The Arithmetic of Drinfeld Modules

(橢圓加群的整數論)

田口 雄一郎

The Arithmetic of Drinfeld Modules

Yuichiro Taguchi

Contents

Preface

The present article contains the author's recent work on the arithmetic of Drinfeld modules. We study in Chapter I the ramification, both at finite places and infinite places, of division points of Drinfeld modules. In Chapter II, we construct a duality for finite t-modules. This is the $\mathbb{F}_q[t]$-analogue of the Cartier duality. Chapter III concerns with the π-adic theory. We calculate Galois cohomology groups with coefficients in certain complete algebraically closed field, and show the existence of a Hodge-Tate decomposition for finite t-modules. Chapter IV pursues the analogy between φ-modules and $\mathcal{D}$-modules; regular singularity of Drinfeld modules and φ-modules are studied. More detailed Introduction will be given at the beginning of each Chapter.

Now let me explain the relation between the Chapters, which are more or less of independent character. The story of Drinfeld modules begins by fixing a place ∞ of an algebraic function field in one variable over a finite field, which is regarded as the analogue of the infinite place of the rational number field or an imaginary quadratic field. Then local theory of Drinfeld modules falls into two classes; one is over a finite place and the other is over an infinite place. Both are indispensable for the full understanding of the arithmetic of Drinfeld modules. In the classical case of characteristic zero, the arithmetic over an infinite place is rather simple; there we have only $\mathbb{C}/\mathbb{R}$ as the ramification of the base field. In contrast, we have more interesting phenomena in function field case, as is observed in Chapter I. Over finite places, an important role has been played by the Cartier duality in arithmetic geometry over number fields. Since the theory of Drinfeld modules has *coefficients* in function fields, it is natural to construct a similar duality with coefficients in function fields. This is done in Chapter II in the case of rational function fields. The π-adic theory, which is the main theme of Chapter III, is the function field theoretic counterpart of the p-adic theory over local fields of characteristic zero. We present analogous and, regrettably, unanalogous results to those in Tate's celebrated paper *p-Divisible Groups*; the necessity for the duality as in Chapter II arose naturally in seeking these analogues. Chapter IV is the most independent of the other Chapters, but shares with Chapter I an interest in the ramification — now the tameness — of division points of Drinfeld modules.

Notations adopted may be different for different Chapters.

References will be given at the end of each Chapter.

The author would like to express his deep gratitude to Saint Kazuya Kato for smooth guidance, proper encouragement and excellent influence. He is also grateful to all members of the Kato Seminar who taught him much and with whom he enjoyed stimulating discussions.

Chapter I

Ramifications arising from Drinfeld modules

Introduction

In this Chapter, we study various ramifications arising from division points of Drinfeld modules, abelian T-modules, formal modules, etc.. A motivation for this is to know how many isogeny classes and isomorphism classes of Drinfeld A-modules exist over a finite extension of the fraction field of A. We will see (cf. Remark (3.4)) that, modulo the isogeny conjecture, an isogeny class can contain infinitely many isomorphism classes and, without any restriction on ramification at the infinite places, there can be infinitely many isogeny classes.

To explain some of the results, let F be a function field in one variable over a finite field, ∞ a fixed place of F, A the ring of elements of F which are regular outside ∞, and K a finite extension of F. Given a Drinfeld A-module ϕ over K and a prime v of A, we denote by $K(\phi; v^n)$ the field of v^n-division points of ϕ. Then it turns out (Corollary 1.6) that the ramification at various primes in the tower $(K(\phi; v^n)/K)_{n\geq 1}$ is bounded at the places over ∞ by a divisor depending only on ϕ, and at the finite places, it is controlled in a fairly precise way in terms of the "discriminant" $\Delta(\phi)$. Roughly speaking, $\Delta(\phi)$ is the coefficient of the leading term of the defining equation of ϕ. For finite places, this result is analogous to the case of abelian varieties over number fields. (At least one has the Hermite-Minkovski theorem for number fields, which assures the existence of an estimate of discriminants.) But at infinite places, there occur new phenomena, which we describe by example in §2. We construct explicitly an infinite family of Drinfeld modules with everywhere good reduction and with ramification at infinity becoming arbitrarily large (Example 2.1), as well as an infinite family of mutually non-isomorphic Drinfeld modules with everywhere good reduction and with bounded ramification at infinity (Example 2.2). In §3, we give a proposition on v-adic Galois representations (a positive characteristic version of a theorem of Faltings), and discuss how many isomorphism and isogeny classes can exist. §4 and §5 are generalizations of §1 to the cases of finite submodules of higher dimensional formal modules. Theorem (4.6) is an A-module version of Théorème 1 of [5].

Acknowledgement. This Chapter is an extended version of my talk at the workshop "The arithmetic of function fields" held at the Ohio State University in June, 1991. I would like to thank the organizer David Goss for his efforts and his hospitality during my stay at the Ohio State University after the workshop (I found Example (2.1) there). I am also grateful to Greg W. Anderson for asking a question, a partial answer to which is the content of §5.

Notation. Throughout this Chapter, A is a "basic" Dedekind ring and F is its fraction field; in §§1 – 3 (global context), F is a function field in one variable over a finite field, ∞ is a fixed place of F, and A is the ring of elements of F regular outside ∞, whereas in §§4 and 5 (local context), A is a complete discrete valuation ring with finite residue field.

In either context, K will mainly be used to denote a finite extension of F, and then $\mathfrak{O}_K$ will denote the integral closure of A in K.

If we are in the global context, a *prime* of $\mathfrak{O}_K$ means a non-zero prime ideal of $\mathfrak{O}_K$, which is identified with a place of K, and called a *finite place* of K. A place of K is called *infinite* if it extends the place ∞ of F. A place of K will often be identified with a *normalized* valuation of K. A non-zero fractional ideal of $\mathfrak{O}_K$ is often regarded as a divisor of K and denoted additively. So we use notations like, e.g., $\mathfrak{a} \leq \mathfrak{b}$ for such $\mathfrak{a}$ and $\mathfrak{b}$. If w is a prime of $\mathfrak{O}_K$ or a place of K, $\mathfrak{O}_{K,w}$ and K_w denote respectively the completions of $\mathfrak{O}_K$ and K with respect to w.

For a field K, K^{sep} denotes a fixed separable closure of K, and G_K denotes the absolute Galois group $\mathrm{Gal}(K^{sep}/K)$. For a finite separable extension L/K, $\mathfrak{D}(L/K)$ (resp. $\mathfrak{d}(L/K)$) denotes the different (resp. discriminant) of L/K if it can be defined at all.

If G is a group scheme and v is a non-zero element or a non-zero ideal of $\mathrm{End}(G)$, then ${}_vG$ denotes the subgroup scheme $\mathrm{Ker}(v)$ of G.

1. Finite places

In this section, we estimate the differents at finite places of the field extensions arising from division points of Drinfeld modules.

Let F be a function field in one variable over a finite field, ∞ a fixed place of F, and A the ring of elements of F regular outside ∞. We assume that the field of constants is $\mathbb{F}_q$, the finite field with $q = p^f$ elements. For $a \in A - 0$, we define $\deg(a)$ by $\mathrm{Card}(A/aA) = q^{\deg(a)}$.

Let K be a field of characteristic $p > 0$, and $\mathbb{G}_a$ the additive group scheme over K. After choosing a coordinate X of $\mathbb{G}_a$, we can identify $\mathrm{End}_K(\mathbb{G}_a)$ with the non-commutative ring of additive polynomials of X with coefficients in K, where the product is the composition of maps. So in the following, if

$$\phi : A \longrightarrow \mathrm{End}_K(\mathbb{G}_a) \; ; \quad a \mapsto \phi_a$$

is a Drinfeld module over K, we think of ϕ_a as a polynomial $\phi_a(X) \in K[X]$ via this identification. If ϕ is of rank r, the degree of $\phi_a(X)$ as a polynomial of X is $q^{r\deg(a)}$ for all $a \in A - 0$.

Let R be, for example, a Dedekind ring over A, and K its fraction field. For a Drinfeld module ϕ over K, we have a minimal model $(\tilde{\phi}, \mathfrak{m})$ of ϕ over R ([10], §2), where $\mathfrak{m}$ is a fractional ideal of R. If R is a discrete valuation ring, we can take $\mathfrak{m} = R$, and $(\tilde{\phi}, R)$ is characterized as the unique (up to isomorphisms) Drinfeld module $\tilde{\phi}$ over K such that $\tilde{\phi}_a(X) \in R[X]$ for all $a \in A$ and the valuations of the coefficients of $\tilde{\phi}_a(X)$ are minimal.

LEMMA (1.1). *Let R be a discrete valuation ring over A, and K its fraction field. Let ϕ be a Drinfeld module over K of rank r, and $(\tilde{\phi}, R)$ be the minimal model of ϕ over R. Then there exists an ideal $\mathfrak{n}$ of R such that the leading coefficient of $\tilde{\phi}_a(X) \in R[X]$ divides $\mathfrak{n}^{\delta(r,a)}$ for any $a \in A - 0$, where $\delta(r,a) := (q^{r\deg(a)} - 1)/(q-1)$.*

PROOF:— Clearly, we may assume $\tilde{\phi} = \phi$. Take a non-constant element $x \in A$, and let $y \in A - 0$. Since y is algebraic over $\mathbb{F}_q[x]$, we have a non-trivial relation

$$\sum \alpha_{ij} x^i y^j \;=\; 0, \qquad \alpha_{ij} \in \mathbb{F}_q.$$

Let $z = \sum \beta_{ij} x^i y^j$ be the sum of the $\alpha_{ij} x^i y^j$'s with degree $d := \max_{i,j}\{\deg(\alpha_{ij} x^i y^j)\}$ in the left side of this equality. We must have then

$$\deg(z) \;<\; d.$$

If $\phi_x(X) = xX + \cdots + x_m X^{q^m}$ and $\phi_y(X) = yX + \cdots + y_n X^{q^n}$ with $m = r\deg(x)$, $n = r\deg(y)$, and x_m, $y_n \in R$, then we have

$$\phi_{x^i y^j}(X) \;=\; x^i y^j X \;+\; \cdots \;+\; x_m^{1+q^m+\cdots+q^{(i-1)m}} y_n^{q^{im}(1+q^n+\cdots+q^{(j-1)n})} X^{q^{im+jn}}.$$

So the coefficient of $X^{q^{rd}}$ in $0 = \sum \alpha_{ij} \phi_{x^i y^j}$ is

$$\sum \beta_{ij} x_m^{\frac{q^{im}-1}{q^m-1}} y_n^{q^{im}\frac{q^{jn}-1}{q^n-1}},$$

where the sum is over i and j with $im + jn = rd$. Since this sum must be zero, there exist two terms in the sum (say, of indices (i,j) and (i',j'), with $i \neq i'$ and $j \neq j'$) with the same valuation. Denoting by v the valuation of R, we have

$$\frac{q^{im}-1}{q^m-1} v(x_m) \;+\; q^{im}\frac{q^{jn}-1}{q^n-1} v(y_n) \;=\; \frac{q^{i'm}-1}{q^m-1} v(x_m) \;+\; q^{i'm}\frac{q^{j'n}-1}{q^n-1} v(y_n).$$

Noticing the relation $rd = im + jn = i'm + j'n$, we see from this that

$$v(y_n) \;=\; \frac{q^n-1}{q^m-1} v(x_m).$$

Hence, if $x_m \mid \mathfrak{n}^{\frac{q^m-1}{q-1}}$, then $y_n \mid \mathfrak{n}^{\frac{q^n-1}{q-1}}$. Now the proof is complete.

DEFINITION (1.2). Let K be a finite extension of F. For a Drinfeld module ϕ over K and a prime w of $\mathfrak{O}_K$, consider its minimal model over $\mathfrak{O}_{K,(w)}$, and define $\Delta_w(\phi)$ to be the smallest ideal n of $\mathfrak{O}_{K,(w)}$ with the property stated in Lemma (1.1). Define also $\Delta(\phi) := \sum_w \Delta_w(\phi)$, where the sum is over all primes of $\mathfrak{O}_K$ and $\Delta_w(\phi)$ is regarded as a divisor of K.

$\Delta(\phi)$ measures in a sense the "badness" of the reductions of ϕ at finite places. To estimate the differents, we begin with

LEMMA (1.3). *Let R be a complete discrete valuation ring, K the fraction field, and $\phi(X) \in R[X]$ a separable polynomial with coefficients in R. Assume the coefficient of the leading term of ϕ is a unit. Let α be a root of ϕ in K^{sep}. Then the different $\mathfrak{D}(K(\alpha)/K)$ divides the principal ideal $(\phi'(\alpha))$.*

Note that $\phi'(\alpha) = a_0$ if ϕ is of the form $\phi(X) = \sum_i a_i X^{p^i}$ and K is of positive characteristic p.

PROOF:— Since the minimal polynomial of α divides $\phi(X)$ and all the roots of $\phi(X)$ are integral over R, this follows from Cor. 2 (p. 66) to Prop. 11 of §6, Chap. III of [8].

LEMMA (1.4). *Let R be a complete discrete valuation ring of characteristic $p > 0$ and K the fraction field. Let $\phi(X) = \sum_{i=0}^{N} a_i X^{p^i}$ be a separable polynomial in $R[X]$ with $a_0 a_N \neq 0$, and α a root of ϕ in K^{sep}. Then the different $\mathfrak{D}(K(\alpha)/K)$ divides the principal ideal $(a_0 a_N^{p^N-2})$.*

PROOF:— $\tilde{\phi}(X) := a_N^{p^N-1}\phi(X/a_N) = \sum_{i=0}^{N} a_i a_N^{p^N-1-p^i} X^{p^i}$ is a separable monic polynomial in $R[X]$ and $a_N\alpha$ is a root of $\tilde{\phi}$. The assertion now follows from the previous lemma.

For a finite extension K of F and $a \in A - 0$, let $K(\phi; a) = K({}_a\phi(K^{sep}))$ denote the finite separable extension of K obtained by adding the a-division points of ϕ. Let $\mathfrak{D}_f(/)$ denote the finite part of $\mathfrak{D}(/)$, i.e., the sum of the components of $\mathfrak{D}(/)$ not lying over ∞. Since the extension $K(\phi; a)/K$ is obtained by adding r roots of $\phi_a(X)$ which form an (A/aA)-base of ${}_a\phi(K^{sep}) \simeq (A/aA)^r$, we see from Lemmas (1.1) and (1.4) the following

PROPOSITION (1.5). *Let ϕ be a Drinfeld module over a finite extension K of F of rank r. For $a \in A - 0$, we have*

$$\mathfrak{D}_f(K(\phi; a)/K) \leq r\big[(a) + \delta(r, a)(q^{\mathrm{rdeg}(a)} - 2) \cdot \Delta(\phi)\big].$$

For an infinite place w of K, let $\Lambda_w(\phi)$ denote the A-lattice in K_w^{sep} correspondeing to $\phi \otimes_K K_w$ ([3], §3). This is a G_{K_w}-stable projective A-module of rank r. In particular, it is finitely generated over A, and the fixed subfield $K_w(\Lambda_w(\phi))$ of K_w^{sep} by the kernel of the natural representation $G_{K_w} \longrightarrow \mathrm{Aut}(\Lambda_w(\phi))$ is a finite extension of K_w. We have for $a \in A - 0$, ${}_a\phi(K_w^{sep}) \simeq \Lambda_w(\phi)/a\Lambda_w(\phi)$ as G_{K_w}-modules, which is rational over $K_w(\Lambda_w(\phi))$. Hence we have:

COROLLARY (1.6). *Let r be a positive integer, v a prime of A, and $\mathfrak{n}$ a non-zero ideal of $\mathfrak{O}_K$. Let S be the set of finite places of K consisting of the finite places lying above v or dividing $\mathfrak{n}$. Then there exists a family $(N(w,n))_{w\in S, n\in\mathbb{N}}$ of non-negative integers which has the following property:*

For any Drinfeld module ϕ over K of rank r with $\Delta(\phi) \leq \mathfrak{n}$ and for any $n \in \mathbb{N}$, we have

$$\mathfrak{d}(K(\phi;v^n)/K) \leq \sum_{w\in S} N(w,n)\cdot(w) \; + \; M(\phi)\cdot\infty,$$

where $M(\phi)$ is an integer ≥ 0 depending on ϕ but not on n.

2. Infinite places — Examples

In contrast to the classical case (where we have only $\mathbb{C}/\mathbb{R}$), we have more complicated field extensions at infinity in the Drinfeld module case, if the rank r is bigger than one. In this section, we give two typical examples which clarify this contrast.

Let A, F, and ∞ be as in §1. For a Drinfeld module ϕ over a finite extension K of F and an infinite place w of K, let $\Lambda_w(\phi)$ denote, as in §1, the A-lattice corresponding to $\phi \otimes_K K_w$.

EXAMPLE (2.1). Let $A = \mathbb{F}_q[T]$, $F = \mathbb{F}_q(T)$, $\infty = (\frac{1}{T})$, and r an integer ≥ 2. Then there exists an infinite family $(\phi^{(n)})_{n\geq 1}$ of Drinfeld modules over F of rank r which has the following properties:
(i) $\phi^{(n)}$ has everywhere good reduction over A;
(ii) the ramification of the corresponding lattice $\Lambda^{(n)} = \Lambda_\infty(\phi^{(n)})$ at ∞ becomes arbitrarily large, i.e., $\mathrm{ord}_\infty(\mathfrak{D}(F_\infty(\Lambda^{(n)})/F_\infty))$ tends to infinity as n does.

Especially, for any finite place v of F, there arise infinitely many isomorphism classes of v-adic G_F-representations $T_v(\phi) \otimes_{A_v} F_v$ from Drinfeld modules ϕ of rank r over F with everywhere good reduction.

CONSTRUCTION:— Consider a Drinfeld module $\phi^{(n)}$ over A defined by

$$\phi_T^{(n)}(X) = TX + a_1X^q + \cdots + a_rX^{q^r}, \qquad a_i \in A,$$

where we assume:
(1) $a_r \in A^\times = \mathbb{F}_q^\times$;
(2) $\mathrm{ord}_\infty(a_{r-1}) = -n(q^r - q^{r-1}) + 1$;
(3) $\mathrm{ord}_\infty(a_{r-1}) \leq \mathrm{ord}_\infty(a_i)$ for $1 \leq i \leq r-1$.

Let v denote the normalized valuation $\mathrm{ord}_\infty(\cdot)$ extended uniquely to a fixed separable closure F_∞^{sep} of F_∞. The Newton polygon of $\phi_T(X) \in F_\infty[X]$ shows that

$$(4) \qquad \phi_T(X) \text{ has } (q^r - q^{r-1}) \text{ roots } \lambda \text{ with } v(\lambda) = -n + \frac{1}{q^r - q^{r-1}}$$

(take and fix one such λ), and the other non-zero roots have non-negative valuations. Conseqently, $V := \{\lambda' \in {}_T\phi(F_\infty^{sep}) \,;\, v(\lambda') \geq 0\}$ forms an $(r-1)$-dimensional $\mathbb{F}_q$-vector space.

By (4), the degree of the minimal polynomial of λ over F_∞ cannot exceed $(q^r - q^{r-1})$. On the other hand, the denominator of $v(\lambda)$, expressed as a reduced rational number, is $(q^r - q^{r-1})$. Hence the extension $F_\infty(\lambda)/F_\infty$ is totally ramified of degree $(q^r - q^{r-1})$, and in particular, it is wildly ramified.

Let L be the Galois closure in F_∞^{sep} of $F_\infty(\lambda)/F_\infty$. Since L/F_∞ is also wildly ramified, there exists an element $\sigma \in \mathrm{Gal}(L/F_\infty)$ of order p. Then $\sigma(\lambda)$ is of the form

$$\sigma(\lambda) \;=\; \alpha\lambda \;+\; \lambda', \qquad \text{for some } \alpha \in \mathbb{F}_q^\times \text{ and } \lambda' \in V.$$

Since $v(\sigma(\lambda')) = v(\lambda') > v(\lambda)$, we again have $\sigma(\lambda') \in V$. Hence $\sigma^p = 1$ implies $\alpha^p = 1$. Thus

$$\sigma(\lambda) \;=\; \lambda \;+\; \lambda', \qquad \lambda' \in V.$$

Set $\pi := \frac{\lambda}{T^n}$, so that $v(\pi) = \frac{1}{q^r - q^{r-1}}$ and π is a uniformizer of $F_\infty(\lambda)$. Since

$$v(\sigma(\pi) - \pi) = v((\sigma(\lambda) - \lambda)/T^n) = n + v(\lambda') \geq n,$$

and

$$\mathfrak{D}(F_\infty(\lambda)/F_\infty) = \prod_{\tau \in \mathrm{Gal}(L/F_\infty) - 1} (\tau(\pi) - \pi),$$

this different, and hence $\mathfrak{D}(F_\infty(\Lambda)/F_\infty)$, can become arbitrarily large, as asserted before.

EXAMPLE (2.2). Let A, F, ∞, and r be as in Example (2.1). Then there exists an infinite family $(\phi^{(n)})_{n \geq 0}$ of mutually non-isomorphic Drinfeld modules of rank r over a finite extension L of F which has the following properties:
(i) $\phi^{(n)}$ has everywhere good reduction over the integral closure $\mathfrak{O}_L$ of A in L.
(ii) Let w be an infinite place of L, and set $\Lambda^{(n)} := \Lambda_w(\phi^{(n)})$. Then there are in fact only finitely many field extensions in the set $\{L_w(\Lambda^{(n)})/L_w \;;\; n \in \mathbb{N}\}$.

CONSTRUCTION:— Let $K = \mathbb{F}_q(t)$, $\mathfrak{O}_K = \mathbb{F}_q[t]$, and C the Carlitz $\mathfrak{O}_K$-module defined by

$$C_t(X) \;=\; tX \;+\; X^q.$$

Take an irreducible element $T = f(t) \in \mathfrak{O}_K$ of degree r, and let A be the subring $\mathbb{F}_q[T]$ of $\mathfrak{O}_K$ ($\infty := (\frac{1}{T}) = (\frac{1}{t^r})$ in K). Define a Drinfeld A-module ϕ over $\mathfrak{O}_K$ by

$$\phi_T \;:=\; C_{f(t)}.$$

Then ϕ has rank r, and everywhere good reduction over $\mathfrak{O}_K$. By explicit class field theory ([7]), the field $L := K(_{f(t)}C(K^{sep})) = K(_T\phi(K^{sep}))$ is an abelian extension of K with Galois group $(\mathfrak{O}_K/(f(t)))^\times \simeq \mathbb{F}_{q^r}^\times$, and the prime $(f(t))$ ramifies totally in L. In particular, the polynomial $C_{f(t)}(X)/X = \phi_T(X)/X$ over $\mathfrak{O}_K$ is Eisenstein at (T); if we write

$$\phi_T(X) \;=\; TX \;+ a_1 X^q \;+ \cdots + \; a_{r-1}X^{q^{r-1}} \;+\; X^{q^r},$$

then we have

$$\mathrm{ord}_T(a_i) \geq 1, \quad 1 \leq i \leq r-1. \tag{1}$$

Write

$$\phi_T(X) = TX \prod_{\lambda \in {}_T\phi - 0} (1 - \frac{X}{\lambda}) \qquad \text{in } K^{sep}[X].$$

Looking at the Newton polygons of $\phi_T(X)$ at various finite places of K, we see that, for any $\lambda \in {}_T\phi(K^{sep}) - 0$, (λ) is the unique prime ideal of $\mathfrak{O}_L$ lying over (T). So we can take a prime element τ (say $\tau :=$ one of the λ's) of $\mathfrak{O}_L$ and write

$$\lambda = \tau\lambda_1, \quad \lambda_1 \in \mathfrak{O}_L^{\times}$$

for each $\lambda \in {}_T\phi(K^{sep}) - 0$. Define Drinfeld modules $\phi^{(n)}$ $(n = 0, 1, 2, \cdots)$ over L by

$$\phi_T^{(n)}(X) = TX \prod_{\lambda \in {}_T\phi - 0} (1 - \frac{X}{\tau\lambda_1^{p^n}}).$$

If $\phi_T^{(n)}(X) = TX + a_1^{(n)}X^q + \cdots + a_r^{(n)}X^{q^r}$, then

$$a_i^{(n)} = T \sum \prod_{(q^i-1)} \frac{1}{-\tau\lambda_1^{p^n}} = T\tau^{1-q^i}(\sum \prod_{(q^i-1)} \frac{1}{\lambda_1})^{p^n},$$

where $\sum\prod_{(q^i-1)}$ denotes the sum of the products of $(q^i - 1)$ elements, the sum taken over all possible choices of $(q^i - 1)$ λ's from ${}_T\phi(K^{sep}) - 0$. Set $b_i := \sum\prod_{(q^i-1)} \frac{1}{\lambda_1}$. Since $(T) = (\tau^{q^r-1})$ and, for $1 \le i \le r-1$,

$$a_i = a_i^{(0)} = T\tau^{1-q^i}b_i$$

is by (1) an element of $\mathfrak{O}_K$ divisible by T, b_i is integral; $b_i \in \mathfrak{O}_L$. Note that

$$\text{ord}_\tau(b_i) = \text{ord}_\tau(a_i) - (q^r - q^i) > 0. \tag{2}$$

Since

$$a_i^{(n)} = T\tau^{1-q^i}b_i^{p^n} = a_i b_i^{p^n-1},$$

we have for a prime w of $\mathfrak{O}_L$,

$$\text{ord}_w(a_i^{(n)}) = \begin{cases} \text{ord}_\tau(a_i) + (p^n - 1)\text{ord}_\tau(b_i) & \text{if } w \mid T \\ p^n \text{ord}_w(a_i) & \text{if } w \nmid T. \end{cases} \tag{3}$$

Moreover we have for $i = r$,

$$a_r^{(n)} = T\tau^{1-q^r}(\prod_{(q^r-1)} \frac{1}{\lambda_1})^{p^n} \in \mathfrak{O}_L^{\times}.$$

We have thus obtained an infinite family $(\phi^{(n)})_{n\in\mathbb{N}}$ of Drinfeld modules over $\mathfrak{O}_L$ with everywhere good reduction. (2) and (3) imply that these are mutually non-isomorphic, and yet the T-division points ${}_T\phi^{(n)}(L^{sep})$ are rational over L. Further, it will be shown in §3 (Cor. (3.2), (ii)) that there arise in fact only finitely many extensions $L_w(\Lambda_w(\phi^{(n)}))/L_w$ for all $w \mid \infty$.

