MÉMOIRES DE LA S. M. F.

MARIUS VAN DER PUT

# The cohomology of Monsky and Washnitzer

*Mémoires de la S. M. F. 2^e série*, tome 23 (1986), p. 33-59
<http://www.numdam.org/item?id=MSMF_1986_2_23__33_0>

Société Mathématique de France
2e Série, Mémoire n° 23, 1986, p. 33-60

# THE COHOMOLOGY OF MONSKY AND WASHNITZER

Dedicated to B. Dwork on the occasion of his 60th anniversary

by

Marius van der Put

Summary

The Zeta-function of an algebraic variety over a finite field can be expressed in terms of a Frobenius operator acting on p-adic cohomology groups of this variety. Those cohomology groups, based on work of B. Dwork, are called the Monsky-Washnitzer cohomology. The first four sections of this paper give a survey of the papers of Monsky and Washnitzer. Their work is simplified and slightly extended by the use af Artin-approximation and some rigid analysis. In section 5 the connection with Dwork's work is indicated, Adolphson's index theorem is given in a different form in section 6. Dwork's remarkable formula for the unit root of an elliptic curve and properties of the solutions of the hypergeometric differential equation with parameters $\frac{1}{2}, \frac{1}{2}, 1$ are proved in detail in section 7.

Résumé

La fonction zêta d'une variété algébrique sur un corps fini peut s'exprimer à l'aide des opérateurs de Frobenius sur des groupes de cohomologie p-adique de cette variété. Ces groupes de cohomologie, qui sont inspirés par des travaux de Dwork, s'appèlent la cohomologie de Monsky et Washnitzer. Les quatre premiers paragraphes développent cette théorie. L'exposé simplifie les papiers de Monsky et Washnitzer grace à une approximation d'Artin et un peu d'analyse rigide. Le paragraphe 5 indique le rapport avec les travaux de Dwork. Un théorème d'indice due à Adolphson est donné dans une forme plus générale dans le paragraphe 6. La formule remarquable de Dwork pour le "unit root" d'une courbe elliptique ainsi

0037-9484/1986/02 33 28 /$ 4.80 

que des propriétés de l'équation hypergéométrique à paramètres $\frac{1}{2}$, $\frac{1}{2}$, 1 sont montrés en détail dans le paragraphe 7.

## § 1. Introduction.

The aim of the Monsky-Washnitzer cohomology, based on and inspired by the work of B. Dwork, is to find and explicit expression for the Zeta-function of an algebraic variety X over a finite field $k = \mathbb{F}_q$.

(1.1) $Z(X|k;t) = \exp(\sum_{s \geq 1} \frac{N_s}{s} t_s)$ is this Zeta-function and $N_s$ denotes the number of points of X with valus in $\mathbb{F}_{q^s}$.

Let R denote a complete discrete valuation ring with $R/\pi R = k$ and $K = Qt(R)$ of characteristic 0. (e.g. $R = W(k)$). One tries to find cohomology groups $H^i(X;K)$ (vectorspaces over K) with an induced action $F_*$ on it, coming from the Frobenius map $x \longmapsto x^q$ on X, such that:

(1.2) $N_s = \Sigma (-1)^i Tr((q^n F_*^{-1})^s | H^i(X;K))$ (Lefschetz' fixed point formula)

(1.3) $Z(X\ k;t) = \prod_{i \text{ odd}} P_i(t) \prod_{i \text{ even}} P_i(t)^{-1}$ where $P_i(t) = \det(1 - tq^n F_*^{-1} | H^i(X;K))$.

The papers of MW [11, 12] are mainly concerned with the case: X an affine, regular variety of dimension n. As we will see, this implies that $H^i(X;K) = 0$ for $i > n$. If one knows that $\dim H^i(X;K) < \infty$ for all i, then (1.3) is an easy consequence of (1.2). Moreover Z is clearly a rational function in this case. However, the authors MW have not shown that the $H^i(X;K)$ are finite dimensional. They work instead with nuclear operators L on a vectorspace M over K. The definition can be given as follows: An <u>eigenvalue</u> of L is a $\lambda \in \overline{K}$ = the algebraic closure of K, such that the minimum polynomial g of $\lambda$ has the property $\ker(g(L)) \neq 0$.

A K-linear map $L: M \longrightarrow M$ is called <u>nuclear</u> if:

(i) For every eigenvalue $\lambda \neq 0$ there exists a decomposition $M = A \oplus B$ with A,B vectorspaces invariant under L; $B = \bigcup_{n \geq 1} \ker(g(L)^n)$ is finite-dimensional and g(L) is bijective on A.

(ii) The nonzero eigenvalues of L, form a finite set or a sequence with limit 0.

B above is the generalized eigenspace by $\lambda$ and A equals $\bigcap_{n \geq 1} \operatorname{im}(g(L)^n)$. For

$n \in \mathbb{N}$ we denote by $M_n$ the sum of the generalized eigenspaces of L with eigenvalues $\lambda$, $|\lambda| \geq |\pi|^n$. Then dim $M_n < \infty$. Define now $\mathrm{Tr}(L^s) = \lim_{n \to \infty} \mathrm{Tr}(L^s | M_n)$ and $\det(1 - tL) = \lim_{n \to \infty} \det(1 - tL|M_n)$. The limits exist and $\det(1 - tL)$ is an entire function on K. Moreover

$$(1.4)\quad \det(1 - tL) = \exp\Big(- \sum_{s \geq 1} \frac{\mathrm{Tr}(L^s)}{s} t^s\Big)$$

MW prove that $q^n F_*^{-1}$ is nuclear. So (1.2) implies (1.3) and $Z(X|k;t)$ is a meromorphic function on all of K. The power series $Z(X|k;t)$ is also convergent w.r.t. the archimedian valuation on Q. A criterium of Dwork-Borel then shows that $Z(X|k;t)$ is actually a rational function.

We note the following property of nuclear operators: Let $L_i : M_i \longrightarrow M_i$ $(i = 1,2)$ be nuclear, let the linear map $\alpha : M_1 \longrightarrow M_2$ satisfy $\alpha L_1 = L_2 \alpha$, then the induces maps $L_0$ on $\ker \alpha$ and $L_3$ on $\mathrm{coker}\ \alpha$ are nuclear. Moreover:

$$(1.5)\quad \prod_{i=0}^{3} \det(1 - tL_i)^{(-1)^i} = 1 \quad \text{and} \quad \sum_{i=0}^{3} \mathrm{Tr}(L_i^s) = 0.$$

## § 2. Definition of the Monsky-Washnitzer cohomology.

Let X be a smooth affine variety over $k = \mathbb{F}_q$ with coordinate ring $\bar{A}$. According to a result of M$^{me}$ Elkik [15] there exists a R-algebra B, finitely generated and smooth over R such that $B/\pi B \cong \bar{A}$.
Write $B = R[t_1,\ldots,t_n]/(f_1,\ldots,f_m)$. One replaces B by the ring

$A = R\langle t_1,\ldots,t_n\rangle^{\dagger}/(f_1,\ldots,f_m)$, where $R\langle t_1,\ldots,t_n\rangle^{\dagger}$ consists of the power series $\Sigma a_\alpha t^\alpha$ such that all $a_\alpha \in R$ and for some $C > 0$ and $\rho, 0 < \rho < 1$, one has $|a_\alpha| \leq C\rho^{|\alpha|}$ for all $\alpha$.
The elements of $R\langle t_1,..,t_n\rangle^{\dagger}$ are called overconvergent power series. Every element converges in a polydisc $\{(t_1,\ldots,t_n) \in K^n \mid |t_1| \leq \rho_1,\ldots,|t_n| \leq \rho_n\}$ with all $\rho_i > 1$.
The ring A satisfies $A/\pi A = \bar{A}$ and A is complete in some weak sense. For our purposes we make the following simplifying definition.

(2.1) Definition. A weakly complete finitely generated (w.c.f.g) algebra over R is a homomorphic image of some $R\langle x_1,\ldots,x_n\rangle^{\dagger}$.

(2.2) Proposition. $R<x_1,\ldots,x_n>^{\dagger}$ satisfies Weierstrass' preparation and division.

The proof of (2.2) contains no surprises. Among the consequences are: $R<X_1,\ldots,X_n>^{\dagger}$ noetherean and $R[X_1,\ldots,X_n] \to R<X_1,\ldots,X_n>^{\dagger}$ is flat.

(2.3) For $A = R<t_1,\ldots,t_n>^{\dagger}/(f_1,\ldots,f_m)$ one defines a module of differentials

$$D^1(A) = Adt_1 + \ldots + Adt_n / \text{ the A-submodule generated by } \{\frac{\partial f_i}{\partial t_1} dt_1 + \ldots + \frac{\partial f_i}{\partial t_n} dt_n \mid i = 1,\ldots m\}$$

This module is the universal finite module of differentials of A/R. It does not depend on the chosen representation of A. It is easily seen that $D^1(A) \otimes \bar{A} = \Omega^1_{\bar{A}/k}$. The module $\Omega^1_{\bar{A}/k}$ is projective and its rank is equal to the dimension d of $\bar{A}$. Using flatness one can conclude that $D^1(A)$ is also projective of rank d. An easier argument uses the Jacobian-criterion. Let I be the ideal in A generated by the (n-d) x (n-d)-minors of $(\frac{\partial f}{\partial t})$. Then $(\pi, I) = A$ since $\bar{A}/k$ is regular of dimension d. Hence I contains an element of the form $(1 - \pi a)$ with $a \in A$. The infinite series $1 + \pi a + \pi^2 a^2 + \ldots$ converges in A and so $1 \in I$. This implies that $D^1(A)$ is a projective module of rank d over A.

As usual one makes the de Rham-complex D(A):
$0 \to D^0(A) \xrightarrow{d^0} D^1(A) \xrightarrow{d^1} D^2(A) \to \ldots$ with $D^i(A) = \Lambda^i D^1(a)$ and $d^i$ = the exterior differentiation. The $i^{th}$-cohomology group of the complex D(A) is denoted by $H^i(X;R)$ or $H^i(\bar{A}/R)$. Further $H^i(X;K) := H^i(\bar{A}/K) := H^i(\bar{A}/R) \otimes_R K$ is the definition of the Monsky-Washuitzer cohomology. The notations are justified in (2.4).

(2.4) Unicity and the lifting of the Frobenius map.
This section contains some new results. In particular the technical assumption "very smooth" in the MW-papers is removed with the help of a special case of Artin-approximation.

We write $R<t_1,\ldots,t_n>$ for the ring of power series $\Sigma\, a_\alpha\, t^\alpha$ with $a_\alpha \in R$ and $\lim a_\alpha = 0$. Clearly $R<t_1,\ldots,t_n>$ is the $\pi$-adic completion of $R<t_1,\ldots,t_n>^{\dagger}$. For any w.c.f.g. algebra A we write $\hat{A} = \varprojlim A/\pi^n A$ for its $\pi$-adic completion.

(2.4.1) Proposition. $R<t_1,\ldots,t_n>^{\dagger}$ has the Artin-approximation property.

The statement means the following: "Let $f_1,\ldots,f_m$ belong to $R<X_1,\ldots,X_a,Y_1,\ldots,Y_b>^{\dagger}$, let $\varepsilon > 0$ and let $\hat{y}_1,\ldots,\hat{y}_b \in R<X_1,\ldots,X_a>$ satisfy $f_i(X_1,\ldots,X_a,\hat{y}_1,\ldots,\hat{y}_b) = 0$ for $i = i,\ldots,m$. There are $y_1,\ldots,y_b \in R<X_1,\ldots,X_a>^{\dagger}$

with $\|y_i - \hat{y}_i\| \leq \varepsilon$ $(i = 1,\ldots,b)$ and $f_i(X_1,\ldots,X_a,y_1,\ldots,y_b) = 0$ for $i = 1,\ldots,m$".

Artin's proof in [2] for analytic local rings can be adapted to the situation above. A complete proof in a somewhat more general situation (i.e. R need not be discrete) is given in [4]. As in [2] there are some nice corollaries.

