{O}_X}$. Every section of $1 + t\mathcal{O}_X[[t]]$ can be written uniquely as a t-adically converging product $\prod_{n \geq 1}(1 - a_n t^n)^{-1}$ with all a_n sections of $\mathcal{O}_X$. Thus the sections of $\underline{\mathscr{W}\mathcal{O}_X}$ can be written uniquely as

$$\sum_{n \geq 1} V_n \underline{\underline{a_n}} . \tag{1}$$

One can construct a continuous product on $\underline{\mathscr{W}\mathcal{O}_X}$ so that $\underline{\mathscr{W}\mathcal{O}_X}$ becomes a sheaf of topological commutative rings with unit, and continuous endomorphisms F_n for $n \in \mathbb{N}$ (see [9]). The following relations are satisfied and give practical tools for computing in $\underline{\mathscr{W}\mathcal{O}_X}$

$$F_m V_m = m, \qquad F_m F_n = F_{mn}, \qquad V_m V_n = V_{mn}, \qquad \underline{\underline{a}} \cdot \underline{\underline{b}} = \underline{\underline{ab}}, \qquad F_n \underline{\underline{a}} = \underline{\underline{a}}^n ,$$

$$F_n(\alpha\beta) = (F_n\alpha)(F_n\beta), \qquad V_n(\alpha(F_n\beta)) = (V_n\alpha)\beta, \qquad V_n F_k = F_k V_n ,$$

for $m, n, k \in \mathbb{N}$ with $(n, k) = 1$, sections α, β of $\underline{\mathscr{W}\mathcal{O}_X}$ and sections a, b of $\mathcal{O}_X$. There is a homomorphism of sheaves of rings $\pi\colon \underline{\mathscr{W}\mathcal{O}_X} \to \mathcal{O}_X$ sending a Witt vector written as in (1) to its first coordinate a_1.

2.2 The operators F_n and V_n on $\underline{\mathscr{W}\mathcal{O}_X}$ give endomorphisms F_n and V_n of the cohomology groups $\mathrm{H}^m(X, \underline{\mathscr{W}\mathcal{O}_X})$. π gives homomorphisms

$$\pi\colon \mathrm{H}^m(X, \underline{\mathscr{W}\mathcal{O}_X}) \to \mathrm{H}^m(X, \mathcal{O}_X) .$$

2.3 A morphism g: $Y \to X$ gives a homomorphism $\underline{\mathscr{W}\mathcal{O}_X} \to g_* \underline{\mathscr{W}\mathcal{O}_Y}$ of sheaves on X sending $\underline{a}$ to $\underline{g^*(a)}$; here a is a section of $\mathcal{O}_X$ and $g^*(a)$ its image in $\mathcal{O}_Y$. This induces homomorphisms $\mathrm{H}^m(X, \underline{\mathscr{W}\mathcal{O}_X}) \to \mathrm{H}^m(Y, \underline{\mathscr{W}\mathcal{O}_Y})$ compatible with the operators F_n and V_n and with the maps π.

2.4 Basic hypotheses. From now on S will be an affine scheme, $S = \operatorname{Spec} A$, which is smooth over an open part of $\operatorname{Spec} \mathbb{Z}$ and f: $X \to S$ is a smooth projective morphism. We assume that $\mathrm{H}^m(X, \mathcal{O}_X)$ is a free A-module for every m.

2.5 Proposition. *In the situation of* (2.4) *the sequence*

$$0 \to \mathrm{H}^m(X, \mathcal{O}_X) \xrightarrow{V_n} \mathrm{H}^m(X, \underline{\mathscr{W}}_n \underline{\mathcal{O}}_X) \to \mathrm{H}^m(X, \underline{\mathscr{W}}_{n-1} \underline{\mathcal{O}}_X) \to 0 .$$

is exact for all n, m. Consequently the maps π are surjective:

$$\pi\colon \mathrm{H}^m(X, \underline{\mathscr{W}\mathcal{O}_X}) \to \mathrm{H}^m(X, \mathcal{O}_X) .$$

Proof. Consider the exact sequence $0 \to \mathcal{O}_X \xrightarrow{V_n} \underline{\mathscr{W}}_n \underline{\mathcal{O}}_X \to \underline{\mathscr{W}}_{n-1} \underline{\mathcal{O}}_X \to 0$ and the associated cohomology sequence. One has the map F_n: $\underline{\mathscr{W}}_n \underline{\mathcal{O}}_X \to \mathcal{O}_X$ and $F_n V_n = n$. Since $\mathrm{H}^{m+1}(X, \mathcal{O}_X)$ is a free A-module and A is flat over $\mathbb{Z}$, multiplication by n, and hence also V_n, is injective on $\mathrm{H}^{m+1}(X, \mathcal{O}_X)$. □

2.6 Fix m. Let $\{\omega_1, \dots, \omega_h\}$ be a basis of the free A-module $\mathrm{H}^m(X, \mathcal{O}_X)$. Choose $\tilde{\omega}_i \in \mathrm{H}^m(X, \underline{\mathscr{W}\mathcal{O}_X})$ such that $\pi\tilde{\omega}_i = \omega_i$ for $i = 1, \dots, h$. Define for every $n \geqq 1$ the $h \times h$-matrix $B_n = (b_{n,ij})$ with entries in A by

$$\pi F_n \tilde{\omega}_i = \sum_{j=1}^{h} b_{n,ij} \omega_j$$

for $i = 1, \dots, h$; or with an obvious and very convenient notation

$$\pi F_n \underline{\tilde{\omega}} = B_n \underline{\omega} .$$

Explicit examples will be presented in Sect. 5.

We write $\underline{\mathscr{W}}(A)$ for the ring of generalized Witt vectors over A. Then $\underline{\mathscr{W}\mathcal{O}_X}$ is a sheaf of $\underline{\mathscr{W}}(A)$-modules and $\mathrm{H}^m(X, \underline{\mathscr{W}\mathcal{O}_X})$ is a $\underline{\mathscr{W}}(A)$-module.

2.7 Corollary. *Let the hypotheses and notations be as in* (2.4)–(2.6). *Then every element α of* $\mathrm{H}^m(X, \underline{\mathscr{W}\mathcal{O}_X})$ *can be written uniquely as*

$$\alpha = \sum_{n \geqq 1} \sum_{i=1}^{h} V_n(\underline{\underline{a_{ni}}} \tilde{\omega}_i)$$

with $a_{ni} \in A$. This sum converges in the topology defined in (2.1). □

2.8 Remark. Let $\alpha_1, \ldots, \alpha_q \in \mathrm{H}^m(X, \underline{\mathscr{W}\mathcal{O}_X})$. Then according to (2.7) there exist $q \times h$-matrices $A_n = (a_{n,ij})$, $n \in \mathbb{N}$, such that

$$\underline{\alpha} = \sum_{n \geq 1} V_n(\underline{\underline{A_n}}\underline{\tilde{\omega}})\,;$$

here $\underline{\underline{A_n}}$ is the matrix with entries $\underline{\underline{a_{n,ij}}}$ in $\underline{\mathscr{W}}(A)$ and $\underline{\tilde{\omega}}$ is the column vector with components $\tilde{\omega}_1, \ldots, \tilde{\omega}_h$; similarly for $\underline{\alpha}$, $\underline{\omega}$. Define the matrices M_n by:

$$\pi F_n \underline{\alpha} = M_n \underline{\omega}\,.$$

Then:

$$M_N = \sum_{n \mid N} n A_n^{(N/n)} B_{N/n} \tag{2}$$

for every $N \in \mathbb{N}$; here $A_n^{(N/n)}$ is the matrix with entries $a_{n,ij}^{N/n}$.

2.9 Corollary. *In* (2.7): $\alpha = 0 \Leftrightarrow \pi F_N \alpha = 0$ *for all* $N \in \mathbb{N}$.

Proof. The implication $\Leftarrow$ can be proved by means of formula (2), the fact $B_1 = I$ and induction showing $A_N = 0$ for all N. □

2.10 Remark. Choosing $\tilde{\omega}_1, \ldots, \tilde{\omega}_h$ in (2.6) amounts to choosing coordinates $\tau_1, \ldots, \tau_h$ for the Artin-Mazur formal group $\mathrm{H}^m(X, \hat{\mathbf{G}}_{\mathrm{m},X})$ [1]. The logarithm of the formal group law corresponding to these coordinates is $\sum_{n \geq 1} n^{-1} B_n^* \tau^n$ with B_n^* the transpose of the matrix B_n in (2.6) and τ^n = column vector with components $\tau_1^n, \ldots, \tau_h^n$.