3. Some finiteness and infiniteness

In this section, A, F and ∞ are as in §1. Let v be a prime of A, K a finite extension of F, and $\mathfrak{n}$ a positive divisor of K. Let V be a finite dimensional F_v-vector space, and $\rho : G_K \longrightarrow \mathrm{GL}(V)$ an F_v-linear continuous representation of G_K. Consider the following condition for ρ:

(*) ρ is unramified outside $\mathrm{Supp}(\mathfrak{n})$, and there exists in V a G_K-stable A_v-lattice T such that $\mathfrak{d}(K'/K) \leq \mathfrak{n}$, where K' is the fixed subfield of K^{sep} by the kernel of the map $G_K \longrightarrow \mathrm{Aut}(T/vT)$ induced by ρ.

PROPOSITION (3.1). *Let r be a positive integer and $\mathfrak{n}$ a positive divisor of K. Then there exists a finite set S of finite places of K disjoint from $Supp(\mathfrak{n})$ which has the following property:*

Let $\rho_i : G_K \longrightarrow GL(V_i)$, $i = 1, 2$, be two r-dimensional v-adic representations which are semi-simple and satisfy the above condition (*). If the characteristic polynonial of $\rho_1(Frob_w)$ and $\rho_2(Frob_w)$ coincide for all $w \in S$, then we have $\rho_1 \simeq \rho_2$.

PROOF:— (Cf. Proof of Theorem 5 of [4]) Since there are only finitely many separable extensions of K with given degree and discriminant, there exists a finite Galois extension $K_{\mathfrak{n}}/K$ which contains all separable extensions K'/K such that $[K' : K] \leq \mathrm{Card}(\mathrm{GL}_r(\mathbb{F}_{q_v}))$ and $\mathfrak{d}(K'/K) \leq \mathfrak{n}$, where $q_v := \mathrm{Card}(A/vA)$. By Čebotarev, there exists a finite set S of finite places of K disjoint from $\mathrm{Supp}(\mathfrak{n})$ such that $\mathrm{Gal}(K_{\mathfrak{n}}/K)$ is filled with the images of the conjugacy classes of $Frob_w$ for $w \in S$. We will show that this S has the required property. Choose G_K-stable A_v-lattices T_i of V_i for $i = 1, 2$, with the property as in the assumption (*), and let M_j, $1 \leq j \leq r$, be the A_v-subalgebra of $\mathrm{End}_{A_v}(\wedge^j T_1 \times \wedge^j T_2)$ generated by the image of $\wedge^j\rho_1 \times \wedge^j\rho_2$. By the assumption of semi-simplicity and by a version of the Brauer-Nesbitt theorem (cf. [9]), it suffices to show $\mathrm{Tr}(m_1; \wedge^j V_1) = \mathrm{Tr}(m_2; \wedge^j V_2)$ for all $m = (m_1, m_2) \in M_j$, $1 \leq j \leq r$, which is already true by assumption if m is conjugate to the image of $Frob_w$ for some $w \in S$. It remains to show that these images together with their conjugates generate M_j over A_v. They generate the A_v/vA_v-module M_j/vM_j, because $G_{K_{\mathfrak{n}}}$ acts trivially on $T_1/vT_1 \times T_2/vT_2$ according to our choice of $K_{\mathfrak{n}}$. By Nakayama's lemma, they generate the A_v-module M_j.

Hereafter in §3, w denotes an infinite place of K.

Since the Galois representations $T_v(\phi) \otimes_{A_v} F_v$ are semi-simple ([10]), Cor. (1.6) and Prop. (3.1) imply

COROLLARY (3.2). *Let v be a prime of A, r a positive integer, and $\mathfrak{n}$ a positive divisor of K. Then:*
(i) There arise only finitely many isomorphism classes of Galois representations $T_v(\phi) \otimes_{A_v} F_v$ from Drinfeld modules ϕ over F of rank r such that $\Delta(\phi) \leq \mathfrak{n}$ and $\mathfrak{d}(K_w({}_v\phi(K_w^{sep}))/K_w) \leq \mathfrak{n}$ for all infinite places w of K.

(ii) For a Drinfeld module ϕ over K and an infinite place w of K, let $\Lambda_w(\phi)$ be the A-lattice ($\subset K_w^{sep}$) corresponding to $\phi \otimes_K K_w$. Then there arise only finitely many field extensions $K_w(\Lambda_w(\phi))/K_w$ from Drinfeld modules ϕ as in (i). Especially, $\mathfrak{d}(K_w(\Lambda_w(\phi))/K_w)$ is bounded.

REMARK (3.3). Over K_w, there may exist an infinite family $(\phi^{(n)})_{n\in\mathbb{N}}$ of Drinfeld modules of rank $r \geq 2$ such that ${}_v\phi^{(n)}(K_w^{sep})$ is rational over K_w but the ramification of the corresponding lattices $\Lambda^{(n)}$ is not bounded. For example, let $A := \mathbb{F}_q[T]$ and $\lambda^{(n)}$ a root of the Artin-Schreier equation $X^q - X = T^n$. Consider the rank two Drinfeld module $\phi^{(n)}$ over F_∞ corresponding to the A-lattice $\Lambda^{(n)} := A\cdot\lambda^{(n)} + A\cdot\frac{1}{T}$ ($\subset F_\infty^{sep}$). Then G_{F_∞} acts trivially on ${}_T\phi^{(n)}(F_\infty^{sep}) \simeq \Lambda^{(n)}/T\Lambda^{(n)}$ (since $\sigma(\lambda^{(n)}) - \lambda^{(n)} \in \mathbb{F}_q \subset A \subset T\Lambda^{(n)}$ for $\sigma \in G_{F_\infty}$), but $\mathfrak{d}(F_\infty(\lambda^{(n)})/F_\infty)$ is not bounded.

REMARK (3.4). It is conjectured that the isogeny classes of Drinfeld modules ϕ over K are in one to one correspondence with the Galois representations $T_v(\phi)\otimes_{A_v} F_v$. If this is true, then Ex. (2.1), Ex. (2.2) and Cor. (3.2) imply the following:

For a Drinfeld module ϕ over K, consider the positive divisor of K

$$\overline{\Delta}(\phi) := \Delta(\phi) + \sum_{w|\infty} \mathfrak{d}(K_w(\Lambda_w(\phi))/K_w).$$

Suppose we are given a positive divisor n of K. Then:
(i) There exist only finitely many isogeny classes of Drinfeld modules ϕ of rank $r \geq 1$ with $\overline{\Delta}(\phi) \leq$ n (Cor. (3.2)).
(ii) Let $A = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$. Then

(ii-1) there exist infinitely many isogeny classes of Drinfeld modules ϕ of rank $r \geq 2$ over F with $\Delta(\phi) \leq$ n (Ex. (2.1));

(ii-2) there exists an isogeny class of Drinfeld modules of rank $r \geq 2$ over some finite extension of F which contains infinitely many isomorphism classes (Ex. (2.2) + Cor. (3.2)).

REMARK (3.5). The above definition of $\overline{\Delta}(\phi)$ is not good. We hope to find a definition of the infinite component of $\overline{\Delta}(\phi)$ which is calculated directly from the defining equation of ϕ and with which we can bound $\sum \mathfrak{d}(K_w(\Lambda_w(\phi))/K_w)$.

4. Higher dimensional cases

The content of this section is an A-module version of a theorem of Fontaine (Théorème 1 of [5]), which can be regarded as a higher dimensional generalization of Lemma (1.3).

First we give a preliminary on Taylor expansions.

Let R be a commutative ring and $R[[X]] = R[[X_1, \cdots, X_h]]$ the ring of formal power series over R in h variables. For a multi-index $n = (n_1, \cdots, n_h) \in \mathbb{N}^h$ ($\mathbb{N}$ is the set of natural numbers including 0), we define a "differential operator" $\frac{\delta^n}{\delta X^n}$ as follows:

If $f(X) = \sum a_m X^m = \sum a_{m_1,\cdots,m_h} X_1^{m_1} \cdots X_h^{m_h} \in R[[X]]$, then

$$\frac{\delta^n}{\delta X^n} f(X) := \sum a_m \binom{m}{n} X^{m-n}$$

$$= \sum a_{m_1,\cdots,m_h} \binom{m_1}{n_1} \cdots \binom{m_h}{n_h} X_1^{m_1-n_1} \cdots X_h^{m_h-n_h},$$

where $\binom{m}{n} = \binom{m_1}{n_1} \cdots \binom{m_h}{n_h}$ is the "multi-binomial coefficient" with $\binom{m_i}{n_i} := 0$ if $n_i > m_i$.

REMARKS (4.1). (1) $\frac{\delta^n}{\delta X^n}$ is R-linear.
(2) $\frac{\partial^n}{\partial X^n} = n! \frac{\delta^n}{\delta X^n}$ (where $n! := n_1! \cdots n_h!$) is the usual differential operator, and $\frac{\delta^n}{\delta X^n} = \frac{1}{n!}(\frac{\delta}{\delta X})^n$ if $n!$ is invertible in R. In particular, we have $\frac{\partial}{\partial X} = \frac{\delta}{\delta X}$.
(3) For $f(X) \in R[[X]]$, put $f_Y(X) := f(X+Y) \in R[[X,Y]] = R[[X]][[Y]]$. We have

$$\frac{\delta^n}{\delta X^n} f_Y(X) = (\frac{\delta^n}{\delta X^n} f)(X+Y) \quad \text{in } R[[X,Y]].$$

(4) $$\frac{\delta^n}{\delta X^n}(fg) = \sum_{k+l=n} (\frac{\delta^k}{\delta X^k} f)(\frac{\delta^l}{\delta X^l} g) \quad \text{for } f,\ g \in R[[X]].$$

(5) Let S be an R-algebra and I an ideal of S. Assume S is complete with respect to the I-adic topology. If $f(X) \in R[[X]]$ has the value $f(x) \in S$ at a point $x = (x_1, \cdots, x_h) \in S^h$, then $\frac{\delta^n}{\delta X^n} f(X)$ also has the value $\frac{\delta^n}{\delta X^n} f(x)$ at x for any $n \in \mathbb{N}^h$

PROPOSITION (4.2). *For $f(X) \in R[[X]]$, we have the formal Taylor expansion (or rather, the binomial expansion)*

(4.2.1) $$f(X+Y) = \sum_{|n| \geq 0} \frac{\delta^n}{\delta X^n} f(X) \cdot Y^n \quad \textit{in } R[[X,Y]].$$

If $f(X)$ has the value $f(x) \in S$ at $x \in S^h$ and y is an element of I^h, then $f(x+y) \in S$ also exists and we have

(4.2.2) $$f(x+y) = \sum_{|n| \geq 0} \frac{\delta^n}{\delta X^n} f(x) \cdot y^n \quad \textit{in } S.$$

PROOF:— Write $f(X+Y) = \sum a_n(X) Y^n$ with $a_n(X) \in R[[X]]$. Applying $\frac{\delta^n}{\delta Y^n}$ to both sides and reducing modulo Y, we obtain (cf. Remark (4.1), (3))

$$\frac{\delta^n}{\delta X^n} f(X) = a_n(X)$$

and hence (4.2.1).

The latter half of the Proposition is obvious.

Next we recall Fontaine's numbering of the ramification groups of a local field and some of his results ([5], §1). In the rest of this section, if L is a discrete valuation field, $\mathfrak{O}_L$ (resp. $\mathfrak{m}_L$, resp. k_L) denotes the integer ring of L (resp. the maximal ideal of $\mathfrak{O}_L$, resp. the residue field $\mathfrak{O}_L/\mathfrak{m}_L$).

In the following, K is a complete discrete valuation field with perfect residue field k of characteristic $p \neq 0$. Let v_K denote the valuation on K normalized by $v_K(K^\times) = \mathbb{Z}$, and also its unique extension to any algebraic extension of K. If $\mathfrak{a}$ is a subset of an algebraic extension of K, we put $v_K(\mathfrak{a}) := \inf\{v_K(x); x \in \mathfrak{a}\}$.

For a finite Galois extension L/K, Fontaine defines a filtration with lower (resp. upper) numbering $G_{(i)}$ (resp. $G^{(u)}$) $(i, u \in \mathbb{R})$ on the Galois group $G = \mathrm{Gal}(L/K)$, which is connected with the usual filtration G_i (resp. G^u) defined in Chapitre IV of [8] by

$$G_i = G_{((i+1)/e)}, \qquad \text{resp.} \quad G^u = G^{(u+1)},$$

where $e = e_{L/K}$ is the ramification index of L/K.

He also defines a real number $i_{L/K}$ (resp. $u_{L/K}$), which is characterized as the largest real number i (resp. u) such that $G_{(i)} \neq 1$ (resp. $G^{(u)} \neq 1$). $i_{L/K}$ and $u_{L/K}$ are connected by

$$u_{L/K} = \int_0^{i_{L/K}} (G_{(x)} : 1)dx.$$

Then he proves the following

PROPOSITION (4.3). *Let L be a finite Galois extension of K.*
(1) ([5], 1.3) $v_K(\mathfrak{D}(L/K)) = u_{L/K} - i_{L/K}$.
(2) ([5], 1.5) For a real number $m \geq 0$, consider the following property (P_m) on the extension L/K:

$$(P_m)\begin{cases} \text{For any algebraic extension } E \text{ of } K, \text{ if there exists} \\ \text{an } \mathfrak{O}_K\text{-algebra homomorphism : } \mathfrak{O}_L \to \mathfrak{O}_E/\mathfrak{a}_{E/K}^m \\ (\text{where } \mathfrak{a}_{E/K}^m := \{x \in \mathfrak{O}_E; v_K(x) \geq m\}), \\ \text{then there exists a } K\text{-embedding : } L \hookrightarrow E. \end{cases}$$

Then

(i) if $m > u_{L/K}$, L/K has the property (P_m);

(ii) if L/K has the property (P_m), we have $m > u_{L/K} - e_{L/K}^{-1}$.

Now we shall refine Fontaine's Proposition 1.7 of [5] as follows. The main point is that it works, *mutatis mutandis*, even in positive characteristics.

PROPOSITION (4.4). *Let B be a finite flat $\mathfrak{O}_K$-algebra which is locally of complete intersection over $\mathfrak{O}_K$. Suppose that there exists an element $a \in \mathfrak{O}_K$ such that $\Omega^1_{B/\mathfrak{O}_K}$ is a flat (B/aB)-module.*

(i) Let S be a finite flat $\mathfrak{O}_K$-algebra and I an ideal of S. Suppose either the S-submodule $a^{-1}I^{p-1}$ of $K \otimes_{\mathfrak{O}_K} S$ is topologically nilpotent (i.e., $\cap_{n\geq 1}(a^{-1}I^{p-1})^n = 0$), or I has a PD-structure such that $\cap_{n\geq 1} I^{[n]} = 0$.

(a) For any $\mathfrak{O}_K$-algebra homomorphism $u : B \longrightarrow S/aI$, there exists an $\mathfrak{O}_K$-algebra homomorphism $\hat{u} : B \longrightarrow S$ which is uniquely determined by $u(mod.I)$ and makes the following diagram commutative:

$$\begin{array}{ccc} B & \xrightarrow{u} & S/aI \\ {\scriptstyle \hat{u}}\downarrow & & \downarrow \\ S & \longrightarrow & S/I\,. \end{array}$$

(b) The canonical map of sets

$$Hom_{\mathfrak{O}_K\text{-alg}}(B,S) \longrightarrow Hom_{\mathfrak{O}_K\text{-alg}}(B,S/I)$$

is injective.

(ii) The K-algebra $B_K := K \otimes_{\mathfrak{O}_K} B$ is étale. Let L be the smallest subfield of a separable closure K^{sep} of K which contains the images $u(B)$ for all $u \in Hom_{K\text{-alg}}(B_K, K^{sep})$. Then L/K is a finite Galois extension and $u_{L/K} \leq v_K(a) + \frac{1}{p-1} \cdot min\{v_K(a), v_K(p)\}$.

The proof is essentially the same as the original one due to Fontaine, but here we reproduce his proof of (i) to make clear the meaning of the condition in (i).

PROOF:— We may and do suppose B is a local ring, because B is the product of a finite number of local rings. Let $\mathfrak{m}_B$ be the maximal ideal of B. Replacing K by an unramified extension if necessary, we may also suppose $B/\mathfrak{m}_B = k$, the residue field of $\mathfrak{O}_K$.

Then $\Omega^1_{B/\mathfrak{O}_K}$ is a free (B/aB)-module. Let $x_1, \cdots, x_h$ be elements of $\mathfrak{m}_B$ the images of which form a k-base of $\mathfrak{m}_B/(\mathfrak{m}_B^2 + \mathfrak{m}_K B)$. We see from the definition of differential modules that $dx_1, \cdots, dx_h$ generate $\Omega^1_{B/\mathfrak{O}_K}$, and further, they form a (B/aB)-base of $\Omega^1_{B/\mathfrak{O}_K}$ because of the canonical isomorphisms

$$\Omega^1_{B/\mathfrak{O}_K} \otimes_B B_o \xrightarrow{\sim} \Omega^1_{B_o/k} \qquad (B_o := B/\mathfrak{m}_K B),$$

$$\mathfrak{m}_B/(\mathfrak{m}_B^2 + \mathfrak{m}_K B) \xrightarrow{\sim} \mathfrak{m}_{B_o}/\mathfrak{m}_{B_o}^2 \xrightarrow{\sim} \Omega^1_{B_o/k} \otimes_{B_o} k,$$

where $\mathfrak{m}_{B_o} = \mathfrak{m}_B/\mathfrak{m}_K B$ is the maximal ideal of B_o.

Now let

$$\alpha : \mathfrak{O}_K[[X_1, \cdots, X_h]] \longrightarrow B$$

be the unique continuous $\mathfrak{O}_K$-algebra homomorphism such that $\alpha(X_j) = x_j$, and let $J := \mathrm{Ker}(\alpha)$. Since B is finite of complete intersection over $\mathfrak{O}_K$, J is generated by h elements, say $P_1, \cdots, P_h \in \mathfrak{O}_K[[X_1, \cdots, X_h]]$.

For each i, we have $\sum_j \frac{\delta P_i}{\delta X_j}(x_1, \cdots, x_h) dx_j = 0$ (note $\frac{\delta}{\delta X_j} = \frac{\partial}{\partial X_j}$), which implies $\frac{\delta P_i}{\delta X_j}(x_1, \cdots, x_h) \in aB$. Hence there are $p_{ij} \in B$ such that $\frac{\delta P_i}{\delta X_j}(x_1, \cdots, x_h) =$

ap_{ij}. The fact that $\Omega^1_{B/\mathfrak{O}_K}$ is a free (B/aB)-module means that the free B-submodule of $\oplus_{j=1}^h BdX_j$ generated by $\sum_j \frac{\delta P_i}{\delta X_j}(x_1, \cdots, x_h)dX_j$, $1 \leq i \leq h$, coincides with the one generated by adX_j, $1 \leq j \leq h$. We can therefore find $q_{li} \in B$ such that

$$adX_l = \sum_i q_{li}(\sum_j \frac{\delta P_i}{\delta X_j}(x_1, \cdots, x_h)dX_j), \quad 1 \leq l \leq h,$$

i.e., $a1_h = (q_{li})(ap_{ij})$. (1_h is the unit matrix of degee h.) Since B is a free $\mathfrak{O}_K$-module, we can divide both sides by a. Thus the matrix (p_{ij}) is invertible in $\mathrm{M}_h(B)$ and $(q_{li}) = (p_{ij})^{-1}$.

The case of PD-ideals is proved in [5], so we suppose $a^{-1}I^{p-1}$ is topologically nilpotent. Then the ideal $a^{-1}I^{p-1} + I$ is also topologically nilpotent. Set $I_n := (a^{-1}I^{p-1} + I)^{n-1}I$, $n \geq 1$ (so that $a^{-1}I_n^{p-1}$ is again topologically nilpotent, and S is canonically isomorphic to the projective limit of the system $(S/I_n)_{n\geq 1}$). It is easily seen that $I_n^p \subset aI_{2n}$ and $I_n^2 \subset I_{2n}$. To show the assertion, it is enough to verify:

For any integer $n \geq 1$ and an $\mathfrak{O}_K$-algebra homomorphism $u : B \longrightarrow S/aI_n$, there exists an $\mathfrak{O}_K$-algebra homomorphism $u' : B \longrightarrow S/aI_{2n}$ such that $u'(\mathrm{mod}.I_{2n})$ is uniquely determined by $u(\mathrm{mod}.I_n)$ and u' makes the following diagram commutative:

$$\begin{array}{ccc} B & \xrightarrow{u} & S/aI_n \\ {\scriptstyle u'}\downarrow & & \downarrow \\ S/aI_{2n} & \longrightarrow & S/I_n. \end{array}$$

In other words, writing I for I_n and I_2 for I_{2n} :

For any elements $u_1, \cdots, u_h$ of S such that

$$P_i(u_1, \cdots, u_h) = a\lambda_i \quad \text{with some } \lambda_i \in I \quad (1 \leq i \leq h),$$

there exist $\mu_1, \cdots, \mu_h \in I$ such that $\mu_j(\mathrm{mod}.I_2)$ are uniquely determined by $u_j(\mathrm{mod}.I)$ and

$$P_i(u_1 + \mu_1, \cdots, u_h + \mu_h) \in aI_2 \quad (1 \leq i \leq h). \tag{4.4.1}$$

If $\mu_j \in I$, we have the Taylor expansion (4.2.2)

$$P_i(u_1 + \mu_1, \cdots, u_h + \mu_h) = a\lambda_i + \sum_j \frac{\delta P_i}{\delta X_j}(u_1, \cdots, u_h)\mu_j + R_i \tag{4.4.2}$$

with $R_i := \sum_{|r|\geq 2} \frac{\delta^r P_i}{\delta X^r}(u_1, \cdots, u_h)\mu^r$.

For any element $P \in J$, we have $\frac{\delta P}{\delta X_j}(x_1, \cdots, x_h) \in aB$, i.e.,

$$\frac{\delta P}{\delta X_j}(X_1, \cdots, X_h) \in a\mathfrak{O}_K[[X_1, \cdots, X_h]] + J.$$

If $|r| \geq 1$ and $r!$ is invertible in $\mathfrak{O}_K$, we see inductively (cf. Remark (4.1), (2))

$$\frac{\delta^r P}{\delta X^r}(X_1, \cdots, X_h) \in a\mathfrak{O}_K[[X_1, \cdots, X_h]] + J,$$

so

$$\frac{\delta^r P}{\delta X^r}(u_1, \cdots, u_h) \in aS + aI = aS.$$

Since $I^2 \subset I_2$, we have

$$\frac{\delta^r P}{\delta X^r}(u_1, \cdots, u_h) \cdot \mu^r \in aI_2,$$

if $|r| \geq 2$ and $r!$ is invertible in $\mathfrak{O}_K$.

On the other hand, we have $\mu^r \in I^{|r|} \subset I^p \subset aI_2$ if p divides $r!$, and $\frac{\delta^r P}{\delta X^r}(u_1, \cdots, u_h)$ are always in S (Remark (4.1), (5)). Thus we have

$$R_i \in aI_2. \tag{4.4.3}$$

Take an element $P_{ij} \in \mathfrak{O}_K[[X_1, \cdots, X_h]]$ such that $\alpha(P_{ij}) = p_{ij} \in B$ for each (i, j). We have

$$\frac{\delta P_i}{\delta X_j}(x_1, \cdots, x_h) = ap_{ij},$$

i.e., $\frac{\delta P_i}{\delta X_j} = aP_{ij} + R_{ij}$ with some $R_{ij} \in J$, from which follows the congruence

$$\frac{\delta P_i}{\delta X_j}(u_1, \cdots, u_h) \equiv aP_{ij}(u_1, \cdots, u_h) \pmod{aI},$$

and

$$\frac{\delta P_i}{\delta X_j}(u_1, \cdots u_h) \cdot \mu_j \equiv aP_{ij}(u_1, \cdots, u_h) \cdot \mu_j \pmod{aI_2}. \tag{4.4.4}$$

Putting (4.4.3) and (4.4.4) into (4.4.2), we have

$$P_i(u_1 + \mu_1, \cdots, u_h + \mu_h) \equiv a(\lambda_i + \sum_j P_{ij}(u_1, \cdots, u_h) \cdot \mu_j) \pmod{aI_2}.$$

Since S is flat over $\mathfrak{O}_K$, the condition (4.4.1) for μ_j is now equivalent to

$$\lambda_i + \sum_j P_{ij}(u_1, \cdots, u_h) \cdot \mu_j \equiv 0 \pmod{I_2}, \quad 1 \leq i \leq h.$$

Since the matrix $(p_{ij}) = (P_{ij}(x_1, \cdots, x_h))$ is invertible, the matrix $(P_{ij}(u_1, \cdots, u_h))$ is invertible modulo aI. Now the existence of $\mu_j \in I$ satisfying (4.4.1) is clear. Moreover $u_j \pmod{I}$, $1 \leq j \leq h$, determine $\mu_j \pmod{I_2}$, $1 \leq j \leq h$, uniquely, because they determine $\lambda_i \equiv 0 \pmod{I}$ and $P_{ij}(u_1, \cdots, u_h) \pmod{I}$ uniquely and $I^2 \subset I_2$.

Part (b) of (i) follows immediately from Part (a).

The proof of (ii) is exactly the same as in [5].

COROLLARY (4.5). *Let the notation and hypothesis be as in Proposition (4.4). Then we have* $v_K(\mathfrak{D}(L/K)) < v_K(a)+\frac{1}{p-1}\min\{v_K(a), v_K(p)\}$ *unless* $v_K(\mathfrak{D}(L/K)) = 0$.