(2.4.2) Corollary. Given a diagram of w.c.f.g. algebra's and a morphism $\hat{u}$: $\hat{A} \to \hat{B}$ with $\hat{f} = \hat{g} \circ \hat{u}$ and $\varepsilon > 0$, there exists a morphism $u$: $A \to B$ with $f = g \circ u$ and $\|u - \hat{u}\| \leq \varepsilon$.

$$\begin{array}{ccc} & & A \\ & & \downarrow f \\ B/J & \xleftarrow[g]{} & B \end{array}$$

(2.4.3) Corollary. Given a diagram of w.c.f.g algebra's and a morphism $\hat{u}$: $\hat{A} \to \hat{B}$ with $g = \hat{u} \circ \hat{f}$ and $\varepsilon > 0$, there exists a morphism $u$: $A \to B$ with $g = u \circ f$ and $\|u - \hat{u}\| \leq \varepsilon$.

$$\begin{array}{ccc} & & A \\ & & \uparrow f \\ C & \xrightarrow{g} & B \end{array}$$

N.B. The norms in (2.4.1)-(2.4.3) are induced by some presentation of the algebra's

Definition. A w.c.f.g. algebra A is called a lift of $\bar{A}$ if A is flat over R and if $A/\pi A \cong \bar{A}$.

(2.4.4) Theorem. Let $\bar{A}/k$ be smooth and finitely generated. There exists a lift A of $\bar{A}$. Moreover:

(i) Every lift of $\bar{A}$ is R-isomorphic to A.

(ii) Let $\bar{C}/k$ be smooth and finitely generated, let C be a lift of $\bar{C}$ and let $f$: $\bar{A} \to \bar{C}$ be a morphism of k-algebra's. There exists an R-homomorphism F: $A \to C$ lifting f.

(iii) Let B be a w.c.f.g algebra and $F_0, F_1$: $A \to B$ two homomorphisms with $F_0 \equiv F_1 \bmod \pi$. The induced mappings

$$(F_0)_*, (F_1)_* : D(A) \otimes_R K \to D(B) \otimes_R K \text{ are homotopic.}$$

Proof. (i) The existence of A, a lift of $\bar{A}$, has already been shown. From A/R flat and $A/\pi A$ smooth over $R/\pi R$ it follows that $A/\pi^n A$ is smooth over $R/\pi^n R$ for all $n \geq 1$. Let B denote another lift of $\bar{A}$. Using that $A/\pi^n A$ is smooth over $R/\pi^n R$ one constructs a projective system of R-homomorphisms $h_n$: $A/\pi^n A \to B/\pi^n B$ with $h_1 = \mathrm{id}$. The limit $\hat{h} = \varprojlim h_n$ can be approximated by an R-homomorphism h: $A \to B$ such that $(h \bmod \pi)$ is an isomorphism. As a consequence of the Weierstrass theorems one finds that h is surjective. Since B has no $\pi$-torsion and $(h \bmod \pi)$ is bijective one sees that h is also injective.

(ii) The same method yields a lift $\hat{F}$: $\hat{A} \to \hat{C}$ of f. This $\hat{F}$ can be approximated by a lift F: $A \to C$ according to (2.4.3).

(iii) Suppose that one has a morphism $F: A \longrightarrow B\langle T\rangle^{\dagger}$ such that $\alpha_o \circ F = F_o$ and $\alpha_1 \circ F = F_1$ where $\alpha_o, \alpha_1: B\langle T\rangle^{\dagger} \longrightarrow B$ are the B-algebra homomorphisms given by $\alpha_o(T) = 0$ and $\alpha_1(T) = 1$.

Then it suffices to verify that $(\alpha_o)_*, (\alpha_1)_*: D(B\langle T\rangle^{\dagger}) \otimes K \longrightarrow D(B) \otimes K$ are homotopic. The space $D^q(B\langle T\rangle^{\dagger} \otimes K)$ is the direct sum of $B\langle T\rangle^{\dagger} \otimes_B (D^q(B) \otimes K)$ and $B\langle T\rangle^{\dagger} dT \otimes_B (D^{q-1}(B) \otimes K)$. The homotopy $\{\delta_q\}$ between $(\alpha_o)_*$ and $(\alpha_1)_*$ is given by: $\delta_q$ is zero on the first vectorspace and $\delta_q$ = integration with respect to T on the second vectorspace.

Now the existence of the map F. Put $S = \pi T$ and consider the homomorphism $h: A \longrightarrow \hat{B}[\![S]\!]/(S^2 - \pi S)$ given by

$$h(a) = F_o(a) + \frac{F_1(a) - F_o(a)}{\pi} S \quad \text{(equals } F_o(a)(1-T) + F_1(a)T\text{)}.$$

Since $A/\pi^n A$ is smooth over $R/\pi^n R$ for every n and since $\hat{B}[\![S]\!]$ equals $\varprojlim \hat{B}[\![S]\!]/(\pi^n, (S^2 - \pi S)^n)$ one obtains a morphism $\hat{h}: A \longrightarrow \hat{B}[\![S]\!]$ which lifts h.

Note that $\hat{B}[\![S]\!] \subseteq \hat{B}\langle T\rangle$ and that $\hat{B}\langle T\rangle$ is the completion of $B\langle T\rangle^{\dagger}$. So we have a morphism $\hat{F}: \hat{A} \longrightarrow (B\langle T\rangle^{\dagger})\hat{}$ with $\hat{F}$ mod $T(1-T) = (1-T)\hat{F}_o + T\hat{F}_1$.
Applying (2.4.2) to A, $B\langle T\rangle^{\dagger}$ and the ideal $T(1-T)$ one obtains the required map $F: A \longrightarrow B\langle T\rangle^{\dagger}$.

(2.4.5.) Corollary. For smooth, finitely generated k-algebra's $\bar{A}$ the map $\bar{A} \longmapsto H^*(\bar{A}; K)$ is well defined and functorial.

## §3. The map $\psi$.

(3.1) Proposition. Let $B \subset A$ denote a finite ringextension of w.c.f.g. algebra's. Suppose that $\bar{B}$ is regular and has no zero-divisors and that B is flat over R. There exists a "trace map" $S_{A/B}: D(A) \longrightarrow D(B)$.

Proof. The natural map $D(B) \longrightarrow D(A)$ extends to an isomorphism $D(B) \otimes_B Qt(A) \xrightarrow{\sim} D(A) \otimes_A Qt(A)$. The trace map is defined by:

$S_{A/B}: D(A) \longrightarrow D(A) \otimes_A Qt(A) \longrightarrow D(B) \otimes_B Qt(A) \longrightarrow D(B) \otimes_B Qt(B)$ where the last map is $id_{D(B)} \otimes Tr_{Qt(A)/Qt(B)}$. One has to show that $S_{A/B}$ maps D(A) into D(B).

The module D(B) is projective and B is normal. Hence $\bigcap_{\text{hgt } \underline{p}=1} D(B)_{\underline{p}} = D(B)$

and it suffices to show that $S_{A/B}(D(A)) \subseteq D(B)_{\underline{p}}$ for every prime ideal $\underline{p}$ of height 1. For $D^o(A) = A$ this is well known. For $D^1(A)$ one uses an exact sequence: $0 \longrightarrow D^1(B) \otimes A_{\underline{p}} \longrightarrow D^1(A) \otimes A_{\underline{p}} \longrightarrow \Omega^1_{A_{\underline{p}}/B_{\underline{p}}} \longrightarrow 0$. According to a result of R. Berger [3]

the universal module of differentials $\Omega^1_{A_{\underline{p}}/B_{\underline{p}}}$ equals $\prod_{i=1}^{s} A_{\underline{p}}/(\alpha_i)$ and Discr $(A_{\underline{p}}/B_{\underline{p}})$ $= \prod_{i=1}^{s} (\alpha_i) \subset A_{\underline{p}}$.

From $D^1(B) \otimes A_{\underline{p}} \subset D^1(A) \otimes A_{\underline{p}} \subset D^1(B) \otimes \prod_{i=1}^{s} (\alpha_i)^{-1} A_{\underline{p}}$ and the classical definition of Discr $(A_{\underline{p}}/B_{\underline{p}})$ it follows that $S_{A/B}(D^1(A))$ lies in $D^1(B) \otimes B_{\underline{p}}$. The case $D^q(A)$ is similar.

(3.2.) Definition and Theorem.

Let A be a lift of $\bar{A}/k$, which is smooth and finitely generated, let F be a lift of the Frobenius of $\bar{A}$. Define $\psi$: $D(A) \longrightarrow D(A)$ by

$\psi$: $D(A) \xrightarrow{S_{A/F(A)}} D(F(A)) \xleftarrow{\sim}_{F} D(A)$. One has the following properties:

(i) $\psi(F(a)\omega) = a\,\psi(\omega)$ for $a \in A$ and $\omega \in D(A)$.

(ii) $\psi(D^i(A)) \subset D^i(A)$ and $\psi$ commutes with the differentiation d on $D(A)$.

(iii) $\psi \circ F =$ multiplication by $q^n$, where $q = \#k$ and $n = \dim \bar{A}$.

(iv) $F_*$ is bijective on $H^*(\bar{A};K)$ and $\psi_* = q^n F_*^{-1}$.

Proof (i), (ii) and (iii) are obvious if one notes that $[A: F(A)] = [\bar{A} : \bar{A}^q] = q^n$ with $q = \#k$ and $n = \dim \bar{A}$.

(iv) This is more difficult. Let us assume that Qt(A) is a Galois-extension of Qt(FA) with group G. Every $\sigma \in G$ maps A onto A and $\sigma \equiv id \pmod{\pi}$. From (2.4.4) it follows that $\sigma_*$ on $H^*(\bar{A};K)$ is also the identity. Let i denote the inclusion $FA \subset A$. From $i \circ S_{A/FA} = \sum_{\sigma \in G} \sigma$: $D(A) \longrightarrow D(A)$ it follows that

$i_* \circ (S_{A/FA})_*$: $H^*(\bar{A};K) \longrightarrow H^*(\bar{A};K)$ is multiplication by $q^n$.

Hence $(S_{A/FA})_*$ and $\psi_*$ are injective. Further $\psi_* \circ F_* = q^n$ holds according to (iii). Hence $\psi_*$ and $F_*$ are bijective.

If Qt(A) is not a Galois-extension of Qt(FA) then one works with $FA \subset A \subset C$, where C is the integral closure of FA in a Galois-extension containing Qt(A). A variant of the argument above will again show that $(S_{A/FA})_*$ is injective.

(3.3) Proposition $\psi$: $D(A) \otimes K \longrightarrow D(A) \otimes K$ is nuclear.

This proposition is a special case of the following lemma.

(3.4) Lemma and Definition. Let A be a w.c.f.g. R-algebra and F a lift of the Frobenius of $\bar{A}$. An additive map $\theta$: $M \longrightarrow M$ of a finitely generated A-module M in itself is called a Dwork operator if $\theta(F(a)m) = a\,\theta(m)$ for all $a \in A$ and $m \in M$. Any Dwork operator $\theta$ induces a nuclear map $\theta$: $M \otimes K \longrightarrow M \otimes K$.

Proof. One may suppose that $A = R\langle t_1,\dots,t_n\rangle^{\dagger}$. The module M has a finite free resolution $0 \longrightarrow M_s \longrightarrow M_{s-1} \longrightarrow \dots \longrightarrow M_o \longrightarrow M \longrightarrow 0$ and on each $M_i$ one can construct a Dwork operator $\theta_i$ such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_s & \longrightarrow & M_{s-1} & \longrightarrow \dots \longrightarrow & M_o & \longrightarrow & M \longrightarrow 0 \\ & & \downarrow\theta_s & & \downarrow\theta_{s-1} & & \downarrow\theta_o & & \downarrow\theta \\ 0 & \longrightarrow & M_s & \longrightarrow & M_{s-1} & \longrightarrow \dots \longrightarrow & M_o & \longrightarrow & M \longrightarrow 0 \end{array}$$

is commutative.

Hence we may suppose that M is a free module over A with basis $e_1,\dots,e_m$. The Dwork operator $\theta$ is determined by

$$\{\theta(t^{\alpha}e_i) \mid i = 1,\dots,m;\ \alpha = (\alpha_1,\dots,\alpha_n);\ 0 \le \alpha_j < q \text{ for all } j\}.$$

since $\theta\Big(\sum_{\substack{\alpha < (q,q,\dots,q)\\ i=1,\dots,m}} F(a_{\alpha,i})t^{\alpha}e_i\Big) = \sum a_{\alpha,i}\ \theta(t^{\alpha}e_i)$.