3 Vectors fixed by Frobenius

3.1 We keep the hypotheses and notations of (2.4)–(2.6). We fix a prime number p and assume $\det B_p \notin pA$. Let

$$A^0 := A[(\det B_p)^{-1}], \qquad A_0 := A^0/pA^0, \qquad A^\wedge = \varprojlim_n A^0/p^n A^0\,.$$

It can be seen from (2) that these rings are independent of the choices in (2.6).

Being smooth over $\mathbb{F}_p$ the ring A_0 is a direct product of domains corresponding to the connected components of $\operatorname{Spec} A_0$. Take one such component and let R be its inverse image in $A^\wedge$. This construction implies immediately that R has properties (i)–(iii) below and that R is formally smooth over $\mathbb{Z}_p$. Because of this formal smoothness R is flat over $\mathbb{Z}_p$ (whence (iv)) and the $\mathbb{Z}_p$-algebra map $\sigma_1\colon R \to R/pR$, $\sigma_1(x) = x^p \bmod pR$, lifts to a projective system of $\mathbb{Z}_p$-algebra maps $\sigma_n\colon R \to R/p^nR$ ($n \geq 1$) and to an endomorphism σ of R as in (v). The properties of R are:

(i) pR is a prime ideal of R, $0 \neq pR \neq R$
(ii) $R = \varprojlim_n R/p^nR$, $\bigcap_n p^nR = 0$
(iii) $\det B_p$ is invertible in R
(iv) p is not a zero divisor in R
(v) the $\mathbb{Z}_p$-algebra R has an endomorphism σ such that for all $x \in R$

$$\sigma(x) \equiv x^p \bmod pR\,.$$

3.2 Let P be the set of primes $\neq p$. Let Y be a scheme such that every $l \in P$ is invertible in $\mathcal{O}_Y$. Then the expression $E_p := \prod_{l \in P}(1 - l^{-1} V_l F_l)$ defines an idempotent operator on $\underline{\mathscr{W}\mathcal{O}_Y}$, such that

$$E_p V_p = V_p E_p, \qquad E_p F_p = F_p E_p, \qquad E_p V_l = F_l E_p = 0, \qquad E_p(ab) = (E_p a)(E_p b)$$

for all $l \in P$ and for all sections a, b of $\underline{\mathscr{W}\mathcal{O}_Y}$.

We write $\mathscr{W}\mathcal{O}_Y$ instead of $E_p \underline{\mathscr{W}\mathcal{O}_Y}$ suppressing p in the notation. One calls $\mathscr{W}\mathcal{O}_Y$ the sheaf of *p-typical Witt vectors* on Y.

3.3 Let $\mathscr{W}(R)$ be the ring of p-typical Witt vectors over R and let, as before, π: $\mathscr{W}(R) \to R$ be the projection onto the first Witt vector coordinate. In general there will be many endomorphisms σ of R as in (3.1v). Given one choice for σ there is a unique homomorphism of rings (see [9, (17.6.9)])

$$\lambda\colon R \to \mathscr{W}(R)\,,$$

such that $\pi F_p^n \lambda = \sigma^n$ for all $n \in \mathbb{N}$; in particular $\pi\lambda = id$.

3.4 In the sequel we use the following notations. Instead of $\sigma(x)$ we often write x^σ. For a matrix $M = (m_{ij})$ with entries in R we set

$$M^{(p^r)} = (m_{ij}^{p^r}), \qquad M^{\sigma^r} = (m_{ij}^{\sigma^r}), \qquad \lambda(M) = (\lambda(m_{ij})), \qquad \underline{\underline{M}} = (\underline{\underline{m_{ij}}})\,.$$

We write F for F_p. If A' is an A-algebra $X \otimes A'$ stands for $X \times_S \operatorname{Spec} A'$. Note: under the hypotheses of (2.4) $\mathrm{H}^m(X \otimes A', \mathcal{O}_{X \otimes A'}) = \mathrm{H}^m(X, \mathcal{O}_X) \otimes_A A'$.

3.5 Theorem. *Fix an endomorphism σ of R as in* (3.1v) *and the corresponding $\lambda\colon R \to \mathscr{W}(R)$ as in* (3.3). *Let further the notation be as in* (2.6). *Then*

(i) *There exists an invertible $h \times h$-matrix H with entries in R such that*

$$B_{p^{r+1}} \equiv B_{p^r}^\sigma H \bmod p^{r+1} \quad \textit{for all } r \geqq 0\,.$$

(ii) *There exist elements $\hat{\omega}_1, \ldots, \hat{\omega}_h$ in $\mathrm{H}^m(X \otimes R, \mathscr{W}\mathcal{O}_{X \otimes R})$ such that*

$$F\underline{\hat{\omega}} = \lambda(H)\underline{\hat{\omega}} \qquad \textit{and} \qquad \pi\hat{\omega}_i = \omega_i$$

in $\mathrm{H}^m(X \otimes R, \mathcal{O}_{X \otimes R})$; $\underline{\hat{\omega}}$ is the column vector with components $\hat{\omega}_1, \ldots, \hat{\omega}_h$.

Proof. (i) We apply the computations in (2.8) with $\alpha_i = F_p\tilde{\omega}_i$. To simplify the notation we set $D_r = B_{p^r}$ and $U_r = A_{p^r}$. Then (2) yields for $r \geqq 0$

$$D_{r+1} = \sum_{i=0}^{r} p^i U_i^{(p^{r-i})} D_{r-i}\,.$$

In particular $U_0 = D_1 = B_p$ and $D_{r+1} \equiv U_0^{(p^r)} D_r \bmod p$. So each D_r is invertible over R. Using $(x^\sigma)^{p^n} \equiv x^{p^{n+1}} \bmod p^{n+1}$ for all n and for all $x \in R$ one proves with induction $(D_r^\sigma)^{-1} D_{r+1} \equiv (D_{r-1}^\sigma)^{-1} D_r \bmod p^r$ for $r \geqq 1$. Thus $H := \lim_{r\to\infty} (D_r^\sigma)^{-1} D_{r+1}$ converges p-adically and has the desired properties.

(ii) We set

$$\underline{\hat{\omega}} = E_p \sum_{r \geqq 0} V_p^r(\underline{\underline{U_r}}\underline{\tilde{\omega}}), \qquad \pi F_n \underline{\hat{\omega}} = M_n \underline{\omega}\,.$$

Because of (2.9) the desired relations for (ii) amount to $M_n = 0$ if n is not a power of p and $M_{pn} = H^{\sigma^r} M_n$ if $n = p^r$. The latter is equivalent with $M_{pn} = M_n^{\sigma} H$. Using (2) this can be turned into

$$U_{r+1} = -\sum_{i=0}^{r} p^{i-r-1}\left(U_i^{(p^{r+1-i})} D_{r+1-i} - U_i^{\sigma(p^{r-i})} D_{r-i}^{\sigma} H\right).$$

The recurrence has a solution with $U_0 = I$. This proves the theorem. □

3.6 We fix an algebraically closed field Ω containing R/pR. The set $\mathscr{B}$ of finite étale extensions of R/pR in Ω is a directed system. Indeed, if B_1 and B_2 in $\mathscr{B}$ are given, take $B_3 :=$ the image of $B_1 \otimes B_2$ in Ω. Then B_3 is a finite étale extension of R/pR which contains B_1 and B_2. We define

$$(R/pR)^{\text{ét}} := \varinjlim_{B \in \mathscr{B}} B .$$

This is an infinite étale extension of R/pR contained in Ω. Its Galois group is the *algebraic fundamental group* $\pi_1(\operatorname{Spec}(R/pR), \Omega)$.