PROOF:— If L/K is unramified, then $v_K(\mathfrak{D}(L/K)) = 0$. If not, we have $i_{L/K} > 0$ and (Prop. (4.3), (1))

$$v_K(\mathfrak{D}(L/K)) = u_{L/K} - i_{L/K} < u_{L/K} \leq v_K(a) + \frac{1}{p-1}\min\{v_K(a), v_K(p)\}.$$

THEOREM (4.6). *Let A be a complete discrete valuation ring with finite residue field, and fix a prime element π of A. Let K be a local field of "mixed characteristic" over A, i.e., a complete discrete valuation field K with perfect residue field which is endowed with an injective ring homomorphism $A \longrightarrow K$ inducing a local homomorphism $A \longrightarrow \mathfrak{O}_K$. Let $n \geq 1$ be an integer and J a finite flat π-module scheme over $\mathfrak{O}_K$ ([10], §1) such that the invariant differential module ω_J of J is a free $(\mathfrak{O}_K/\pi^n\mathfrak{O}_K)$-module. (A typical example of such a π-module is the kernel of π^n on a π-divisible group (loc. cit.)). Let* $u_o := nv_K(\pi)+\frac{1}{p-1}\min\{nv_K(\pi), v_K(p)\}$, *$H$ the kernel of the action of $G_K = Gal(K^{sep}/K)$ on $J(K^{sep})$, $L := (K^{sep})^H$. Then we have $G_K^{(u)} \subset H$ for all $u > u_o$, and $v_K(\mathfrak{D}(L/K)) < u_o$.*

PROOF:— As in the proof of Théorème 1 of [5], the affine ring B of J is locally of complete intersection. Since $\Omega^1_{B/\mathfrak{O}_K} = B \otimes_{\mathfrak{O}_K} \omega_J$ is a free $(B/\pi^n B)$-module, we can apply Prop. (4.4) and Cor. (4.5) with $a = \pi^n$ and obtain the theorem.

REMARK (4.7). In some simple cases, direct calculations yield sharper results. For example, let A and π be as above, F the fraction field of A, and F_n, $n \geq 0$, the field of π^n-division points of a Lubin-Tate group over A associated with π. If $L/K = F_m/F_n$ with $m > n$, we have

$$u_{L/K} = \begin{cases} m, & \text{if } n = 0, \\ q^n + (m-n-1)(q^n - q^{n-1}), & \text{if } n \geq 1, \end{cases}$$

$$i_{L/K} = \begin{cases} \frac{1}{q-1}, & \text{if } n = 0, \\ q^{n-1}, & \text{if } n \geq 1, \end{cases}$$

$$v_K(\mathfrak{D}(L/K)) = \begin{cases} m - \frac{1}{q-1}, & \text{if } n = 0, \\ (m-n)(q^n - q^{n-1}), & \text{if } n \geq 1. \end{cases}$$

5. The case of non-scalar A-actions on tangent spaces

Important classes of abelian T-modules ([1]), such as higher Carlitz modules $C^{\otimes n}$ ([2]) and tensor products of Drinfeld modules ([1], [6]), are such that the actions of T on the tangent spaces are not just multiplication by T, but T plus nilpotent linear maps. In this section, we study the ramification arising from division points of such objects.

Let A, π and K be as in Th. (4.6); A a complete discrete valuation ring with finite residue field, π a uniformizer of A, and K a local field of "mixed characteristic" over A. Consider a smooth connected commutative formal group J over $\mathfrak{O}_K$ with an A-action

$$\phi : A \longrightarrow \mathrm{End}_{\mathfrak{O}_K}(J)\,; \qquad a \mapsto \phi_a$$

such that, for all $a \in A$, ϕ_a induces a linear map $\mathrm{Lie}(\phi_a)$ on $\mathrm{Lie}(J)$ of the form (multiplication by a) + (nilpotent map). If J is, for example, the tensor product of abelian T-modules with scalar T-actions on their tangent spaces, Th. (4.6) for $J_n = \mathrm{Ker}(\phi_{T^n})$ would be valid because $\otimes$ and $T_v(\cdot)$ should be compatible (this is shown in [6] at least for tensor products of two Drinfeld modules). What can be said on the ramification of the geometric points of $J_n := \mathrm{Ker}(\phi_{\pi^n})$ in other cases ?

(5.1). First assume that the nilpotent map $\mathrm{Lie}(\phi_{\pi^n}) - \pi$ is divisible by π in $\mathrm{End}_{\mathfrak{O}_K}(\mathrm{Lie}(J))$. Then, since the image of $\mathrm{Lie}(\phi_{\pi^n})$ is $\pi^n \mathrm{Lie}(J)$, we have

$$\Omega^1_{J_n} \;=\; \Omega^1_J/\pi^n\Omega^1_J,$$

which is a flat $B/\pi^n B$-module (B is the affine ring of J_n). So we can apply Prop. (4.4), and Th. (4.6) remains valid for such J_n.

(5.2). We now return to a general J. Let $d := \dim(J) = \mathrm{rank}_{\mathfrak{O}_K}(\mathrm{Lie}(J))$, and let p^k be the smallest power of p, the residue characteristic of A, such that $p^k \geq d$. Then for any multiple m of p^k, the nilpotent map $\mathrm{Lie}(\phi_{\pi^m}) - \pi^m$ is divisible by π^m in $\mathrm{End}_{\mathfrak{O}_K}(\mathrm{Lie}(J))$, as is easily seen by looking at the binomial expansion of $[\pi + (\mathrm{Lie}(\phi_\pi) - \pi)]^{p^k}$. In view of (5.1), we have

THEOREM (5.3). *Let J and p^k be as above. For a positive integer n, let n' be the smallest multiple of p^k not less than n, $u_o := n' v_K(\pi) + \frac{1}{p-1} min\{n' v_K(\pi),\ v_K(p)\}$, H the kernel of the action of G_K on $J_n(K^{sep})$, and $L := (K^{sep})^H$. Then we have $G_K^{(u)} \subset H$ for all $u > u_o$, and $v_K(\mathfrak{D}(L/K)) < u_o$.*

This theorem reduces to Th. (4.6) when n is divisible by p^k. But if n is not divisible by p^k, the ramification can be bigger than expected from Th. (4.6), as the following example shows:

EXAMPLE (5.4). Let $A = \mathbb{F}_q[[T]]$ and $K = \mathbb{F}_q((T))$, and consider the d-dimensional

formal group $\widehat{\mathbb{G}}_a^{\oplus d}$ over A with an A-action defined by

$$\phi_T \begin{pmatrix} X_1 \\ \vdots \\ X_d \end{pmatrix} = \begin{pmatrix} T & -1 & & \\ & \ddots & \ddots & \\ & & \ddots & -1 \\ & & & T \end{pmatrix} \begin{pmatrix} X_1 \\ \vdots \\ X_d \end{pmatrix} + \begin{pmatrix} X_1^q \\ \vdots \\ X_d^q \end{pmatrix}.$$

Then we have

$$K(J_1(K^{sep})) \;=\; K(_{T^d}C(K^{sep})),$$

where C is the Carlitz module defined by $C_T(X) = TX + X^q$. This means that $\mathfrak{D}(K(J_1(K^{sep}))/K)$ can become arbitrarily large according to d.

References

[1] G. W. Anderson, t-motives, Duke Math. J. 53 (1986), 457 – 502

[2] G. W. Anderson and D. S. Thakur, Tensor powers of the Carlitz module and zeta values, Ann. of Math. 132 (1990), 159 – 191

[3] V. G. Drinfeld, Elliptic modules, Math. USSR Sb. 23 (1974), 561 – 592

[4] G. Faltings, Endlichkeitssätze für Abelsche Varietäten über Zahlkörpern, Inv. Math. 73 (1983), 349 – 366

[5] J-M. Fontaine, Il n'y a pas de variété abélienne sur $\mathbb{Z}$, Inv. Math. 81 (1985), 515 – 538

[6] Y. Hamahata, On the Tate module associated to the tensor product of two Drinfeld modules I, II, preprint

[7] D. Hayes, Explicit class field theory for rational function fields, Trans. Am. Math. Soc. 189 (1974), 77 – 91

[8] J-P. Serre, Corps locaux (3ème édition), Hermann, Paris (1980)

[9] J-P. Serre, A letter to D. Goss, dated April 14, 1990

[10] Y. Taguchi, Semi-simplicity of the Galois representations attached to Drinfeld modules over fields of "infinite characteristics", preprint

Chapter II

A duality for finite t-modules

Introduction

In this Chapter, we establish a duality for finite t-modules and study its basic properties. Our duality is the $\mathbb{F}_q[t]$-analogue of the Cartier duality, where the multiplicative group $\mathbb{G}_m$ is replaced by the Carlitz module C. Finite t-modules are, roughly speaking, finite locally free group schemes which are $\mathbb{F}_q[t]$-submodules of abelian t-modules ([1]) with scalar t-action on their tangent spaces. See (2.1) for the precise definition. In fact, it is only for a *finite v-module* (Definition (3.1)) that we can define the duality (Definition (4.1)), in a way with Dieudonné theoretic flavor. See Remarks (4.4), (4.5), and Example (4.6) for accounts of the necessity of a v-module structure.

A typical case of our duality is supplied by division points of Drinfeld modules and *dual Drinfeld modules*, and is studied in some detail in Section 5. In Section 6, some results on the duality of π-divisible groups are given.

One may hope to have such a duality for a wider class of t-modules, namely, torsion points of abelian t-modules which do not have scalar t-action on the tangent spaces, such as higher Carlitz modules $C^{\otimes n}$ ([2]). But this would be possible only if the target C of the pairing were replaced by a tensor power $C^{\otimes n}$ with sufficiently large n.

Throughout this Chapter, $\mathcal{O}_S$ denotes the structure sheaf of a scheme S. In general, we will use the following unusual

NOTATION. A morphism of schemes is denoted by a capital letter, and the corresponding morphism of the structure sheaves is denoted by the corresponding small letter.

1. Finite φ-modules

For the moment, let A be any commutative ring, and recall the definition of an A-module scheme. For an A-scheme S, we denote by $\alpha : A \to \Gamma(S, \mathcal{O}_S)$ the structure morphism.

DEFINITION (1.1). An *A-module scheme* over an A-scheme S is a pair (G, Ψ) consisting of a commutative group scheme G over S and a ring homomorphism

$\Psi : A \to \mathrm{End}(G/S)$; $a \mapsto \Psi_a$ such that, for each $a \in A$, Ψ_a induces multiplication by $\alpha(a)$ on the $\mathcal{O}_S$-module $\mathrm{Lie}^*(G/S)$.

A *morphism* $M : (G, \Psi) \to (G', \Psi')$ of A-module schemes is a morphism $M : G \to G'$ of group schemes such that $M \circ \Psi_a = \Psi'_a \circ M$ for all $a \in A$.

EXAMPLE (1.2). A vector bundle G on S can be naturally regarded as a $\Gamma(S, \mathcal{O}_S)$-module scheme. We shall mean by a *vector group scheme* such a $\Gamma(S, \mathcal{O}_S)$-module scheme.

We will often write simply G for an A-module scheme in place of (G, Ψ).

Hereafter in this section, let A be the finite field $\mathbb{F}_q$ of q elements and S an $\mathbb{F}_q$-scheme.

For an $\mathbb{F}_q$-module scheme (G, Ψ) over S, set $\mathcal{E}_G := \underline{\mathrm{Hom}}_{\mathbb{F}_q, S}(G, \mathbb{G}_a)$. ($\underline{\mathrm{Hom}}_{\mathbb{F}_q, S}$ denotes the Zariski sheaf on S of $\mathbb{F}_q$-linear homomorphisms.) If G/S is affine (as is always the case in the following), we may confuse $\mathcal{O}_G$ and $\pi_* \mathcal{O}_G$ (where π is the structure morphism of G/S) and may think of $\mathcal{O}_G$ as an $\mathcal{O}_S$-algebra. Then $\mathcal{E}_G$ is the $\mathcal{O}_S$-submodule of the augmentation ideal $\mathcal{I}_G$ of $\mathcal{O}_G$ consisting of the local sections X which satisfy

$$\begin{cases} \delta(X) = X \otimes 1 + 1 \otimes X, & \text{and} \\ \psi_a(X) = \alpha(a)X & \text{for all } a \in \mathbb{F}_q. \end{cases}$$

Here $\delta : \mathcal{O}_G \to \mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_G$ is the coproduct of $\mathcal{O}_G$ and $\psi_a : \mathcal{O}_G \to \mathcal{O}_G$ is the $\mathcal{O}_S$-algebra homomorphism corresponding to $\Psi_a : G \to G$.

Note the correspondence $G \mapsto \mathcal{E}_G$ is similar to the "t-motive" construction ([1], §1). See also Remark (3.7) below.

DEFINITION (1.3). An $\mathbb{F}_q$-module scheme (G, Ψ) over S is called a *finite φ-module* if $\mathcal{O}_G$ and $\mathcal{E}_G$ are locally free of finite rank over $\mathcal{O}_S$ with $\mathrm{rank}(\mathcal{O}_G) = q^{\mathrm{rank}(\mathcal{E}_S)}$, and $\mathcal{E}_G$ generates the $\mathcal{O}_S$-algebra $\mathcal{O}_G$.

A *morphism* of finite φ-modules is by definition a morphism of $\mathbb{F}_q$-module schemes.

REMARK (1.4). (i) A finite φ-module G over S can be embedded canonically into the vector group scheme $E_G := \mathbb{V}(\mathcal{E}_G) = \underline{\mathrm{Spec}}(\mathrm{Sym}_{\mathcal{O}_S} \mathcal{E}_G)$ as an $\mathbb{F}_q$-submodule scheme (See also Proposition (1.8)), because $\mathcal{E}_G$ generates $\mathcal{O}_G$. Let us agree to call E_G/S the *ambient space* of G/S. It is clear that a morphism $M : G \to G'$ of finite φ-modules extends uniquely to a morphism $E_M : E_G \to E_{G'}$ of $\mathbb{F}_q$-module schemes.

(ii) The group scheme μ_p of p-th roots of unity over an $\mathbb{F}_p$-scheme is *not* a finite φ-module.

Note that, if $M : G \to G'$ is a morphism of $\mathbb{F}_q$-module schemes, then the corresponding morphism $m : \mathcal{O}_{G'} \to \mathcal{O}_G$ restricts to give an $\mathcal{O}_S$-module homomorphism $m : \mathcal{E}_{G'} \to \mathcal{E}_G$. Since $\mathcal{E}_{G'}$ generates $\mathcal{O}_{G'}$ if G' is a finite φ-module, we have

LEMMA (1.5). *Let G and G' be finite φ-modules. Then the natural homomorphism* $\mathrm{Hom}_{\varphi, S}(G, G') \to \mathrm{Hom}_{\mathcal{O}_S\text{-mod}}(\mathcal{E}_{G'}, \mathcal{E}_G)$ *is injective.*

In the following, for an $\mathcal{O}_S$-module $\mathcal{E}$ (resp. an $\mathcal{O}_S$-module homomorphism m), $\mathcal{E}^{(q)}$ (resp. $m^{(q)}$) denotes the base extension $\mathcal{E} \otimes_{\mathcal{O}_S} \mathcal{O}_S$ (resp. $m \otimes 1$) by the q-th power map $\mathcal{O}_S \to \mathcal{O}_S$. For example, if G is a group scheme over S, then $\mathcal{O}_G^{(q)}$ is the structure sheaf of the *Frobenius gruop scheme* $G^{(q)}$. Also, we denote by $F_G : G \to G^{(q)}$ (resp. $f_G : \mathcal{O}_G^{(q)} \to \mathcal{O}_G$) the *Frobenius morphism*. If G is an $\mathbb{F}_q$-module scheme, then so is $G^{(q)}$ and F_G is a morphism of $\mathbb{F}_q$-module schemes.

To understand the role of $\mathcal{E}_G$, recall

DEFINITION (1.6). (Drinfeld [3], §2) A *φ-sheaf* is a pair $(\mathcal{E}, \varphi)$ consisting of a locally free $\mathcal{O}_S$-module $\mathcal{E}$ on S of finite rank and an $\mathcal{O}_S$-module homomorphism $\varphi : \mathcal{E}^{(q)} \to \mathcal{E}$.

A *morphism* $m : (\mathcal{E}, \varphi) \to (\mathcal{E}', \varphi')$ of φ-sheaves is an $\mathcal{O}_S$-module homomorphism $m : \mathcal{E} \to \mathcal{E}'$ which makes the diagram

$$\begin{array}{ccc} \mathcal{E}^{(q)} & \xrightarrow{m^{(q)}} & \mathcal{E}'^{(q)} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ \mathcal{E} & \xrightarrow[m]{} & \mathcal{E}' \end{array}$$

commutative.

Let $(\mathcal{E}, \varphi)$ be a φ-shaef and $E = \mathbb{V}(\mathcal{E})$ the vector bundle corresponding to $\mathcal{E}$. $\varphi : \mathcal{E}^{(q)} \to \mathcal{E}$ induces a morphism $\Phi : E \to E^{(q)}$ of $\mathbb{F}_q$-module schemes. Drinfeld defines then

$$\begin{aligned} \mathrm{Gr}(\mathcal{E}, \varphi) &:= \mathrm{Ker}(\Phi - F_E : E \to E^{(q)}) \\ &= \underline{\mathrm{Spec}}\left(\mathcal{S}/[(\varphi - f_S)(\mathcal{E}^{(q)})]\right), \end{aligned}$$

where $\mathcal{S} = \mathcal{O}_E$ is the symmetric algebra $\mathrm{Sym}_{\mathcal{O}_S}^{\cdot} \mathcal{E}$, $f_S = f_E$ is the Frobenius morphism $\mathcal{S}^{(q)} \to \mathcal{S}$, and the bracket $[\cdots]$ denotes the ideal generated by its contents. This is a finite φ-module of rank $q^{\mathrm{rank}(\mathcal{E}_G)}$, with $\mathbb{F}_q$-action induced by the natural $\mathbb{F}_q$-module structure on $\mathcal{E}$. Note $\mathcal{E}_{\mathrm{Gr}(\mathcal{E},\varphi)} = \mathcal{E}$.

Conversely, if G is a finite φ-module over S, the Frobenius morphism $f_G : \mathcal{O}_G^{(q)} \to \mathcal{O}_G$ induces an $\mathcal{O}_S$-module homomorphism $\varphi_G : \mathcal{E}_G^{(q)} \to \mathcal{E}_G$. Then $(\mathcal{E}_G, \varphi_G)$ is a φ-sheaf. The natural $\mathcal{O}_S$-algerbra homomorphism $\mathrm{Sym}_{\mathcal{O}_S}^{\cdot} \mathcal{E}_G \to \mathcal{O}_G$ is surjective, and its kernel contains $(\varphi_G - f_{E_G})(\mathcal{E}_G^{(q)})$. Hence we have a surjection $\mathcal{O}_{\mathrm{Gr}(\mathcal{E}_G, \varphi_G)} \to \mathcal{O}_G$ of locally free $\mathcal{O}_S$-algebras. The equality $\mathrm{rank}(\mathcal{O}_G) = q^{\mathrm{rank}(\mathcal{E}_G)}$ implies $\mathrm{Gr}(\mathcal{E}_G, \varphi_G) \simeq G$.

The commutativity of m and φ in the definition of a morphism $m : (\mathcal{E}, \varphi) \to (\mathcal{E}', \varphi')$ of φ-sheaves means that $m : \mathcal{E} \to \mathcal{E}'$ extends to an $\mathcal{O}_S$-Hopf algebra homomorphism

$$m : \mathcal{S}/[(\varphi - f_S)(\mathcal{E}^{(q)})] \longrightarrow \mathcal{S}'/[(\varphi' - f_{S'})(\mathcal{E}'^{(q)})].$$

($\mathcal{S}'$ is the symmetric algebra made of $\mathcal{E}'$.) This is clearly compatible with the natural $\mathbb{F}_q$-actions. Noticing Lemma (1.5), we have thus

PROPOSITION (1.7). *The category of finite φ-modules over S is anti-equivalent to the category of φ-sheaves on S.*

Also the next proposition should be noted.

PROPOSITION (1.8). *A finite locally free group scheme G over S is a finite φ-module if and only if it can be embedded into a vector group scheme E as the kernel of an endomorphism of the $\mathbb{F}_q$-module scheme E.*

PROOF:— Let G be a finite φ-module, and let the notation be as before;

$$G = \mathrm{Gr}(\mathcal{E},\varphi) = \underline{\mathrm{Spec}}\left(\mathcal{S}/[(\varphi - f_S)(\mathcal{E}^{(q)})]\right).$$

Then G is the kernel of an endomorphism of E defined by sections of $(\varphi - f_S)(\mathcal{E}^{(q)})$.

Conversely, an $\mathbb{F}_q$-endomorphism of a vector group scheme E is given, locally on S, by a polynomial in τ, the q-th power map, with coefficients in the matrix algebra over $\mathcal{O}_S$. By using additional variables if necessary, we can write the kernel G of such a morphism in the form

$$\mathrm{Spec}\ \mathcal{O}_S[X_1,\cdots,X_n]/[AX - BX^{(q)}],$$

where A and B are $n \times n$ matrices, and $X := {}^t(X_1,\cdots,X_n)$ and $X^{(q)} := {}^t(X_1^q,\cdots,X_n^q)$. Since G is locally free over $\mathcal{O}_S$, B must be invertible, and hence G is of the form $\mathrm{Gr}(\mathcal{E},\varphi)$. Q.E.D.

The set of valued points of $\mathrm{Gr}(\mathcal{E},\varphi)$ is described as follows:

PROPOSITION (1.9). *Let $(\mathcal{E},\varphi)$ be a φ-sheaf on S, and let T be an S-scheme. Then the set of T-valued points of $\mathrm{Gr}(\mathcal{E},\varphi)$ is*

$$\mathrm{Gr}(\mathcal{E},\varphi)(T) = \mathrm{Hom}_{\varphi,\mathcal{O}_S}(\mathcal{E},\mathcal{O}_T),$$

the set of $\mathcal{O}_S$-linear homomorphisms $f : \mathcal{E} \to \mathcal{O}_T$ such that $f(\varphi(x)) = f(x)^q$ for any local section x of $\mathcal{E}$.

PROOF:— This is clear from the definiton of $\mathrm{Gr}(\mathcal{E},\varphi)$. Q.E.D.

2. Finite t-modules

In the rest of this Chapter, A is the polynomial ring $\mathbb{F}_q[t]$ in one variable t over $\mathbb{F}_q$. We work over a fixed A-scheme S, and denote by θ the image of t under the structure morphism $\alpha : A \to \Gamma(S,\mathcal{O}_S)$.

DEFINITION (2.1). A *finite t-module* (G,Ψ) over S is an A-module scheme over S such that
(1) G is killed by some $a \in A - \mathbb{F}_q$; and
(2) $(G, \Psi\,|_{\mathbb{F}_q})$ is a finite φ-module over S.

A *morphism* of finite t-modules is by definition a morphism of A-module schemes.

A typical example of a finite t-module is a finite $\mathbb{F}_q[t]$-submodule of an abelian t-module ([1]) with scalar t-action on its tangent space. As is well-known, we have

LEMMA (2.2). *A finite t-module G/S which is killed by $a \in A - 0$ is étale over S if a is invertible on S.*

PROOF:— It is enough to see $\Omega^1_{G/S} = 0$, but $a \cdot \Omega^1_{G/S} = 0$ and a is invertible. Q.E.D.

REMARK (2.3). If (G, Ψ) is a finite t-module, Ψ induces an action of A on the ambient space E_G (Remark (1.4), (i)). But E_G with this action is *not* in general an A-module scheme in the sense of Definition (1.1).

DEFINITION (2.4). A *t-sheaf* $(\mathcal{E}, \varphi, \psi_t)$ (or simply, $(\mathcal{E}, \varphi, \psi)$) on S is a pair consisting of a φ-sheaf $(\mathcal{E}, \varphi)$ and an endomorphism ψ_t of $(\mathcal{E}, \varphi)$ such that
(1) there exists a polynomial $a(X) \in \mathbb{F}_q[X]$ such that $a(\varphi_t) = 0$ on $\mathcal{E}$; and
(2) ψ_t induces multiplication by θ on $\mathrm{Coker}(\varphi)$. (Recall that $\mathrm{Coker}(\varphi)$ is canonically isomorphic to $\mathrm{Lie}^* \mathrm{Gr}(\mathcal{E}, \varphi)$ ([3], Proposition 2.1, 2)).)

Equivalently, we may think that ψ is a ring homomorphism $A \to \mathrm{End}_{\varphi, \mathcal{O}_S}(\mathcal{E})$; $a \mapsto \psi_a$ such that $\psi_a = 0$ for some $a \in A - \mathbb{F}_q$ and, for each $a \in A$, ψ_a induces multiplication by $\alpha(a)$ on $\mathrm{Coker}(\varphi)$.

A *morphism* $m : (\mathcal{E}, \varphi, \psi_t) \to (\mathcal{E}', \varphi', \psi'_t)$ is a morphism of φ-sheaves such that $m \circ \psi_t = \psi'_t \circ m$.

The following proposition, extending (1.7), is obvious.

PROPOSITION (2.5). *The category of finite t-modules over S is anti-equivalent to the category of t-sheaves on S.*

We write $\mathrm{Gr}(\mathcal{E}, \varphi, \psi)$ for the finite t-module corresponding to a t-sheaf $(\mathcal{E}, \varphi, \psi)$.

EXAMPLE (2.6). Let (E, Ψ) be a Drinfeld A-module of rank r over S. Assume for simplicity that $S = \mathrm{Spec}\ R$ with R an A-algebra, and that the action of t is given by

$$\psi_t(X) = \theta X + a_1 A^q + \cdots + a_r X^{q^r}, \quad a_i \in R,\ a_r \in R^\times,$$

with respect to a trivialization $E \simeq \mathbb{G}_a = \mathrm{Spec}\ R[X]$. Then for $a \in A - 0$, $G := \mathrm{Ker}(\Psi_a)$ is a finite t-module over R. $\mathcal{E}_G$ is a free R-module of rank $r \cdot \deg(a)$ with a basis $(X^{q^j};\ 0 \le j \le r \cdot \deg(a) - 1)$, and $\varphi : \mathcal{E}_G^{(q)} \to \mathcal{E}_G$ is given by

$$\varphi(X^{q^j} \otimes 1) = X^{q^{j+1}}.$$

Here $X^{q^{j+1}}$ for $j + 1 \ge r \cdot \deg(a)$ should be rewritten in terms of $(X^{q^j};\ 0 \le j \le r \cdot \deg(a) - 1)$ according to the relation $\psi_a(X) = 0$.

In the simple case where $a = t^k$, we can take the basis $(\psi_{t^i}(X)^{q^j};\ 0 \le i \le k - 1, 0 \le j \le r - 1)$ of $\mathcal{E}_G$, with respect to which ψ_t is represented by the matrix whose (i, j)-component is 1 if $i = j + r$ and 0 otherwise.

3. Finite v-modules

To establish a nice duality, we need one more structure.

Recall that a finite φ-module G is embedded canonically into its ambient space E_G (Remark (1.4), (i)), which is a vector group scheme.