For $r > 1$ we write $A(r)$ for the subspace of A consisting of the power series $\sum a_{\alpha}t^{\alpha}$ with $\lim |a_{\alpha}|r^{|\alpha|} = 0$. This $A(r)$ is a Banach space with respect to the norm $\|\sum a_{\alpha}t^{\alpha}\| = \max|a_{\alpha}|r^{|\alpha|}$. Put $M(r) = \sum_{i=1}^{m} A(r)e_i$. This is also a Banach space. For r close enough to 1 one has $\theta(M(r)) \subseteq M(r^q)$ and $\theta_r^1\colon M(r) \longrightarrow M(r^q)$ is continuous. The inclusion map $M(r^q) \subset\longrightarrow M(r)$ is completely continuous, i.e. the uniform limit of linear maps of finite rank, and so is $\theta_r\colon M(r) \xrightarrow{\theta_r^1} M(r^q) \subset\longrightarrow M(r)$. It is well known that a completely continuous endomorphism of a Banach space is nuclear. For all r with $1 < r \le r_o$ the map $\theta_r$ is nuclear. The trace of $\theta_r$ may be calculated w.r.t. any orthogonal basis $\{b_n \mid n \ge 1\}$ of $M(r)$. If $\theta_r(b_n) = \sum_{m=1}^{\infty} \lambda_{n,m}b_m$ $(n \ge 1)$ then $tr(\theta_r) = \sum_{n=1}^{\infty} \lambda_{n,n}$.

The spaces $M(r)$ have a common orthogonal basis, namely $\{t^{\alpha}e_i \mid i = 1,\dots,m;\ \alpha \in \mathbb{N}_o^n\}$. Hence $tr(\theta_r)$ for $1 < r \le r_o$ does not depend on r and similar for $tr(\theta_r^n)$ and $\det(1 - t\,\theta_r)$. An easy calculation shows that $\theta = \varinjlim \theta_r\colon M = \bigcup_{r>1} M(r) \longrightarrow M$ is also nuclear and that $\det(1 - t\theta) = \det(1 - t\theta_r)$ for $1 < r \le r_o$.

## §4. The Lefschetz theorem.

In this we will prove the formula (1.2). It suffices to do this for $s = 1$.

(4.1) Lefschetz fixed point formula. Let $\bar{A}/k$ be smooth and integral of dimension n.

Let $N(\overline{A})$ denote the number of k-homomorphisms $\overline{A} \longrightarrow k = \mathbf{F}_q$. Then $N(\overline{A}) = \sum_{i=o}^{n} (-1)^i \mathrm{Tr}(q^n F_*^{-1} | H^i(\overline{A};K))$.

Proof. We remark that the formula makes sense, since $\psi_* = q^n F_*^{-1}$ is nuclear on each $H^i(\overline{A};K)$. The righthandside can be rewritten as $\sum_{i=o}^{n} (-1)^i \mathrm{Tr}(\psi | D^i(A) \otimes K)$. We write $L(\overline{A})$ for this expression.

Choose elements $\overline{f}_1,\ldots,\overline{f}_s \in \overline{A}$ such that:

(i) $D(\overline{f}_1),\ldots,D(\overline{f}_s)$ is a covering of Spec $(\overline{A})$.

(ii) $D(\overline{f}_i)$ contains at most one $k = \mathbf{F}_q$-valued point.

(iii) $D(\overline{f}_i \overline{f}_j)$ with $i \neq j$ contains no k-valued points.

(N.B. For $\overline{f} \in \overline{A}$ we denote $\{\underline{p} \in \mathrm{Spec}(\overline{A}) \mid \overline{f} \notin \underline{p}\}$ by $D(\overline{f})$ as usual.)

According to J. Tate, the sheaf $D(\ ) \otimes K$ is acyclic w.r.t. finite affinoid coverings. The implies the following exact sequence:

$$0 \longrightarrow D(A) \otimes K \longrightarrow \bigoplus_i D(A\langle \tfrac{1}{f_i} \rangle^\dagger) \otimes K \longrightarrow \bigoplus_{i<j} D(A\langle \tfrac{1}{f_i f_j} \rangle^\dagger) \otimes K \longrightarrow \ldots$$

In particular $L(\overline{A}) = \sum_i L(A_{\overline{f}_i}) - \sum_{i<j} L(\overline{A}_{\overline{f}_i \overline{f}_j}) + \ldots$

It suffices to give the proof of (4.1) in two special cases, namely:

(4.1.0) Lemma. If $N(\overline{A}) = 0$ then $L(\overline{A}) = 0$

(4.1.1) Lemma. If $N(\overline{A}) = 1$ then there exists $\overline{f} \in \overline{A} - \{0\}$ such that $N(\overline{A}_{\overline{f}}) = L(\overline{A}_{\overline{f}}) = 1$.

Proof of (4.10). Let $\theta$: $M \longrightarrow M$ be any Dwork operator. For $a \in A$ we denote by $L_a$ the multiplication on M by a. Consider the commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{\theta \circ L_a} & M \\ {\scriptstyle L_a}\downarrow & & \downarrow{\scriptstyle L_a} \\ M & \xrightarrow{L_a \circ \theta} & M \end{array}$$

The maps induced by $\theta \circ L_a$ and $L_a \circ \theta$ on $\ker(L_a)$ and $\mathrm{coker}\ (L_a)$ are 0. Hence $\mathrm{Tr}(\theta \circ L_a) = \mathrm{Tr}(L_a \circ \theta)$ for every $a \in A$. So $\mathrm{Tr}(\theta \circ L_{F(a)-a}) = 0$ for every $a \in A$. The condition $N(\overline{A}) = 0$ implies that the ideal $\overline{J}$ in $\overline{A}$ generated by all $\overline{a}^q - \overline{a}$ equals $\overline{A}$. Then J, the ideal in A generated by all $F(a) - a$, is also the unit ideal. Write $1 = \sum_{i=1}^{s} b_i(F(a_i) - a_i)$. Then $\theta = \sum_{i=1}^{s} (\theta \circ L_{b_i}) \circ L_{F(a_i)-a_i}$ and so $\mathrm{Tr}(\theta) = 0$. The special case $\theta = \psi$ and $M = D^i(A)$ of the above implies $L(\overline{A}) = 0$.

Proof of (4.1.1). The proof of MW requires the Gysin exact sequence. Our proof requires far less since we can localize the problem at a suitable neighbourhood of the k-valued point of $\bar{A}$. We may suppose that $\bar{A}$ has the form

$\bar{A} = K[X_1,\dots,X_m]_{\bar{g}}/(\bar{f}_{n+1},\dots,\bar{f}_m)$ such that

(i) $(0,\dots,0)$ is the only k-rational point of Spec $(\bar{A})$.

(ii) $\bar{f}_i = X_i + \text{order} \geq 2$.

(iii) $\det\left(\left(\frac{\partial \bar{f}_i}{\partial x_j}\right)_{i,j=n+1}^{m}\right) = \bar{g}$

Put $A = R\langle X_1,\dots X_m, Y\rangle^{\dagger}/(f_{n+1},\dots,f_m, g\,Y-1)$ and define the complex C by the exact sequence $0 \to D(A) \otimes K \to D(A\langle X_n^{-1}\rangle^{\dagger}) \otimes K \to C \to 0$. There is a well-defined degree 1 morphism $\tau$: $D(A/X_n) \otimes K \to C$ given by $\omega \longmapsto$ the image of $\tilde{\omega} \wedge \frac{dX_n}{X_n}$ in C, where $\tilde{\omega} \in D(A) \otimes K$ has image $\omega$ in $D(A/X_n) \otimes K$.

If one shows that $\tau$ induces an isomorphism on the cohomology groups then $L(\bar{A}) = L(\bar{A}/X_n)$ since $L(\bar{A}_{X_n}) = N(\bar{A}_{X_n}) = 0$.
Further $N(\bar{A}) = N(\bar{A}/X_n) = 1$ and by induction to the dimension of $\bar{A}$ formula (4.1.1) follow.

In a more general situation MW prove that $\tau$ is a quasi-isomorphism of complexes. The Gysin exact sequence then follows. Our special case seems easier to handle. First a lemma.

(4.1.2) Lemma. There exists a residue map Res: $A\langle X_n^{-1}\rangle^{\dagger} \otimes K \to A/X_n \otimes K$.
It has the properties: (i) Res $\circ\, \partial/\partial X_n = 0$; (ii) every element of $A\langle X_n^{-1}\rangle^{\dagger} \otimes K$ can be written as a $X_n^{-1} + \partial/\partial X_n(F)$ with $a \in A \otimes K$ and $F \in A\langle X_n^{-1}\rangle^{\dagger} \otimes K$.
(iii) if $G \in A\langle X_n^{-1}\rangle^{\dagger} \otimes K$ and $\frac{\partial G}{\partial X_n} \in A \otimes K$ then $G \in A \otimes K$.

Proof. As before $A = R\langle X_1,\dots,X_m, Y\rangle^{\dagger}/(f_{n+1},\dots,f_m, gY-1)$ and

$\hat{A} = \varprojlim A/(X_1,\dots,X_m)^s = A[\![T_1,\dots,T_m]\!]/(T_1-X_1,\dots,T_m-X_m)$ is easily seen to be $R[\![X_1,\dots,X_n]\!]$. The derivations $\frac{\partial}{\partial X_i}$ $(i = 1,\dots,n)$ on A extend to $\hat{A} = R[\![X_1,\dots,X_n]\!]$ and they are the obvious derivations of $\hat{A}/R$. Let $R[\![X_1,\dots,X_n]\!]\langle X_n^{-1}\rangle$ denote the completion of $R[\![X_1,\dots,X_n]\!][X_n^{-1}]$ with respect to the $\pi$-adic topology. Again $\frac{\partial}{\partial X_n}$ extends in a unique continuous way. Further $A\langle X_n^{-1}\rangle^{\dagger}$ is a subring of $R[\![X_1,\dots,X_n]\!]\langle X_n^{-1}\rangle$ and the two derivations $\frac{\partial}{\partial X_n}$ coincide on $A\langle X_n^{-1}\rangle^{\dagger}$. Let us first prove part (iii): $G \in A\langle X_n^{-1}\rangle^{\dagger}$ with $\frac{\partial G}{\partial X_n} \in A$ can be expanded as

$G = \sum_{m \in \mathbb{Z}} G_m(X_1,\ldots,X_{n-1})X_n^m$ in $R[\![X_1,\ldots,X_n]\!]\langle X_n^{-1}\rangle$. Clearly $G \in R[\![X_1,\ldots,X_n]\!]$ and (iii) follows from $A = A\langle X_n^{-1}\rangle^{\dagger} \cap R[\![X_1,\ldots,X_n]\!]$. In the sequel we will write $'$ for $\frac{\partial}{\partial X_n}$. We note the following formula for $a \in A$ and $k \geq 1$:

$$\frac{a}{X_n^k} = -\left(\frac{a}{(k-1)X_n^{k-1}} + \frac{a'}{(k-1)(k-2)X_n^{k-2}} + \ldots + \frac{a^{(k-1)}}{(k-1)!X_n}\right)' + \frac{a^{(k)}}{(k-1)!X_n}.$$

For $a \in A$ also $\frac{a^{(k)}}{k!} \in A$ since $\frac{a^{(k)}}{k!} \in (A \otimes K) \cap R[\![X_1,\ldots,X_n]\!] = A$.

Let $G = \sum_{r=1}^{\infty} a_k X_n^{-k}$ be a general element of $A\langle X_n^{-1}\rangle^{\dagger} \otimes K$, then $G = F' + a X_n^{-1}$ where

$$a = \sum_{k=1}^{\infty} \frac{a_k^{(k)}}{(k-1)!} \quad \text{and} \quad F = -\sum_{k=1}^{\infty} \left(\frac{a_k}{(k-1)X_n^{k-1}} + \frac{a_k'}{(k-1)(k-2)X_n^{k-2}} + \ldots + \frac{a_k^{(k-1)}}{(k-1)!X_n}\right).$$

It is an exercise to show that the two infinite sums converge to elements $a \in A \otimes K$ and $F \in A\langle X_n^{-1}\rangle^{\dagger} \otimes K$. This proves (ii).