The assignment $R' \mapsto R'/pR'$ gives an equivalence of categories between finite étale extensions of R and finite étale extensions of R/pR (see [8, (18.3.2)]). Each $B \in \mathscr{B}$ lifts uniquely to a finite étale extension $\tilde{B}$ of R. We define

$$R^{\text{ét}} := \text{the } p\text{-adic completion of } \varinjlim_{B \in \mathscr{B}} \tilde{B} .$$

Let σ be an endomorphism of R be as (3.1v). Then for every finite étale extension R' of R there is a unique extension σ': $R' \to R'$ of σ which satisfies $\sigma'(x) \equiv x^p \bmod pR'$ for all $x \in R'$.These extensions of σ pass to an endomorphism, again denoted by σ, of the $\mathbb{Z}_p$-algebra $R^{\text{ét}}$. So the ring $R^{\text{ét}}$ also enjoys the properties (i)–(v) in (3.1). Moreover $R^{\text{ét}}/pR^{\text{ét}} = (R/pR)^{\text{ét}}$. By continuity the algebraic fundamental group $\pi_1 := \pi_1(\operatorname{Spec}(R/pR), \Omega)$ acts on $R^{\text{ét}}$. Simple calculations show

$$(R^{\text{ét}})^{\pi_1} = R, \quad (R^{\text{ét}})^{\sigma} = \mathbb{Z}_p . \tag{3}$$

3.7 Proposition. *There exists an invertible $h \times h$-matrix C with entries in $R^{\text{ét}}$ such that*

$$C^{\sigma} H = C . \tag{4}$$

Proof. The system of equations $C_0^{(p)} H - C_0 = 0$, $\delta \cdot \det C_0 - 1 = 0$,

$C_{i+1}^{(p)} H - C_{i+1} + p^{-1}[C_i^{\sigma} - C_i^{(p)}] H = 0$ $(i \geqq 0)$ can inductively be solved with $h \times h$-matrices C_i over $R^{\text{ét}}$. Then $C := \sum_i p^i C_i$ is a solution for (4). □

3.8 The inclusion $R \subset R^{\text{ét}}$ induces an embedding of $\mathrm{H}^m(X \otimes R, \mathscr{W}\mathscr{O}_{X \otimes R})$ into $\mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathscr{O}_{X \otimes R^{\text{ét}}})$. Denote the image of $\hat{\omega}_i$ (see (3.5)) also by $\hat{\omega}_i$. Let λ: $R^{\text{ét}} \to \mathscr{W}(R^{\text{ét}})$ be the homomorphism which (3.3) associates with the endomorphism σ of $R^{\text{ét}}$. Define $\xi_1, \ldots, \xi_h \in \mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathscr{O}_{X \otimes R^{\text{ét}}})$ by

$$\underline{\xi} = \lambda(C)\underline{\hat{\omega}} \tag{5}$$

where C is any solution of (4) and $\underline{\xi}$ resp. $\underline{\hat{\omega}}$ are the column vectors with components $\xi_1, \ldots, \xi_h$ resp. $\hat{\omega}_1, \ldots, \hat{\omega}_h$. Then by (3.7), (3.5) and (3.3)

$$F\underline{\xi} = \underline{\xi} \qquad \text{and} \qquad \pi\underline{\xi} = C\underline{\omega}\ . \tag{6}$$

3.9 Proposition. (i) $\mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathcal{O}_{X \otimes R^{\text{ét}}})$ *is a free* $\mathscr{W}(R^{\text{ét}})$*-module with bases* $\{\xi_1, \ldots, \xi_h\}$ *and* $\{\hat{\omega}_1, \ldots, \hat{\omega}_h\}$.

(ii) $\mathrm{H}^m(X \otimes R, \mathscr{W}\mathcal{O}_{X \otimes R})$ *is a free* $\mathscr{W}(R)$*-module with basis* $\{\hat{\omega}_1, \ldots, \hat{\omega}_h\}$.

Proof. (i) By (6) $\{\pi\xi_1, \ldots, \pi\xi_h\}$ is an $R^{\text{ét}}$-basis of $\mathrm{H}^m(X \otimes R^{\text{ét}}, \mathcal{O}_{X \otimes R^{\text{ét}}})$. So every element α of $H^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathcal{O}_{X \otimes R^{\text{ét}}})$ can be written uniquely as in (2.7). The operator E_p fixes α and $\xi_1, \ldots, \xi_h$. Moreover $E_p V_n = 0$ if n is not a power of p. Thus

$$\alpha = \sum_{r \geqq 0} \sum_{i=1}^{h} V_p^r(E_p(\underline{\underline{a_{ri}}})\xi_i) = \sum_{i=1}^{h} \left(\sum_{r \geqq 0} V_p^r E_p(\underline{\underline{a_{ri}}}) \right) \xi_i\ ,$$

where the second equality is a consequence of $F_p\xi_i = \xi_i$. This proves that $\mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathcal{O}_{X \otimes R^{\text{ét}}})$ is a free $\mathscr{W}(R^{\text{ét}})$-module with basis $\{\xi_1, \ldots, \xi_h\}$. By (5) $\{\hat{\omega}_1, \ldots, \hat{\omega}_h\}$ is also a $\mathscr{W}(R^{\text{ét}})$-basis for this module.

(ii) follows from (i) and (3). □

3.10 Define

$$\Lambda := \ker(F - 1\colon \mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathcal{O}_{X \otimes R^{\text{ét}}}) \to \mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathcal{O}_{X \otimes R^{\text{ét}}}))\ .$$

Because of (2.9) the map π: $\mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathcal{O}_{X \otimes R^{\text{ét}}}) \to \mathrm{H}^m(X \otimes R^{\text{ét}}, \mathcal{O}_{X \otimes R^{\text{ét}}}))$ restricts to an isomorphism $\pi\colon \Lambda \simeq \pi\Lambda$. We will use π to identify Λ and its elements with their image and write Λ resp. ξ instead of $\pi\Lambda$ resp. $\pi\xi$.

3.11 Theorem. Λ *is a free* $\mathbb{Z}_p$*-module with basis* $\{\xi_1, \ldots, \xi_h\}$.

$$\mathrm{H}^m(X, \mathcal{O}_X) \otimes_A R^{\text{ét}} = \Lambda \otimes_{\mathbb{Z}_p} R^{\text{ét}}\ .$$

In terms of the A*-basis* $\underline{\omega}$ *of* $\mathrm{H}^m(X, \mathcal{O}_X)$ *and the* $\mathbb{Z}_p$*-basis* $\underline{\xi}$ *of* Λ *this equality is given by* (6): $\underline{\xi} = C\underline{\omega}$.

Proof. According to (3.9) every element of Λ can be written as a linear combination of $\xi_1, \ldots, \xi_h$ with coefficients in $\mathscr{W}(R^{\text{ét}})^F$. Argueing as in (2.9) one shows that the projection π: $\mathscr{W}(R^{\text{ét}}) \to R^{\text{ét}}$ restricts to an isomorphism $\mathscr{W}(R^{\text{ét}})^F \simeq \pi(\mathscr{W}(R^{\text{ét}})^F)$. The inverse isomorphism is λ. From $\pi F \lambda = \sigma$ (see (3.3)) and (3) we then see $\pi(\mathscr{W}(R^{\text{ét}})^F) = (R^{\text{ét}})^\sigma = \mathbb{Z}_p$. This shows that Λ is spanned over $\mathbb{Z}_p$ by $\xi_1, \ldots, \xi_h$. The rest follows from (3.9), (3.10) and (6). □

3.12 The algebraic fundamental group $\pi_1 := \pi_1(\operatorname{Spec}(R/pR), \Omega)$ acts on $R^{\text{ét}}$. By functoriality this induces an action of π_1 on $\mathrm{H}^m(X, \mathcal{O}_X) \otimes_A R^{\text{ét}}$ and on $\mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathcal{O}_{X \otimes R^{\text{ét}}})$. The maps F and π are π_1 equivariant. Thus one obtains a representation

$$\mathscr{M}\colon \pi_1(\operatorname{Spec}(R/pR), \Omega) \to \operatorname{Aut}_{\mathbb{Z}_p}(\Lambda)$$

which we call the *p-adic monodromy representation*. Its image $\mathscr{M}(\pi_1)$ is called the *p-adic monodromy group*. In terms of the basis $\{\xi_1, \ldots, \xi_h\}$ this is described by

$$\mathscr{M}(\tau)\underline{\xi} = C^\tau C^{-1}\underline{\xi} \quad \text{for } \tau \in \pi_1\ .$$

4 p-adic monodromy

In this section we want to justify the terminology p-adic monodromy representation in (3.12). We keep the hypotheses of (2.4). Throughout this section p is a fixed prime and we write F and V instead of F_p and V_p respectively.

4.1 Let s be a geometric point of S of characteristic p, i.e. a homomorphism $A \to k(s)$ into an algebraically closed field $k(s)$ of characteristic p. The fiber of f over s is $X_s := X \otimes_S \operatorname{Spec} k(s)$. We apply (2.3) to $X_s \to X$ and project with E_p onto the p-typical part (3.2). We thus obtain for every m the commutative diagram

$$\begin{array}{ccc} \mathrm{H}^m(X, \mathscr{W}\mathcal{O}_X) & \xrightarrow{\alpha_s} & \mathrm{H}^m(X_s, \mathscr{W}\mathcal{O}_{X_s}) \\ \pi \downarrow & & \downarrow \pi \\ \mathrm{H}^m(X, \mathcal{O}_X) & \xrightarrow{\otimes k(s)} & \mathrm{H}^m(X_s, \mathcal{O}_{X_s}) \ . \end{array} \tag{7}$$

The Frobenius endomorphism of $\mathcal{O}_{X_s}$ which raises sections to the p-th power induces a σ-linear endomorphism F on $\mathrm{H}^m(X_s, \mathcal{O}_{X_s})$; here σ is the Frobenius endomorphism of $k(s)$. In (7) α_s and the right hand π commute with F. The left hand π is surjective by (2.5). This implies the surjectivity of the right hand π.