DEFINITION (3.1). A *finite v-module* (G, Ψ, V) over S is a finite t-module scheme (G, Ψ) over S together with a morphism $V : E_G^{(q)} \to E_G$ of $\mathbb{F}_q$-module schemes such that $\Psi_t = (\theta + V \circ F_{E_G}) \mid_G$. (Here θ means multiplication by $\theta = \alpha(t) \in \Gamma(S, \mathcal{O}_S)$ on E_G, and F_{E_G} is the Frobenius morphism of E_G.)

A *morphism* $M : (G, \Psi, V) \to (G', \Psi', V')$ of finite v-modules is a morphism of finite φ-modules which renders the diagram

$$\begin{array}{ccc} E_G & \xrightarrow{E_M} & E_{G'} \\ {\scriptstyle V}\uparrow & & \uparrow{\scriptstyle V'} \\ E_G^{(q)} & \xrightarrow[E_M^{(q)}]{} & E_{G'}^{(q)} \end{array}$$

commutative.

DEFINITION (3.2). A *v-sheaf* $(\mathcal{E}, \varphi, v)$ on S is a pair consisting of a φ-sheaf on S and an $\mathcal{O}_S$-module homomorphism $v : \mathcal{E} \to \mathcal{E}^{(q)}$ such that $(\mathcal{E}, \varphi, \psi_t)$ with $\psi_t := \theta + \varphi \circ v$ is a t-sheaf on S. (Here θ means multiplication by θ on $\mathcal{E}$.)

A *morphism* $m : (\mathcal{E}, \varphi, v) \to (\mathcal{E}', \varphi', v')$ of v-sheaves is a morphism of φ-sheaves which renders the diagram

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{m} & \mathcal{E}' \\ {\scriptstyle v}\downarrow & & \downarrow{\scriptstyle v'} \\ \mathcal{E}^{(q)} & \xrightarrow[m^{(q)}]{} & \mathcal{E}'^{(q)} \end{array}$$

commutative.

These definitions are made so that Proposition (2.5) extends to

PROPOSITION (3.3). *The category of finite v-modules over S is anti-equivalent to the category of v-sheaves on S.*

We write $\mathrm{Gr}(\mathcal{E}, \varphi, v)$ for the finite v-module corresponding to a v-sheaf $(\mathcal{E}, \varphi, v)$.

EXAMPLE (3.4). Let (E, Ψ) and $G = \mathrm{Ker}(\Psi_a)$ be as in Example (2.6). Then the finite t-module G is furnished with a standard v-module structure by

$$\begin{aligned} &v : \mathcal{E}_G \to \mathcal{E}_G^{(q)}, \\ &X^{q^i} \mapsto X^{q^{i-1}} \otimes (\theta^{q^i} - \theta) + X^{q^i} \otimes a_1^{q^i} + \cdots + X^{q^{r+i-1}} \otimes a_r^{q^i}. \end{aligned}$$

(Here $X^{q^{i-1}} \otimes (\theta^{q^i} - \theta) := 0$ if $i = 0$.) If $G = \mathrm{Ker}(\Psi_t)$ for example and if we regard $\mathcal{E}_G$ and $\mathcal{E}_G^{(q)}$ as the column vectors of rank r by fixing the R-basis $(X^{q^j})_{0 \le j \le r-1}$ and $(X^{q^j} \otimes 1)_{0 \le j \le r-1}$ respectively, then v is represented by the matrix

$$\begin{pmatrix} a_1 & -\theta & & \\ \vdots & & \ddots & \\ \vdots & & & -\theta \\ a_r & & & \end{pmatrix}.$$

(The vacant components are 0.) Note that $\psi_t = 0$ on $\mathcal{E}_G$ in this case, and still v has enough information to recover the dual of G. But this v-module structure is *not* unique unless $\mathrm{Ker}(\varphi_G : \mathcal{E}_G^{(q)} \to \mathcal{E}_G) = 0$.

In fact, finite v-modules over "mixed characteristic" bases are not so far from finite t-modules, since we have:

PROPOSITION (3.5). *Let (G, Ψ) be a finite t-module which is étale over the generic points of S. Then (G, Ψ) has a unique v-module structure V_G extending the given t-module structure; $\Psi_t = (\theta + V_G \circ F_{E_G}) \mid_G$. If G and G' are two such finite t-modules, then a morphism $G \to G'$ of finite t-modules preserves this v-module structure. In particular, if $\alpha : A \to \mathcal{O}_S$ is injective (cf. Lemma (2.2)), the two concepts, a finite t-module and a finite v-module, are equivalent.*

The same is valid for a t-sheaf $(\mathcal{E}, \varphi, \psi_t)$ such that $\varphi : \mathcal{E}^{(q)} \to \mathcal{E}$ is injective over the generic points.

PROOF:— We prove this for t-sheaves. By (2) of Definition (2.4), we have

$$\mathrm{Im}(\psi_t - \theta) \subset \mathrm{Im}(\varphi).$$

Hence $v := \varphi^{-1} \circ (\psi_t - \theta) : \mathcal{E} \to \mathcal{E}^{(q)}$ is well-defined and gives a unique v-sheaf structure on $(\mathcal{E}, \varphi)$ extending the t-sheaf structure ψ_t.

Let $m : (\mathcal{E}, \varphi, \psi_t) \to (\mathcal{E}', \varphi', \psi_t')$ be a morphism of t-sheaves. If φ and φ' are generically injective, we have the diagram

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{m} & \mathcal{E}' \\ {\scriptstyle v}\downarrow & & \downarrow{\scriptstyle v'} \\ \mathcal{E}^{(q)} & \xrightarrow{m^{(q)}} & \mathcal{E}'^{(q)} \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle \varphi'} \\ \mathcal{E} & \xrightarrow[m]{} & \mathcal{E}' \end{array}$$

in which v and v' are defined as above and in which the outer and the lower squares are commutative. Since φ' is generically injective, the upper square is also commutative, i.e., m is a morphism of v-sheaves. Q.E.D.

EXAMPLE (3.6). Let C be the Carlitz module over Spec A, i.e., the rank one Drinfeld A-module on $\mathbb{G}_a = \text{Spec } A[Z]$ with t-action given by $\gamma_t : Z \mapsto \theta Z + Z^q$. (Here, one may choose another t-action $Z \mapsto \theta Z + aZ^q$ for any $a \in \mathbb{F}_q^\times$, but then $a^{-1}t$ acts by $Z \mapsto \alpha(a^{-1}t)Z + Z^q$. So in the following, we fix $t \in A$ and its action on C as above.) Let G be a finite A-submodule of C. Then over A, G has a unique v-module structure

$$\begin{aligned} v_C : \mathcal{E}_G &\to \mathcal{E}_G^{(q)}, \\ Z^{q^i} &\mapsto Z^{q^{i-1}} \otimes (\theta^{q^i} - \theta) + Z^{q^i} \otimes 1. \end{aligned}$$

In §4, we shall think of $G \times_{\text{Spec } A} S$, over any base scheme S, as a finite v-module with v-structure induced by this canonical one. Also, it would be convenient in what follows to think of C itself as a "v-module" with $v_C : \mathcal{E}_C \to \mathcal{E}_C^{(q)}$ defined as above, though we deal in fact with its finite subgroups.

The following Remark is not used in this paper, but provides us with some feeling on $\mathcal{E}_G$.

REMARK (3.7). Let G be a finite v-module over S. Then the $\mathcal{O}_S$-module $\mathcal{E}_G$ would deserve the name the "Dieudonné module" of G, because we have $\mathcal{E}_G = \underline{\text{Hom}}_{v,S}(G, CW)$. Here CW is the v-module of "Witt covectors", defined as follows (we disregard the topology): CW is, as a group scheme, the infinte direct product of $\mathbb{G}_a$'s with affine algebra $\mathcal{O}_{CW} = \mathcal{O}_S[\cdots, X_{-n}, \cdots, X_{-1}, X_0]$, and the t-module and v-module structures are defined by

$$\begin{aligned} t : X_{-n} &\mapsto \theta X_{-n} + X_{-n-1}^q, \\ v : X_{-n} &\mapsto X_{-n-1} \otimes 1 \end{aligned}$$

for all $n \geq 0$.

4. The duality

For an $\mathcal{O}_S$-module $\mathcal{E}$, put $\mathcal{E}^* := \underline{\text{Hom}}_{\mathcal{O}_S}(\mathcal{E}, \mathcal{O}_S)$. If $(\mathcal{E}, \varphi, v)$ is a v-sheaf on S, then φ and v induce respectively the $\mathcal{O}_S$-module homomorphisms

$$\varphi^* : \mathcal{E}^* \to \mathcal{E}^{*(q)} \quad \text{and} \quad v^* : \mathcal{E}^{*(q)} \to \mathcal{E}^*.$$

It is easy to check that $(\mathcal{E}^*, v^*, \varphi^*)$ is a v-sheaf on S.

DEFINITION (4.1). We define the *dual* $(\mathcal{E}, \varphi, v)^*$ of a v-sheaf $(\mathcal{E}, \varphi, v)$ to be the v-sheaf $(\mathcal{E}^*, v^*, \varphi^*)$. For a finite v-module $G = \text{Gr}(\mathcal{E}, \varphi, v)$, define its *dual* G^* to be $\text{Gr}(\mathcal{E}^*, v^*, \varphi^*)$.

Note that if, as in Proposition (3.5), (G, Ψ) is a finite t-module which is étale over the generic points (resp. $(\mathcal{E}, \varphi, \psi_t)$ is a t-sheaf such that φ is injective over the generic points), then we can define its dual. We have clearly the following

PROPOSITION (4.2). *Let G be a finite v-module.*
(i) G^* has the same rank as G.
(ii) The correspondence $G \mapsto G^*$ is functorial. This functor is exact.
(iii) G^{**} is canonically isomorphic to G.
(iv) $(G \times_S T)^* \simeq G^* \times_S T$ for any S-scheme T.

The same is true for the duality of v-sheaves.

THEOREM (4.3). *Let C be the Carlitz module over Spec A (cf. Example (3.6)), and let G be a finite v-module over S.*
(i) The functor

$$\underline{\mathrm{Hom}}_{v,S} : (S\text{-schemes}) \to (A\text{-modules})$$
$$T \mapsto \mathrm{Hom}_{v,T}(G \times_S T,\ C \times_{\mathrm{Spec}\ A} T)$$

is represented by (the underlying finite t-module of) G^*.
(ii) There exists a canonical A-bilinear pairing of A-module schemes:

$$\Pi_G : G \times_S G^* \to C$$

such that:

(ii-1) If G' is a finite t-module over S sitting in an A-bilinear pairing $\Pi' : G \times_S G' \to C$, then there exists a unique morphism $M : G' \to G^*$ of finite t-modules which makes the diagram

$$\begin{array}{ccc} G \times_S G' & \xrightarrow{\Pi'} & C \\ {\scriptstyle 1\times M}\downarrow & & \| \\ G \times_S G^* & \xrightarrow[\Pi_G]{} & C \end{array}$$

commute.

(ii-2) If $M : G \to H$ is a morphism of finite v-modules and $M^* : H^* \to G^*$ is its dual morphism induced by functoiality, then we have

$$\Pi_H \circ (M \times 1) \ = \ \Pi_G \circ (1 \times M^*) \qquad \text{on } \ G \times H^*.$$

Conversely, M^* is the unique morphism which has this property.

(ii-3) If $\alpha : A \to \mathcal{O}_S$ is injective and S is integral with function field K, then Π_G induces a non-degenerate Galois equivariant A-bilinear pairing between the A-modules of geometric points:

$$G(K^{\mathrm{sep}}) \times G^*(K^{\mathrm{sep}}) \to C(K^{\mathrm{sep}}).$$

PROOF:— Recall that $\mathcal{O}_C$ is the polynomial ring $A[Z]$ with t-action $\gamma_t : Z \mapsto \theta Z + Z^q$ and v-module structure $v_C : \mathcal{E}_C \to \mathcal{E}_C^{(q)}$; $Z \mapsto Z \otimes 1$. Let $G = \mathrm{Gr}(\mathcal{E}_G, \varphi_G, v_G)$.

An $\mathcal{O}_T$-algebra homomorphism $m : \mathcal{O}_C \otimes_A \mathcal{O}_T \to \mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_T$ corresponds to a morphism of v-modules $G \times_S T \to C \times_{\mathrm{Spec}\ A} T$ if and only if

$$m(Z) \in \Gamma(T, \mathcal{E}_G \otimes_{\mathcal{O}_S} \mathcal{O}_T), \qquad \text{and} \tag{4.3.1}$$

$$m^{(q)} \circ v_C(Z) = (v_G \otimes 1) \circ m(Z). \tag{4.3.2}$$

Let $\mathcal{S}^*$ be the symmetric $\mathcal{O}_S$-algebra $\mathrm{Sym}^{\cdot}_{\mathcal{O}_S} \mathcal{E}_G^*$, and Z_0 a global section of $\mathcal{E}_G \otimes_{\mathcal{O}_S} \mathcal{E}_G^*$ which gives a basis of the rank one $\mathcal{O}_S$-submodule of $\mathcal{E}_G \otimes_{\mathcal{O}_S} \mathcal{E}_G^*$ on which one has $m \otimes 1 = 1 \otimes m^*$ for all $m \in \mathrm{End}_{\mathcal{O}_S}(\mathcal{E}_G)$. A *canonical* choice for Z_0 is $\sum_i X_i \otimes X_i^*$, where $(X_i)_i$ is a local basis of $\mathcal{E}_G$ and $(X_i^*)_i$ is its dual basis. Let

$$\begin{aligned} \iota : \mathcal{E}_G \otimes_{\mathcal{O}_S} \mathcal{E}_G^* &\to \mathcal{E}_G^{(q)} \otimes_{\mathcal{O}_S} \mathcal{E}_G^{*(q)} \\ X \otimes Y &\mapsto (X \otimes 1) \otimes (Y \otimes 1) \end{aligned}$$

be the natural map. Then we have $(v \otimes 1)(Z_0) = (1 \otimes v^*) \circ \iota(Z_0)$ for all $v \in \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{E}_G, \mathcal{E}_G^{(q)})$. If we take $\mathcal{O}_T = \mathcal{S}^*$ and $Z \mapsto Z_0$, then (4.3.2) reads

$$(1 \otimes f_{\mathcal{S}^\cdot}) \circ \iota(Z_0) = (1 \otimes v_G^*) \circ \iota(Z_0).$$

($f_{\mathcal{S}^\cdot}$ is the $\mathcal{O}_S$-linear Frobenius morphism $\mathcal{S}^{*(q)} \to \mathcal{S}^*$.) Let $\mathcal{J}^*$ be the smallest ideal of $\mathcal{S}^*$ such that

$$(1 \otimes (v_G^* - f_{\mathcal{S}^\cdot})) \circ \iota(Z_0) \in \mathcal{E}_G^{(q)} \otimes_{\mathcal{O}_S} \mathcal{J}^*.$$

Then it follows from what we observed at the beginning of the proof that the functor $\underline{\mathrm{Hom}}_{v,S}(G, C)$ is represented by $\underline{\mathrm{Spec}}(\mathcal{S}^*/\mathcal{J}^*) = \mathrm{Gr}(\mathcal{E}_G^*, v_G^*)$, with t-action induced by ψ_t^* on $\mathcal{E}_G^*$.

REMARK (4.4). To represent the functor $\underline{\mathrm{Hom}}_{v,S}(G, C)$, the v-module structure of G^* is not needed (and in fact a v-module structure on $\mathrm{Gr}(\mathcal{E}_G^*, v_G^*)$ may not be unique (cf. Example (3.4)), but for G to represent $\underline{\mathrm{Hom}}_{v,S}(G^*, C)$, G^* must have the v-module structure φ_G^*.

PROOF CONTINUED:— The pairing $G \times_S G^* \to C$ is given by

$$\begin{aligned} \pi : \mathcal{O}_C &\to \mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_{G^*}, \\ Z &\mapsto Z_1, \end{aligned}$$

where Z_1 is the image of Z_0 in $\mathcal{O}_G \otimes_{\mathcal{O}_S} (\mathcal{S}^*/\mathcal{J}^*)$. The universality of G^* (ii-1) is clear from the above discussion.

The non-degeneracy of (ii-2) is a consequence of a basic fact in linear algebra; let (X_i) and (Y_j) be $\mathcal{O}_S$-bases of $\mathcal{E}_G$ and $\mathcal{E}_H$ respectively, (X_i^*) and (Y_j^*) the dual bases, $m : \mathcal{E}_H \to \mathcal{E}_G$ an $\mathcal{O}_S$-linear map, and $m^* : \mathcal{E}_G^* \to \mathcal{E}_H^*$ its dual map. Then we have $\sum_i X_i \otimes m^*(X_i^*) = \sum_j m(Y_j) \otimes Y_j^*$ in $\mathcal{E}_G \otimes_{\mathcal{O}_S} \mathcal{E}_H^*$. Conversely, m^* is the unique $\mathcal{O}_S$-linear map with this property.

Since G is étale over K if α is injective (Lemma (2.2)), (ii-3) follows from the well-known equivalence between the category of finite étale K^{sep}-schemes and the category of finite sets. Q.E.D.

REMARK (4.5). If we consider only the t-module structure, we will have the following:

(i) The functor

$$\underline{\mathrm{Hom}}_{t,S}(G,C) : (S\text{-schemes}) \to (A\text{-modules})$$
$$T \mapsto \mathrm{Hom}_{t,T}(G \times_S T,\ C \times_{\mathrm{Spec}A} T)$$

is represented by an A-module scheme $\widetilde{G}^*$ over S.

(ii) If G is étale over the generic points of S, then $\widetilde{G}^*$ is of the form $G^* \cup \widetilde{G}_0^*$, where G^* is (the underlying finite t-module of) the dual finite v-module of G, G being considered to be a finite v-module with the unique v-module structure (Proposition (3.5)), and where $\widetilde{G}_0^*$ is supported on the locus in S over which G is not étale. In general, $\widetilde{G}_0^*$ has a positive dimension. For example:

EXAMPLE (4.6). Let R be an (A/tA)-algebra (i.e., we are in the "characteristic" (t) situation in the sense that the kernel of the structure map $\alpha : A \to R$ is (t)), and let $G = \mathrm{Spec}\ R[X_1,X_2]/(X_1^q, X_2^q)$ be a finite t-module with t acting by $X_i \mapsto 0$ for $i = 1,2$. If we think of G as the t-division points of the abelian t-module $(E,\Psi) = C^{\oplus 2}$;

$$E = \mathrm{Spec}\ R[X_1,X_2], \quad \psi_t\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = t\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} + \begin{pmatrix} X_1^q \\ X_2^q \end{pmatrix},$$

then it is natural to make G into a finite v-module by $v : X_i \mapsto X_i \otimes 1$ for $i = 1,2$. On the other hand, G can be regarded as the t-division points of another abelian t-module(E',Ψ') with

$$E' = \mathrm{Spec}\ R[X_1,X_2], \quad \psi'_t\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = t\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} + \begin{pmatrix} X_2^q \\ X_1^q \end{pmatrix}.$$

Now it is natural to make G into a finite v-module by $v : X_i \mapsto X_{3-i} \otimes 1$ for $i = 1,2$. In the former case, we have $G^* = \mathrm{Spec}\ R[Y_1,Y_2]/(Y_1 - Y_1^q, Y_2 - Y_2^q)$ (the constant group scheme $\mathbb{F}_q \oplus \mathbb{F}_q$), whereas in the latter case, we have $G^* = \mathrm{Spec}\ R[Y]/(Y - Y^{q^2})$ (the étale group scheme $\mathbb{F}_{q^2}$). Of course, we could choose any v-module structure $v : X_i \mapsto X_1 \otimes a_{1i} + X_2 \otimes a_{2i}$ for $i = 1,2$ with $a_{ji} \in R$. Without v-module structures, we will have $\widetilde{G}^* \simeq \mathbb{A}^2_R$ in this case.

Finally in this section, we describe a relation between the Frobenius and the Verschiebung over a "finite characteristic" base.

PROPOSITION (4.7). *Let (G,Ψ,V) be a finite v-module over S.*

(i) Let d be a positive integer, and $F_G^d : G \to G^{(q^d)}$ the q^d-th power Frobenius morphism. Then $G^{(q^d)}$ (resp. F_G^d) is a finite v-module (resp. a morphism of finite v-modules) if $\mathrm{Im}(\alpha) \subset \mathbb{F}_{q^d}$. If this is the case and $M : G \to G'$ is a morphism of finite v-modules, then we have $M^{(q^d)} \circ F_G^d = F_{G'}^d \circ M$.

(ii) Assume $\mathrm{Ker}(\alpha : A \to \mathcal{O}_S) = (\mathfrak{p})$ *with* $\mathfrak{p} \in A$ *being a monic prime element of degree* d. *Let* $V_{G,\mathfrak{p}} : G^{(q^d)} \to G$ *be the dual morphism of* $F_{G^*,\mathfrak{p}} := F^d_{G^*} : G^* \to G^{*(q^d)}$. *Then we have*

$$\Psi_{\mathfrak{p}} = V_{G,\mathfrak{p}} \circ F_{G,\mathfrak{p}} \quad \text{and} \quad \Psi_{\mathfrak{p}}^{(q^d)} = F_{G,\mathfrak{p}} \circ V_{G,\mathfrak{p}}.$$

In particular, we have an exact sequence of finite t*-modules*

$$0 \to \mathrm{Ker}(F_{G,\mathfrak{p}}) \to \mathrm{Ker}(\Psi_{\mathfrak{p}}) \to \mathrm{Ker}(V_{G,\mathfrak{p}}) \to 0.$$

PROOF:— (i) The only point we must care about is the action of $a \in A$ on $\mathrm{Lie}^*(G^{(q^d)})$, which is multiplication by $\alpha(a)^{(q^d)}$. This should be $\alpha(a)$, which is the case if $\mathrm{Im}(\alpha) \subset \mathbb{F}_{q^d}$. The compatibility conditions for v-module structures and morphisms are then automatically satisfied.

(ii) Let $Z \in \mathcal{O}_C$ and $Z_1 \in \mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_{G^*}$ have the same meaning as in the proof of Theorem (4.3). Let

$$\begin{aligned} \pi : \mathcal{O}_C &\to \mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_{G^*} \\ Z &\mapsto Z_1 \end{aligned}$$

be the $\mathcal{O}_S$-algebra homomorphism corresponding to the pairing $\Pi_G : G \times_S G^* \to C$. Then the A-linearity of the pairing is written as

$$(\psi_{\mathfrak{p}} \otimes 1)(Z_1) = \pi(\gamma_{\mathfrak{p}}(Z)) = (1 \otimes \psi_{\mathfrak{p}}^*)(Z_1).$$

Here $\gamma : A \to \mathrm{End}_{\mathcal{O}_S}(\mathcal{O}_C)$; $a \mapsto \gamma_a$ is the map describing the A-action on C. Since $\gamma_{\mathfrak{p}}(Z) \equiv Z^{(q^d)} (\mathrm{mod}.\mathfrak{p})$ (e.g. [5], Proposition 2.4), we have

$$\begin{aligned} (\psi_{\mathfrak{p}} \otimes 1)(Z_1) = \pi(Z^{q^d}) &= (f_{G,\mathfrak{p}} \otimes f_{G^*,\mathfrak{p}}) \circ \iota(Z_1) \\ &= (f_{G,\mathfrak{p}} \circ v_{G,\mathfrak{p}} \otimes 1)(Z_1). \end{aligned}$$

Hence $\psi_{\mathfrak{p}} = f_{G,\mathfrak{p}} \circ v_{G,\mathfrak{p}}$, and $\Psi_{\mathfrak{p}} = V_{G,\mathfrak{p}} \circ F_{G,\mathfrak{p}}$.

By (i), we have also the commutative diagram

$$\begin{array}{ccc} G^{(q^d)} & \xrightarrow{V_{G,\mathfrak{p}}} & G \\ {\scriptstyle F_{G^{(q^d)},\mathfrak{p}}}\downarrow & & \downarrow{\scriptstyle F_{G,\mathfrak{p}}} \\ G^{(q^{2d})} & \xrightarrow[V_{G^{(q^d)},\mathfrak{p}}]{} & G^{(q^d)}, \end{array}$$

from which follows the equality

$$\Psi_{\mathfrak{p}}^{(q^d)} = V_{G^{(q^d)},\mathfrak{p}} \circ F_{G^{(q^d)},\mathfrak{p}} = F_{G,\mathfrak{p}} \circ V_{G,\mathfrak{p}}. \qquad \text{Q.E.D.}$$

5. Duality for Drinfeld modules

In this section, we construct explicitly the *dual* $\check{E}$ of a Drinfeld $\mathbb{F}_q[t]$-module E, and prove the compatibility of this construction and the duality of §4 for the torsion points of E and $\check{E}$. $\check{E}$ is an $(r-1)$-dimensional abelian t-module ([1]) if E is of rank $r \geq 2$.

Let $A = \mathbb{F}_q[t]$ and R an A-algebra. The image of $t \in A$ in R will be denoted by θ. (Though all constructions below work over any A-scheme S, we work over an affine $U = \mathrm{Spec}R$ for simplicity.)

Let (E, Ψ) be a Drinfeld module over R of rank $r \geq 2$. Suppose the action of $t \in A$ is given by

$$\psi_t(X) = \theta X + a_1 X + \cdots + a_r X^{q^r}, \quad a_i \in R,\ a_r \in R^\times$$

with respect to a coordinate X of E. (As before, we use a small letter ψ to denote a map of affine rings.) On $\check{E} := \mathbb{G}_{a\ /R}^{\oplus(r-1)}$, define an A-module scheme structure $\check{\Psi} : A \longrightarrow \mathrm{End}_R(\mathbb{G}_a^{\oplus(r-1)})$, in terms of the coordinates $\mathbb{Y} = {}^t(Y_1, \cdots, Y_{r-1})$ of $\mathbb{G}_a^{\oplus(r-1)} = \mathrm{Spec}R[Y_1, \cdots, Y_{r-1}]$, by

$$\check{\psi}_t(\mathbb{Y}) = \theta\mathbb{Y} + \mathbb{B}_1\mathbb{Y}^{(q)} + \mathbb{B}_2^{(q)}\mathbb{Y}^{(q^2)},$$

with

$$\mathbb{B}_1 := \begin{pmatrix} & & -a_r^{-1}a_1 \\ 1 & & \vdots \\ & \ddots & \vdots \\ & 1 & -a_r^{-1}a_{r-1} \end{pmatrix}, \quad \mathbb{B}_2 := \begin{pmatrix} & & a_r^{-1} \\ & & \\ & & \end{pmatrix}.$$

Here and elsewhere, for a matrix $\mathbb{B}$, $\mathbb{B}^{(q^j)}$ denotes the matrix $\mathbb{B}$ but with entries raised to the q^j-th power. We will call this type of A-module schemes $(\check{E}, \check{\Psi})$ *dual Drinfeld modules*. Note that one can recover the Drinfeld module E starting with a dual Drinfeld module $\check{E}$, so that we may think $\check{\check{E}} = E$.