The map Res is defined by $\mathrm{Res}(G) = a \bmod X_n \in (A/X_n) \otimes K$. One easily sees that Res is well-defined and has property (i).

Continuation of the proof of (4.1.1).

One defines $\mathrm{Res}: C \longrightarrow D(A/X_n) \otimes K$, a morphism of complexes by defining the Res of a q-form of $D(A\langle X_n^{-1}\rangle^{\dagger}) \otimes K$;

$$\mathrm{Res}\Big(\sum_{i_1<\ldots<i_q<n} a_i\, dx_{i_1} \wedge \ldots \wedge dx_{i_q} + \sum_{i_1<\ldots<i_{q-1}<n} b_i dx_{i_1} \wedge \ldots \wedge dx_{i_{q-1}} \wedge dx_n\Big) =$$

$$= \sum_{i_1<\ldots<i_{q-1}<n} \mathrm{Res}(b_i)\, dx_{i_1} \wedge \ldots \wedge dx_{i_{q-1}} \in D(A/X_n)^{q-1} \otimes K.$$

Clearly $\mathrm{Res} \circ \tau = \mathrm{id}$. In order to show that $\tau \circ \mathrm{Res}$ is the identity on the cohomology groups one must prove: "If $\omega \in D^q(A\langle X_n^{-1}\rangle^{\dagger}) \otimes K$ satisfies $\mathrm{Res}(\omega) = 0$ and $d\omega \in D^{q+1}(A) \otimes K$ then $\omega = d\eta_o + \eta_1$ with $\eta_o \in D^{q-1}(A\langle X_n^{-1}\rangle^{\dagger}) \otimes K$ and $\eta_1 \in D^q(A) \otimes K$."

We use the notation as above. Every $\mathrm{Res}(b_i) = 0$ and so $b_i = \partial/\partial X_n\,(B_i)$ for some $B_i \in A\langle X_n^{-1}\rangle^{\dagger} \otimes K$. Put $\eta_o = (-1)^{q-1} \sum_{i_1<\ldots<i_{q-1}<n} B_i dx_{i_1} \wedge \ldots \wedge dx_{i_{q-1}}$.

Then $\omega - d\eta_o$ has the form $\sum_{i_1<\ldots<i_q<n} \tilde{a}_i\, dx_{i_1} \wedge \ldots \wedge dx_{i_q}$. Since $d(\omega - d\eta_o)$ lies in $D(A)^{q+1} \otimes K$ it follows that all $\frac{\partial \tilde{a}_i}{\partial X_n} \in A$. Hence all $\tilde{a}_i \in A$.

Remark. We have now established a complete proof of the formula's (1.2) and (1.3) of the introduction. In the following sections we will consider explicit cases of the M.W. Cohomology and we try to explain the connection with work of B. Dwork, N. Katz and others which are often written in a different "language". In particular in §7 we give a proof of B. Dwork's formula for the Zeta function of an elliptic curve in the terminology of the M.W. Cohomology using ideas from N. Katz [9].

## §5. Hypersurfaces.

Let $X \subset \mathbb{P}^n$ be a non-singular hypersurface of degree d defined over a field K of characteristic 0. In the calculation of the de Rham cohomology groups $H^i_{DR}(\mathbb{P}^n - X)$ we follow [8].

According to a theorem of A. Grothendieck we may suppose that $K = \mathbb{C}$ and then $H^i_{DR} = H^i_{sing}(-, \mathbb{C})$. We will write $H^i$ for $H^i_{sing}(-, \mathbb{C})$ for the singular cohomology groups and $H^i_{(c)}$ for the singular cohomology with compact support. We gather some facts about $H^i_{(c)}$ and $H^i$.

(5.1) The exact sequence of a closed subset (in our case).

$$\ldots \longrightarrow H^{q-1}_{(c)}(\mathbb{P}^n - X) \longrightarrow H^{q-1}(\mathbb{P}^n) \longrightarrow H^{q-1}(X) \longrightarrow H^q_{(c)}(\mathbb{P}^n - X) \longrightarrow H^q(\mathbb{P}^n) \longrightarrow H^q(X) \rightarrow \ldots$$

(5.2) $H^i(\mathbb{P}^n) = \mathbb{C}$ if i is even and $0 \leq i \leq 2n$ and $H^i(\mathbb{P}^n) = 0$ for the other values of i.

(5.3) Poincaré duality (in our case): $H^{2n-q}(\mathbb{P}^n - X) \tilde{=} H^q_{(c)}(\mathbb{P}^n - X)'$

(5.4) Lefschetz' theorem $H^q(\mathbb{P}^n) \longrightarrow H^q(X)$ is an isomorphism for $q \leq n-2$ and is injective for $q = n-1$.

(5.5) $H^q(\mathbb{P}^n - X) = 0$ for $q > n$ because $\mathbb{P}^n - X$ is affine and has dimension n.

(5.6) Proposition. $H^q_{DR}(\mathbb{P}^n - X) = 0$ for $q \neq 0, n$.

For even n, the map $H^n_{DR}(\mathbb{P}^n - X) \longrightarrow H^{n-1}_{DR}(X)$ is an isomorphism.

For odd n, $0 \longrightarrow H^n_{DR}(\mathbb{P}^n - X) \longrightarrow H^{n-1}_{DR}(X) \longrightarrow \mathbb{C} \longrightarrow 0$ is exact.

$$\dim H^n_{DR}(\mathbb{P}^n - X) = \frac{d-1}{d}((d-1)^n + (-1)^{n+1})$$

Remark. The first three statements are consequences of (5.1)-(5.5). The calculation of $\dim H^n_{DR}(\mathbb{P}^n - X)$ can be done as in [8]. We note that the case $n = 2$ corresponds to:

the genus g of X is $\frac{(d-1)(d-2)}{2}$ and $H^1_{DR}(X)$ has dimension 2g.

(5.7) We return now to $\overline{X} \subset \mathbb{P}^n_k$, a non-singular hypersurface of degree d, defined by $\overline{f}$, over a the field $k = \mathbb{F}_q$. Let $\overline{A}$ denote the coordinate-ring of the affine open set $\overline{U} = \mathbb{P}^n - \overline{X}$.

Let K denote the quotient field of $R = W(k)$. Then $U = \mathbb{P}^n_K - V(f)$ is open affine and we know its de Rham-cohomology.

We have $\overline{A} = (k[X_o,\ldots,X_n]_{\overline{f}})_o$, $O(U) = (K[X_o,\ldots,X_n]_f)_o$ and $A = (R<X_o,\ldots,X_n,Y>^{\dagger}/(Yf-1))_o$ where $(\ )_o$ means the subring consisting of the homogeneous elements of degree 0. One observes that $O(U)$ is a dense subring of $A \otimes K$. This induces a morphism of complexes $\tau$: $\Omega^{\cdot}(O(U)/K) \longrightarrow D(A) \otimes K$. The first complex defines the de Rham-cohomology groups $H^i_{DR}(U;K)$ and the second one defines the MW groups $H^i(\overline{U};K)$. The map $\tau$ is injective and has dense image. From the papers of N. Katz [8] and P. Monsky [13] one can draw the conclusion that $\tau$ is an isomorphism on the cohomology. No easy proof seems to be available. Assuming that $\tau$ is a quasi-isomorphism, one has:

(i) $H^i(\overline{U};K) = 0$ for $i \neq 0,n$ ; $H^o(\overline{U};K) = K$ and $H^n(\overline{U};K)$ has dimension $\frac{d-1}{d}((d-1)^n + (-1)^{n+1})$

(ii) $Z(\overline{U}/k;t) = (1-q^n t)\det(1 - q^n F_*^{-1} t/H^n(\overline{U};K))^{(-1)^{n+1}}$.

(iii) Since $Z(\overline{U}/k;t)Z(\overline{X}/k;t) = Z(\mathbb{P}^n/k;t) = \prod_{i=o}^{n}(1-q^i t)^{-1}$ one finds an expression for $Z(\overline{X}/k;t)$.
In particular $N_s(\overline{X}) = \frac{q^{(n+1)s}-1}{q^s-1} + (-1)^{n+1}\sum \gamma_i^s$ where $\gamma_1,\ldots,\gamma_\ell$ are essentially the eigenvalues of $F_*$ on $H^n(\overline{U};K)$.

The Zeta function of $\overline{X}/k$ is so determined by the action of some Frobenius on a finite-dimensional vectorspace over K. In the work of B. Dwork [6] also the Frobenius on a finite-dimensional vectorspace $W^s$ determines the Zeta-function. In N. Katz [8] and P. Monsky [13] the connection between the spaces $W^s$, $H^n_{DR}(U)$ and $H^n(\overline{U};K)$ is given in more detail.

(5.8) The trace-formula of Dwork and Reich.

The situation differs slightly from the one in (5.7). Let $\overline{f} \in k[X_o,\ldots,X_n]$, $\overline{f}$ homogeneous of degree d, $k = \mathbb{F}_q$. One wants to count the number of $\mathbb{F}_{q^s}$-rational points of $\overline{U} = \mathbb{P}^n - V(X_o\ldots X_n\ \overline{f})$. The substitution $x_o = 1$ yields

$\overline{U} \cong \mathbb{A}^n - V(X_1\ldots X_n\ \overline{f}(1,X_1,\ldots,X_n))$.

Let $f \in W(k)[X_o,\ldots,X_n]$ be a homogeneous lift of $\bar{f}$. The corresponding w.c.f.g. algebra B is $R<X_1,\ldots,X_n,\frac{1}{X_1\ldots X_n f(1,X_1,\ldots,X_n)}>^{\dagger}$. Then

$$D^s(B) = \sum_{i_1<\ldots<i_s} B\,\frac{dX_{i_1}}{X_{i_1}} \wedge\ldots\wedge \frac{dX_{i_s}}{X_{i_s}} \quad \text{(free B-module)}.$$

The action of F on B is given by $F(X_i) = X_i^q$. We note that

$F(\frac{dX_{i_1}}{X_{i_1}} \wedge\ldots\wedge \frac{dX_{i_s}}{X_{i_s}}) = q^s \frac{dX_{i_1}}{X_{i_1}} \wedge\ldots\wedge \frac{dX_{i_s}}{X_{i_s}}$ and there is similar formula for $\psi$ since

$\psi \circ F = q^n$.

The corresponding zeta-function $Z(\bar{U}/k;t)$ is equal to

$$\prod_{s=o}^{n} \det(1 - t\psi_*/D^s(B) \otimes K)^{(-1)^{s+1}} = \prod_{s=o}^{n} \det(1 - tq^s\psi/B \otimes K)^{\binom{n}{s}(-1)^{s+1}}.$$

Let H denote the hypersurface $V(\bar{f}) \subseteq \mathbb{P}_k^n$ and let $H^{\phi}$ denote the open subset of H consisting of the points where all coordinates are $\neq 0$. Then
$Z(H^{\phi};t) = Z(\bar{U};t)^{-1} Z((\mathbb{P}^n)^{\phi};t)$.
With the notation $[h(t)]^{\delta} = \frac{h(t)}{h(qt)}$ one then finds the trace formula of Dwork and Reich: (see [14]).

$$Z(H^{\phi}/k;t) = [\frac{\det(1 - t\psi_*/B \otimes K)}{(1-t)}]^{(-\delta)^n}.$$

## §6. De Rham cohomology on affinoid spaces.

The field K is supposed to have characteristic zero. An affinoid space X over K can in many cases be embedded in the interior of another affinoid space Y, in notation $X \subset\subset Y$. If X has this property one defines $O(X)^{\dagger} = \varinjlim O(U)$ where U runs in the set of all affinoid spaces with $X \subset\subset U \subseteq Y$. We call $O(X)^{\dagger}$ an overconvergent representation of $O(X)$. The algebra $O(X)^{\dagger}$ has the form $K<t_1,\ldots,t_n>^{\dagger}/(\text{some ideal})$ and $O(X)^{\dagger}$ is dense in $O(X)$.
In analogy with earlier notations $K<t_1,\ldots,t_n>^{\dagger}$ denotes the set of all power series in $t_1,\ldots,t_n$, coefficients in K, converging on a polydisk $\{(t_1,\ldots,t_n) \in K^n \mid |t_1| \leq r_1,\ldots,|t_n| \leq r_n\}$ with all $r_i > 1$. Using $O(X)^{\dagger}$ one defines a de Rham complex $0 \to O(X)^{\dagger} \to \Omega^1(O(X)^{\dagger}) \to \ldots$ and cohomology groups $H^i_{DR}(X)$ which are vectorspaces over K. The groups depend only on X (again by Artin-approximation). For the special case that X is a lift of a non-singular variety $\bar{X}$ over $k = \mathbb{F}_q$ the overconvergent representation $O(X)^{\dagger}$ exists and moreover $H^i_{DR}(X) \cong H^i(\bar{X};K)$.