The diagram (7) shows that for m fixed as in (2.6) the matrix of the σ-linear endomorphism F of $\mathrm{H}^m(X_s, \mathcal{O}_{X_s})$ with respect to the basis $\{\omega_1, \ldots, \omega_h\}$ is precisely $B_p(s)$, the image of B_p with entries in $k(s)$. The matrix $B_p(s)$ is known as the *Hasse-Witt matrix* of $X_s/k(s)$ in dimension m.

Using the exact sequences in (2.5) for X_s and the fact that in characteristic p Frobenius F_p commutes with all V_n one checks:

$$F \text{ is bijective on } \mathrm{H}^m(X_s, \mathscr{W}\mathcal{O}_{X_s}) \Leftrightarrow \det B_p(s) \neq 0 \ .$$

4.2 The set of geometric points s of S with $\operatorname{char} k(s) = p$ and $\det B_p(s) \neq 0$, coincides with the set of geometric points of $\operatorname{Spec} A_0$ (see (3.1)). Let s lie on the connected component $S_0 := \operatorname{Spec}(R/pR)$ of $\operatorname{Spec} A_0$, corresponding to a homomorphism $\rho\colon R \to k(s)$. This homomorphism extends in many ways to a homomorphism $R^{\text{ét}} \to k(s)$; any two extensions differ by an element of $\pi_1(S_0, \Omega)$. Fix one extension $\tilde{\rho}\colon R^{\text{ét}} \to k(s)$. It induces a homomorphism

$$\tilde{\rho}^*\colon \mathrm{H}^m(X \otimes R^{\text{ét}}, \mathscr{W}\mathcal{O}_{X \otimes R^{\text{ét}}}) \to \mathrm{H}^m(X_s, \mathscr{W}\mathcal{O}_{X_s}) \ .$$

As in (3.11) one shows that $\{\tilde{\rho}^*\xi_1, \ldots, \tilde{\rho}^*\xi_h\}$ is a basis of the free $\mathbb{Z}_p$-module $\mathrm{H}^m(X_s, \mathscr{W}\mathcal{O}_{X_s})^F$. So $\tilde{\rho}^*$ induces the first isomorphism in

$$\Lambda \simeq \mathrm{H}^m(X_s, \mathscr{W}\mathcal{O}_{X_s})^F \simeq \mathrm{H}^m_{\text{ét}}(X_s, \mathbb{Z}_p) \ . \tag{8}$$

The second isomorphism is constructed in ([11, II(5.2); 12, IV (3.5.1)]). The right hand side of (8) is the fiber at s of the étale locally constant sheaf $R^m_{\text{ét}}(f_0)_*(\mathbb{Z}_p)$ on S_0; here $f_0\colon X \otimes_S S_0 \to S_0$ is induced by f. The canonical representation of the fundamental group $\pi_1(S_0, \Omega)$ in the fiber of this local system at $\operatorname{Spec} \Omega$ coincides via (8) with the representation in (3.12).

This appearance of the representation in (3.12) as the canonical representation of the fundamental group in the fibers of a p-adic étale locally constant sheaf is one good reason for calling it *p-adic monodromy representation.*

4.3 Assume in addition to (2.4) that all cohomology groups $\mathrm{H}^j(X, \Omega^i_{X/S})$ are free A-modules and $p \neq 2$. Then we can combine the results of Sect. 3 with those of [18, §4]. The Gauss-Manin connection on the De Rham cohomology of X/S induces a p-adically continuous connection

$$\nabla\colon \mathbb{H}^m(X, \Omega^\bullet_{X/S}) \otimes R^{\text{ét}} \to \mathbb{H}^m(X, \Omega^\bullet_{X/S}) \otimes \Omega^{1,\text{cont}}_{R^{\text{ét}}/\mathbb{Z}_p} .$$

As in loc. cit. one can show that, because all elements of Λ are fixed by F the inclusion $\Lambda \subset \mathrm{H}^m(X, \mathcal{O}_X) \otimes R^{\text{ét}}$ lifts to an inclusion

$$\Lambda \subset \ker \nabla \subset \mathbb{H}^m(X, \Omega^\bullet_{X/S}) \otimes R^{\text{ét}} .$$

As in [18, Theorem (4.6)], this result can be reformulated in terms of differential equations for the entries of the matrix C.

Thus Λ becomes the set of solutions of a system of differential equations and the action of the fundamental group is the precise analogue of what is classically called monodromy.

5 Hypergeometric curves

In this section we illustrate the general theory in the preceding sections with explicit results for hypergeometric curves. In particular we demonstrate in (5.2) and (5.4) how one computes for H^1 of these curves the data ω, $\tilde{\omega}$ and B_N in (2.6). For the curve $y^5 = x(x-1)^2(x-\lambda)^3$ we determine in (5.14) the p-adic monodromy group.

5.1 Let $0 < \mathbf{a}, \mathbf{b}, \mathbf{c} < \mathbf{n}$ be integers with $\gcd(\mathbf{n}, \mathbf{a}, \mathbf{b}, \mathbf{c}) = 1$. Let $\mu_{\mathbf{n}}$ be the group of $\mathbf{n}$-th roots of unity. The *hypergeometric curve* $X = X_{\mathbf{n};\,\mathbf{a},\mathbf{b},\mathbf{c}}$ with parameters $\mathbf{n}$, $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ is the smooth projective model over $A := \mathbb{Z}[\mu_n][\lambda, (\mathbf{n}\lambda(1-\lambda))^{-1}]$ of the affine equation

$$y^{\mathbf{n}} = x^{\mathbf{a}}(x-1)^{\mathbf{b}}(x-\lambda)^{\mathbf{c}} .$$

The name hypergeometric curve refers to its relation with hypergeometric differential equations (see (5.3)).

Let $S := \operatorname{Spec} A$. The curve X/S is an $\mathbf{n}$-fold covering of the projective line $\mathbf{P}^1_S$ with branch locus $\{0, 1, \infty, \lambda\}$. The Riemann-Hurwitz formula computes the genus $\operatorname{rank}_A \mathrm{H}^1(X, \mathcal{O}_X)$ of X to be equal to $h := \mathbf{n} + 1 - \frac{1}{2}(d_0 + d_1 + d_\infty + d_\lambda)$ with $d_0 = (\mathbf{n}, \mathbf{a})$, $d_1 = (\mathbf{n}, \mathbf{b})$, $d_\lambda = (\mathbf{n}, \mathbf{c})$, $d_\infty = (\mathbf{n}, \mathbf{a}+\mathbf{b}+\mathbf{c})$.

5.2 The open affine covering $\{x \neq \infty\} \cup \{x \neq 0\}$ of $\mathbf{P}^1_S$ pulls back to an open affine covering $X_1 \cup X_2$ of X. The group $\mathrm{H}^1(X, \mathcal{O}_X)$ is equal to the Čech cohomology group $\check{H}^1(\{X_1, X_2\}, \mathcal{O}_X)$ with respect to this covering.