Let C be the Carlitz module on which t acts by $\gamma_t : Z \mapsto \theta Z + Z^q$ with respect to a coordinate Z of C.

THEOREM (5.1). *(i) If R is a perfect field, $\check{E}$ is an abelian t-module of t-rank $r(\check{E}) = r$, τ-rank $\rho(\check{E}) = r-1$, and weight $w(\check{E}) = (r-1)/r$ in the sense of [1].*
(ii) For a non-zero $a \in A$, the kernel ${}_a\check{E}$ of the action of a on $\check{E}$ is a finite t-module over R of rank $q^{r \cdot \deg(a)}$.
(iii) For a non-zero $a \in A$, there exists an A-bilinear pairing defined over R:

$${}_a\Pi_E : {}_aE \times_R {}_a\check{E} \longrightarrow {}_aC.$$

(iv) If we furnish ${}_aE$ with the standard v-module structure as in (3.4), then we have ${}_a\check{E} \simeq {}_aE^*$, and the pairing ${}_a\Pi_E$ of (iii) coincides with the pairing Π_{aE} of Theorem (4.3).

REMARK (5.2). (i) Anderson takes $A = \mathbb{F}_p[t]$ with a *prime* p in [1]. So we should assume in (5.1),(i) $q = p$, or define the t motive $\mathrm{M}(\check{E}) = \mathrm{Hom}_R(\mathbb{G}_a^{\oplus(r-1)}, \mathbb{G}_a)$ to be the $\mathbb{F}_q$-linear homomorphisms. Here we will take the latter, and denote it, as before, by $\mathcal{E}_{\check{E}}$.

(ii) The statements of the Theorem are valid also for a higher dimensional abelian t-module (E, Ψ) if $\Psi : A \longrightarrow \mathrm{End}_R(\mathbb{G}_a^{\oplus d})$ is defined by an equation of the form

$$\psi_t(X) \;=\; \theta X \;+\; a_1 X^{(q)} \;+\cdots+\; a_r X^{(q^r)}, \quad X \;=\; {}^t(X_1, \cdots, X_d),$$

with $a_i \in \mathrm{M}_d(R)$ and $a_r \in \mathrm{GL}_d(R)$.

(iii) For a Drinfeld module E of rank 1, there exists an ind-finite étale A-module scheme $\check{E}$ (a twist of the constant A-module scheme $\mathbb{F}_q(t)/\mathbb{F}_q[t]$), together with a pairing as in (iii) of the Theorem.

(iv) Even if E does not have good reduction over R, we can define an A-bilinear pairing between the division points of E and $\check{E}'$, a twist of $\check{E}$, with target C', a twist of C. Especially, we can take $\check{E}'$ to be the $(r-1)$-st exterior product $\wedge^{r-1}E$ of E ([1]) defined by

$$\check{\psi}'_t(\mathbb{Y}) \;=\; \theta\mathbb{Y} \;+\; \mathbb{B}_1'^{(q)}\mathbb{Y}^{(q)} \;+\; \mathbb{B}_2'^{(q^2)}\mathbb{Y}^{(q^2)}$$

with

$$\mathbb{B}'_1 := (-1)^r \begin{pmatrix} & & & (-1)^r a_1 \\ a_r & & & \vdots \\ & \ddots & & (-1)^{r+1-i} a_i \\ & & \ddots & \vdots \\ & & a_r & a_{r-1} \end{pmatrix}, \quad \mathbb{B}'_2 := (-1)^r \begin{pmatrix} & & a_r \\ & & \\ & & \end{pmatrix},$$

and C' to be the r-th exterior product $\wedge^r E$ of E ([1], [4]) defined by

$$\gamma'_t(Z) \;=\; \theta Z - (-1)^r a_r X^q.$$

$\check{E}'$ and C' may have non-stable reduction. It would be interesting to seek a good model of $\check{E}'$.

PROOF OF THE THEOREM:— (i) This is clear; an $R[\check{\psi}_t]$-base of $\mathcal{E}_{\check{E}} = \mathrm{Hom}_{\mathbb{F}_q,R}(\mathbb{G}_a^{\oplus(r-1)}, \mathbb{G}_a)$ is $(a_r^{-1}Y_{r-1}^q, Y_1, \cdots, Y_{r-1})$, which implies $r(\check{E}) = r$. The other assertions are obvious.

(ii) Put $G = {}_a\check{E}$. The affine ring $\mathcal{O}_G$ of G can be identified with the quotient $R[Y_1, \cdots, Y_{r-1}]/\check{\psi}_a(\mathbb{Y})$. It is enough to show that $\mathcal{O}_G$ is free over R of rank $q^{r\cdot\deg(a)}$, and that $\mathcal{E}_G$ is free over R of rank $r \cdot \deg(a)$.

We may assume $a \in A = \mathbb{F}_q[t]$ is monic of degree $k \geq 1$, and write $a = t^k + g(t)$, $g(t) = \sum_{i=0}^{k-1} g_i t^i$, $g_i \in \mathbb{F}_q$. Define elements $Y_{ij} \in \mathcal{O}_G$ for $0 \leq i \leq k-1$ and $1 \leq j \leq r-1$ by

$$Y_{k-1,j} \;=\; Y_j \qquad (1 \leq j \leq r-1),$$

and

$$\mathbb{Y}_{i-1} \;=\; \check{\psi}_t(\mathbb{Y}_i) \;+\; g_i\mathbb{Y}_{k-1} \qquad (1 \le i \le k-1), \tag{5.1.1}$$

where $\mathbb{Y}_i := {}^t(Y_{i1}, \cdots, Y_{i,r-1})$. Applying (5.1.1) repeatedly, we find

$$\mathbb{Y}_i = \check{\psi}_{t^{k-1-i}}(\mathbb{Y}_{k-1}) + g_{k-1}\check{\psi}_{t^{k-2-i}}(\mathbb{Y}_{k-1}) + \cdots + g_{i+1}\mathbb{Y}_{k-1}$$

$$= \check{\psi}_{(t^{k-1-i}+g_{k-1}t^{k-2-i}+\cdots+g_{i+1})}(\mathbb{Y}_{k-1}), \tag{5.1.1a}$$

and especially,

$$\mathbb{Y}_0 \;=\; \check{\psi}_{(t^{k-1}+g_{k-1}t^{k-2}+\cdots+g_1)}(\mathbb{Y}_{k-1}),$$

whence

$$\check{\psi}_t(\mathbb{Y}_0) \;=\; \check{\psi}_a(\mathbb{Y}_{k-1}) \;-\; g_0\mathbb{Y}_{k-1}.$$

This shows that the equality $\check{\psi}_a(\mathbb{Y}_{k-1}) = 0$ (which means $G = {}_a\check{E}$) is equivalent to

$$\check{\psi}_t(\mathbb{Y}_0) \;=\; -g_0\mathbb{Y}_{k-1}. \tag{5.1.2}$$

We can thus regard $\mathcal{O}_G$ as the quotient of $R[Y_{01}, \cdots, Y_{k-1,r-1}]$ by the relations (5.1.1) and (5.1.2).

By setting $(Y'_{ij})^q := Y_{ij}$ if $j < r-1$ and $Y'_{i,r-1} := Y_{i,r-1}$, we embed $\mathcal{O}_G$ into the quotient $\mathcal{O}'$ of $R[Y'_{01}, \cdots, Y'_{k-1,r-1}]$ by the same relations (5.1.1) and (5.1.2). Then (5.1.1) and (5.1.2) read:

$$(\text{unit})(Y'_{ij})^{q^2} \;+\; (\text{lower terms}) \;=\; 0, \quad 0 \le i \le k-1,\ 1 \le j \le r-1.$$

By Lemma 1.9.1 of [2], O' is free of rank $q^{2k(r-1)}$ over R, with a base

$$\Big(\prod_{i,j}(Y'_{ij})^{l_{ij}} \;;\; 0 \le l_{ij} \le q^2-1\Big).$$

Since $\mathcal{O}_G$ is the R-submodule of O' generated by

$$\Big(\prod_{i,j}(Y'_{ij})^{l_{ij}} \;;\; q|l_{ij} \text{ if } 1 \le j \le r-2\Big),$$

it is also free, and of rank $q^{k(r-2)} \cdot q^{2k} = q^{kr}$. $\mathcal{E}_G$ is also free on the R-base $(Y_{ij};\ 0 \le i \le k-1,\ 0 \le j \le r-1)$, so we have $\mathrm{rank}(\mathcal{O}_G) = q^{\mathrm{rank}(\mathcal{E}_G)}$.

(iii) Passing to the language of affine rings, we shall give an R-algebra homomorphism

$$\pi \;:\; \mathcal{O}_{{}_aC} \longrightarrow \mathcal{O}_{{}_aE} \otimes_R \mathcal{O}_{{}_a\check{E}},$$

or more explicitly,

$$\pi \;:\; R[Z]/\gamma_a(Z) \longrightarrow R[X]/\psi_a(X) \otimes_R R[Y_1, \cdots, Y_{r-1}]/\check{\psi}_a(\mathbb{Y})$$

which is compatible with the comultiplications ($Z \mapsto Z \otimes 1 + 1 \otimes Z$, etc.) and the A-actions. Write $a = t^k + g(t)$, $g(t) = \sum_{i=0}^{k-1} g_i t^i$ and define $Y_{ij} \in \mathcal{O}_{a\hat{E}}$ as in the proof of (ii). Set further

$$Y_{i0} := a_r^{-1} Y_{i,k-1}^q \qquad (0 \le i \le k-1). \tag{5.1.3}$$

Simplifying the notaion, we also set $X_{ij} := \psi_{t^i}(X)^{q^j}$ for $i, j \ge 0$. Then we have

$$X_{i+1,0} = \psi_t(X_{i0}) = \theta X_{i0} + \sum_{j=1}^{r} a_j X_{ij} \tag{5.1.4}$$

and

$$0 = \psi_a(X) = \psi_{t^k}(X) + \psi_{g(t)}(X) = X_{k0} + \sum_{i=0}^{k-1} g_i X_{i0} \tag{5.1.5}$$

$$= \theta X_{k-1,0} + \sum_{j=1}^{r} a_j X_{k-1,j} + \sum_{i=0}^{k-1} g_i X_{i0}. \tag{5.1.5a}$$

Now define the map π by

$$\pi : Z \mapsto \sum_{i=0}^{k-1} \sum_{j=0}^{r-1} X_{ij} \otimes Y_{ij}.$$

This is obviously compatible with the comultiplications and the actions of $\mathbb{F}_q$ ($\subset A$); it only remains to check the commutativity of the following diagram:

$$\begin{array}{ccc} \mathcal{O}_{a}C & \xrightarrow{\pi} & \mathcal{O}_{a}E \otimes_R \mathcal{O}_{a\hat{E}} \\ {\scriptstyle \gamma_t}\downarrow & & \downarrow{\scriptstyle \psi_t \otimes 1,\ 1 \otimes \hat{\psi}_t} \\ \mathcal{O}_{a}C & \xrightarrow[\pi]{} & \mathcal{O}_{a}E \otimes_R \mathcal{O}_{a\hat{E}} . \end{array}$$

The three composite maps in the diagram are calculated as follows:

$$(\psi_t \otimes 1) \circ \pi(Z) = \sum_{i=0}^{k-1} \sum_{j=0}^{r-1} X_{i+1,j} \otimes Y_{ij}$$

$$= \sum_{i=1}^{k-1} \sum_{j=0}^{r-1} X_{ij} \otimes Y_{i-1,j} - \sum_{i=0}^{k-1} \sum_{j=0}^{r-1} g_i X_{ij} \otimes Y_{k-1,j} \qquad (\text{by } (5.1.5)^{q^j})$$

$$= -\sum_{j=0}^{r-1} X_{0j} \otimes g_0 Y_{k-1,j} + \sum_{i=1}^{k-1} \sum_{j=0}^{r-1} X_{ij} \otimes (Y_{i-1,j} - g_i Y_{k-1,j}) . \tag{5.1.6}$$

In view of (5.1.1) and (5.1.2), we find this equal to

$$(1 \otimes \check{\psi}_t) \circ \pi(Z) \;=\; \sum_{i=0}^{k-1} \sum_{j=0}^{r-1} X_{ij} \otimes \check{\psi}_t(Y_{ij}) \;.$$

Finally,

$$\pi \circ \gamma_t(Z) \;=\; \theta\Big(\sum_{i=0}^{k-1} \sum_{j=0}^{r-1} X_{ij} \otimes Y_{ij}\Big) \;+\; \Big(\sum_{i=0}^{k-1} \sum_{j=0}^{r-1} X_{ij} \otimes Y_{ij}\Big)^q$$

$$(5.1.7) \qquad = \sum_{i=0}^{k-1} \sum_{j=0}^{r-1} X_{ij} \otimes \theta Y_{ij} \;+\; \sum_{i=0}^{k-1} \sum_{j=1}^{r-1} X_{ij} \otimes Y_{i,j-1}^q \;+\; \sum_{i=0}^{k-1} X_{ir} \otimes Y_{i,r-1}^q \;.$$

If $0 \le i \le k-2$, we see from (5.1.4)

$$X_{ir} \;=\; -a_r^{-1}\Big(\theta X_{i0} \;+\; \sum_{j=1}^{r-1} a_j X_{ij} \;-\; X_{i+1,0}\Big).$$

For $i = k-1$, we see from (5.1.5a)

$$X_{k-1,r} \;=\; -a_r^{-1}\Big(\theta X_{k-1,0} \;+\; \sum_{j=1}^{r-1} a_j X_{k-1,j} \;+\; \sum_{i=0}^{k-1} g_i X_{i0}\Big).$$

Hence the companion with which X_{ij} is tensored in the above expression (5.1.7) of $\pi \circ \gamma_t(Z)$ is, if $i = j = 0$,

$$\theta Y_{00} \;-\; a_r^{-1}\theta Y_{0,r-1}^q \;-\; a_r^{-1} g_0 Y_{k-1,r-1}^q \;=\; -g_0 Y_{k-1,0} \quad \text{(by (5.1.3))};$$

if $i = 0$ and $1 \le j \le r-1$,

$$\theta Y_{0j} \;+\; Y_{0,j-1}^q \;-\; a_r^{-1} a_j Y_{0,r-1}^q \;=\; -g_0 Y_{k-1,j} \quad \text{(by (5.1.2))};$$

if $1 \le i \le k-1$ and $j = 0$,

$$\theta Y_{i0} \;-\; a_r^{-1}\theta Y_{i,r-1}^q \;+\; a_r^{-1} Y_{i-1,r-1}^q \;-\; a_r^{-1} g_i Y_{k-1,r-1}^q$$

$$= Y_{i-1,0} \;-\; g_i Y_{k-1,0} \quad \text{(by (5.1.3))};$$

if $1 \le i \le k-1$ and $1 \le j \le r-1$,

$$\theta Y_{ij} \;+\; Y_{i,j-1}^q \;-\; a_r^{-1} a_j Y_{i,r-1}^q \;=\; Y_{i-1,j} \;-\; g_i Y_{k-1,j} \quad \text{(by (5.1.1))}.$$

Putting all these together, we find $\pi \circ \gamma_t(Z)$ is also equal to (5.1.6).

(iv) We may regard $\mathcal{E}_{a}E$ and $\mathcal{E}_{a}\check{E}$ dual to each other by making (X_{ij}) and (Y_{ij}) the dual bases. Then our construction of the pairing here coincides with the construction in §4, and we have ${}_a\check{E} \simeq {}_aE^*$. Q.E.D.

REMARK (5.3). In what follows, we regard ${}_aE^* = {}_a\check{E}$ by this concrete construction (iv).

PROPOSITION (5.4). *Let $M : E \to F$ be an isogeny of Drinfeld modules (resp. dual Drinfeld modules) over R of rank $r \geq 2$.*

(i) There exists a unique isogeny $\check{M} : \check{F} \to \check{E}$ of dual Drinfeld modules (resp. Drinfeld modules) such that, for all non-zero $a \in A$,

$$(5.4.1) \qquad {}_a\Pi_E \circ (1 \times \check{M}) = {}_a\Pi_F \circ (M \times 1) \qquad \text{on } {}_aE \times {}_a\check{F},$$

where ${}_a\Pi_E : {}_aE \times {}_a\check{E} \to {}_aC$ and ${}_a\Pi_F : {}_aF \times {}_a\check{F} \to {}_aC$ are the duality pairings (5.1), (ii) on the a-division points.

(ii) Let $M^* : {}_aF^* \to {}_aE^*$ be the morphism of finite t-modules which $M : {}_aE \to {}_aF$ induces by functoriality of *. Then we have $M^* = \check{M}$ on ${}_aF^* = {}_a\check{F}$ (cf. (5.3)).

(iii) We have canonically $\mathrm{Ker}(\check{M}) = \mathrm{Ker}(M)^*$.

PROOF:— We assume E and F are Drinfeld modules; the dual case is proved similarly.

(i) Let $\mathcal{E}_E := \mathrm{Hom}_{\mathbb{F}_q,R}(E, \mathbb{G}_a)$, the $\mathbb{F}_q$-linear homomorphisms defined over R. The rings R and A acts naturally on $\mathcal{E}_E$. It is easy to see, by the explicit form of the defining equation of E, that $\mathcal{E}_E$ is a free $R[t]$-module of rank r. For E and F (resp. $\check{E}$ and $\check{F}$), we use the common symbol $(X_0, X_1, \cdots, X_{r-1}) = (X, X^q, \cdots, X^{q^{r-1}})$ (resp. $(Y_0, Y_1, \cdots, Y_{r-1})$) for the $R[t]$-basis of $\mathcal{E}_E$ and $\mathcal{E}_F$ (resp. $\mathcal{E}_{\check{E}}$ and $\mathcal{E}_{\check{F}}$), and regard (X_i) and (Y_i) as the dual basis to each other (cf. Proof of (5.1)).

An isogeny $M : E \to F$ induces an $R[t]$-module homomorphism $m : \mathcal{E}_F \to \mathcal{E}_E$. Let $\check{m}$ be its transpose; $\check{m}$ is the unique $R[t]$-module homomorphism $\mathcal{E}_{\check{E}} \to \mathcal{E}_{\check{F}}$ such that $\sum_{i=0}^{r-1} m(X_i) \otimes Y_i = \sum_{i=0}^{r-1} X_i \otimes \check{m}(Y_i)$ in $\mathcal{E}_E \otimes_{R[t]} \mathcal{E}_{\check{F}}$. If $m(X_j) = \sum_{h=0}^{r-1} m_{hj} X_h$, $m_{hj} \in R[t]$, then $\check{m}(Y_h) = \sum_{j=0}^{r-1} m_{hj} Y_j$. Clearly $\check{m}$ defines an isogeny $\check{M} : \check{F} \to \check{E}$. We will show $\check{M}$ has the required property.

Fix a non-zero $a \in A$, and let $Z_a = \sum X_{ij} \otimes Y_{ij}$ be the element of $\mathcal{E}_{{}_aE} \otimes_R \mathcal{E}_{{}_a\check{E}}$ and $\mathcal{E}_{{}_aF} \otimes_R \mathcal{E}_{{}_a\check{F}}$ as in the proof of (5.1), (iii) (we use again the symbol Z_a in common for E and F). Then the equality (5.4.1) is equivalent to the equality

$$(5.4.2) \qquad (1 \otimes \check{m})(Z_a) = (m \otimes 1)(Z_a) \qquad \text{in } \mathcal{E}_{{}_aE} \otimes_R \mathcal{E}_{{}_a\check{F}}.$$

The uniqueness of $\check{M}$ follows from this equality, because it determines $\check{m}(Y_i) (\mathrm{mod}\ a\mathcal{E}_{\check{F}})$ for all non-zero $a \in A$.

Let us prove the equality (5.4.2). Recall that $X_{ij} = t^i X_j$ (= abbreviation of $\psi_{t^i}(X_j)$) and $Y_{ij} = b_i Y_j$ (= abbreviation of $\check{\psi}_{b_i}(Y_j)$). If $a = t^k + \sum_{l=0}^{k-1} g_l t^l$ with $g_l \in \mathbb{F}_q$, then by (5.1.1a), we see that $b_i = t^{k-1-i} + g_{k-1} t^{k-2-i} + \cdots + g_{i+1}$. Since

m commutes with elements of A, we have

$$\begin{aligned}(m\otimes 1)(Z_a) &= (m\otimes 1)\sum_{i,j}(t^i\otimes b_i)(X_j\otimes Y_j)\\ &= \sum_{i,j}(t^i\otimes b_i)(\sum_{h=0}^{r-1} m_{hj}X_h)\otimes Y_j\\ &= \sum_{h,j}(m_{hj}\otimes 1)(\sum_{i=0}^{k-1} t^i\otimes b_i)(X_h\otimes Y_j).\end{aligned}$$

Similarly,

$$(1\otimes \check{m})(Z_a) = \sum_{h,j}(1\otimes m_{hj})(\sum_{i=0}^{k-1} t^i\otimes b_i)(X_h\otimes Y_j).$$

So the coincidence of these two elements is implied by the annhilation of $X_h\otimes Y_j$ by

$$(m_{hj}\otimes 1 - 1\otimes m_{hj})\sum_{i=0}^{k-1}(t^i\otimes b_i) \tag{5.4.3}$$

Since the $\otimes$ is over R and $m_{hj}\in R[t]$, it suffices to prove this for $m_{hj}=t^n$ for all $n\geq 1$. But $t^n\otimes 1 - 1\otimes t^n$ has the factor $t\otimes 1 - 1\otimes t$, so we may assume $m_{hj}=t$. In that case, a simple calculation shows that (5.4.3) equals $a\otimes 1 - 1\otimes a$. This kills $X_h\otimes Y_j$ because we are now working on a-division points.

(ii) is clear from the uniqueness of M^* as shown in (ii-2) of (4.3).

(iii) Take any non-zero $a\in A$ such that $\mathrm{Ker}(M)\subset {}_aE$. Then there exists an isogeny $N: F\to E$ such that $N\circ M = a$ on E and $M\circ N = a$ on F. Restricting the dual maps to a-division points, we have $\mathrm{Ker}(\check{M}) = \mathrm{Im}(\check{N})$ and $\mathrm{Ker}(\check{N}) = \mathrm{Im}(\check{M})$. Applying the exact functor * to the exact sequence

$$0 \longrightarrow \mathrm{Ker}(M) \longrightarrow {}_aE \xrightarrow{M} {}_aF\ ,$$

we find the sequence

$$0 \longleftarrow \mathrm{Ker}(M)^* \longleftarrow {}_aE^* \xleftarrow{M^*} {}_aF^*$$

exact. Using (ii), we conclude

$$\begin{aligned}\mathrm{Ker}(M)^* &\simeq {}_aE^*/\mathrm{Im}(M^*) = {}_a\check{E}/\mathrm{Im}(\check{M})\\ &= {}_a\check{E}/\mathrm{Ker}(\check{N}) \simeq \mathrm{Im}(\check{N}) = \mathrm{Ker}(\check{M}).\end{aligned}$$ Q.E.D.

6. Duality for π-divisible groups

Let π be a monic prime element of $A = \mathbb{F}_q[t]$, and let G be a π-divisible group over an A-scheme S of hight h. Thus G is an inductive system $(G_n, i_n)_{n\geq 0}$ of finite v-modules G_n over S with transition maps $i_n : G_n \to G_{n+1}$ such that, for all $n \geq 0$,

(1) G_n is killed by π^n, and of rank $|\pi|^{nh} = q^{nh\cdot \deg(\pi)}$; and

(2) the sequence

$$0 \longrightarrow G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{\pi^n} G_{n+1}$$

is exact.

An anti-equivalent definition can be stated in terms of v-sheaves; we call a projective system $\mathcal{E} = (\mathcal{E}_n, p_n)_{n\geq 0}$ of v-sheaves a *π-adic v-sheaf* on S of hight h if, for all $n \geq 0$,

(1) $\mathcal{E}_n$ is killed by π^n, and of rank $nh \cdot \deg(\pi)$; and

(2) the sequence

$$\mathcal{E}_{n+1} \xrightarrow{\pi^n} \mathcal{E}_{n+1} \xrightarrow{p_n} \mathcal{E}_n \longrightarrow 0$$

is exact.

It is clear that the category of π-divisible groups over S is anti-equivalent to the category of π-adic v-sheaves on S (cf. Proposition (3.3)).

The dual $G^* = (G_n^*, i_n^*)_{n\geq 0}$ of G is defined as follows: G_n^* is the dual of G_n in the sense of §4, and the transition map $i_n^* : G_n^* \to G_{n+1}^*$ is the dual morphism of the surjective morphism $\pi : G_{n+1} \to G_n$. It is clear that G^* is a π-divisible group and has the same hight as G.

Assume now that S is integral and, for all $n \geq 0$, G_n is étale over the generic point of S. Let K^{sep} be a separable closure of the function field K of S. Define two Galois modules $\Phi_\pi(G)$ and $T_\pi(G)$ as usual:

$$\Phi_\pi(G) := \varinjlim_n G_n(K^{\mathrm{sep}}),$$
$$T_\pi(G) := \varprojlim_n G_n(K^{\mathrm{sep}}),$$

where the transition maps are those induced by i_n and π respectively. If A_π denotes the π-adic completion of A, and F_π denotes the fraction field of A_π, then $\Phi_\pi(G)$ is a divisible A_π-module, and $T_\pi(G) = \mathrm{Hom}_{A_\pi}(F_\pi/A_\pi, \Phi_\pi(G))$ is a free A_π-module of rank h. Write C_n for the kernel of π^n on the Carlitz module C. Noticing the compatibility ((4.3), (ii-2)), and passing to the limit as $n \to \infty$ of the pairing ((4.3), (ii-3)): $G_n(K^{\mathrm{sep}}) \times G_n^*(K^{\mathrm{sep}}) \to C_n(K^{\mathrm{sep}})$, inductively with G_n and C_n and projectively with G_n^*, we obtain:

PROPOSITION (6.1). *There exist canonical isomorphisms of Galois modules:*

$$\begin{aligned} T_\pi(G^*) &\simeq \mathrm{Hom}_{A_\pi}(\Phi_\pi(G), \Phi_\pi(C)) \\ &\simeq \mathrm{Hom}_{A_\pi}(T_\pi(G), T_\pi(C)). \end{aligned}$$

Assume now that $S = \mathrm{Spec}\, R$, where R is a complete nötherian local A-algebra such that the structure morphism $\alpha : A \to R$ is injective and $\alpha(\pi)$ is in the maximal ideal of R. As was shown in (1.4) of [6], the category of connected π-divisible groups over R is equivalent to the category of divisible formal A_π-modules over R. The *dimension* of a π-divisible group G over R is defined to be the dimension of the formal A_π-module corresponding to the maximal connected sub-π-divisible group G^0 of G. The following proposition is proved in the same way as Proposition 3 of [7], using Proposition (4.7).