For more complicated regular affinoid spaces X, the groups $H^i_{DR}(X)$ seem still to have a nice geometric meaning. One result to illustrate is the following proposition which is an extension of a theorem of A. Adolphson. [1].

(6.1) Proposition. Let X be a connected, non-singular, 1-dimensional affinoid space. Then X can be embedded in a complete non-singular curve C such that C - X is the disjoint union of open disks $B_1,\ldots,B_n$. Choose points $a_i \in B_i$ $(i = 1,\ldots,n)$. Then $H^o_{DR}(X) = K$, $\dim H^1_{DR}(X) = 2g + (n-1)$ where g denotes the genus of C and $H^i_{DR}(X) = 0$ for $i > 1$.

Moreover $H^1_{DR}(X)$ coincides with the algebraic de Rham-cohomology group $H^1_{DR}(C - \{a_1,\ldots,a_n\})$.

## §7. The Legendre family of elliptic curves.

Let p be a prime number with $p \neq 2$. Legendre's family in characteristic p is:

$$E = \mathrm{Proj}(R[X_o,X_1,X_2]/(X_2^2X_o - X_1(X_1 - X_o)(X_1 - \lambda X_o))) \longrightarrow \mathrm{Spec}(R)$$

where $R = \mathbb{F}_p[\lambda, \frac{1}{\lambda(1-\lambda)}]$. For every value $\mu(\neq 0,1)$ of $\lambda$ in a finite field $\mathbb{F}_q$ with $q = p^\tau$ the fiber above $\mu$ is the elliptic curve $E_\mu$ over $\mathbb{F}_q$. We write $E^*_\mu = E_\mu - \{\infty\}$ for the corresponding affine curve "$y^2 = x(x-1)(x-\mu)$". In this section we aim at an explicit calculation of the Zetafunction of $E_\mu$. The obvious formula $Z(E_\mu/\mathbb{F}_q;t) = (1-t)^{-1}Z(E^*_\mu/\mathbb{F}_q;t)$ shows that we can restrict our attention to the affine curve $E^*_\mu$. To the latter one can apply the Monsky-Washnitzer cohomology.

(7.1) Proposition. Let K denote the quotient field of $W(\mathbb{F}_q)$. Then $H^o(E^*;K) = K$ and $H^1(E^*;K)$ is a 2-dimensional vectorspace over K. The images of $\frac{dx}{y}$ and $x\frac{dx}{y}$ form a basis of $H^1(E^*_\mu;K)$.

Proof. Let $\underset{\sim}{\mu} \in W(\mathbb{F}_q)$ have residue $\mu \in \mathbb{F}_q$. Put $A = A_{\underset{\sim}{\mu}} = W(\mathbb{F}_q)\langle x,y\rangle^\dagger/(y^2 - x(x-1)(x-\underset{\sim}{\mu}))$. Then $D^1(A) = A\frac{dx}{y}$ is easily seen and one has to show that $d: A \otimes K \longrightarrow (A \otimes K)\frac{dx}{y}$ has kernel K and cokernel $\simeq K^2$. The dense subring $A_\infty = W(\mathbb{F}_q)[X,Y](Y^2 - x(x-1)(x-\underset{\sim}{\mu}))$ of A has the property:
$d = d_\infty: A_\infty \otimes K \longrightarrow (A_\infty \otimes K)\frac{dx}{y}$ has kernel K and a cokernel of dimension 2 represented by $K\frac{dx}{y} + K \times \frac{dx}{y}$. This easily follows from the explicit formula for d, namely $d(a_o(x) + a_1(x)y) = \{a_o^1(x)y + a_1^1(x)x(x-1)(x-\underset{\sim}{\mu}) + a_1(x)(\frac{3}{2}x^2 - (1+\lambda)x + \frac{\lambda}{2})\}\frac{dx}{y}$. In order to compare this with the situation for A we give A some topology.

Let $\rho > 1$ and put $W(\mathbf{F}_q)\langle x,y;\rho^2,\rho^3\rangle$ = the ring of all power series $\Sigma\, a_{n,m} X^n Y^m$ with all $a_{n,m} \in W(\mathbf{F}_q)$ and $\lim |a_{n,m}|\rho^{2n+3m} = 0$. The norm of the power series $\Sigma\, a_{n,m} X^n Y^m$ is denoted by $\| \Sigma\, a_{n,m} X^n Y^m \|_\rho$ and equals $\max|a_{n,m}|\rho^{2n+3m}$. We define $A_\rho = W(\mathbf{F}_q)\langle X,Y;\rho^2,\rho^3\rangle/(y^2 - x(x-1)(x-\underset{\sim}{\mu}))$ and $\| \ \|_\rho$ denotes the induced norm on $A_\rho$. We note that $A_\rho$ and $A_\rho \otimes K$ are complete w.r.t. this norm $\| \ \|_\rho$. If $\rho$ is a rational power of p then $A_\rho \otimes K$ is an affinoid algebra and $\| \ \|_\rho$ is its spectral norm. Now $A = \varinjlim A_\rho = \bigcup_{\rho>1} A_\rho$ is given the direct limit topology. This topology is the strongest one on A such that all the inclusions $A_\rho \hookrightarrow A$ are continuous. In particular, a subset F of A is closed if and only if $F \cap A_\rho$ is closed in $A_\rho$ for all $\rho > 1$. This direct limit topology is also used on $A \otimes K$ and $A \otimes K\frac{dx}{y}$.

We need still another ring, namely $W(\mathbf{F}_q)[\![T]\!]\langle T^{-1}\rangle^\dagger$ = the union of $W(\mathbf{F}_q)[\![T]\!]\langle T^{-1};\rho\rangle$ for all $\rho > 1$, where $W(\mathbf{F}_q)[\![T]\!]\langle T^{-1};\rho\rangle$ consists of all Laurent-series $\sum_{n\in\mathbb{Z}} a_n T^n$ with $a_n \in W(\mathbf{F}_q)$ for all n and $\lim_{n\to-\infty} |a_n|\rho^{-n}) 0$.
On $W(\mathbf{F}_q)[\![T]\!]\langle T^{-1};\rho\rangle$ we use the norm $\| \ \|_\rho^*$ given by

$$\| \sum_{n\in\mathbb{Z}} a_n T^n \|_\rho^* = \max\Big( \max_{n\geq o}|a_n|, \max_{n<o}|a_n|\rho^{-n}\Big).$$

There exists a wellknown embedding $A_\rho \xrightarrow{\varphi} W(\mathbf{F}_q)[\![T]\!]\langle T^{-1};\rho\rangle$ given by $\varphi(X) = T^{-2}$ and $\varphi(Y) = T^{-3}\sqrt{(1-T^2)(1-\underset{\sim}{\mu}T^2)}$.

(7.2) Lemma. For $f \in A_\rho$ and $\varphi(f) = \Sigma\, c_n T^n$ one has $\|f\|_\rho = \|\varphi(f)\|_\rho^*$ and moreover $\|\varphi(f)\|_\rho^* = \max_{n\leq o}(|c_n|\rho^{-n})$.

Proof. f can uniquely be written as $\sum_{n\geq o} a_n X^n + \sum_{n\geq o} a'_n X^n Y$ with all $a_n, a'_n \in W(\mathbf{F}_q)$. Then $\|f\|_\rho = \max(\max|a_n|\rho^{2n}, \max|a'_n|\rho^{2n+3})$. For $\varphi(f)$ one finds the formula $\varphi(f) = \Sigma\, a_n T^{-2n} + \Sigma\, a'_n T^{-2n-3}\sqrt{(1-T^2)(1-\underset{\sim}{\mu}T^2)}$. The development of $\sqrt{(1-T^2)(1-\underset{\sim}{\mu}T^2)}$ uses only positive, even powers of T. From this the statements follow easily.

(7.3) Lemma. The image of $d: A \otimes K \longrightarrow (A \otimes K)\frac{dx}{y}$ is closed.

Proof. According to the definition of the topology on $(A \otimes K)\frac{dx}{y}$, one has to prove the following statement: "Let $\omega_m = d(f_m)$ be a sequence in $(A_\rho \otimes K)\frac{dx}{y}$ converging to $w \in (A_\rho \otimes K)\frac{dx}{y}$ w.r.t. the norm $\| \ \|_\rho$. Then $\omega = d(f)$ for some $f \in A \otimes K$".

In proving this we may suppose that $\varphi(f_m) \in W(\mathbf{F}_q)[\![T]\!]\langle T^{-1}\rangle^\dagger \otimes K$ has no

constant term. So $\varphi(f_m) = \sum_{n \neq o} f_m(n)T^n$. Then $\omega_m$ has image $\varphi(\omega_m) = d(\varphi(f_m)) =$ $\Sigma n\, f_m(n)T^{n-1}dT$. Choose a $\rho_1$ with $1 < \rho_1 < \rho$. Then $\|f_m\|\rho_1 =$

$= \sup_{n<o} |f_m(n)|\rho_1^{-n} = \sup_{n<o} (|n\, f_m(n)|\rho^{-n})(\frac{1}{|n|}(\frac{\rho_1}{\rho})^{-n}) \leq C\|w_n\|\rho$ where the constant C depends only on $\rho$ and $\rho_1$. In particular $f_m \in A\rho_1 \otimes K$ and the sequence $\{f_m\}$ is a Cauchy-sequence w.r.t. $\| \|\rho_1$. The limit $f = \lim f_m$ lies in $A\rho_1 \otimes K$ and satisfies $d(f) = \omega$.

End of the proof of (7.1). The cokernel $H^1(E_\mu^*;K)$ of d is given the induced topology. It is a Hausdorff space for this topology according to (7.3). Let H denote the cokernel of $d_\infty$: $A_\infty \otimes K \longrightarrow (A_\infty \otimes K)\frac{dx}{y}$. The obvious map $\tau$: $H \longrightarrow H^1(E_\mu^*;K)$ has dense image L. The vectorspace L is finite-dimensional. The topology on L induced by the topology of $H^1(E_\mu^*;K)$ is the usual topology on L since it is a Hausdorff-topology. For this topology L is complete and so $L = H^1(E_\mu^*;K)$ and $\tau$ is surjective. The remaining steps in the proof of (7.1) are now rather easy. One has to show that $\tau$ is also injective. This means that $d(f) = \omega$ with $\omega \in (A_\infty \otimes K)\frac{dx}{y}$ implies that $f \in A_\infty \otimes K$. This follows from the observation that $f \in A \otimes K$ lies in $A_\infty \otimes K$ if and only if $\varphi(f) \in (W(\mathbb{F}_q)[\![T]\!] < T^{-1} >^+) \otimes K$ lies in $W(\mathbb{F}_q)[\![T]\!][T^{-1}] \otimes K$.

(7.4) Remarks. The action of the Frobenius map $F_*^\tau$ on $H^o(E_\mu^*;K)$ is the identity. We lack an explicit formula for the action of $F_*^\tau$ on $H^1(E_\mu^*;K)$. From duality of $H^1(E_\mu^*;K)$ one obtains that the two eigenvalues $a_1, a_2 \in W(\mathbb{F}_q)$ of $F_*^\tau$ on $H^1(E_\mu^*;K)$ have the property $a_1 a_2 = q$. The zeta-function must then have the form:

$$Z(E_\mu^* | \mathbb{F}_q;t) = \frac{(1-a_1t)(1-a_2t)}{(1-qt)} = \frac{1-at+qt^2}{(1-qt)} \quad \text{where } p = p^\tau.$$

Further $a = q - N_1^*$ where $N_1^*$ is the number of points of $E_\mu$ in $\mathbb{F}_q$. In the sequel of this section we determine first the value of a modulo p. By "varying $\mu$" we will then find the explicit formula of B. Dwork for $a, a_1, a_2$ as functions of $\mu$.