For more detailed descriptions we need:

$$\alpha = \mathbf{a}/\mathbf{n}, \qquad \beta = \mathbf{b}/\mathbf{n}, \qquad \gamma = \mathbf{c}/\mathbf{n} ,$$

$$\|l\| = -[-\langle l\alpha\rangle - \langle l\beta\rangle - \langle l\gamma\rangle] \quad \text{for } l \in \mathbb{Z}/\mathbf{n}\mathbb{Z} ,$$

$$\mathcal{T} := \{(l, j) \in (\mathbb{Z}/\mathbf{n}\mathbb{Z}) \times \mathbb{Z} \mid 0 < j < \|l\|\} ;$$

here $[\cdot]$ and $\langle\cdot\rangle$ denote the usual integral and fractional part functions. Note $\|l\|\in\{0,1,2,3\}$. For $l\in\mathbb{Z}/\mathbf{n}\mathbb{Z}$ set

$$v_l = y^{\tilde{l}}x^{-[\tilde{l}\alpha]}(x-1)^{-[\tilde{l}\beta]}(x-\lambda)^{-[\tilde{l}\gamma]}\,.$$

with $\tilde{l}\in\mathbb{N}$, $l\equiv\tilde{l} \bmod \mathbf{n}$. Then, in the function field of X,

$$\Gamma(X_1,\mathcal{O}_X) = \oplus_{l\in\mathbb{Z}/\mathbf{n}\mathbb{Z}}\, A[x]v_l$$

$$\Gamma(X_2,\mathcal{O}_X) = \oplus_{l\in\mathbb{Z}/\mathbf{n}\mathbb{Z}}\, A[x^{-1}]x^{-\|l\|}v_l$$

$$\Gamma(X_1\cap X_2,\mathcal{O}_X) = \oplus_{l\in\mathbb{Z}/\mathbf{n}\mathbb{Z}}\, A[x,x^{-1}]v_l$$

For $(l,j)\in\mathcal{T}$ define $\check{\omega}_{(l,j)} := \mathbf{n}^{-1}x^{j-1}v_l^{-1}dx$ and

$\omega_{(l,j)} :=$ the cohomology class of the Čech 1-cocycle $x^{-j}v_l$.

Then $\{\omega_{(l,j)}\}_{(l,j)\in\mathcal{T}}$ is a basis of $\mathrm{H}^1(X,\mathcal{O}_X)$ and $\{\check{\omega}_{(l,j)}\}_{(l,j)\in\mathcal{T}}$ is the dual basis for $\mathrm{H}^0(X,\Omega^1_{X/S})$.

5.3 It is well known (e.g. [6, 16, 17]) that the Gauss-Manin connection ∇ on $\mathbb{H}^1(X,\Omega^\bullet_{X/S})$ leads to *hypergeometric differential equations* as follows. Define for $(l,j)\in\mathcal{T}$ the differential operator $P_{(l,j)}$ by

$$\Theta(\Theta - j + \langle l\alpha\rangle + \langle l\gamma\rangle) - \lambda(\Theta + \langle l\gamma\rangle)(\Theta - j + \langle l\alpha\rangle + \langle l\beta\rangle + \langle l\gamma\rangle)$$

with $\Theta = \lambda\dfrac{d}{d\lambda}$. A straightforward calculation shows that $P_{(l,j)}(x^{j-1}v_l^{-1})$ is equal to $\dfrac{d}{dx}(\langle l\gamma\rangle\lambda x^j(x-1)(x-\lambda)^{-1}v_l^{-1})$ and hence

$$\nabla(P_{(l,j)})\check{\omega}_{(l,j)} = 0 \quad \text{in } \mathbb{H}^1(X,\Omega^\bullet_{X/S})\,.$$

5.4 We lift $\omega_{(l,j)}$ to an element $\tilde{\omega}_{(l,j)}$ of $\mathrm{H}^1(X,\underline{\mathcal{W}\mathcal{O}}_X)$ as follows. $\underline{\underline{x^{-j}v_l}}$ is a section of $\underline{\mathcal{W}\mathcal{O}}_X$ over $X_1\cap X_2$. The Čech cocycle condition is trivially satisfied. Take

$\tilde{\omega}_{(l,j)} =$ cohomology class of the Čech 1-cocycle $\underline{\underline{x^{-j}v_l}}$.

Choosing $\underline{\omega}$ and $\underline{\tilde{\omega}}$ this way we can compute the matrices B_N, defined in (2.6):

$$\pi F_N\underline{\tilde{\omega}} = B_N\underline{\omega}\,.$$

The element $\pi F_N\tilde{\omega}_{(l,j)}$ of $\mathrm{H}^1(X,\mathcal{O}_X)$ is just the cohomology class of the Čech 1-cocycle $(x^{-j}v_l)^N$. Note

$$(x^{-j}v_l)^N = (x^{-jN}x^{[N\langle l\alpha\rangle]}(x-1)^{[N\langle l\beta\rangle]}(x-\lambda)^{[N\langle l\gamma\rangle]})v_{l'}$$

with $l' = lN$ in $\mathbb{Z}/\mathbf{n}\mathbb{Z}$. Thus, indexing the rows and columns of B_N with the elements of $\mathcal{T}$, we find that the entry $B_{N,(l,j),(l',j')}$ in row (l,j) and column (l',j') is 0 if $l'\neq lN$, whereas in case $l' = lN$

$$B_{N,(l,j),(l',j')} = (-1)^L\sum_k \binom{[N\langle l\beta\rangle]}{L-k}\binom{[N\langle l\gamma\rangle]}{k}\lambda^k$$

with $L = j' - jN + [N\langle l\alpha\rangle] + [N\langle l\beta\rangle] + [N\langle l\gamma\rangle]$.

5.5 Example. Assume $l' = lN$ in $\mathbb{Z}/\mathbf{n}\mathbb{Z}$. Then $B_{N,(l,j),(l',j')}$ is annihilated by the differential operator $\Theta(\Theta + [N\langle l\beta\rangle] - L) - \lambda(\Theta - [N\langle l\gamma\rangle])(\Theta - L)$. From this observation one easily sees

$$\nabla(P_{(l',j')})B_{N,(l,j),(l',j')} \equiv 0 \bmod NA \ .$$

This gives a nice illustration of [18, Theorem (4.6)].

5.6 Proposition. *Let p be a prime number not dividing* $\mathbf{n}$ *and let* $l \in \mathbb{Z}/\mathbf{n}\mathbb{Z}$, $l \neq 0$. *Assume* $[p\langle l\alpha\rangle] + [p\langle l\beta\rangle] + [p\langle l\gamma\rangle] \geqq p$. *Then the polynomial* $B_{p,(l,1),(pl,1)} \bmod p \in \mathbb{F}_p[\lambda]$ *has degree u and has zeros of order v resp. w at $\lambda = 0$ resp.* 1 *with*

$$u = \min([p\langle l\gamma\rangle], [p\langle l\alpha\rangle] + [p\langle l\beta\rangle] + [p\langle l\gamma\rangle] + 1 - p)$$

$$v = \max(0, [p\langle l\alpha\rangle] + [p\langle l\gamma\rangle] + 1 - p)$$

$$w \leqq \max(0, [p\langle l\beta\rangle] + [p\langle l\gamma\rangle] + 1 - p) \ .$$

The zeros of $B_{p,(l,1),(pl,1)} \bmod p$ in $\overline{\mathbb{F}}_p$ different from 0 *and* 1 *are simple zeros.*

Proof. The values of u and v can immediately be read off from the explicit formula for $B_{p,(l,1),(pl,1)}$ in (5.4). To compute w one uses $B_{p,(l,1),(pl,1)} =$

$$(-1)^L \sum_m \binom{[p\langle l\beta\rangle] + [p\langle l\gamma\rangle] - m}{p - 1 - [p\langle l\alpha\rangle]}\binom{[p\langle l\gamma\rangle]}{m}(\lambda - 1)^m \ .$$

The zeros of $B_{p,(l,1),(pl,1)} \bmod p$ different from 0 and 1 are simple zeros because this is a polynomial of degree $< p$ annihilated by a differential operator of the form $\lambda(1-\lambda)\left(\frac{d}{d\lambda}\right)^2 + \dots$. □

5.7 Condition. $\|l\| = 2$ for every non-zero $l \in \mathbb{Z}/\mathbf{n}\mathbb{Z}$.
Equivalently: $1 < \langle l\alpha\rangle + \langle l\beta\rangle + \langle l\gamma\rangle \leqq 2$ for every non-zero $l \in \mathbb{Z}/\mathbf{n}\mathbb{Z}$.

5.8 Example. (5.7) holds for $(\mathbf{n}; \mathbf{a}, \mathbf{b}, \mathbf{c}) = (2; 1, 1, 1), (3; 1, 1, 2), (5; 1, 2, 3)$.

5.9 As a consequence of (5.7) the indexing set $\mathscr{T}$ consists exactly of the pairs $(l, 1)$ with $l \in \mathbb{Z}/\mathbf{n}\mathbb{Z}$, $l \neq 0$. So we identify $\mathscr{T}$ with $(\mathbb{Z}/\mathbf{n}\mathbb{Z})\backslash\{0\}$ and simplify the notation by writing l instead of $(l, 1)$.