PROPOSITION (6.2). *Let d and d^* be the dimensions of G and its dual G^* respectively. Then we have $d + d^* = h$, the hight of G and G^*.*

References

[1] G. W. Anderson, t-motives, Duke math. J. 53 (1986), 457–502

[2] G. W. Anderson and D. S. Thakur, Tensor powers of the Carlitz module and zeta values, Ann. of Math. 132 (1990), 159–191

[3] V. G. Drinfeld, Moduli varieties of F-sheaves, Funktsional'nyi Analiz i Ego Prilozheniya 21 (1987), 23–41

[4] Y. Hamahata, On the Tate module associated to the tensor product of two Drinfeld modules, I, II, preprint

[5] D. Hayes, Explicit class field theory for rational function fields, Trans. A.M.S. 189 (1974), 77–91

[6] Y. Taguchi, Semi-simplicity of the Galois representations attached to Drinfeld modules over fields of "infinite characteristics", to appear in J. of Number Theory

[7] J. Tate, p-divisible groups, in: Proceedings of a conference on local fields, Driebergen, 1966, Springer-Verlag, Berlin-Heidelberg-New York, 1967, 158–183

Chapter III

π-adic theory

Introduction

This Chapter is an attempt to develope the π-adic theory similar to [3] and [6]. It turns out (§1) that the Galois representations attached to π-divisible groups lose so much information after being tensored with $\mathbb{C}_\pi$, the completion of a separable closure of $\mathbb{F}_q((\pi))$, that a Hodge-Tate decomposition of π-divisible groups, if exists any, is nonsense at least from the view point of Galois action. Nevertheless, we have (§2) a kind of Hodge-Tate decomposition à la Fontaine ([3]) for finite t-modules whose meaning is quite visible from the construction.

1. Galois cohomology

In this Section, we exhibit, by calculating Galois cohomology, a crucial difference of the π-adic theory in positive characteristic from the usual p-adic theory in characteristic zero. One reason for this difference is that the Carlitz module, which plays in our theory the role of the multiplicative group $\mathbb{G}_m$ in the classical theory, is an *additive* group scheme.

Let A be the polynomial ring $\mathbb{F}_q[t]$ in one variable t over the finite field $\mathbb{F}_q$ of q elements. Let K be a complete discrete valuation field of "mixed characteristic" over A, by which we mean that K is endowed with an injective ring homomorphism $\alpha : A \to K$ such that the inverse image by α of the maximal ideal of the integer ring of K is a non-zero prime ideal of A. We assume that the residue field of K is perfect. Our objective is to calculate the Galois cohomology group $H^i(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathbb{C}(r))$ for $i = 0, 1$ and $r \in \mathbb{Z}$. (The notations are explained below.) Of special importance is that $H^0(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathbb{C}(r))$ does not vanish even if $r \neq 0$. See the concluding Remark 2 for more discussion.

Let π be the unique monic prime element of A such that $\alpha(\pi)$ is a non-unit in the integer ring of K (so (π) is the "residual characteristic" of K). In the following, we think of A as a subring of K by means of α. Let C be the *Carlitz A-module* over A such that the action of $t \in A$ on C is given by $[t](Z) = tZ + Z^q$ with respect to a coordinate Z of C. The π-adic Tate module of C is a rank one free A_π-module, where A_π is the π-adic completion of A. C being considered to be an object over K, the absolute Galois group $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ of K acts on $T_\pi(C)$ continuously. (K^{sep} is a fixed separable closure of K. In general, we denote

by G_L the absolute Galois group of a field L.) The character $\chi : G_K \to A_\pi^\times$ which describes this action is called the *Carlitz character*.

For any valuation field L, we denote by $\widehat{L}$ the completion of L with respect to the valuation topology. Let $\mathbb{C} := \widehat{K^{\mathrm{sep}}}$. The action of G_K on K^{sep} extends uniquely to a continuous action on $\mathbb{C}$. $\mathbb{C}$ is algebraically closed. For a subfield L of $\mathbb{C}$, we denote by L^{rad} the inseparable closure of L in $\mathbb{C}$.

For any topological A_π-module M with a continuous G_K-action, and for any $r \in \mathbb{Z}$, we define the r-th *Tate twist* $M(r)$ of M by the Carlitz character to be the G_K-module with the same underlying A_π-module M and with a twisted Galois action $\sigma.m = \chi(\sigma)^r \cdot \sigma(m)$ for all $\sigma \in G_K$ and $m \in M$, where $\sigma(m)$ denotes the presupposed action.

For a topological group G and a topological module M with a continuous G-action, we denote by $H^i(G, M)$ the i-th cohomology group defined by the i-th right derived functor of the functor "fixed part" : $M \mapsto M^G$ (or equivalently, defined by continuous cochains). Our main result is:

THEOREM. *For all $r \in \mathbb{Z}$, we have*

$$H^0(G_K, \mathbb{C}(r)) = (\widehat{K^{\mathrm{rad}}} \cdot c^{-r})(r) \simeq \widehat{K^{\mathrm{rad}}}, \quad \text{and} \tag{1}$$

$$H^1(G_K, \mathbb{C}(r)) = 0. \tag{2}$$

Here c is an element of $\mathbb{C}$ such that $\sigma(c) = \chi(\sigma)c$ for all $\sigma \in G_K$, and constructed explicitly in the following.

REMARK 1. The followings are previously known:
(i) (Tate [3], Theorems 1 and 2) If K is of characteristic zero and $\mathbb{C}_p(r)$ denotes the completion of an algebraic closure of K, with the usual Tate twist, then one has, for $i = 0, 1$,

$$H^i(G_K, \mathbb{C}_p(r)) \simeq \begin{cases} K & \text{if } r = 0, \\ 0 & \text{if } r \neq 0. \end{cases}$$

(ii) (Ax [1]) If K is a rank one valuation field (of arbitrary characteristic) which is henselian with respect to the valuation, then one has

$$H^0(G_K, \mathbb{C}) = \widehat{K^{\mathrm{rad}}}.$$

This result includes the case $r = 0$ in (1) of the Theorem. □

First of all, note that, when we are working over A_π, we may replace the Carlitz module C by an isomorphic Lubin-Tate A_π-module C' on which the action of π is given by $[\pi](Z') = \pi Z' + Z'^{q^d}$, where $d = \deg(\pi)$. So in the following, we assume $C = C'$, $q = q^d$, and $A_\pi = \mathbb{F}_q[[\pi]]$.

We construct now the element $c \in \mathbb{C}$. Choose and fix a system $(\pi_n)_{n \geq 0}$ of elements of K^{sep} which corresponds to a generator of $T_\pi(C)$. So π_n is a generator of the π^n-division points of C, and we have $[\pi](\pi_n) = \pi_{n-1}$ for all $n \geq 1$. We define our element $c \in \mathbb{C}$ as follows:

$$c := \sum_{n \geq 1} \pi^n \pi_n.$$

The series on the right clearly converges. (1) of the Theorem is implied by Ax's theorem (Remark 1, (ii)) and the following

LEMMA 1. *For $x \in \mathbb{C}^\times$ and $r \in \mathbb{Z}$, write $x = x_1 c^r$ with $x_1 \in \mathbb{C}^\times$. Then we have, for all $\tau \in G_K$,*

$$\tau(x) = \tau(x_1)\chi(\tau)^r c^r.$$

In particular, if L is a G_K-stable subfield of $\mathbb{C}$ which contains c, then multiplication by c^{-r} induces an isomorphism $L \to L(r)$ of G_K-modules.

PROOF. The claim is easily reduced to the case $x = c$ and $r = 1$; we are to show $\tau(c) = \chi(\tau)c$ for all $\tau \in G_K$. Write $f(\pi) = \sum_{i \geq 0} a_i \pi^i$, with $a_i \in \mathbb{F}_q$, for the formal power series $\chi(\tau) \in A_\pi^\times$. Then

$$\begin{aligned} \tau(c) &= \sum_{n \geq 1} \pi^n \tau(\pi_n) = \sum_{n \geq 1} \pi^n [f(\pi)](\pi_n) = \sum_{i \geq 0} a_i \sum_{n \geq 1} \pi^n [\pi^i](\pi_n) \\ &= \sum_{i \geq 0} a_i \pi^i \sum_{n-i \geq 1} \pi^{n-i} \pi_{n-i} = f(\pi)c = \chi(\tau)c. \end{aligned}$$

We used in the third equality that the group law of C is $\mathbb{F}_q$-linear. Q.E.D.

To prove (2) of the Theorem, we consider certain subextensions of $\mathbb{C}/K$ as in [3]. Let K_∞ be the subfield of K^{sep} corresponding to $\mathrm{Ker}(\chi)$; thus the element c is in $\widehat{K_\infty}$, and $\mathrm{Gal}(K_\infty/K)$ is identified with the subgroup $\mathrm{Im}(\chi)$ of $A_\pi^\times$. Choose

(a) a non-trivial element σ of $\mathrm{Gal}(K_\infty/K)$ such that $\chi(\sigma) \in 1 + \pi A_\pi$, and

(b) a closed subgroup B of $\mathrm{Gal}(K_\infty/K)$

such that $\mathrm{Gal}(K_\infty/K) = \langle\sigma\rangle \times B$, where $\langle\sigma\rangle$ is the closure in $\mathrm{Gal}(K_\infty/K)$ of the cyclic subgroup generated by σ (so $\langle\sigma\rangle \simeq \mathbb{Z}_p$, with p the characteristic of K). Denote by L_∞ and M_∞ respectively the subextensions of K_∞ which correspond to B and $\langle\sigma\rangle$. So we have $\mathrm{Gal}(K_\infty/M_\infty) \simeq \mathrm{Gal}(L_\infty/K) \simeq \langle\sigma\rangle$ and $\mathrm{Gal}(K_\infty/L_\infty) \simeq \mathrm{Gal}(M_\infty/K) \simeq B$. The above splitting yields, for each $n \geq 0$, a splitting $\chi^{-1}(1 + \pi^{p^n} A_\pi) = \langle\sigma_n\rangle \times B_n$, where σ_n is a power of σ and B_n is a subgroup of B. Accordingly, we have three fields K_n, L_n and M_n, with $K_n = L_n M_n$, which are the subfields of K_∞ correspoding respectively to $\chi^{-1}(1 + \pi^{p^n} A_\pi)$, $\langle\sigma_n\rangle$ and B_n. Note that $K_n = K(\pi_{p^n})$.

LEMMA 2. *Let X be one of the following fields: $\widehat{K_\infty}$, $\widehat{L_\infty}$, $\widehat{K_\infty^{\mathrm{rad}}}$, and $\widehat{L_\infty^{\mathrm{rad}}}$. Then we have $H^1(\langle\sigma\rangle, X) = 0$.*

In fact, as Lemma 3 shows, we have $\widehat{K_\infty^{\mathrm{rad}}} = \widehat{K_\infty}$ and $\widehat{L_\infty^{\mathrm{rad}}} = \widehat{L_\infty}$.

PROOF. We prove this for $X = \widehat{K_\infty^{\mathrm{rad}}}$ and $\widehat{L_\infty^{\mathrm{rad}}}$. The other cases are proved in the same way. Since a continuous 1-cocycle : $\langle\sigma\rangle \to X$ is determined by its value at σ, $H^1(\langle\sigma\rangle, X)$ is a subspace of $\mathrm{Coker}(\sigma - 1 : X \to X)$. So it is enough to show the map $\sigma - 1 : X \to X$ is surjective.

For any valuation field F, we denote by $\mathcal{O}_F$ its valuation ring. Let $\mathcal{O}$ be either $\mathcal{O}_{K_\infty^{\mathrm{rad}}}$ or $\mathcal{O}_{L_\infty^{\mathrm{rad}}}$. We first show that $(\sigma - 1)(\mathcal{O})$ contains the maximal ideal of $\mathcal{O}$.

Suppose $\mathcal{O} = \mathcal{O}_{K_\infty^{\mathrm{rad}}}$, and set $\mathcal{O}_n := \mathcal{O}_{K_n^{\mathrm{rad}}}$. For any $n \geq 1$, the map $\sigma_{n-1} - 1 : \mathcal{O}_n \to \mathcal{O}_n$ is $\mathcal{O}_{n-1}$-linear. On the other hand, if n is sufficiently large, there exists an element of $\mathcal{O}_n$ which is mapped by $\sigma_{n-1} - 1$ to an element of $\mathcal{O}_{n-1}$ with absolute value not very small. In fact, if $\chi(\sigma_{n-1}) = 1 + u\pi^k$ with $u \in A_\pi^\times$ and $p^{n-1} \leq k < p^n$, put $m := \min\{p^{n-1} + k,\ p^n\}$. Then π_m is in $\mathcal{O}_n$, and $(\sigma_{n-1} - 1)(\pi_m) = [u](\pi_{m-k})$ is in $\mathcal{O}_{n-1}$ (Here again we used the additivity of the Carlitz module). Thus $(\sigma_{n-1} - 1)(\mathcal{O}_n)$ contains $\pi_{m-k}\mathcal{O}_{n-1}$. Since σ_{n-1} is a power of σ, $(\sigma - 1)(\mathcal{O}_n)$ also contains $\pi_{m-k}\mathcal{O}_{n-1}$. Passing to the union, and noticing that $m - k$ increases geometrically with n, we see that $(\sigma - 1)(\mathcal{O})$ contains the maximal ideal of $\mathcal{O}$.

The statement for $\mathcal{O} = \mathcal{O}_{L_\infty^{\mathrm{rad}}}$ follows by noting that $\mathcal{O}_{K_\infty^{\mathrm{rad}}}$ is a free $\mathcal{O}_{L_\infty^{\mathrm{rad}}}$-module which admits a free basis consisting of units of $\mathcal{O}_{M_\infty}$. This can be seen, for example, by applying repeatedly the decomposition

$$\mathcal{O}_{L_\infty^{\mathrm{rad}} \cdot M_n} = \bigoplus_{i=0}^{[M_n : M_{n-1}]-1} \mathcal{O}_{L_\infty^{\mathrm{rad}} \cdot M_{n-1}} \cdot \mu_n^i,$$

where μ_n is a unit of $\mathcal{O}_{M_n}$ such that $\mathcal{O}_{M_n} = \mathcal{O}_{M_{n-1}}[\mu_n]$.

Now again let $\mathcal{O}$ be either $\mathcal{O}_{K_\infty^{\mathrm{rad}}}$ or $\mathcal{O}_{L_\infty^{\mathrm{rad}}}$. As above, we can choose a K^{rad}-basis $(\varpi_\nu)_{\nu \geq 0}$ of K_∞^{rad} (resp. L_∞^{rad}) consisting of elements, e.g., of $\pi\mathcal{O}^\times$. Then any element x of X can be written as a convergent series

$$x = \sum_{\nu \geq 0} x_\nu \cdot \varpi_\nu,$$

where $x_\nu \in K^{\mathrm{rad}}$ and $|x_\nu| \to 0$ as $\nu \to \infty$. Since $\pi\mathcal{O}^\times$ is contained in $(\sigma - 1)(\mathcal{O})$, there exists for each ν an element ϖ'_ν of $\mathcal{O}$ such that $(\sigma - 1)(\varpi'_\nu) = \varpi_\nu$. The element

$$x' := \sum_{\nu \geq 0} x_\nu \cdot \varpi'_\nu \qquad \in X$$

is then mapped by $\sigma - 1$ to x. Q.E.D.

The next step is:

LEMMA 3. *(cf. [3], Proposition 10) Let K be any complete discrete valuation field with perfect residue field, K_∞ an infinite APF-extension of K ([4]), and L a Galois extension of K_∞. Then we have*

$$H^i(G_{K_\infty}, \widehat{L}) = \begin{cases} 0 & \text{if } i > 0, \\ \widehat{K_\infty} & \text{if } i = 0. \end{cases}$$

In particular, we have $\widehat{K_\infty} = \widehat{K_\infty^{\mathrm{rad}}}$ $(= \widehat{K_\infty}^{\mathrm{rad}})$, and hence $\widehat{K_\infty}$ is perfect.

Note that our K_∞, L_∞ and M_∞ are all APF-extensions of K.

As in [3], the above lemma is a formal (though somewhat tricky) consequence of:

LEMMA 4. *(cf. [3], Proposition 9) Let K_∞/K be as above, and let L/K_∞ be a finite separable extension. Denote by $\mathcal{O}_L$ the valuation ring of L, and by $\mathfrak{m}_\infty$ the valuation ideal of K_∞. Then we have* $\mathrm{Tr}_{L/K_\infty}(\mathcal{O}_L) \supset \mathfrak{m}_\infty$.

PROOF. We reproduce the proof of Tate [3], pointing out how to use our assumption. Replacing K by a finite subextension of L/K, we may suppose that there is a finite extension L_0 of K, linearly disjoint from K_∞, such that $L = L_0K_\infty$ (see [2], p. 97, Lemma 6). We may also suppose that L_0/K is a Galois extension, because we my replace L/K_∞ by its Galois closure.

For $u \geq -1$, let K_u be the fixed subfield of K_∞ by the u-th ramification group $\mathrm{Gal}(K_\infty/K)^u$ in the upper numbering, and put $L_u := L_0K_u$. Let v denote the normalized valuation of K. Then the valuation of the different $\mathfrak{D}_{L_u/K_u}$ of L_u/K_u is

$$v(\mathfrak{D}_{L_u/K_u}) = \int_{-1}^{\infty} \left(\frac{1}{(\mathrm{Gal}(K_u/K)^y : 1)} - \frac{1}{(\mathrm{Gal}(L_u/K)^y : 1)} \right) dy .$$

If $h \in \mathbb{R}$ is so large that $y \geq h$ implies $\mathrm{Gal}(L/K)^y \subset \mathrm{Gal}(L/L_0)$ (i.e., $\mathrm{Gal}(K_u/K)^y \simeq \mathrm{Gal}(L_u/K)^y$ for all $u \geq -1$), then we have

$$v(\mathfrak{D}_{L_u/K_u}) \leq \int_{-1}^{h} \frac{dy}{(\mathrm{Gal}(K_u/K)^y : 1)} .$$

Since K_∞/K is APF of infinite degree, for any fixed y, $\mathrm{Gal}(K_\infty/K)^y$ is open in $\mathrm{Gal}(K_\infty/K)$ and $(\mathrm{Gal}(K_u/K)^y : 1)$ tends to infinity with u. Hence the above integral tends to zero with u.

Recall (from e.g. [2], p. 60, Proposition 7) that, in general, for a finite integral extension B/A of Dedekind domains and an ideal $\mathfrak{b}$ (resp. $\mathfrak{a}$) of B (resp. A), we have

$$\mathrm{Tr}_{B/A}(\mathfrak{b}) \subset \mathfrak{a} \quad \Leftrightarrow \quad \mathfrak{b} \subset \mathfrak{a}\mathfrak{D}_{B/A}^{-1} .$$

Applying this for $\mathfrak{b} = \mathcal{O}_{L_u}$ and $\mathfrak{a} = \mathrm{Tr}_{L_u/K_u}(\mathcal{O}_{L_u})$, we see that

$$\mathfrak{D}_{L_u/K_u} \subset \mathrm{Tr}_{L_u/K_u}(\mathcal{O}_{L_u})\mathcal{O}_{L_u} .$$

Since $v(\mathfrak{D}_{L_u/K_u}) \to 0$ as $u \to \infty$, so does $v(\mathrm{Tr}_{L_u/K_u}(\mathcal{O}_{L_u})\mathcal{O}_{L_u})$. This means that $\mathrm{Tr}_{L/K_\infty}(\mathcal{O}_L) \supset \mathfrak{m}_\infty$. Q.E.D.

Now we can complete the proof of (2) of the Theorem. By Lemma 1, we may assume $r = 0$. Look at the spectral sequence

$$0 \to H^1(\mathrm{Gal}(L_\infty/K), H^0(G_{L_\infty}, \mathbb{C})) \to H^1(G_K, \mathbb{C}) \to H^1(G_{L_\infty}, \mathbb{C}).$$

By Lemma 3, $H^1(G_{L_\infty}, \mathbb{C}) = 0$. By Ax (Remark 1, (ii)), $H^0(G_{L_\infty}, \mathbb{C}) = \widehat{L_\infty^{\mathrm{rad}}}$. By Lemma 2, $H^1(\mathrm{Gal}(L_\infty/K), \widehat{L_\infty^{\mathrm{rad}}}) = 0$. Hence we obtain (2).

REMARK 2. Lemma 1 shows that $\mathbb{C}$ is (and in fact, even $\widehat{K_\infty}$ is) "so big" that a topological $A_\pi[G_K]$-module loses much information after being tensored with $\mathbb{C}$. This is because we have our element c in $\mathbb{C}$, and at this point, our $\mathbb{C}$ might be more analogous to B_{dR} or B_{cris} in the usual p-adic theory, rather than to $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}_p^{\mathrm{sep}}}$ (this observation was communicated to the author by Nobuo Tsuzuki, to whom the author is grateful). But our $\mathbb{C}$ does not have enough structures to recover π-adic Galois representations. Is there a cleverer ring than $\mathbb{C}$?

2. The Hodge-Tate decomposition of finite t-modules

The purpose of this Section is to give the Hodge-Tate decomposition of finite t-module, which is very similar to that in [6], §4. Since the story goes exactly in the same way, we merely give definitions and the statements of our results, and point out some minor differences from the classical case.

Let A be the polynomial ring $\mathbb{F}_q[t]$ in one variable t over the finite field $\mathbb{F}_q$ of q elements, and let F be its fraction field $\mathbb{F}_q(t)$. Let $\alpha : A \to K$ be a complete discrete valuation field of "mixed characteristic" over A. Let (π) be the residual "characteristic" of K, where π is the unique monic prime element of A such that $\alpha(\pi)$ is in the valuation ideal of K. We denote by A_π (resp. F_π) the π-adic completion of A (resp. F).

For a finite t-module (Chapter II, §2) $J = \mathrm{Spec}\, B$ over $\mathcal{O}_K$, let $\mathcal{E}_J := \mathrm{Hom}_{\mathbb{F}_q,\mathcal{O}_K}(J, \mathbb{G}_a)$ be the $\mathcal{O}_K$-submodule of $B = \mathrm{Hom}_{\mathcal{O}_K}(J, \mathbb{A}^1)$ consisting of $\mathbb{F}_q$-linear morphisms of group schemes defined over $\mathcal{O}_K$. Let $\mathcal{E}_J^{(q)}$ denote the base extension of $\mathcal{O}_J$ by the q-th power map of $\mathcal{O}_K$. Then, as in §§1 and 2 of Chapter II, we are given an $\mathcal{O}_K$-module homomorphism $\varphi_J : \mathcal{E}_J^{(q)} \to \mathcal{E}_J$ which comes from the Frobenius morphism of J, and an $\mathcal{O}_K$-endomorphism $\psi_t : \mathcal{E}_J \to \mathcal{E}_J$ which describes the action of t. Since J is étale over K (Chapter II, Lemma (2.2)), it has a unique v-module structure $v_J : \mathcal{E}_J \to \mathcal{E}_J^{(q)}$ (Chapter II, Proposition (3.5)).

Let $B^1 = \mathrm{Ker}(\varepsilon_J^* : B \to \mathcal{O}_K)$ be the augmentation ideal of B (ε_J^* is the counit of B). B^1 is the ideal generated by $\mathcal{E}_J$. If B^2 denotes the square of B^1, we have $B^1/B^2 \simeq \mathrm{Coker}(\varphi_J)$ (cf. [5], Proposition 2.1, 2)). For an $\mathcal{O}_K$-module M, we put $t_J(M) := \mathrm{Hom}_{\mathcal{O}_K}(\mathrm{Coker}(\varphi_J), M)$ (the *tangent space of J with values in M*), and $t_J^*(M) := M \otimes_{\mathcal{O}_K} \mathrm{Coker}(\varphi_J)$ (the *cotangent space of J with values in M*). The $\mathcal{O}_K$ module $\underline{\omega}_J$ of invariant differentials of J can be identified with $t_J^*(\mathcal{O}_K) = \mathrm{Coker}(\varphi_J)$. In our case, this identification is induced simply by $d : \mathcal{E}_J \to \underline{\omega}_J$; $x \mapsto dx$. Also for t_J, we have canonical identifications

$$\mathrm{Der}_{\mathcal{O}_K}(B, M) = \mathrm{Hom}_B(\Omega_{\mathcal{O}_K}(B), M) = \mathrm{Hom}_{\mathcal{O}_K}(\underline{\omega}_J, M) = t_J(M).$$

Recall that for a finite v-module J, there is defined its dual J' (Chapter II, §4; where it was written J^*). We have

$$\mathcal{E}_{J'} = \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{E}_J, \mathcal{O}_K)$$

and $v_{J'} = \varphi'_J$ (resp. $\varphi_{J'} = v'_J$), the transpose of φ_J (resp. v_J).