(7.5) Proposition. $a \equiv (-1)^{\frac{q-1}{2}} H(\mu)H(\mu^p)\ldots H(\mu^{p^{\tau-1}})$ modulo p, where H denotes the polynomial $H(X) = \sum_{r=o}^{p-1} \binom{\frac{p-1}{2}}{r}^2 X^r$ and where $q = p^\tau$.

Proof. We have chosen for the elementary proof given in [5]. We have already seen in (7.4) that $a = q - N_1^*$ where $N_1^*$ is the number of solutions of $y^2 = x(x-1)(x-\mu)$ over $\mathbb{F}_q$. One has

$N_1^* = \#\{(0,0),(1,0),(\mu,0)\} + 2\ \#\{x \in \mathbb{F}_q \mid x \neq 0,1,\mu \text{ and } x(x-1)(x-\mu) \text{ is a square in } \mathbb{F}_q\}$.

Hence $N_1^* \equiv \sum_{x \in \mathbb{F}_q} (1 + (x(x-1)(x-\mu))^{\frac{q-1}{2}})$ modulo p. Using the elementary formula:

$\sum_{x \in \mathbb{F}_q} x^k = -1$ if $(q-1 \mid k$ and $k \geq 1)$ and $= 0$ for the other values of k. This gives

$a \equiv$ the coefficient of $X^{q-1}$ in $(X(X-1)(X-\mu))^{\frac{q-1}{2}}$ modulo p. Write

$(X(X-1)(X-\mu))^{\frac{p-1}{2}} = \sum_{i=0}^{3\frac{p-1}{2}} a_i X^i$. Then $a_{p-1} = a_{p-1}(\mu) = (-1)^{\frac{p-1}{2}} \sum_{r=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{r}^2 \mu^r = (-1)^{\frac{p-1}{2}} H(\mu)$

Further $(X(X-1)(X-\mu))^{\frac{q-1}{2}} = ((X(X-1)(X-\mu))^{\frac{p-1}{2}})^{1+p+p^2+\ldots+p^{\tau-1}}$ and this leads easily to the computation of the coefficient of $X^{q-1}$. Namely

$(-1)^{\frac{q-1}{2}} H(\mu)H(\mu^p) \ldots H(\mu^{p^{\tau-1}})$.

(7.6) Remarks and notations. The polynomial $H(X)(-1)^{\frac{p-1}{2}}$ represents the $1 \times 1$-Hasse-Witt matrix of the elliptic curve. In particular $E_\mu$ is supersingular if and only if $H(\mu) = 0$. ([16 p.333]). From (7.5) it follows that $a \equiv 0$ mod p holds for a supersingular $E_\mu$. In fact one can show that $a = 0$ holds for any supersingular curve and so its zeta-function is known in this case. In the sequel we will exclude the supersingular values $\mu$. If $\mu$ is not supersingular then the two eigenvalues $a_1, a_2$ of $F_*^\tau$ have the property $a_1 a_2 = q$ and $|a_1 + a_2| = 1$. So one of the eigenvalues has absolute value 1. This eigenvalue is called the "unit root of $E_\mu$" and denotee by $\omega(\mu)$. The other eigenvalue is $q\omega(\mu)^{-1}$. So

$$Z(E_\mu;t) = \frac{(1-\omega(\mu)t)(1-q\omega(\mu)^{-1}t)}{(1-t)\quad(1-qt)}.$$

It seems rather hopeless to find an explicit expression for the action of $F_*^\tau$ on $H^1(E_\mu^*;K)$. Instead, one considers not a single curve but the whole family of affine curves excluding the supersingular ones. This family is:

$$\mathrm{Spec}(R[X,Y]/Y^2 - X(X-1)(X-\lambda))) \longrightarrow \mathrm{Spec}(R) \text{ where } R = \mathbb{F}_p[\lambda, \frac{1}{\lambda(1-\lambda)H(\lambda)}].$$

This family is lifted to characteristic zero in the following way:

$$\mathrm{Spec}(B\langle X,Y\rangle^+/(Y^2 - X(X-1)(X-\lambda))) \longrightarrow \mathrm{Spec}(B) \text{ where}$$

$B = \mathbb{Z}_p\langle \lambda, \frac{1}{\lambda(1-\lambda)H(\lambda)}\rangle =$ the p-adic completion of $\mathbb{Z}[\lambda, \frac{1}{\lambda(1-\lambda)H(\lambda)}]$.

The algebra $B \hat{\otimes} Q_p$ is the algebra of holomorphic functions on the subset V of $Q_p$ given by the inequalities $|\lambda| \leq 1$ and $|\lambda(1-\lambda)H(\lambda)| \geq 1$. The affinoid subspace V of $Q_p$ is equal to the unit disk where one has deleted $(2+\frac{p-1}{2})$ open disks of radic 1. The deleted disks are: the two singular disks $B(0,1^-), B(1,1^-)$ and the $\frac{p-1}{2}$ super-singular disks $B(a_1,1^-), \ldots, B(a_{\frac{p-1}{2}},1^-)$. The numbers $a_1,\ldots,a_{\frac{p-1}{2}}$ in the algebraic closure of $Q_p$ are the zero's of $H(\lambda)$. Using the remark of Igusa that $H(\lambda)$ satisfies modulo p the hypergeometric differential equation $\lambda(1-\lambda)H''(\lambda)+(1-2\lambda)H'(\lambda)-\frac{1}{4}H(\lambda) \equiv 0 \pmod{p}$ one can conclude that the residues of $a_1,\ldots,a_{\frac{p-1}{2}}$ in the algebraic closure of $\mathbb{F}_p$ are distinct. This means that our $2+\frac{p-1}{2}$ excluded disks are distinct. We write A for the "overconvergent" algebra $B\langle X,Y\rangle^{\dagger}/(Y^2 - X(X-1)(X-\lambda))$. The module D(A/B) of continuous differentials of A over B is easily identified with $A\frac{dx}{y}$. The next main step in our treatment of the Legendre-family is a relative version of (7.1).

(7.7) Proposition. The kernel of $d: A \hat{\otimes} Q_p \longrightarrow A \hat{\otimes} Q_p \frac{dx}{y}$ is equal to $B \hat{\otimes} Q_p$. The cokernel is a free $B \hat{\otimes} Q_p$-module of rank two. The images of $\frac{dx}{y}$ and $x\frac{dx}{y}$ form a free basis over $B \hat{\otimes} Q_p$.

Proof. We follow closely the proof of (7.1). One embeds A into $B[\![T]\!]\langle T^{-1}\rangle^{\dagger}$ by $\varphi(x) = T^{-2}$ and $\varphi(y) = T^{-3}\sqrt{(1-T^2)(1-\lambda T^2)}$. Put $A_\infty = B[X,Y]/Y^2 - X(X-1)(X-\lambda)$. An element $f \in A$ belongs to $A_\infty$ if and only if $\varphi(f) \in B[\![T]\!][T^{-1}]$. This shows already that $B \hat{\otimes} Q_p$ is the kernel of d. The cokernel of $d_\infty: A_\infty \hat{\otimes} Q_p \longrightarrow A_\infty \hat{\otimes} Q_p \frac{dx}{y}$ is easily seen to be a free $B \hat{\otimes} Q_p$-module of rank two with as generators the images of $\frac{dx}{y}$ and $x\frac{dx}{y}$. The map $(B \hat{\otimes} Q_p)\frac{dx}{y} + (B \hat{\otimes} Q_p)x\frac{dx}{y} \longrightarrow \operatorname{coker}(d)$ is injective and its image L is dense. As in the lemmata (7.2) and (7.3) one shows that im(d) is a closed $B \hat{\otimes} Q_p$-submodule of $A \hat{\otimes} Q_p \frac{dx}{y}$. The induced topology on coker(d) makes coker(d) into a Hausdorff, topological $B \hat{\otimes} Q_p$-module. On L one finds an induced structure of a Hausdorff topological $B \hat{\otimes} Q_p$-module. It is well known that any finitely generated module M over an affinoid algebra C carries a unique structure as Hausdorff, topological C-module. Moreover M is complete w.r.t. this topology. This implies $L = \operatorname{coker}(d)$.

(7.8) Remarks and notations. The use of the direct limit topology in the proof (7.7) and (7.1) can be avoided. It could be replaced by an estimation of the following form: "For every $n \geq 0$ there are $a_n, b_n \in Q_p[\lambda]$ and $z_n(x) \in Q_p[x,\lambda]$ such that $x^n\frac{dx}{y} = (a_n + b_n x)\frac{dx}{y} + d(y.z_n(x))$. The Gauss-norms $\|a_n\|, \|b_n\|$ and $\|z_n(x)\|$ are such that for every $r, 0 < r < 1$, $\lim \|a_n\| r^n = \lim \|b_n\| r^n = \lim \|z_n(x)\| r^n = 0$". A direct proof of this estimate seems rather difficult.

Let us write $H^1$ for the cokernel of $d: A \otimes Q_p \longrightarrow A \otimes Q_p \frac{dx}{y}$. Let $\mu \in \mathbf{F}_q$, $\mu \neq 0,1,\mu$ not supersingular and let $\underset{\sim}{\mu} \in W(\mathbf{F}_q)$ have residue $\mu$. Substitution of $\underset{\sim}{\mu}$ for $\lambda$ is a map $B \otimes Q_p \longrightarrow K$ = the quotient field of $W(\mathbf{F}_q)$. This substitution changes the exact sequence of (7.7):

$$0 \longrightarrow B \otimes Q_p \longrightarrow A \otimes Q_p \xrightarrow{d} A \otimes Q_p \frac{dx}{y} \longrightarrow H^1 \longrightarrow 0$$

into the exact sequence of (7.1):

$$0 \longrightarrow K \longrightarrow A_{\underset{\sim}{\mu}} \otimes K \xrightarrow{d} A_{\underset{\sim}{\mu}} \otimes K \frac{dx}{y} \longrightarrow H^1(E_\mu^*;K) \longrightarrow 0,$$

in which

$$A_{\underset{\sim}{\mu}} = W(\mathbf{F}_q) < X,Y >^\dagger / (y^2 - x(x-1)(x-\underset{\sim}{\mu})). \text{ So } H^1 \otimes K = H^1(E_\mu^*;K).$$

(7.9) The Frobenius map on $H^1$.

Let us fix an endomorphism $\varphi$ of B of the form $\varphi(\lambda) \equiv \lambda^p \bmod p\,B$. Using that A/B is smooth one finds an endomorphism $F: \hat{A} \longrightarrow \hat{A}$ with $\hat{A} = B< X,Y >/(Y^2 - X(X-1)(X-\lambda))$; $F/B = \varphi$; $F(z) \equiv z^p \bmod p\,\hat{A}$.

Using (2.4.3), a consequence of Artin-approximation, one sees that F can be chosen such that $F(A) \subseteq A$. Then F acts on $A \otimes Q_p$, $A \otimes Q_p \frac{dx}{y}$ and $H^1$. The action $F_*$ of F on $H^1$ is $\varphi$-linear which means that $F_*(bm) = \varphi(b)F_*(m)$ for any $b \in B \otimes Q_p$ and $m \in H^1$. For $\mu \in \mathbf{F}_q$, $\mu(1-\mu)H(\mu) \neq 0$, $q = p^\tau$, there exists a unique choice $\underset{\sim}{\mu} \in W(\mathbf{F}_q)$ with residue $\mu$ and such that $\varphi^\tau(\underset{\sim}{\mu}) = \underset{\sim}{\mu}$. Then $F_*^\tau$ on $H^1$ induces the canonical action of $F_*^\tau$ on the Monsky-Washnitzer cohomology group $H^1 \otimes K = H^1(E_\mu^*;K)$.

(7.10) The differential equation on $H^1$.