The multiplicative group $(\mathbb{Z}/\mathbf{n}\mathbb{Z})^*$ acts on $\mathscr{T}$ by multiplication. We define the permutation matrix $\Phi_N = (\Phi_{N,ll'})$ for $N \in (\mathbb{Z}/\mathbf{n}\mathbb{Z})^*$ by

$$\Phi_{N,ll'} = 1 \quad \text{if } l' = Nl,\ \Phi_{N,ll'} = 0 \quad \text{if } l' \neq Nl \ (l, l' \in \mathscr{T}) \ .$$

We fix a primitive $\mathbf{n}$-th root of unity ζ and set

$$\Xi := \sum_{N \in (\mathbb{Z}/\mathbf{n}\mathbb{Z})^*} \zeta^N \Phi_N \ .$$

The crucial property of this matrix is: $\Xi^\sigma = \Xi^{(p)} = \Xi\Phi_p^{-1}$.

5.10 Assume condition (5.7). Fix a prime number $p > n$. Then the condition of Proposition (5.6) is also satisfied for every l. Using the explicit form of the matrix B_p and (5.6) one checks $\det B_p \notin pA$. So the theory of Sect. 3 applies here. We use the notations R, $R^{\text{ét}}$, σ, H, C, Λ, $\pi_1, \ldots$ as in Sect. 3.

For every r such that $p^r \equiv 1 \bmod \mathbf{n}$, the matrices B_{p^r} and $\Phi_p^{-1} B_{p^{r+1}}$ are diagonal matrices. Consequently $\Phi_p^{-1} H$ is also a diagonal matrix.

Lemma. *The equation $C^\sigma H = C$ has a solution $C = \Xi G$ with G a diagonal matrix with entries in $(R^{\text{ét}})^*$.*

Proof. Write $H = \Phi_p Q$. Then $C^\sigma H = C$ is equivalent to $\Phi_p^{-1} G^\sigma \Phi_p Q = G$; i.e. in terms of the entries of the diagonal matrices G and Q: $g_{pl} = g_l^\sigma q_{pl}$ for all $l \in \mathscr{T}$. For a given l let $m \geqq 1$ be minimal such that $p^m l = l$. Then this leads to an equation of the form $g_l = g_l^{\sigma^m} k_l$ which has a solution in $(R^{\text{ét}})^*$. Once a solution g_l is fixed $g_{l'}$ is determined for $l' = pl, \ldots, p^{m-1} l$. □

5.11 This lemma leads to an "upper bound" for the p-adic monodromy group. Recall (3.12):

$$\mathscr{M}(\pi_1) = \{C^\tau C^{-1} \mid \tau \in \pi_1\} \subset Gl_{\mathbf{n}-1}(\mathbb{Z}_p)\,.$$

Since the $\mathbf{n}$-th roots of unity are contained in the base ring A they are fixed by every $\tau \in \pi_1$. In particular, $\Xi^\tau = \Xi$. Therefore $C^\tau C^{-1} = \Xi G^\tau G^{-1} \Xi^{-1}$ and $\Phi_p^{-1} (G^\tau G^{-1})^\sigma \Phi_p = G^\tau G^{-1}$. Thus we see

$$\mathscr{M}(\pi_1) \subset \Xi \mathscr{D} \Xi^{-1}$$

where $\mathscr{D}$ is the group of diagonal matrices D in $Gl_{\mathbf{n}-1}(\mathscr{W}(\overline{\mathbb{F}_p}))$ which satisfy $\Phi_p^{-1} D^\sigma \Phi_p = D$. Notice the isomorphism

$$\mathscr{D} \simeq \mathscr{W}(\mathbb{F}_{q_1})^* \times \ldots \times \mathscr{W}(\mathbb{F}_{q_t})^*\,;$$

${}^p\!\log q_1, \ldots, {}^p\!\log q_t$ are the lengths of the orbits of multiplication by p on $\mathscr{T}$.

In general it is difficult to compute $\mathscr{M}(\pi_1)$ more precisely. Specific properties of $(\mathbf{n}; \mathbf{a}, \mathbf{b}, \mathbf{c})$ strongly influence the result. One has for instance

5.12 Proposition. *Assume besides* (5.7) *also* $\mathbf{b} + \mathbf{c} = \mathbf{n}$ *and* $p > \mathbf{n}$. *Then the diagonal entries* g_l $(l \in \mathscr{T})$ *of the matrix* G *in* (5.10) *satisfy*

$$g_l = d_l \lambda^{\langle l\beta \rangle - \langle l\alpha \rangle} g_{(-l)}$$

for certain constants $d_l \in \mathscr{W}(\mathbb{F}_{p^f})^*$; *here* f *is the order of* p *in* $(\mathbb{Z}/\mathbf{n}\mathbb{Z})^*$.

Proof. $\mathbf{b} + \mathbf{c} = \mathbf{n}$ implies $\langle l\beta \rangle + \langle l\gamma \rangle = 1$ for every $l \in \mathscr{T}$. The explicit formula for $B_{N,l,Nl}$ in (5.4) (with l instead of $(l, 1)$) shows

$$B_{N,(-l),(-Nl)} = (-1)^{N-1} \lambda^{[N\langle l\beta \rangle] - [N\langle l\alpha \rangle]} B_{N,l,Nl} \tag{9}$$

for every $l \in \mathscr{T}$, $N \in \mathbb{N}$. So

$$\Phi_{-1} B_N \Phi_{-1} = U^N B_N U^{-1}\,; \tag{10}$$

U is the diagonal matrix with ll-entry $-\lambda^{\langle l\beta\rangle - \langle l\alpha\rangle} \in R^{\text{ét}}$. In view of (10) the matrix H satisfies $\Phi_{-1} H \Phi_{-1} = U^{\sigma} H U^{-1}$. Consequently $\Xi\Phi_{-1} G \Phi_{-1} U$ is another solution of (4) and hence

$$\Phi_{-1} G \Phi_{-1} U D = G \tag{11}$$

for some matrix $D \in \mathscr{D}$ (see (5.11)). □

5.13 Recalling $\mathscr{M}(\tau) = C^{\tau} C^{-1} = \Xi G^{\tau} G^{-1} \Xi^{-1}$ for $\tau \in \pi_1$ we see that (11) leads to a new constraint on monodromy:

$$\Phi_{-1} G^{\tau} G^{-1} \Phi_{-1} U^{\tau} U^{-1} = G^{\tau} G^{-1} .$$

5.14 Example. Let us compute the p-adic monodromy group for H^1 of the hypergeometric curve

$$y^5 = x(x-1)^2 (x-\lambda)^3 .$$

Fix a prime number $p > 5$. Proposition (5.12) shows

$$g_1 = d_1 \lambda^{1/5} g_4, \qquad g_2 = d_2 \lambda^{2/5} g_3 . \tag{12}$$

We distinguish four cases depending on $p \bmod 5$.

Case $p \equiv 1 \bmod 5$. We will show that in this case:

$$\mathscr{M}(\pi_1) = \left\{ \Xi \begin{pmatrix} a & & & 0 \\ & b & & \\ & & \eta^2 b & \\ 0 & & & \eta a \end{pmatrix} \Xi^{-1} \;\middle|\; \begin{matrix} a, b \in \mathbb{Z}_p^* , \\ \eta \in \mu_5 \end{matrix} \right\} \tag{13}$$

The inclusion $\subset$ follows from (12). Let us prove the inclusion $\supset$. Note that $\mathbb{Z}_p^*$ is generated by any two elements κ and $1 + pv$ with $v \not\equiv 0 \bmod p$ and $\kappa \bmod p$ a generator of $\mathbb{F}_p^*$. It therefore suffices to show that both sides in (13) have the same image in $Gl_4(\mathbb{Z}/p^2\mathbb{Z})$.