For an $\mathcal{O}_K$-module M, we put

$$\underline{\alpha}_{J'}(M) := \mathrm{Ker}(\mathrm{id}_M \otimes v_{J'} : M \otimes \mathcal{E}_{J'} \to M \otimes \mathcal{E}_{J'}^{(q)}).$$

This is identified with

$$\begin{aligned} &\mathrm{Ker}(\varphi'_J \otimes M : \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{E}_J, M) \to \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{E}_J^{(q)}, M)) \\ &= \mathrm{Hom}_{\mathcal{O}_K}(\mathrm{Coker}(\varphi_J), M) = t_J(M). \end{aligned}$$

The finite t-module J represents the functor (Chapter II, Theorem (4.3))

$$\begin{aligned}\mathrm{Hom}_v(J', C) \ : \ (\mathcal{O}_K\text{-algebras}) &\to (A\text{-modules}) \\ R &\mapsto \mathrm{Hom}_{v,R}(R \otimes_{\mathcal{O}_K} J', R \otimes_A C).\end{aligned}$$

Once we fix a coordinate Z of C, the ring homomorphism $R[Z] \to R \otimes_{\mathcal{O}_K} B'$ corresponding to a homomorphism $R \otimes_{\mathcal{O}_K} J' \to R \otimes_A C$ is determined by the image of Z. Since the v-module structure of C is given by $\mathcal{E}_C \to \mathcal{E}_C^{(q)}$; $Z \mapsto 1 \otimes Z$, we have

$$J(\mathcal{O}_{\overline{K}}) \ = \ \{x \in \mathcal{O}_{\overline{K}} \otimes_{\mathcal{O}_K} \mathcal{E}_{J'};\ v_J(x) = 1 \otimes x\}.$$

The map

$$\begin{aligned}\mathcal{O}_{\overline{K}} \otimes \mathcal{E}_{J'} &\to \Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{K}} \otimes_{\mathcal{O}_K} B') \\ x &\mapsto dx\end{aligned}$$

restricts to give a map

$$J(\mathcal{O}_{\overline{K}}) \to \Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{K}} \otimes_{\mathcal{O}_K} B').$$

Extending the scalars, we obtain a map

$$\widehat{\phi}_J : \mathcal{O}_{\overline{K}} \otimes_{A_*} J(\mathcal{O}_{\overline{K}}) \to \Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{K}} \otimes_{\mathcal{O}_K} B'),$$

which is $\mathcal{O}_{\overline{K}}$-linear and G_K-equivariant. There is a canonical decomposition

$$\Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{K}} \otimes B') \ = \ (\mathcal{O}_{\overline{K}} \otimes_{\mathcal{O}_K} \Omega_{\mathcal{O}_K}(B')) \oplus (\Omega \otimes_{\mathcal{O}_K} B'),$$

where $\Omega := \Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{K}})$. As in [6], 4.5, we find that the image of $\widehat{\phi}_J$ is actually in

$$(\mathcal{O}_{\overline{K}} \otimes_{\mathcal{O}_K} \underline{\omega}_{J'}) \oplus \underline{\alpha}_{J'}(\Omega) \ = \ t^*_{J'}(\mathcal{O}_K) \oplus t_J(\Omega).$$

Thus we obtain a map

$$\phi_J = \phi_J^0 \oplus \phi_J^1 \ : \ \mathcal{O}_{\overline{K}} \otimes_{A_*} J(\mathcal{O}_{\overline{K}}) \ \to \ t^*_{J'}(\mathcal{O}_K) \oplus t_J(\Omega).$$

The maps ϕ_J^0 and ϕ_J^1 admit another interpretation as in [6], §4, Propositions 6 and 7. The following results are obtained exactly in the same way as in [6]. In our case, the argument is even simpler, sinece we used $x \mapsto dx$ (rather than $x \mapsto \frac{dx}{x}$) to define the map ϕ_J. Note that in proving our version, we should work with $\mathcal{E}_J$ and $\mathcal{E}_{J'}$ (rather than B and B').

PROPOSITION 1. *The following diagram is commutative:*

$$\begin{array}{ccc}(\mathcal{O}_{\overline{K}} \otimes_{A_*} J(\mathcal{O}_{\overline{K}})) \times (\mathcal{O}_{\overline{K}} \otimes_{A_*} J'(\mathcal{O}_{\overline{K}})) & \xrightarrow{\phi_J \times \phi_{J'}} & t^*_{J'}(\mathcal{O}_{\overline{K}}) \oplus t_J(\Omega) \oplus t^*_J(\mathcal{O}_{\overline{K}}) \oplus t_{J'}(\Omega) \\ \theta \downarrow & & \downarrow \nu \\ (\overline{K}/\mathcal{O}_{\overline{K}})(1) & \xrightarrow{\bar{\xi}} & \Omega\ ,\end{array}$$

where

—— θ *is the map obtained by extension of scalars from the duality pairing* $\theta : J(\mathcal{O}_{\overline{K}}) \times J'(\mathcal{O}_{\overline{K}}) \to {}_{\pi^\infty}C(\mathcal{O}_{\overline{K}})$,

—— $\widetilde{\xi}$ *is the map induced by* $\xi : \overline{K}(1) \to \Omega$ *of §1 of [6], and*

—— $\nu(a', \lambda, a, \lambda') := \lambda(a) + \lambda'(a')$ *for*
$(a', \lambda, a, \lambda') \in t^*_{J'}(\mathcal{O}_{\overline{K}}) \oplus t_J(\Omega) \oplus t^*_J(\mathcal{O}_{\overline{K}}) \oplus t_{J'}(\Omega)$.

The proof is the same as the proof of Proposition 8 of [6], but the concluding equality is

$$(\nu \circ (\phi_J \times \phi_{J'}))(u, v) \;=\; d(\sum u(b_i)v(b'_J)),$$

because the duality pairing $J \times J' \to C$ is given by $Z \mapsto \sum_i b_i \otimes b'_i$ (see the proof of Theorem (4.3) of Chapter II).

Using the same formalism as in [6], we have

THEOREM. *Let* a *be an element of* $\mathcal{O}_K$ *such that* $v_F(a) = \frac{1}{q-1} + v_F(\mathfrak{D}_{K/F})$. *Then the kernel and the cokernel of the map*

$$\phi_J : \mathcal{O}_{\overline{K}} \otimes_{A_\star} J(\mathcal{O}_{\overline{K}}) \to t^*_{J'}(\mathcal{O}_{\overline{K}}) \oplus t_J(\Omega)$$

is killed by a.

Now let π be a prime element of A, and let H be a π-divisible group over $\mathcal{O}_K$ of height h, i.e., an inductive system $(H_n, i_n)_{i \in \mathbb{N}}$ in which

(i) H_n is a finite t-module over $\mathcal{O}_K$ of rank q^{nh}; and

(ii) for all $n \in \mathbb{N}$, $i_n : H_n \to H_{n+1}$ as a morphism of finite t-modules which identifies the kernel of multiplication by π^n on H_{n+1}.

Let $T_\pi(\cdot)$ denote the π-adic Tate module; $T_\pi(H) := \operatorname{projlim} H_n(\mathcal{O}_{\overline{K}})$ and $T_\pi(\Omega) := \operatorname{Hom}_{A_\star}(F_\pi/A_\pi, \Omega)$. Then the Theorem passes to the projective limit (cf. [6], §5, n$^{\text{os}}$ 5.8 à 5.10) to give

PROPOSITION 2. *There exists a canonical* $\mathbb{C}_\pi[G_K]$*-module homomorphism*

$$\phi_H : \mathcal{O}_{\mathbb{C}_\star} \otimes_{A_\star} T_\pi(H) \to t^*_{H'}(\mathcal{O}_{\mathbb{C}_\star}) \oplus t_H(T_\pi(\Omega)),$$

which is injective and whose cokernel is of finite length over $\mathcal{O}_{\mathbb{C}_\star}$.

Tensoring with $\mathbb{C}_\pi$, *we obtain the Hodge-Tate decomposition*

$$\phi_H : \mathbb{C}_\pi \otimes_{A_\star} T_\pi(H) \xrightarrow{\;\simeq\;} t^*_{H'}(\mathbb{C}_\pi) \oplus t_H(\mathbb{C}_\pi(1)) \,.$$

References

[1] J. Ax, *Zeros of polynomials over local fields — the Galois action*, J. of Algebra **15** (1970), 417 – 428.

[2] J-P. Serre, *Corps Locaux (3^e éd.)*, Hermann, Paris, 1980.

[3] J. Tate, *p-divisible groups*, in: Proceedings of a conference on local fields, Driebergen, 1966 (1967), Springer-Verlag, Berlin-Heidelberg-New York, pp. 158 – 183.

[4] J-P. Wintenberger, *Le corps des normes de certaines extensions infinies de corps locaux; applications*, Ann. Sci. Éc. Norm. Sup., 4^e série **16** (1983), 59 – 89.

[5] V. G. Drinfeld, *Moduli varieties of F-sheaves*, Funktsional'nyi Analiz i Ego Prilozheniya **21** (1987), 23 – 41.

[6] J-M. Fontaine, *Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux*, Invent. Math. **65** (1982), 379 – 409.

Chapter IV

Regular singularity of Drinfeld modules

Introduction

In analogy with the classical theory of ordinary differential equations (see e.g. [6], [1], [5]), we define in this Chapter the notion *regular singularity* of a Drinfeld module at infinity. It turns out (Theorem (2.2)) that a Drinfeld module with regular singularity can not have a complex multiplication if the infinite place is of degree one, and has a tamely ramified period lattice which is of diamond shape. In §3, we study regular singularity of φ-modules, which have more similar formalism to $\mathcal{D}$-modules. We express the regularity of the singularity of φ-modules over a local field in four ways (Theorems (3.8) and (3.9)); (1) naively in terms of the valuations of the coefficients of certain polynomials, (2) by the existence of φ-stable lattices, (3) by the tameness of Galois actions, and (4) in terms of the norm of connections.

For a field K, we denote by K^{sep} a fixed separable closure of K, and let $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$, the absolute Galois group of K.

1. Regular polynomials

Let K be a discrete valuation field of characteristic $p > 0$, with valuation denoted v. Choose and fix an extension of v to K^{sep}, denoted also v.

DEFINITION (1.1). A polynomial $f(X) = a_0X + a_1X^p + \cdots + a_nX^{p^n} \in K[X]$ is said to be *regular* (at v) if $a_0 \neq 0$, $a_n \neq 0$, and

$$v(a_i) - v(a_n) \geq \frac{p^n - p^i}{p^n - 1}(v(a_0) - v(a_n)) \tag{1.1.1}$$

for all $i = 1, \cdots, n-1$.

A regular polynomial $f(X)$ is separable because $f'(X) = a_0 \neq 0$. The condition (1.1.1) is saying that the Newton polygon of $f(X)$ is a straight line. This is equivalent to that all non-zero roots of $f(X)$ have the same valuation $(v(a_0) - v(a_n))/(p^n - 1)$.

Regularity of $f(X)$ is invariant by multiplying $f(X)$ by an element of $K^\times$. If a_n is a unit (i.e. $v(a_n) = 0$), then (1.1.1) is simply

$$v(a_i) \geq \frac{p^n - p^i}{p^n - 1}v(a_0). \tag{1.1.2}$$

Regularity of $f(X)$ is invariant also under the change of variable $X \mapsto aX$ with $a \in K^\times$.

The terminology "regular" for $f(X)$ has a dual meaning, because it may be the zero *or* the pole (singularity) at v of the roots of $f(X)$ that is meant by this word to be not so wild. In §2, however, "regular" always alludes to singularity.

For any separable polynomial $f(X) \in K[X]$, we denote by K_f the minimal splitting field of f contained in K^{sep}.

PROPOSITION (1.2). *Let f be a regular polynomial over K. Then the extension K_f/K is tamely ramified at v.*

PROOF:— We may assume f is monic; $a_n = 1$. Dividing by X^{p^n} the both sides of the equation

$$a_0 X + a_1 X^p + \cdots + a_{n-1} X^{p^{n-1}} + X^{p^n} \;=\; 0,$$

we have

$$(1.2.1) \qquad a_0 \left(\frac{1}{X}\right)^{p^n-1} + a_1 \left(\frac{1}{X}\right)^{p^n-p} + \cdots + a_{n-1} \left(\frac{1}{X}\right)^{p^n-p^{n-1}} + 1 \;=\; 0.$$

Take an element $s \in K^{\mathrm{sep}}$ such that $a_0 s^{p^n-1} = 1$, and put $Y := 1/sX$ and $b_i := a_i s^{p^n-p^i}$. Then the equation (1.2.1) is equivalent, over $K(s)$, to

$$(1.2.2) \qquad Y^{p^n-1} + b_1 Y^{p^n-p} + \cdots + b_{n-1} Y^{p^n-p^{n-1}} + 1 \;=\; 0$$

Write $g(Y)$ for the left hand side of (1.2.2). Since $K(s)/K$ is tamely ramified at v, it is enough to show the minimal splitting field of $g(Y)$ is tamely ramified over $K(s)$. Since the composition of two tamely ramified extensions is again tamely ramified, it is enough to show that $K(s,y)$ is tamely ramified over $K(s)$, where y is any root of $g(Y)$ in K^{sep}.

Since $v(s) = -v(a_0)/(p^n-1)$, we see, by the assumption that f is regular, that

$$v(b_i) \;=\; v(a_i) - \frac{p^n - p^i}{p^n - 1} v(a_0) \;\geq\; 0.$$

Hence the roots y of (1.2.2) are all units. Thus $g'(y) = -y^{p^n-2}$ is a unit, and $K(s,y)/K(s)$ is unramified. Q.E.D.

2. Drinfeld modules with regular singularity at infinity

Let k be an algebraic function field in one variable over its field of constants $\mathbb{F}_q$, the finite field of q elements. Fix a place ∞ of k, and let A be the ring of elements of k which are regular outside ∞. For $a \in A$, define $\deg(a)$ by $q^{\deg(a)} = \#(A/aA)$ if $a \neq 0$, and $\deg(0) := 0$.

Let K be any complete discrete valuation field which contains k in such a way that the valuation v of K extends the zero-order valuation at ∞, ord_∞, of k. Let $\phi : A \to \mathrm{End}_K(\mathbb{G}_a)$; $a \mapsto \phi_a$ be a Drinfeld A-module over K of rank r. We think of ϕ as being given, for each $a \in A$, by a polynomial

$$\phi_a(X) = aX + a_1 X^q + \cdots + a_n X^{q^n}, \qquad a_i \in K \quad (n = r \cdot \deg(a))$$

with respect to a fixed coordinate X of $\mathbb{G}_a$. Write $\delta_\phi(a)$ for the coefficient a_n of the leading term of $\phi_a(X)$.

DEFINITION (2.1). A Drinfeld module ϕ over K is said to have *regular singularity* (at v) if there exists a non-constant element a of A such that ϕ_a is a regular polynomial (1.1).

This definition does not depend on the choice of the coordinate X of $\mathbb{G}_a$.

Recall ([2], §3) that a Drinfeld module over K of rank r can be uniformized by its *period lattice* Λ, which is a projective A-module of rank r contained in K^{sep}. The situation is best described by the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & K^{\mathrm{sep}} & \xrightarrow{e} & K^{\mathrm{sep}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle \phi_a} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & K^{\mathrm{sep}} & \xrightarrow{e} & K^{\mathrm{sep}} & \longrightarrow & 0\,, \end{array}$$

where $e : K^{\mathrm{sep}} \to K^{\mathrm{sep}}$ is the map defined by

$$e(z) = z \prod_{\lambda \in \Lambda - 0} \left(1 - \frac{z}{\lambda}\right)$$

for all $z \in K^{\mathrm{sep}}$. Let $|\cdot|$ denote the absolute value of K^{sep} such that $|a| = \#(A/aA)$ for all $a \in A - 0$.

THEOREM (2.2). *Let ϕ be a Drinfeld module over K of rank r. Let Λ be the period lattice of ϕ, and put*

$$l_1 := \min\{|\lambda| \ ; \ \lambda \in \Lambda - 0\} \qquad \textit{(the first successive minimum of } \Lambda),$$
$$\Lambda_1 := \{\lambda \in \Lambda \ ; \ |\lambda| = l_1\}.$$

(i) Let a be a non-constant element of A. Then ϕ_a is regular if and only if Λ is generated by Λ_1 over $\mathbb{F}_q[a]$. If this is the case, we have

(1) $l_1 = |a| \cdot |a/\delta_\phi(a)|^{1/(q^{r\cdot \deg(a)}-1)}$;

(2) for any $b \in A$, $\deg(b)$ *is a multiple of* $\deg(a)$;

(3) if the place ∞ *is of degree one (i.e., the residue field of* ∞ *is* $\mathbb{F}_q$*), then we have* $A = \mathbb{F}_q[a]$.

(ii) Let $K(\Lambda)/K$ *(resp.* $K({}_a\phi)/K$*) be the field extension obtained by adjoining the elements of* Λ *(resp. a-division points of* ϕ*). If* ϕ *has regular singularity, then we have* $K(\Lambda) = K({}_a\phi)$ *for all non-constant element* a *of* A. *In particular,* $K(\Lambda)/K$ *is tamely ramified.*

PROOF:— (i) Assume ϕ_a is regular. Then all non-zero roots x_0 of ϕ_a have the same absolute value

$$|x_0| = |a/\delta_\phi(a)|^{1/(q^{r\cdot \deg(a)}-1)}, \tag{2.2.1}$$

and are of the form

$$x_0 = e(\frac{\lambda_0}{a}) = \frac{\lambda_0}{a} \prod_{\lambda \in \Lambda - 0} (1 - \frac{\lambda_0}{a\lambda})$$

for some $\lambda_0 \in \Lambda$. Take $\lambda_1 \in \Lambda_1$ and set $x_1 := e(\frac{\lambda_1}{a})$, a root of ϕ_a. Then $|1 - \frac{\lambda_1}{a\lambda}| = 1$ for all $\lambda \in \Lambda - 0$. Hence we have $|x_1| = |\frac{\lambda_1}{a}|$. This together with (2.2.1) proves (1).

If Λ_1 does not generate Λ over $\mathbb{F}_q[a]$, then there exists a non-zero element λ_2 of Λ which is not a linear combination of elements of Λ_1 over $\mathbb{F}_q[a]$ and which is minimal with respect to the absolute value $|\cdot|$. Set $x_2 := e(\frac{\lambda_2}{a})$, another root of ϕ_a. We must have

$$|x_1| = |x_2| = |\frac{\lambda_2}{a} \prod_{\lambda \in \Lambda - 0} (1 - \frac{\lambda_2}{a\lambda})|.$$

Suppose $|a\lambda| = |\lambda_2|$ for some $\lambda \in \Lambda$. Then $|\lambda| < |\lambda_2|$. The minimality of $|\lambda_2|$ implies that λ is a linear combination of elements of Λ_1 over $\mathbb{F}_q[a]$, and that $|a\lambda - \lambda_2| = |\lambda_2| = |a\lambda|$. Hence $|1 - \frac{\lambda_2}{a\lambda}| = |\frac{a\lambda - \lambda_2}{a\lambda}| = 1$. We have thus

$$|x_2| = |\frac{\lambda_2}{a} \prod_{\lambda \in \Lambda - 0} (1 - \frac{\lambda_2}{a\lambda})| \geq |\frac{\lambda_2}{a}| > |\frac{\lambda_1}{a}| = |x_1|,$$

yielding a contradiction.

Suppose conversely that Λ_1 generates Λ over $\mathbb{F}_q[a]$ for some $a \in A$. Then any non-zero root of ϕ_a is of the form $e(\frac{\lambda_1}{a})$ for some $\lambda_1 \in \Lambda_1$. All these have the same absolute value $l_1/|a|$, whence ϕ_a is regular.

Before proving (2), we note the following

LEMMA (2.2.2). *Let* a *be an element of* K^{sep} *with* $|a| > 1$, *and let* $\lambda_1, \cdots, \lambda_d$ *be elements of* Λ_1 *which are linearly independent over* $\mathbb{F}_q$. *Then we have*

$$|c_1\lambda_1 + \cdots + c_d\lambda_d| = \max\{|c_i\lambda_i|;\ 1 \leq i \leq d\}$$

for any $c_1, \cdots, c_d \in \mathbb{F}_q((\frac{1}{a}))$. *In particular, the elements* $\lambda_1, \cdots, \lambda_d \in K^{\mathrm{sep}}$ *are linearly independent over* $\mathbb{F}_q((\frac{1}{a}))$.

PROOF:— Suppose $c_i = \sum_{j \le n} c_{ij} a^j$ with $c_{ij} \in \mathbb{F}_q$ for $1 \le i \le d$, and $c_{in} \neq 0$ for some i (i.e. $n = \max\{\deg_a(c_i);\ 1 \le i \le d\}$). Then

$$\sum_{i=1}^{d} c_i \lambda_i \ = \ \sum_{j \le n} (\sum_{i=1}^{d} c_{ij} \lambda_i) a^j,$$

and

$$\max\{|c_i \lambda_i|;\ 1 \le i \le d\} \ = \ |a^n \lambda_i| \ = \ |a|^n l_1.$$

Since $\lambda_1, \cdots, \lambda_d \in \Lambda_1$ are linearly independent over $\mathbb{F}_q$, we have $\sum_{i=1}^{d} c_{in} \lambda_i = l_1$. Hence the claimed equality follows.

Now suppose that ϕ_a is regular for a non-constant element a of A, and that there exists an element b of A such that $\deg(b)$ is not a multiple of $\deg(a)$. Take $\lambda_1 \in \Lambda_1$ and consider the a-division point

$$x_1' := e(\frac{b\lambda_1}{a}) \ = \ \frac{b\lambda_1}{a} \prod_{\lambda \in \Lambda - 0} (1 - \frac{b\lambda_1}{a\lambda}).$$

By (i), any $\lambda \in \Lambda$ is a linear combination of elements of Λ_1 over $\mathbb{F}_q[a]$. Then by Lemma (2.2.2), $|a\lambda|$ is l_1 times a power of $|a|$, so we cannot have $|a\lambda| = |b\lambda_1|$. Thus $|1 - \frac{b\lambda_1}{a\lambda}| = \max(1, |\frac{b\lambda_1}{a\lambda}|)$, and

$$|x_1'| \ \ge \ |\frac{b\lambda_1}{a}| \ > \ |\frac{\lambda_1}{a}| \ = \ |x_1|.$$

This contradicts the fact that the roots of ϕ_a all have the same absolute value.

To prove (3), suppose Λ_1 generates Λ over $\mathbb{F}_q[a]$. Let k_∞ be the topological closure of k in K. If ∞ is of degree one, then by Lemma (2.2.2), elements of $\Lambda_1 \cup \{0\}$ which are linearly independent over $\mathbb{F}_q$ are still linearly independent over k_∞. In particular, we have $\mathbb{F}_q[a] \otimes_{\mathbb{F}_q} (\Lambda_1 \cup \{0\}) \simeq \Lambda \simeq A \otimes_{\mathbb{F}_q} (\Lambda_1 \cup \{0\})$. Since $\Lambda_1 \cup \{0\}$ is faithfully flat over $\mathbb{F}_q$, we have $A = \mathbb{F}_q[a]$.

(ii) Let a be a non-constant element of A. We have $K(\Lambda) \supset K({}_a\phi)$, since $\Lambda / a\Lambda \simeq {}_a\phi$ as Galois modules. We will show $K(\Lambda) = K({}_a\phi)$. If $\sigma \in \mathrm{Gal}(K(\Lambda)/K({}_a\phi))$, then σ fixes Λ (mod. $a\Lambda$), that is, for each $\lambda \in \Lambda$, we have

$$\sigma(\lambda) \ = \ \lambda + a\lambda' \qquad \text{for some } \lambda' \in \Lambda.$$

For $\lambda \in \Lambda_1$, this λ' must be zero, because we must have $|\sigma(\lambda)| = |\lambda| = l_1$, while $|a| > 1$. Since Λ_1 generates Λ over A by (i), σ fixes all of Λ. Thus $K(\Lambda) = K({}_a\phi)$, which is tamely ramified over K by Proposition (1.2). Q.E.D.

3. Regular singularity of φ-modules

Let K be a field which contains the finite field $\mathbb{F}_q$ of q elements.

DEFINITION (3.1). A *φ-module* over K is a pair (D,φ) consisting of a finite dimensional K-vector space D and an $\mathbb{F}_q$-linear map $\varphi : D \to D$ such that

(1) $\varphi(ax) = a^q\varphi(x)$ for all $a \in K$ and $x \in D$;

(2) $K \cdot \varphi(D) = D$.

The dimension of the K-vector space D is called the *rank* of (D,φ). A *morphism* of φ-modules is a morphism of K-vector spaces which commutes with the φ's. We denote by $\mathcal{F}_K$ the category of φ-modules over K.

Our notion of φ-modules is the simplest case of more general notions such as those considered in [3], [8], [4], etc.. Note that, in a general context, our φ-modules should be called *étale* φ-modules.

In what follows, K is always the bese field on which we work, and n is the rank of the φ-module under consideration.

We define the tensor product $(D,\varphi) = (D_1,\varphi_1) \otimes (D_2,\varphi_2)$ of two φ-modules (D_1,φ_1) and (D_2,φ_2) by setting $D := D_1 \otimes_K D_2$ and defining $\varphi : D \to D$ to be the map $\varphi_1 \otimes \varphi_2$. With this tensor product, $\mathcal{F}_K$ becomes a $\otimes$-category.

For any φ-module (D,φ) over K and any field extension L/K, we make $D_L := L \otimes_K D$ a φ-module over L by defining $\varphi : D_L \to D_L$ to be the map

$$\sum a \otimes x \mapsto \sum a^q \otimes \varphi(x).$$

If the extension is Galois, then the Galois group acts on D_L via the firt factor.

For a φ-module (D,φ) over K, put

$$V(D) := (K^{\text{sep}} \otimes_K D)^{\varphi},$$

the set of fixed points of $D_{K^{\text{sep}}}$ by φ. It is clear that $V(D)$ is an $\mathbb{F}_q$-vector space which is stable under the action of G_K on $D_{K^{\text{sep}}}$. We have thus an $\mathbb{F}_q$-linear representation $V(D)$ of G_K.

Conversely, if V is a finite dimensional $\mathbb{F}_q$-linear representation of G_K, put

$$D(V) := (K^{\text{sep}} \otimes_{\mathbb{F}_q} V)^{G_K},$$

the set of points of $K^{\text{sep}} \otimes_{\mathbb{F}_q} V$ which are fixed by the diagonal action of G_K. Clearly $D(V)$ is a K-vector space, which we make a φ-module by defining $\varphi : D(V) \to D(V)$ to be the map

$$\sum a \otimes x \mapsto \sum a^q \otimes x.$$

The following lemma holds in fact in much greater generality; for a proof, we refer the reader to §0 of [7], or §A.1 of [4]. See also [3], Proposition 2.1 and Chapter II, Proposition (1.7).