Let $D^1(A)$ denote the module of continuous differentials of A over $\mathbb{Z}_p$. The A-module $D^1(A)$ is generated by $\{dx,dy,d\lambda\}$ and these generators satisfy the equation: $(-3x^2 + 2(1+\lambda)x - \lambda)dx + 2ydy + (x^2 - x)d\lambda = 0$ (i.e. $d(y^2 - x(x-1)(x-\lambda)) = 0$). Let $P,Q \in B[X]$ denote the polynomials of degree 1 and 2 having the property

$$x(x-1)(x-\lambda)P + \frac{3x^2-2(1+\lambda)x+\lambda}{2} Q = 1.$$

Then $d\lambda$ and $\tau = Py\,dx + Qdy$ are free generators of $D^1(A)$. Indeed $dx = y\tau + Q\frac{x(x-1)}{2}d\lambda$ and $dy = \frac{3x^2-2(1+\lambda)x+\lambda}{2}\tau - P\frac{x(x-1)y}{2}d\lambda$. One has the usual de Rham complex:

$$0 \longrightarrow A \otimes Q_p \xrightarrow{d^0} D^1(A) \otimes Q_p \xrightarrow{d^1} D^2(A) \otimes Q_p \longrightarrow 0.$$

We note that $D^2(A)$ is a free A-module with generator $d\lambda \wedge \tau$; that $D^1(A/B) \cong D^1(A)/Ad\lambda \cong A\frac{dx}{y}$; the image of $\tau$ in $D^1(A/B)$ is $\frac{dx}{y}$; that the map $D^1(A/B) \longrightarrow D^2(A)$ given by $\eta \longmapsto d\lambda \wedge \eta$ is an isomorphism. From this one obtains a "connection" $D: H^1 \longrightarrow H^1$, i.e. D is additive and $D(bm) = bD(m) + \frac{db}{d\lambda}m$ for $m \in H^1$ and and $b \in B \otimes Q_p$. We define D first as a mapping: $D^1(A/B) \longrightarrow D^1(A/B) = A\frac{dx}{y}$ by the formula $D(a\frac{dx}{y}) = L(a)\frac{dx}{y}$ with a, $L(a) \in A$ where L(a) is given by the equation $d^1(a\tau) = L(a)d\lambda \wedge \tau$.

D maps exact froms to exact forms. So D induces a mapping: $H^1 \longrightarrow H^1$ which is also denoted by D. We remark that the action of D on $D^1(A/B)$ depends on the choice of the basis of $D^1(A)$ and that the action of D on $H^1$ does not depend on this choice. The mapping $D: H^1 \longrightarrow H^1$ is called the Gauss-Manin connection of the family of curves.

(7.11) Explicit formula's for D and $F_*$.

Proposition. Let $\omega \in H^1$ denote the image of $\frac{dx}{y}$ in $H^1$. Then:

(i) $\{\omega, D(\omega)\}$ is a free basis of $H^1$.

(ii) $\lambda(1-\lambda)D^2(\omega) + (1-2\lambda)D(\omega) - \frac{1}{4}\omega = 0$.

(iii) Let C be a ring-extension of $B \otimes Q_p$ which carries an extension of $\frac{d}{d\lambda}$. Then $\eta \in H^1 \otimes C$ satisfies $D(\eta) = 0$ if and only if $\eta$ has the form $\eta = \lambda(1-\lambda)\frac{df}{d\lambda}\omega - \lambda(1-\lambda)fD(\omega)$ where $f \in C$ satisfies the hypergeometric differential equation $(1-\lambda)\frac{d^2f}{d\lambda} + (1-2\lambda)\frac{df}{d\lambda} - \frac{1}{4}f = 0$.

(iv) $DF_* = \frac{d\varphi(\lambda)}{d\lambda} F_*D$ holds on $H^1$. In particular for any C as in (iii), $\ker(D, H^1 \otimes C)$ is invariant under $F_*$.

(v) The free B-submodule H of $H^1$ generated by $\omega$ and $D(\omega)$ is invariant under D and $F_*$.

(vi) The matrix $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ of $F_*$ with respect to the basis $\{\frac{dx}{y}, x\frac{dx}{y}\}$ of H has the property $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \equiv \begin{pmatrix} 0 & ? \\ 0 & (-1)^{\frac{p-1}{2}} H(\lambda) \end{pmatrix}$ modulo p H.

Proof. In principal one could use the definitions in (7.10) in order to obtain the formula's above. However, it is easier to replace A by $\tilde{A} = B\langle X, Y, Y^{-1}\rangle^+/(y^2 - x(x-1)(x-\lambda))$ for the calculations. As in (7.7) one shows that the cokernel of $d: \tilde{A} \otimes Q_p \longrightarrow D^1(\tilde{A}/B) \otimes Q_p$ is a free $B \otimes Q_p$-module on the basis $\frac{dx}{y}, x\frac{dx}{y}, \frac{dx}{x}, \frac{dx}{x-1}$ and $\frac{dx}{x-\lambda}$. Let us write $\tilde{H}^1$ for this cokernel. Also on $\tilde{H}^1$

one has a connection D and a $\varphi$-linear endomorphism $F_*$. These two mappings coincide with D and $F_*$ on the direct summand $H^1$ of $\widetilde{H}^1$. Explicit formula's for D, F on $\widetilde{A}$ are:

($\alpha$) Let $\frac{\partial}{\partial\lambda}$ denote the derivation on $\widetilde{A}$ given by $\frac{\partial}{\partial\lambda}(\lambda) = 1$, $\frac{\partial}{\partial\lambda}(x) = 0$ and

$\frac{\partial}{\partial\lambda}(y) = \frac{-x(x-1)}{2y} = \frac{-y}{x-\lambda}$. Then $D(adx) = \frac{\partial}{\partial\lambda}(a)dx$ holds for $a \in \widetilde{A} \otimes Q_p$

($\beta$) $F: \widetilde{A} \longrightarrow \widetilde{A}$ can be given by $F(\lambda) = \varphi(\lambda)$, $F(x) = x^p$ and

$F(y) = y^p \left(1 + \frac{x^p(x^p-1)(x^p-\varphi(\lambda)) - y^{2p}}{y^{2p}}\right)$. This expression lies in $\widetilde{A}$ since

$x^p(x^p-1)(x^p-\varphi(\lambda)) - y^{2p} \in p\,\widetilde{A}$.

(i) In $D^1(\widetilde{A}/B)$ one has the formula's

$$D\left(\frac{dx}{y}\right) = \frac{1}{2(x-\lambda)}\frac{dx}{y} = \frac{-1}{2(\lambda-1)}\frac{dx}{y} + \frac{1}{2\lambda(\lambda-1)}\,x\,\frac{dx}{y} + d\left(\frac{-1}{\lambda(\lambda-1)}\frac{y}{x-\lambda}\right)$$

$$D\left(x\,\frac{dx}{y}\right) = \frac{-1}{2(\lambda-1)}\frac{dx}{y} + \frac{1}{2(\lambda-1)}\,x\,\frac{dx}{y} + d\left(\frac{-1}{\lambda-1}\frac{y}{x-\lambda}\right).$$

This shows that $\{\omega, D(\omega)\}$ form a basis of $H^1$ since we know that $\{\frac{dx}{y}, x\,\frac{dx}{y}\}$ is a basis.

(ii) follows easily from the formula's in (i)

(iii) Easy calculation.

(iv) We verify this again on $\widetilde{H}^1$. There $DF_*(adx) = \frac{\partial}{\partial\lambda}(F(a))p\,x^{p-1}dx$ and $F_*D(a\,dx) = F\left(\frac{\partial}{\partial\lambda}(a)\right)p\,x^{p-1}dx$. The required equality is easily verified for $a = \lambda, x, y^2$. Then it holds also for y and finally for all elements $a \in \widetilde{A}$.

(v)(vi) An explicit calculation is possible but rather complicated. It is easier to remark that $H \otimes B/pB$ is the de Rham-cohomology of the family

$$\mathrm{Proj}\left(\mathbb{F}_p\left[\lambda, \frac{1}{\lambda(1-\lambda)H(\lambda)}\right][X,Y,Z]/ZY^2 - X(X-Z)(X-\lambda Z)\right) \longrightarrow \mathrm{Spec}\left(\mathbb{F}_p\left[\lambda, \frac{1}{\lambda(1-\lambda)H(\lambda)}\right]\right).$$

The action of Frobenius on $H \otimes B/pB$ is know to have the matrix

$$\begin{pmatrix} 0 & ? \\ 0 & (-1)^{\frac{p-1}{2}} H(\lambda) \end{pmatrix}$$ with respect to the basis $\frac{dx}{y}$ and $x\,\frac{dx}{y}$.

This explains parts (v),(vi). Another possibility would be to evaluate the matrix at values $\mu$ for $\lambda$ and to use (7.9),(7.8) and (7.5).

(7.12) Proposition. There exists a unique direct summand U of the B-module H with $F_*(U) = U$. (U is called the unit root part of H)

Proof. Consider the subset $V = \{a = \alpha\omega - \lambda(1-\lambda)D(\omega) \mid \alpha \in B\}$ of H and the map $S: V \longrightarrow V$ given by $S(a) = -\lambda(1-\lambda)\delta^{-1}F_*(a)$ where $F_*(a) = \gamma\omega + \delta D(\omega)$. Then S is a contraction and has a unique fixed point $a = \beta\omega - \lambda(1-\lambda)D(\omega)$. Then $U = Bu$ is the unique direct summand of H with $F_*(U) = U$.

(7.13) We write $F_*(u) = \xi u$ with $\xi \in B^*$. Then $F_*^\tau(u) = \xi\varphi(\xi)\ldots\varphi^{\tau-1}(\xi)u$. For a value $\mu \in \mathbb{F}_q$, with $\mu(1-\mu)H(\mu) \neq 0$, we denote by $\underset{\sim}{\mu} \in W(\mathbb{F}_q)$ the unique element with $\varphi^\tau(\underset{\sim}{\mu}) = \underset{\sim}{\mu}$ and $\underset{\sim}{\mu}$ has residue $\mu$. (Again $q = p^\tau$).
Evaluating at $\underset{\sim}{\mu}$ as in (7.8) one finds that the two eigenvalues $\omega(\mu)$ and $q\omega(\mu)^{-1}$ of $F_*^\tau$ acting on $H^1(E_\mu^*;K)$ are given by

$$\omega(\mu) = \xi\varphi(\xi)\ldots\varphi^{\tau-1}(\xi)(\underset{\sim}{\mu}).$$

In order to make this explicit we have to determine the function $\xi$. We note that $\xi$ depends on the choice of $\varphi$. In the following theorem we will make the choice $\varphi(\lambda) = \lambda^p$.

(7.14) Theorem (B. Dwork)

(i) The function $\xi$ extends to a holomorphic and invertible function on the affinoid set $\{\lambda \in Q_p \mid |\lambda| \leq 1 \text{ and } |H(\lambda)| = 1\}$. On the open disc $\{\lambda \in Q_p \mid |\lambda| < 1\}$ one has the equality $\xi = (-1)^{\frac{p-1}{2}} \frac{\alpha(\lambda)}{\alpha(\lambda^p)}$ where $\alpha(\lambda) = F(\frac{1}{2},\frac{1}{2};1;\lambda)$ is the hypergeometric function.

(ii) The element $\eta \in B$ given by $D(u) = \eta u$ extends to a holomorphic function on the affinoid set $\{\lambda \in Q_p \mid |\lambda| \leq 1 \text{ and } |H(\lambda)| = 1\}$. On the open disc $\{\lambda \in Q_p \mid |\lambda| < 1\}$ one has the equality $\eta = -\frac{\alpha'(\lambda)}{\alpha(\lambda)}$.

(iii) $Z(E_\mu \mid \mathbb{F}_q; t) = (1-t)^{-1}(1-qt)^{-1}(1-(-1)^{\frac{q-1}{2}}\frac{\alpha(\underset{\sim}{\mu})}{\alpha(\underset{\sim}{\mu}^q)}t)(1-(-1)^{\frac{q-1}{2}}q\frac{\alpha(\underset{\sim}{\mu})^q}{\alpha(\underset{\sim}{\mu})}t)$

in which $\underset{\sim}{\mu} \in W(\mathbb{F}_q)$ has residue $\mu; \underset{\sim}{\mu}^q = \underset{\sim}{\mu}$ and $\frac{\alpha(\lambda)}{\alpha(\lambda)^q}$ denotes the extension of this function to $\{\lambda \in Q_p \mid |\lambda| \leq 1 \text{ and } |H(\lambda)| = 1\}$.