Equation (4) reads in this case $G^{\sigma} H = G$. As in the proof of (3.7) we set $G = \sum_{i \geqq 0} p^i G_i$. Then G_0 and G_1 must satisfy

$$G_0^{p-1} H \equiv I \bmod p$$

$$G_1^p H - G_1 + p^{-1}[G_0^{\sigma} H - G_0] \equiv 0 \bmod p .$$

Note $H \equiv B_p \bmod p$ and $H \equiv B_p^{-\sigma} B_{p^2} \bmod p^2$. We multiply the second equation by $(B_p G_0^{-1})^{\sigma}$ and set $\Gamma := B_p G_0^{-1} G_1$. This leads to the following equivalent system of equations

$$G_0^{p-1} B_p \equiv I \bmod p \tag{14}$$

$$B_p \Gamma^p - B_p^p \Gamma + p^{-1}[B_{p^2} - B_p^{\sigma} G_0^{1-\sigma}] \equiv 0 \bmod p . \tag{15}$$

Each of these matrix equations represents four scalar equations. According to (5.6) the polynomial $B_{p,l,l} \bmod p$ has at least one simple zero different from 0 and 1. Therefore each scalar equation in (14) is irreducible and gives a cyclic extension of

R/pR with Galois group $\mathbb{F}_p^*$. By (5.6) $B_{p,1,1} \bmod p$ and $B_{p,2,2} \bmod p$ are both polynomials of degree $\frac{p-1}{5}$ which do not vanish at 0 and 1. Checking the values at 0 and 1 one sees that $B_{p,1,1} \bmod p$ and $B_{p,2,2} \bmod p$ are not multiples of each other. So each has at least one zero which is not a zero of the other. Consequently the two extensions of R/pR by $g_1 \bmod p$ and $g_2 \bmod p$ are independent. On the other hand one has (12). Taking into account that the extensions by $g_1 \bmod p$ and $g_2 \bmod p$ do not ramify at $\lambda = 0$ whereas the extension by $\lambda^{1/5}$ does ramify at $\lambda = 0$, we conclude that the solution of (14) gives an extension of R/pR with Galois group $\mathbb{F}_p^* \times \mathbb{F}_p^* \times \mu_5$. More precisely the image of the monodromy group $\mathscr{M}(\pi_1)$ in $Gl_4(\mathbb{F}_p)$ coincides with the image of the right hand group in (13).

Next consider Eq. (15). Remark (2.8) applied to $\underline{\alpha} = F_p\underline{\tilde{\omega}}$ shows that there is a matrix A_p with entries in the ring A such that $B_{p^2} = B_p^{(p)} B_p + pA_p$. So one can write

$$p^{-1}[B_{p^2} - B_p^\sigma G_0^{1-\sigma}] \equiv A_p + p^{-1}[B_p^p - B_p^\sigma] B_p + p^{-1}[B_p - G_0^{1-\sigma}] B_p^p \bmod p\,.$$

Again we look at a zero of $B_{p,l,l} \bmod p$ different from 0 and 1. Lemma (5.15) will show that the ll-entry of $A_p \bmod p$ is not zero at this point. Granting this for the moment we see that each scalar equation in (15) is irreducible and gives a cyclic extension of our previous extension of R/pR with Galois group $\mathbb{F}_p$. The extension corresponding with the fourth (resp. third) line of (15) coincides with the one for the first (resp. second) line. On the other hand looking at the ramification one sees that the extensions corresponding with the first and second line are independent. Following the arguments back to the equation $C^\sigma H = C$ one finds that both sides of (13) have the same image in $Gl_4(\mathbb{Z}/p^2\mathbb{Z})$. So to complete the proof of (13) we only have to show:

5.15 Lemma. *The ll-entry of $A_p \bmod p$ is not zero at a zero of $B_{p,l,l} \bmod p$ different from* 0 *and* 1.

Proof. Take $l = 1$ to fix ideas. Let s be a geometric point of S corresponding to a homomorphism $\rho: A \to \overline{\mathbb{F}}_p$ such that $\rho(\lambda) \neq 0, 1$ and $\rho(B_{p,1,1}) = 0$. Because of (9) then also $\rho(B_{p,4,4}) = 0$. Assume $\rho(B_{p,2,2}) \neq 0$; hence also $\rho(B_{p,3,3}) \neq 0$. The matrix $\rho(B_p)$ is the Hasse-Witt matrix describing the action of F on $\mathrm{H}^1(X_s, \mathcal{O}_{X_s})$ (cf. (4.1)). In the present situation $\rho(B_p)$ is a diagonal matrix with exactly two non-zero entries. This implies that the Newton polygon for the action of F on $H^1_{\mathrm{crys}}(X_s)$ has a slope 0 segment of multiplicity 2 and a slope 1 segment of multiplicity 2 [2]. As a consequence the rank of the free $\mathscr{W}(\overline{\mathbb{F}}_p)$-module $\mathrm{H}^1(X_s, \mathscr{W}\mathcal{O}_{X_s})$ is 6 (see [11, II(2.19), (3.5)]). So in the exact sequence of $\overline{\mathbb{F}}_p$-vector spaces

$$0 \to \mathrm{H}^1(X_s, \mathscr{W}\mathcal{O}_{X_s})/F \xrightarrow{V} \mathrm{H}^1(X_s, \mathscr{W}\mathcal{O}_{X_s})/p \to \mathrm{H}^1(X_s, \mathscr{W}\mathcal{O}_{X_s})/V \to 0$$

the middle term has dimension 6 and the right hand term has dimension 4. Hence $\dim \mathrm{H}^1(X_s, \mathscr{W}\mathcal{O}_{X_s})/F = 2$. Recall that we obtained A_p from Remark (2.8) with $\underline{\alpha} = F_p\underline{\tilde{\omega}}$, i.e. $F_p\underline{\tilde{\omega}} = \sum V_n(\underline{\underline{A_n}}\underline{\tilde{\omega}})$. This specializes at s to

$$F\underline{\tilde{\omega}}(s) = E_p(\underline{\underline{\rho(A_1)}})\underline{\tilde{\omega}}(s) + VE_p(\underline{\underline{\rho(A_p)}})\underline{\tilde{\omega}}(s) + \dots \tag{16}$$

where $\underset{\sim}{\omega}(s)$ is the image of $\underset{\sim}{\omega}$ under the specialization map α_s in (4.1) and E_p is as in (3.2). By construction $\underset{\sim}{A_1} = B_p$. Taken modulo F and V^2 relation (16) gives a way to determine the dimension of the vector space $\mathrm{H}^1(X_s, \mathscr{W}\mathcal{O}_{X_s})/(F, V^2)$ and thus get a lower bound for the dimension of $\mathrm{H}^1(X_s, \mathscr{W}\mathcal{O}_{X_s})/F$. In particular, if $\rho(A_{p,1,1}) = 0$ one finds that these dimensions are $\geqq 3$, contradicting the fact $\dim \mathrm{H}^1(X_s, \mathscr{W}\mathcal{O}_{X_s})/F = 2$. So $\rho(A_{p,1,1}) \neq 0$ if $\rho(B_{p,1,1}) = 0$ and $\rho(B_{p,2,2}) \neq 0$. A similar argument can be used to show that $\rho(A_{p,1,1}) \neq 0$ if $\rho(B_{p,1,1}) = 0$ and $\rho(B_{p,2,2}) = 0$. □

Example (5.14) continued. Case $p \equiv -1 \bmod 5$. First we pass to the extension $R[\lambda^{1/5}]$ of R. The matrix U in the proof of (5.12) is defined over $R[\lambda^{1/5}]$. Combining the Eqs. (4) and (11) we obtain

$$G^\sigma(DU)^{-\sigma}\Phi_p H = G \tag{17}$$

where D is some diagonal matrix with entries in $\mathscr{W}(\mathbb{F}_{p^2}) \subset R$. Following the method used in the previous case one now arrives at

$$G_0^{p-1}(DU)^{-p}\Phi_p B_p \equiv I \bmod p$$

$$(\Phi_p B_p)\Gamma^p - (\Phi_p B_p)(B_p\Phi_p)^{p-1}\Gamma + \Delta \equiv 0 \bmod p$$

with

$$\Delta = p^{-1}[B_{p^2} - (B_p\Phi_p)^\sigma(DU)^\sigma G_0^{1-\sigma}]\,.$$

As before $B_{p^2} = (B_p\Phi_p)^p\Phi_p B_p + pA_p$ and

$$\Delta = A_p + p^{-1}[(B_p\Phi_p)^p - (B_p\Phi_p)^\sigma](\Phi_p B_p)$$

$$+ p^{-1}[\Phi_p B_p - (DU)^\sigma G_0^{1-\sigma}](B_p\Phi_p)^\sigma\,.$$

Note that by (10) we have $B_p\Phi_p = \Phi_p U^p B_p U^{-1} = U^{-p-1}\Phi_p B_p$. So we can proceed as before. For the correct statement and proof of Lemma (5.15) in case $p \equiv -1 \bmod 5$ one has to replace $B_{p,l,l}$ by $B_{p,l,pl}$. The result of this analysis shows that $\Xi^{-1}\mathscr{M}(\pi_1(\mathrm{Spec}((R/pR)[\lambda^{1/5}]), \Omega))\Xi$ is the group of diagonal matrices $\mathrm{diag}(a, b, b, a)$ with $a, b \in \mathbb{Z}_p^*$. The monodromy group $\mathscr{M}(\pi_1)$, with $\pi_1 = \pi_1(\mathrm{Spec}(R/pR), \Omega)$, is an extension of the one above by a group of order 5. Since $\mathscr{M}(\pi_1)$ is an abelian group by (5.11) and since p is not $0, 1 \bmod 5$ this extension is in fact a direct product. The matrix representation of the 5-cyclic factor can be derived from (5.13). The result is: if $p \equiv -1 \bmod 5$ then

$$\mathscr{M}(\pi_1) = \left\{ \Xi \begin{pmatrix} \eta a & & & 0 \\ & \eta^2 b & & \\ & & \eta^{-2} b & \\ 0 & & & \eta^{-1} a \end{pmatrix} \Xi^{-1} \;\middle|\; \begin{matrix} a, b \in \mathbb{Z}_p^*, \\ \eta \in \mu_5 \end{matrix} \right\}.$$