LEMMA (3.2). *Let $\mathcal{F}_K$ (resp. $\mathcal{G}_K$) be the category of φ-modules over K (resp. the category of finite dimensional $\mathbb{F}_q$-linear representaions of G_K). Then by the construction explained above, we have a $\otimes$-equivalence of $\otimes$-categories $V : \mathcal{F}_K \to \mathcal{G}_K$, with a quasi-inverse $D : \mathcal{G}_K \to \mathcal{F}_K$.* □

A vector x of a φ-module D is said to be *cyclic* if the n vectors $x, \varphi(x), \cdots, \varphi^{n-1}(x)$ form a K-base of D. As in Lemme 1.3, Chapitre II of [1], we have

LEMMA (3.3). *If the base field K is infinite, there exists a cyclic vector for (D, φ).*

PROOF:— Let m be the largest integer such that there exists a vector $x \in D$ such that $x, \varphi(x), \cdots, \varphi^{m-1}(x)$ are linearly independent over K. Suppose $m < n$. Then there exist two vectors x and y in D such that

$$(3.3.1) \qquad \begin{cases} \text{the } (m+1) \text{ vectors } x,\ \varphi(x), \cdots, \varphi^{m-1}(x),\ \varphi^m(y) \\ \text{are linearly independent over } K. \end{cases}$$

For any $a \in K$, the $(m+1)$ vectors

$$x + ay,\ \varphi(x + ay),\ \cdots,\ \varphi^m(x + ay)$$

are linearly dependent over K. So we have

$$\begin{aligned} 0 &= (x + ay) \wedge (\varphi(x) + a^q \varphi(y)) \wedge \cdots \wedge (\varphi^m(x) + a^{q^m} \varphi^m(y)) \\ &= \sum_{I \cup J = m+1} \varepsilon_I a^{q^J} \varphi^{\wedge I}(x) \wedge \varphi^{\wedge J}(y), \end{aligned}$$

where the sum is taken over all partitions of $m + 1 := \{0, 1, \cdots, m\}$;

$$\begin{cases} I = \{i_1, \cdots, i_r\},\ \ J = \{j_1, \cdots, j_s\}, \quad (r + s = m + 1) \\ I \cup J \ = \ m + 1, \quad I \cap J \ = \ \varnothing, \end{cases}$$

and the abbreviated notations are:

$$\begin{cases} \varepsilon_I \ = \ \pm 1, \qquad a^{q^J} := a^{q^{j_1} + \cdots + q^{j_s}}, \\ \varphi^{\wedge I}(x) := \ \varphi^{i_1}(x) \wedge \cdots \wedge \varphi^{i_r}(x), \\ \varphi^{\wedge J}(y) := \ \varphi^{j_1}(y) \wedge \cdots \wedge \varphi^{j_s}(y). \end{cases}$$

Since q^J's are different for different J's, and since we have assumed K is infinite, all the exterior products which appear as the coefficients of a^{q^J}'s must be zero. In particular, we obtain

$$x \wedge \varphi(x) \wedge \cdots \wedge \varphi^{m-1}(x) \wedge \varphi^m(y) \ = \ 0,$$

contradicting to (3.3.1). Q.E.D.

Now we return to a general K, and assume the φ-module (D,φ) has a cyclic vector x. We associate with x a polynomial $P_x(X) \in K[X]$ as follows: if

$$a_0 x + a_1 \varphi(x) + \cdots + a_{n-1}\varphi^{n-1}(x) + \varphi^n(x) \;=\; 0 \qquad \text{with } a_i \in K,$$

then put

$$P_x(X) := \; a_0 X + a_1 X^q + \cdots + a_{n-1} X^{q^{n-1}} + X^{q^n}.$$

This polynomial is determined by x uniquely. Multiplying x by a scalar $a \in K^\times$ yields:

$$\begin{aligned} P_{ax}(X) \;&=\; a^{q^n} P_x(a^{-1}X) \\ &=\; a_0 a^{q^n-1} X + a_1 a^{q^n-q} X^q + \cdots + a_{n-1} a^{q^n-q^{n-1}} X^{q^{n-1}} + X^{q^n}. \end{aligned}$$

We also define

$$\check{V}_x(D) := \; \{\alpha \in K^{\mathrm{sep}};\; P_x(\alpha) = 0\}.$$

This is clearly an $\mathbb{F}_q$-vector space on which G_K acts.

Recall that we have a canonical inclusion $D \subset D_{K^{\mathrm{sep}}}$ (by definition) and a canonical identification $D_{K^{\mathrm{sep}}} = K^{\mathrm{sep}} \otimes_{\mathbb{F}_q} V(D)$ (by Lemma (3.2)).

LEMMA (3.4). *Suppose that x is expressed by a column vector ${}^t(x_0, \cdots, x_{n-1})$, $x_i \in K^{\mathrm{sep}}$, with respect to an $\mathbb{F}_q$-base $(e_i)_{0\le i\le n-1}$ of $V(D)$. Then the n elements $x_0, \cdots, x_{n-1}$ form an $\mathbb{F}_q$-base of $\check{V}_x(D)$, so $\check{V}_x(D)$ is an n-dimensional $\mathbb{F}_q$-linear representation of G_K. The two representations of G_K, $V(D)$ and $\check{V}_x(D)$, are contragredient to each other.*

PROOF:— Since $\varphi^j(x) = {}^t(x_0^{q^j}, \cdots, x_{n-1}^{q^j})$ with respect to the base (e_i), each x_i is a root of $P_x(X)$; we have $x_i \in \check{V}_x(D)$. Since $\det(x_i^{q^j})_{0\le i,j\le n-1} \neq 0$ by cyclicity of x, the n elements $x_0, \cdots, x_{n-1}$ are linearly independent over $\mathbb{F}_q$. Since the cardinality of $\check{V}_x(D)$ does not exceed the degree of $P_x(X)$, it follows that $\check{V}_x(D)$ is n-dimensional and is spanned by $x_0, \cdots, x_{n-1}$.

Since $x = x_0 e_0 + \cdots + x_{n-1} e_{n-1} \in D$ is fixed by G_K, the representations $V(D)$ (which has (e_i) as an $\mathbb{F}_q$-base) and $\check{V}_x(D)$ (which has (x_i) as an $\mathbb{F}_q$-base) are contragredient to each other. Q.E.D.

In the rest, we assume that K is a complete discrete valuation field, with valuation v and residue field k. We shall interpret the regularity (in the sense of (1.1)) of the polynomial P_x in terms of lattices, Galois actions, and connections. Let $|\cdot| = q^{-v(\cdot)}$ be the absolute value associated with v. For any algebraic extension L/K, the valuation v and the absolute value $|\cdot|$ of K extend uniquely to L, which are again denoted v and $|\cdot|$ respectively. We denote by $\mathcal{O}_L$ the valuation ring of L.

Let (D,φ) be a φ-module over K. An $\mathcal{O}_K$-lattice D^0 of D is said to be *φ-stable* if $\varphi(D^0) \subset D^0$ and $\mathcal{O}_K \cdot \varphi(D^0) = D^0$. The next lemma is easy to see.

LEMMA (3.5). *Let D^0 be an $\mathcal{O}_K$-lattice of D.*

(i) The $\mathcal{O}_K$-lattice D^0 is φ-stable if and only if φ is given by a matrix in $\mathrm{GL}_n(\mathcal{O}_K)$ with respect to an $\mathcal{O}_K$-base of D^0.

(ii) If D^0 is φ-stable, we have

$$D^0 = \{x \in D;\ \text{the set } \{\varphi^j(x);\ j \geq 0\} \text{ is bounded }\}.$$

In particular, if a φ-module D has a φ-stable $\mathcal{O}_K$-lattice, then it is unique. □

The existence of a φ-stable $\mathcal{O}_K$-lattice means that $V(D)$ is "finite étale" over $\mathcal{O}_K$;

LEMMA (3.6). *Let (D,φ) be a φ-module over K.*

(i) The following conditions are equivalent:

(1) There exists a φ-stable $\mathcal{O}_K$-lattice D^0 in D.

(2) The representation of G_K on $V(D)$ is unramified.

(ii) If G_K acts on $V(D)$ trivially, then the φ-stable $\mathcal{O}_K$-lattice is the $\mathcal{O}_K$-submodule of D spanned by $V(D)$.

(iii) There exists a finite separable extension L/K such that D_L has a φ-stable $\mathcal{O}_L$-lattice.

PROOF:— Since $\mathrm{GL}_{\mathbb{F}_q}(V(D))$ is finite, Part (iii) follows immediately from Part (i).

To show (i), it is enough to assume that K has a separably closed residue field k and to show the equivalence of the statement (1) with

(2)′ The representation of G_K on $V(D)$ is trivial.

Suppose D^0 is a φ-stable $\mathcal{O}_K$-lattice in D. Let t be a uniformizer of K. Then $\overline{D^0} := D^0/tD^0$ is a φ-module over k of the same rank n as D. By a theorem of Lang (which says the exactness of the sequence $1 \to \mathrm{GL}_n(\mathbb{F}_q) \to \mathrm{GL}_n \to \mathrm{GL}_n \to 1$ in the étale topology, where the third arrow is the map: $(a_{ij}) \mapsto (a_{ij}^q)(a_{ij})^{-1}$), there exists a k-base $(\overline{x}_0, \cdots, \overline{x}_{n-1})$, of $\overline{D^0}$ such that $\varphi(\overline{x}_i) = \overline{x}_i$. Choose a lifting $x_i \in D^0$ of $\overline{x}_i$ for each i. Then the limit $\varphi^\infty(x_i) = \lim_{j\to\infty} \varphi^j(x_i)$ exists in D^0. Since $\varphi(\varphi^\infty(x_i)) = \varphi^\infty(x_i)$, we have $\varphi^\infty(x)$ in $V(D)$. Since $\varphi^\infty(x_i)$ (mod. tD^0) $= \overline{x}_i$, Nakayama's lemma assures that $(\varphi^\infty(x_0), \cdots, \varphi^\infty(x_{n-1}))$ is an $\mathcal{O}_K$-base of D^0, and *a fortiori* an $\mathbb{F}_q$-base of $V(D)$. Thus $V(D) \subset D$, and G_K acts trivially on $V(D)$.

Assume now conversely that G_K acts on $V(D)$ trivially. Then (without any assumption on k) we have $V(D) \subset D$. The $\mathcal{O}_K$-submodule of D spanned by $V(D)$ is an $\mathcal{O}_K$-lattice (Lemma (3.2) assures that $K \cdot V(D) = D$), and is φ-stable; whence (1), and also (ii). Q.E.D.

DEFINITION (3.7). A φ-module (D,φ) over K is said to have *regular singularity* (at v) if it is the direct sum of φ-submodules (D_i,φ_i) each of which has a cyclic vector x_i such that the associated polynomial P_{x_i} is regular in the sense of (1.1).

When the residue field k of K is separably closed, the D_i in the above definition can be taken to be irreducible if once (D,φ) has regular singularity, as the proof of the following theorem shows.

THEOREM (3.8). *Assume the residue field k of K is separably closed. Let (D,φ) be a φ-module over K. Then the following conditions are equivalent:*

(1) The φ-module (D,φ) is regular.

(2) There exists a finite tamely ramified extension L/K such that D_L has a φ-stable $\mathcal{O}_L$-lattice D_L^0.

(3) The Galois representation $V(D)$ is tamely ramified.

PROOF:— The equivalence of (2) and (3) follows from Lemma (3.6), (i). The implication (1) $\Rightarrow$ (3) follows from Proposition (1.2) and Lemma (3.4), but here we proceed another way.

(1) $\Rightarrow$ (2): It is enough to show (2) for each D_i, so we assume x is a cyclic vector of D such that the polynomial P_x is regular;

$$P_x(X) = a_0X + a_1X^q + \cdots + a_{n-1}X^{q^{n-1}} + X^{q^n}, \qquad a_i \in K,\ a_0 \neq 0,$$

with

$$v(a_i) \geq \frac{q^n - q^i}{q^n - 1}v(a_0) \qquad \text{for } 1 \leq i \leq n-1. \tag{3.8.1}$$

Take an element α of K^{sep} such that

$$\alpha^{q^n-1} = a_0^{-1}, \tag{3.8.2}$$

and put $L := K(\alpha)$. The extension L/K is then tamely ramified. The vector αx is a cyclic vector of D_L, and we have

$$a_0\alpha^{q^n-1}(\alpha x) + a_1\alpha^{q^n-q}\varphi(\alpha x) + \cdots + a_{n-1}\alpha^{q^n-q^{n-1}}\varphi^{n-1}(\alpha x) + \varphi^n(\alpha x) = 0.$$

By (3.8.1) and (3.8.2), we see

$$a_0\alpha^{q^n-1} = 1, \quad \text{and} \quad a_i\alpha^{q^n-q^i} \in \mathcal{O}_L \quad \text{for } 1 \leq i \leq n-1.$$

According to Lemma (3.5), (i), this shows that the $\mathcal{O}_L$-lattice D_L^0 spanned by $(\alpha x, \varphi(\alpha x), \cdots, \varphi^{n-1}(\alpha x))$ is φ-stable.

(3) $\Rightarrow$ (1): Let L be the subfield of K^{sep} which corresponds to the kernel of the action of G_K on $V(D)$. By assumption, $\mathrm{Gal}(L/K)$ is a cyclic group of degree prime to q, so the representation

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_{\overline{\mathbb{F}}_q}(V(D))$$

is semi-simple, and factors through a Cartan subgroup of $\mathrm{GL}_{\overline{\mathbb{F}}_q}(V(D))$. We may assume that ρ is irreducible. Then D is also irreducible as a φ-module by Lemma (3.2). If ρ is trivial, there is nothing to prove. So we come to assume that ρ factors through the non-split Cartan subgroup $H \simeq \mathbb{F}_{q^n}^{\times}$, and does not factor through any subgroup isomorphic to $\mathbb{F}_{q^m}^{\times}$ with $m|n$ and $m < n$. Here we note:

LEMMA (3.8.3). *(i) Let $V := \mathbb{F}_q^{\oplus n}$ be the column vectors of dimension n, and let H be the non-split Cartan subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ acting on V. Then there exists a vector $x \in \mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} V$ and a character (isomorphism) $\chi : H \to \mathbb{F}_{q^n}^\times$ such that*

$$\sigma.x \;=\; \chi(\sigma)x \qquad \text{for all } \sigma \in H.$$

If we regard V as a trivial φ-module and $\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} V$ its base extension, then all such pairs (x, χ) are of the form

$$(c\varphi^j(x), \chi^{q^j}) \qquad \text{with } c \in \mathbb{F}_{q^n}^\times \text{ and } 0 \le j \le n-1.$$

Since $\chi^{q^j}(\sigma)$, $0 \le j \le n-1$, are different from each other if σ is a generator of H, the corresponding eigen vectors $x, \varphi(x), \cdots, \varphi^{n-1}(x)$ are linearly independent over $\mathbb{F}_{q^n}$ (i.e., x is a cyclic vector). In particular, all entries of x are non-zero.

(ii) In the polynomial ring $\mathbb{F}_q[X_0, \cdots X_{n-1}]$, one has the identity (Moore's determinant):

$$\det(X_i^{q^j})_{0 \le i,j \le n-1} \;=\; \prod_{m=0}^{n-1} \prod_{(a_i) \in \mathbb{F}_q^{\oplus m}} (X_m + \sum_{i=0}^{m-1} a_i X_i).$$

In particular, if $x = {}^t(x_0, \cdots, x_{n-1}) \in \mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} V$ is a cyclic vector as in (i), then $x_m + \sum_{i=0}^{m-1} a_i x_i$ is non-zero for all $m = 0, \cdots, n-1$ and $(a_0, \cdots, a_{m-1}) \in \mathbb{F}_q^{\oplus m}$, so the n elements $x_0, \cdots, x_{n-1} \in \mathbb{F}_{q^n}$ are linearly independent over $\mathbb{F}_q$. □

By (i) above, there exists a cyclic vector $x \in \mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} V(D)$ and a character $\chi : \mathrm{Gal}(L/K) \to \mathbb{F}_{q^n}^\times$ such that

$$\rho(\sigma)(\varphi^j(x)) \;=\; \chi(\sigma)^{q^j} \varphi^j(x) \qquad \text{for all } \sigma \in \mathrm{Gal}(L/K) \text{ and } 0 \le j \le n-1.$$

Since L/K is tamely ramified and the residue field k is separably closed, there exists an element α of L such that

$$\begin{cases} L = K(\alpha), & v(\alpha) > 0, \\ \sigma(\alpha) \;=\; \chi(\sigma)^{-1}\alpha & \text{for all } \sigma \in \mathrm{Gal}(L/K). \end{cases}$$

Then for any $b_j \in k$, $0 \le j \le n-1$, the vector

$$y := b_0 \alpha x + b_1 \alpha^q \varphi(x) + \cdots + b_{n-1} \alpha^{q^{n-1}} \varphi^{n-1}(x)$$

is in D because it is fixed by G_K. We shall show that, if b_j's are sufficiently general, then y is a cyclic vector of D and the associated polynomial P_y is regular.

If x is expressed by a column vector ${}^t(x_0, \cdots, x_{n-1})$, $x_i \in \mathbb{F}_{q^n}$, with respect to a $\mathbb{F}_q$-base of $V(D)$, then we have $y = {}^t(y_0, \cdots, y_{n-1})$ with

$$y_i \;=\; b_0(\alpha x_i) + b_1(\alpha x_i)^q + \cdots + b_{n-1}(\alpha x_i)^{q^{n-1}}.$$

By Moore's determinant identity ((3.8.3), (ii)), we have

$$\det(y, \varphi(y), \cdots, \varphi^{n-1}(y)) = \prod_{m=0}^{n-1} \prod_{(a_i) \in \mathbb{F}_q^{\oplus m}} (\sum_{j=0}^{n-1} b_j \alpha^{q^j} (x_m + \sum_{i=0}^{m-1} a_i x_i)^{q^j}).$$

Since $x_m + \sum_{i=0}^{m-1} a_i x_i \neq 0$ for all m and a_i ((3.8.3), (ii)), this determinant does not vanish (i.e., y is a cyclic vector of D) for general b_i's. By Lemma (3.4), the n elements $y_0, \cdots, y_{n-1}$ of L form an $\mathbb{F}_q$-base of the space $\hat{V}_y(D)$ of all roots of $P_y(X)$. Since

$$\begin{cases} y_i = (b_0 x_i)\alpha + (b_1 x_i^q)\alpha^q + \cdots + (b_{n-1} x_i^{q^{n-1}})\alpha^{q^{n-1}}, \\ b_j \in k, \qquad x_i \in \mathbb{F}_{q^n}, \qquad v(\alpha) > 0, \end{cases}$$

and $x_0, \cdots, x_{n-1}$ are linearly independent over $\mathbb{F}_q$ ((3.8.3), (ii)), all roots of $P_y(X)$ have the same valuation $v(\alpha)$. Thus the Newton polygon of $P_y(X)$ is straight, i.e., $P_y(X)$ is regular. Q.E.D.

Now we turn our attention to the connection associated with a φ-module D. Recall (e.g. [4], A.2.2) that there exists on D a unique connection $\nabla : D \to D \otimes_K \Omega^1_{K/k}$ for which $\varphi : D \to D$ is horizontal; $\nabla \circ \varphi = (\varphi \otimes \mathrm{id}) \circ \nabla$. If the Galois representation $V(D)$ is trivial, then $D^{\nabla} (:= \mathrm{Ker}(\nabla)) = k \otimes_{\mathbb{F}_q} V(D)$. So if $x \in D$ is expressed by a column vector ${}^t(x_0, \cdots, x_{n-1})$, $x_j \in K$, with respect to an $\mathbb{F}_q$-base of $V(D)$, then we have

$$\nabla(x) = {}^t(dx_0, \cdots, dx_{n-1}).$$

The connection may also be regarded as a K-linear map

$$\nabla : \mathrm{Der}_k(K) \to \mathrm{End}_k(D)$$

such that, for all $\partial \in \mathrm{Der}_k(K) \simeq \mathrm{Hom}_K(\Omega^1_{K/k}, K)$, one has $\nabla(\partial) = (1 \otimes \partial) \circ \nabla$.

Let $\| \cdot \|$ be the norm on $D_{K^{\mathrm{sep}}}$ for which the unit ball is the φ-stable $\mathcal{O}_{K^{\mathrm{sep}}}$-lattice $D^0_{K^{\mathrm{sep}}} = \mathcal{O}_{K^{\mathrm{sep}}} \cdot V(D)$.

THEOREM (3.9). *Assume the residue field k of K is separably closed. Let t be a uniformizer of K. Then the following conditions are equivalent:*

(1) The φ-module D has regular singularity;

(2) For any $x \in D$, we have $\|\nabla(t\frac{d}{dt})(x)\| \leq \|x\|$.

The condition (2) may be rephrased that the *norm* of ∇, $\|\nabla\| := \sup_{x \in D-0} \|\nabla(t\frac{d}{dt})(x)\|/\|x\|$, equals 1 (We have always $\|\nabla\| \geq 1$). Also, it may be rephrased that there exists in D a $\nabla(t\frac{d}{dt})$-stable $\mathcal{O}_K$-lattice which is a "proper ball" with respect to the norm $\| \cdot \|$.

PROOF:— Noting Theorem (3.8), we prove the equivalence of the tameness of $V(D)$ and the condition (2). Let L be the subfield of K^{sep} which corresponds to the kernel of the action of G_K on $V(D)$.

Assume L/K is tamely ramified of degree e. Then it is of the form $L = K(s)$, with $s^e = t$. On D_L, which contains $V(D)$, the effect of $\nabla(t\frac{d}{dt})$ is described simply by the formula

$$\nabla\left(t\frac{d}{dt}\right)(x_j)_{0\le j\le n-1} = \left(t\frac{dx_j}{dt}\right)_{0\le j\le n-1} = \left(\frac{1}{e}s\frac{dx_j}{ds}\right)_{0\le j\le n-1}, \qquad x_j \in L,$$

in terms of the coordinates with respect to an $\mathbb{F}_q$-base of $V(D)$. Since $|s\frac{dx_j}{ds}| \le |x_j|$, (2) follows. Note that this argument shows the inequality of (2) holds for all $x \in K^{\mathrm{tame}} \otimes_{\mathbb{F}_q} V(D)$, where K^{tame}/K is the maximum tamely ramified subextension of K^{sep}/K.

Assume L/K is wildly ramified. Let p be the characteristic of $\mathbb{F}_q$. Replacing K by a tamely ramified extension, we may assume $\mathrm{Gal}(L/K)$ is a p-group. Replacing D and $V(D)$ by subquotients, we may assume that the action of G_K on $V(D)$ is non-trivial and is of the form $\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$, $* \in \mathbb{F}_q$. Fix an $\mathbb{F}_q$-base of $V(D)$ with respect to which the G_K-action looks like this. Let σ be an element of $\mathrm{Gal}(L/K)$ whose action on $V(D)$ is given by a matrix $\begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix}$ with λ non-zero and in the prime field $\mathbb{F}_p$. Let L_1/K be a subextension of L/K such that $\mathrm{Gal}(L_1/K)$ is generated by the image of σ. Then a vector $x = {}^t(x_0, x_1) \in D_{L_1}$ belongs to D if and only if

$$\sigma(x_0) = x_0 - \lambda x_1 \quad \text{and} \quad x_1 \in K.$$

In particular, there exists a vector $x = {}^t(u, 1)$ in D such that u is a root of an Artin-Schreier equation $u^p - u = t^{-e}$, $e \ge 1$, $p \nmid e$. We have $t\frac{du}{dt} = et^{-e}$. Since $|t^{-e}| = q^e > q^{e/p} = |u|$, it follows that $\|\nabla(t\frac{d}{dt})(x)\| > \|x\|$. Q.E.D.

References

[1] P. Deligne, Equations différentielles à points singuliers réguliers, LNM 163, Springer, Berlin-Heidelberg-New York, 1970

[2] V. G. Drinfeld, Elliptic modules, Math. USSR Sb. 23 (1974), 561–592

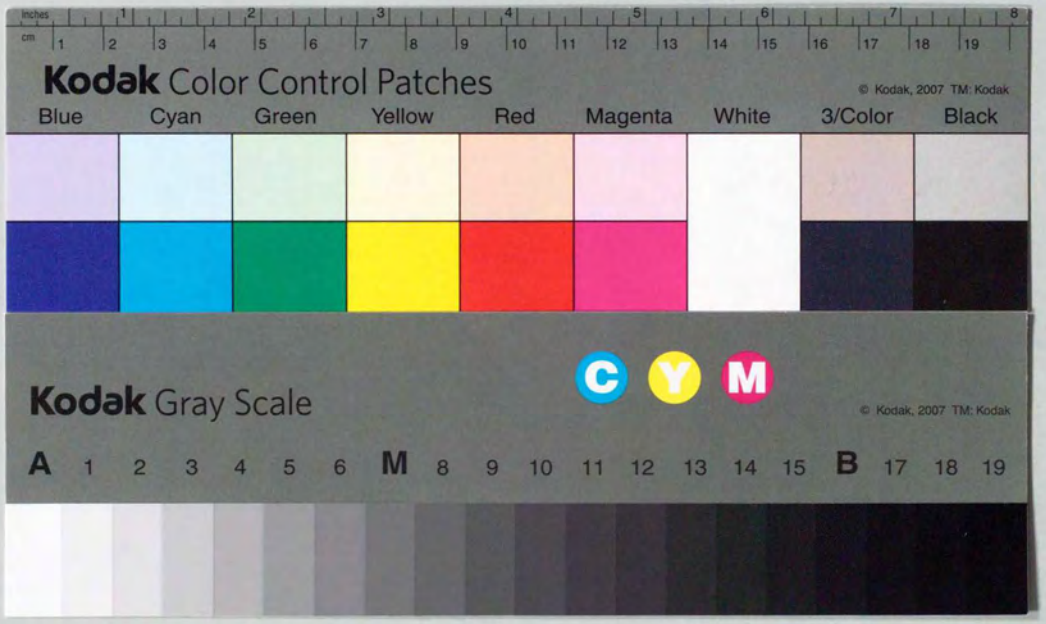
[3] V. G. Drinfeld, Moduli varieties of F-sheaves, Functsional'nyi Analiz i Ego Prirozheniya 21 (1987), 23–41

[4] J-M. Fontaine, Représentations p-adiques des corps locaux, in: The Grothendieck Festschrift II, Birkhäuser, Boston-Basel-Berlin, 1990, pp. 249–309

[5] N. Katz, Nilpotent connections and the monodromy theorem: applications of a result of Turrittin, Publ. Math. IHES 39 (1970), 175–232

[6] Ju. I. Manin, Moduli Fuchsiani, Annali Scuola Normale Sup. di Pisa, Ser. III 19 (1965), 113–126

[7] J-P. Wintenberger, Un scindage de la filtration de Hodge pour certaines variétés algébriques sur corps locaux, Annals of Math. 119 (1984), 511–548


Inches
cm
Kodak Color Control Patches
© Kodak, 2007 TM: Kodak
Blue
Cyan
Green
Yellow
Red
Magenta
White
3/Color
Black
Kodak Gray Scale
C
Y
M
© Kodak, 2007 TM: Kodak
A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19