Proof. Consider the ring-extension $B \subset B_o = \mathbb{Z}_p[\lambda]\langle\lambda^{-1}\rangle =$ the set of all Laurent series $\sum_{n\in\mathbb{Z}} a_n \lambda^n$ with $a_n \in \mathbb{Z}_p$ and $\lim_{n\to-\infty} a_n = 0$. We note that $B_o$ is a complete discrete valuationring with maximal ideal $p\,B_o$ and residue field $\mathbb{F}_p((\bar{\lambda}))$.

On $H_o = H \otimes_B B_o$ we have again the action of $F_*$ and $D$.

The element $z = \lambda(1-\lambda)\alpha'\omega - \lambda(1-\lambda)\alpha D(\omega)$ satisfies $D(z) = 0$. Moreover $\ker(D \text{ on } H_o) = \mathbb{Z}_p z$. From $DF_* = p\lambda^{p-1}F_*D$ on concludes that $F_*(z) = cz$ for some $c \in \mathbb{Z}_p^*$. Then $F_*(B_o z) = B_o z$ and according to (7.12) (the unicity holds also for $B_o$) $z = \alpha u$.

Then $\xi(\lambda) = c\,\dfrac{\alpha(\lambda)}{\alpha(\lambda)^p}$ and $\eta(\lambda) = \dfrac{\alpha'(\lambda)}{\alpha(\lambda)}$ hold in $B_o$. The Mittag-Leffler decomposition of the elements $\xi, \eta \in B$ show that $\xi, \eta$ extend to $\{\lambda \mid |\lambda| < 1\}$. The symmetry of the differential equation implies that $\xi$ and $\eta$ extend also to $\{\lambda \mid |\lambda - 1| < 1\}$. We still have to show that $c = (-1)^{\frac{p-1}{2}}$. This follows from an evaluation of $F_*$ and $\xi$ at $\lambda = 0$.

Finally we remark that $(-1)^{\frac{p-1}{2}}\xi(\lambda)$ has the form $\sum_{n=o}^{\infty} a_n \lambda^n$, $a_n \in \mathbb{Z}_p$, $a_o = 1$ and that the infinite product $\prod_{m=o}^{\infty}((-1)^{\frac{p-1}{2}}\xi(\lambda^{p^m}))$ converges coefficientwise to $\alpha(\lambda) = F(\tfrac{1}{2}, \tfrac{1}{2}; 1; \lambda)$.

(7.15) A further study of the hypergeometric differential equation with parameters $\frac{1}{2}, \frac{1}{2}, 1$.

Theorem (B. Dwork).
In an ordinary disc $\{\lambda \mid |\lambda - \lambda_o| < 1\}$ where $\lambda_o^q = \lambda_o$ and $|\lambda_o(1-\lambda_o)H(\lambda_o)| = 1$ the differential equation $\lambda(1-\lambda)f'' + (1-2\lambda)f' - \frac{1}{4}f = 0$ has two independent convergent solutions $f_{\lambda_o}, g_{\lambda_o}$. They have the properties:

(i) $f_{\lambda_o} \in 1 + (\lambda - \lambda_o)W(\mathbb{F}_q)[\![\lambda - \lambda_o]\!]$.

(ii) $g_{\lambda_o} \in K[\![\lambda - \lambda_o]\!]$, where $K = Qt(W(\mathbb{F}_q))$ has radius of convergence 1. The function $g_{\lambda_o}$ is unbounded and has logarithmic growth, i.e.

$$\|g_{\lambda_o}\|_{|\lambda-\lambda_o| \le \rho} \le C \left\|\log \frac{\lambda}{\lambda_o}\right\|_{|\lambda-\lambda_o| \le \rho}$$ for some constant $C$ and all $\rho < 1$.

(iii) $f'_{\lambda_o}/f_{\lambda_o} = -\eta$

(iv) $$\frac{f_{\lambda_o}(\lambda)}{f_{\lambda_o}(\lambda^q)} = \omega(\bar{\lambda}_o)^{-1}\xi(\lambda)\xi(\lambda^p)\ldots\xi(\lambda^{p^{\tau-1}}).$$

Proof. We consider the ring extension $B \subset B_{\lambda_o} = W(\mathbb{F}_q)[\![\lambda - \lambda_o]\!]$ and the corresponding $H_{\lambda_o} = H \otimes_B B_{\lambda_o}$ with the action of $D$ and $F_*^\tau$.

The element $\xi(\lambda) = w(\overline{\lambda}_o)^{-1}\xi(\lambda)\xi(\lambda^p)\ldots\xi(\lambda^{p^{\tau-1}}) \in B$ has development $\sum_{n\geq o} a_n(\lambda-\lambda_o)^n$, $a_n \in W(\mathbb{F}_q)$, $a_o = 1$ in $B_{\lambda_o}$. The infinite product $\alpha(\lambda) = \prod_{m=o}^{\infty} \zeta(\lambda^{q^m})$ converges coefficientswise in $B_{\lambda_o}$. Then $\alpha(\lambda) = \zeta(\lambda)\alpha(\lambda^q)$ and $F_*^\tau(\alpha u) = w(\overline{\lambda}_o)\alpha u$. From $DF_* = p\lambda^{p-1}F_*D$ it follows that $D(\alpha u) = 0$. Then $f_{\lambda_o} = \alpha$ satisfies (i),(iii) and (iv). Let $K\{\lambda-\lambda_o\}$ denote the ring of convergent power series over K. Again we have an action of D and $F_*$ on $\widetilde{H}_{\lambda_o} = H \otimes_B K\{\lambda-\lambda_o\}$. Since $\lambda_o$ is a regular point for the differential equation we find a 2-dimensional vector space over K of solutions: $\ker(D \text{ on } \widetilde{H}_{\lambda_o}) = V$. This vectorspace is invariant under $F_*^\tau$. The eigenvalues of $F_*^\tau$ on V are $c_1 = w(\overline{\lambda}_o)$ and $c_2 = qw(\overline{\lambda}_o)^{-1}$. Let $e_i = \lambda(1-\lambda)f_i'\omega - \lambda(1-\lambda)f_iD(\omega)$ $(i = 1,2)$ denote the corresponding eigenvectors. Then $f_{\lambda_o} = f_1$ and $g_{\lambda_o} = f_2$. The action of $F_*^\tau$ can be given by the matrix

$$F_*^\tau(\lambda(1-\lambda)\omega) = a\ \lambda(1-\lambda)\omega + b(-\lambda(1-\lambda)D(\omega))$$

$$F_*^\tau(-\lambda(1-\lambda)D(\omega)) = c\ \lambda(1-\lambda)\omega + d(-(1-\lambda)D(\omega))$$

with $a,b,c,d \in B_{\lambda_o}$. This implies in particular that $f_2 = c_2^{-1}(b\,\varphi^\tau(f_2') + d\,\varphi^\tau(f_2))$

The action of $\varphi^\tau$ on $K\{\lambda-\lambda_o\}$ is given by $\varphi^\tau(\Sigma\, a_n(\lambda-\lambda_o)^n) = \Sigma\, a_n(\lambda^q-\lambda_o)^n$. This suffices to show that $f_2$ has radius of convergence 1 and that $f_2$ is unbounded. For the calculation it is easier to make another choice of $\varphi^\tau$, namely $\varphi^\tau(\lambda-\lambda_o) = (\lambda-\lambda_o)^q$. This makes no essential changes in the calculations above. With the notation $t = (\lambda-\lambda_o)$ one has the formula:

$$f_2(t) = q^{-1}w(\overline{\lambda}_o)(b(t)f_2'(t^q) + d(t)f_2(t^q)) \text{ where } b \in pW(\mathbb{F}_q)[\![t]\!]$$

and $d(t) \in W(\mathbb{F}_q)[\![t]\!]^*$. Obviously $f_2$ has radius of convergence $\geq 1$.

Let $\|\ \|_{|t|\leq\rho}$, with $\rho < 1$, denote the spectral norm on the set $\{\lambda \in \mathbb{C}_p \mid |\lambda-\lambda_o| \leq \rho\}$.

One finds $\|f_2\|_{|t|\leq\rho} = q\|f_2\|_{|t|\leq\rho^q}$.

So $f_2$ is unbounded in the disc $\{\lambda \mid |\lambda-\lambda_o| < 1\}$ and $f_2$ has the following growth property: $\|f_2\|_{|t|\leq\rho} \leq \text{constant } \|\log\frac{\lambda}{\lambda_o}\|_{|t|\leq\rho}$ since the function

$\log(\frac{\lambda}{\lambda_o}) = \sum_{m=1}^{\infty} \frac{1}{m}(\frac{\lambda_o-\lambda}{\lambda_o})^m$ satisfies also the growth condition

$$\|\log(\tfrac{\lambda}{\lambda_o})\|_{|t|\leq\rho} = q\|\log(\tfrac{\lambda}{\lambda_o})\|_{|t|\leq\rho^q}.$$

(7.16) Remarks.

The family of curves $y^n = x^a(x-1)^b(x-\lambda)^c$ can also be treated with the Monsky-Washnitzer cohomology. They provide hypergeometric differential equations with other parameters (See [10]).

In B. Dwork's book [7] one considers liftings $\varphi(\lambda) = \lambda^p + pb$ ($b \in B$ and $b \neq 0$) of the Frobenius map on $B \otimes \mathbf{F}_p$. It is shown that the corresponding function $\xi = (-1)^{\frac{p-1}{2}} \frac{F(\frac{1}{2},\frac{1}{2};1;\lambda)}{F(\frac{1}{2},\frac{1}{2};1,\varphi(\lambda))}$ can be extended in ringdomains inside the supersingular discs. The function $\eta = -\frac{F(\frac{1}{2},\frac{1}{2};1;\lambda)'}{F(\frac{1}{2},\frac{1}{2};1;\lambda)}$ however does not extend at all in the supersingular disks.

References.

[1] A. Adolphson - An index theorem for p-adic differential operators. Trans.Amer. Math.Soc. 216(1976) 297-293.

[2] M. Artin - On the solutions of analytic equations. Invent.math. 5, 277-291 (1968).

[3] R. Berger - Über Verschiedene Differentenbegriffe, Sitzungsberichte der Heidelberger Akademie der Wissenschaften. Jahrg. 1960. Abh. 1.

[4] S. Bosch - A rigid analytic version of M. Artin's theorem on analytic equations. Math.Ann. 255, 395-404 (1981).

[5] C.H. Clemers - A Scrapbook of Complex Curve Theory. Plenum Press. 1980.

[6] B. Dwork - A deformation theory for the zeta function of a hypersurface. Proc.Int.Cong.Math. (1962) 247-259.

[7] B. Dwork - Lectures on p-adic Differential Equations. Grundlehren. N°253, Springer Verlag 1982.

[8] N. Katz - On the differential equations satisfied by period matrices. Publ. I.H.E.S. N°35 - 1968.

[9] N. Katz - Travaux de Dwork - Séminaire Bourbaki. 1971/72 n°409.

[10] N. Katz - Algebraic Solutions of Differential Equations. (p-Curvature and the Hodge Filtration/Invent.math. 18, 1-118 (1972).

[11] P. Monsky, G. Washnitzer - Formal cohomology I. Annals of Math. 1968.

[12] P. Monsky - Formal cohomology II and III. Annals of Math. 1968 and 1971.

[13] P. Monsky - p-adic analysis and zeta-functions 1970. Lectures at Kyoto-University.

[14] D. Reich - A p-adic fixed point formula, Amer.J.Math. 91 (1969) 835-850.

[15] R. Elkik - Solutions d'équations à coefficients dans un anneau hensélien. Ann.Scient.Ec.Norm.Syp. 6, n°4, 553-604 (1973.

[16] R. Hartshorne - Algebraic Geometry. GTM 52, Springer Verlag 1977.