Example (5.14) continued. Case $p \equiv 2 \bmod 5$. As in the previous case we first pass to $R[\lambda^{1/5}]$. Now $\Xi^{-1}\mathscr{M}(\pi_1(\mathrm{Spec}((R/pR)[\lambda^{1/5}]), \Omega))\Xi$ is contained in the group of diagonal matrices $\mathrm{diag}(a, a^\sigma, a^\sigma, a)$ with $a \in \mathscr{W}(\mathbb{F}_{p^2})^*$ (use (5.11) and (5.13)). We claim that the inclusion is an equality. From this one then concludes as in the previous case

$$\mathcal{M}(\pi_1) = \left\{ \Xi \begin{pmatrix} \eta a & & & 0 \\ & \eta^2 a^\sigma & & \\ & & \eta^{-2} a^\sigma & \\ 0 & & & \eta^{-1} a \end{pmatrix} \Xi^{-1} \;\middle|\; \begin{array}{l} a \in \mathscr{W}(\mathbb{F}_{p^2})^*, \\ \eta \in \mu_5 \end{array} \right\}.$$

We shall prove our claim that the inclusion is actually an equality by combining equations (4) and (11) into

$$G^{\sigma^2-1}(UD)^{-\sigma^2}\Phi_p^2 H^\sigma H = I \tag{18}$$

and by showing that (18) modulo p^2 leads to an extension of $\overline{\mathbb{F}_p(\lambda)}$ with ramification of order $p^2(p^2-1)$ at any zero $\lambda_0 \neq 0, 1$ of $B_{p,1,2} \bmod p$ which is not a zero of $B_{p,2,4} \bmod p$. Let v be a valuation of $\overline{\mathbb{F}_p(\lambda)}$ with $v(\lambda - \lambda_0) = 1$. Equation (18) can be solved in two steps

$$K^{\sigma-1}(UD)^{-\sigma^2}\Phi_p^2 H^\sigma H = I \tag{19}$$

$$G^{\sigma+1} = K\,. \tag{20}$$

To solve (19) we set $K = \sum_{i \geq 0} p^i K_i$. Then K_0 and K_1 must satisfy

$$K_0^{p-1}(UD)^{-p^2}\Phi_p^{-1}(\Phi_p^{-1}B_p)^p\Phi_p\Phi_p^{-1}B_p \equiv I \bmod p \tag{21}$$

$$K_1 = K_0\Phi_p^{-1}(\Phi_p^{-1}B_p)^{-1}\Phi_p\Gamma \tag{22}$$

$$(\Phi_p^{-1}B_p)\Gamma^p - (\Phi_p^{-1}B_p)\Phi_p^{-1}(\Phi_p^{-1}B_p)^{p-1}\Phi_p\Gamma + \Delta \equiv 0 \bmod p \tag{23}$$

with

$$\Delta = p^{-1}[\Phi_p^2 B_{p^2} - \Phi_p^2 B_p^\sigma H^{-\sigma}\Phi_p^2(UD)^{\sigma^2}K_0^{1-\sigma}]\,.$$

To solve (20) we set $G = \sum_{i \geq 0} p^i G_i$ with

$$G_0^{\sigma+1} \equiv K_0 \bmod p^2\,. \tag{24}$$

Then G_1 satisfies

$$(G_0^{-1}G_1)^p + (G_0^{-1}G_1) - K_0^{-1}K_1 \equiv 0 \bmod p\,. \tag{25}$$

It suffices to look at the (1, 1)-entries of the above matrix equations. Equation (21) yields $v(K_{0,1,1} \bmod p) = -(p-1)^{-1}$. Using an argument like (5.15) one checks $v(\Delta_{1,1} \bmod p) = 0$. From (23) and (22) one sees $v((K_0^{-1}K_1)_{1,1} \bmod p) = v(\Gamma_{1,1} \bmod p) = -p^{-1}$. Then $v(G_{0,1,1} \bmod p) = -(p^2-1)^{-1}$ by (24) and $v((G_0^{-1}G_1)_{1,1} \bmod p) = -p^{-2}$ by (25). So the total ramification for solving (18) modulo p^2 is $p^2(p^2-1)$.

The *case* $p \equiv 3 \bmod 5$ can be developed in exactly the same way as the case $p \equiv 2 \bmod 5$. The result is exactly the same.

5.16 Remark. The method used in (5.14) and (5.15) works also for

- families of elliptic curves
- families of K3-surfaces which have a special fiber where the formal Brauer group has height 2
- isotypical components $\mathrm{H}^1(X \otimes \mathbb{F}_p, \mathscr{W}\mathcal{O}_{X \otimes \mathbb{F}_p})_l$ for the action of μ_n induced by $(x, y) \mapsto (x, \zeta y)$ $(\zeta \in \mu_n)$ in (5.1), provided $pl = l$ and $\|l\| = 2$.

References

1. Artin, M., Mazur, B.: Formal groups arising from algebraic varieties. Ann. Sci. Éc. Norm. Supér. **10**, 87–132 (1977)
2. Berthelot, P.: Slopes of Frobenius in crystalline cohomology. (Proc. Symp. Pure Math., vol. XXIX, pp. 315–328) Providence, RI: Am. Math. Soc. 1975
3. Cartier, P.: Groupes formels associés aux anneaux de Witt généralisés. resp. Modules associés à un groupe formel commutatif. Courbes typiques. C.R. Acad. Sci. Paris, Sér I. **265**, 49–52, resp. 129–132 (1967)
4. Crew, R.: F-isocrystals and p-adic representations. (Proc. Symp. Pure Math., vol. 46, pp. 111–138) Providence, RI: Am. Math. Soc. 1987
5. Dwork, B.: A deformation theory for the zeta function of a hypersurface. In: Proc. Int. Congress of Mathematicians 1962, pp. 247–259. Uppsala: Almqvist and Wiksells 1963
6. Euler, L.: Opera Omnia, vol. 12, p. 229
7. Fontaine, J.-M., Messing, W.: p-Adic periods and p-adic étale cohomology. Contemp. Math. **67**, 179–207 (1987)
8. Grothendieck, A., Dieudonné, J.: Éléments de géométrie algébrique IV. Publ. Math., Inst. Hautes Étud. Sci. **20** (1964); **32** (1967)
9. Hazewinkel, M.: Formal groups and applications. New York: Academic Press 1978
10. Hyodo, O.: On variation of Hodge-Tate structures. Math. Ann. **284**, 7–22 (1989)
11. Illusie, L.: Complexe de De Rham-Witt et cohomologie cristalline. Ann. Sci. Éc. Norm. Supér **12**, 501–661 (1979)
12. Illusie, L., Raynaud, M.: Les suites spectrales associées au complexe de De Rham-Witt. Publ. Math., Inst. Hautes Étud. Sci. **57**, 73–212 (1983)
13. Katz, N.: Travaux de Dwork. Seminaire Bourbaki, exp. 409. (Lect. Notes Math., vol. 317) Berlin Heidelberg New York: Springer 1973
14. Katz, N.: Internal reconstruction of unit-root F-crystals via expansion coefficients. Ann. Sci. Éc. Norm. Supér **18**, 245–268 (1985)
15. Katz, N.: p-adic properties of modular schemes and modular forms. In: Kuyk, W., Serre, J.-P. (eds.) Modular Functions III. (Lect. Notes Math., vol. 350) Berlin Heidelberg New York: Springer 1973
16. Klein, F.: Vorlesungen über die hypergeometrische Funktion. Berlin: Springer 1933 (reprinted 1981)
17. Messing, W.: On the nilpotence of the hypergeometric equation. J. Math. Kyoto Univ. **12**, 369–383 (1972)
18. Stienstra, J.: The generalized De Rham-Witt complex and congruence differential equations. In: Van der Geer, Oort, Steenbrink (eds.) Arithmetic Algebraic Geometry. (Prog. Math., vol. 89) Boston: Birkhäuser 1991