数理解析研究所講究録
第 759 巻 1991 年 46-57

Galois representations attached to Drinfeld modules

都立大理　田口 雄一郎　(Yuichiro Taguchi)

In the talk, I announced some results on Galois representations attached to Drinfeld modules (see §1 below) and sketched the proof of the finiteness theorem (1.2). In this note, I will show how a theorem of Fontaine (Théorème 1 of [4]) can be modified (§3) so as to work in the course of the proof of Theorem (1.3).

1. Results and proofs

In this section, let K be an algebraic function field in one variable over a finite field. Fix once for all a place ∞ of K, and let A be the ring of elements of K which are regular outside ∞.

Let F be a field of finite type over A, *i.e.*, a field F which is endowed with a ring homomorphism $\gamma : A \longrightarrow F$ and is finitely generated over $\mathrm{Im}(\gamma)$ as a field. We say that the "characteristic" of F is *infinite* if γ is injective and *finite* if $\mathrm{Ker}(\gamma)$ is a non-zero prime ideal $\mathfrak{p}$ of A, and write "char"$(F) = \infty$ or $\mathfrak{p}$ accordingly.

Given a Drinfeld module ϕ over F of rank r, one can attach the v-adic *Tate module* $T_v(\phi)$ for any non-zero prime ideal $v \neq$ "char"(F). This is a free A_v-module (A_v is the v-adic completion of A) of rank r on which the absolute Galois group $\mathrm{Gal}(F^{sep}/F)$ acts continuously. For fundamentals of Drinfeld modules, see [1] and [2]. (See also [5] in this volume.)

Denote by K_v the fraction field of A_v. Our main result is:

THEOREM (1.1) ([6], [7]). *Assume F is a finite extension of K or "char"(F) is finite. Let ϕ be a Drinfeld module over F. Then for any non-zero prime ideal v of A different from "char"(F), $T_v(\phi) \otimes_{A_v} K_v$ is a semi-simple $K_v[\mathrm{Gal}(F^{sep}/F)]$-module.*

This follows ([6], Appendix) from

THEOREM (1.2) ([6], [7]). *Let F, ϕ and v be as in (1.1). For any $\mathrm{Gal}(F^{sep}/F)$-stable A_v-direct summand of $T_v(\phi)$, to which corresponds a sequence $\phi \to \phi_1 \to \phi_2 \to \cdots$ of isogenies of Drinfeld modules over F, there are only finitely many isomorphism classes of Drinfeld modules in $\{ \phi_n \,;\, n \geq 1 \}$.*

Remark. The assumption that the extension F/K is finite (when "char"$(F) = \infty$) should be removed, but I have not yet checked it.

The proof of (1.2) goes in a similar way as in Zarhin [8] and Faltings [3], and uses the theory of *modular heights*. In the infinite "characteristic" case, the Arakelov theoretic arguments and the study of π-divisible groups are needed. For details, see [6] and [7].

Now we restrict ourselves to the case where F is a finite extension of K. Then for a Drinfeld module ϕ over F, we can define the "discriminant" $\Delta(\phi)$ of ϕ ([7], §6), which is an ideal of the integral closure R of A in F.

THEOREM (1.3) ([7], §6). *Let $\mathfrak{n}$ be a non-zero ideal of R and v a non-zero prime ideal of A. Then there are only finitely many isomorphism classes of Galois representations $T_v(\phi) \otimes_{A_v} K_v$ arising from Drinfeld modules ϕ over F with $\Delta(\phi)|\mathfrak{n}$.*

In the case of abelian varieties, the corresponding theorem ([3], Satz 5) holds under a weaker restriction (*i.e.* "Supp($\Delta(\phi)$) $\subset$ Supp($\mathfrak{n}$)" replacing "$\Delta(\phi)|\mathfrak{n}$"). But it is unlikely that we can weaken the restriction in our case because of the lack of the Hermite-Minkovski theorem for function fields. So the proof of our theorem requires an estimate of the differents of field extensions arising from division points of Drinfeld modules:

PROPOSITION (1.4) ([7], §6). *Let ϕ be a Drinfeld module over F of rank r, and let $a \in A - 0$. Then we have the following inequality of divisors (denoted additively) of F:*

$$\mathfrak{D}(F(\phi;a)/F) \leq r\left[(a) + \delta(r,a)q^{r\deg(a)-2}\Delta(\phi) + (q^r - 2)\cdot\infty\right],$$

where $F(\phi;a)$ is the field of a-division points of ϕ/F, $\mathfrak{D}(/)$ the different, q the cardinality of the constant field of K, $\deg(a) := \log_q \#(A/aA)$, and $\delta(r,a) := (q^{r\deg(a)} - 1)/(q-1)$.

The estimate of the different is performed separatedly at each infinite or finite place of F. In the case of infinite places, a "successive minimum base" of an A-lattice is used ([7], (6.6)). The case of finite places is easy ([7], (6.4) and (6.5)), but it would be interesting to give a general statement (Theorem (3.4) below), which can be regarded as a higher dimensional generalization of (6.4) of [7].

2. The Taylor expansion

This section is a preliminary for §3.

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 (2.1). (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 (2.2). *For $f(X) \in R[[X]]$, we have the formal Taylor expansion (or rather, the binomial expansion)*

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

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

$$f(x+y) = \sum_{|n|\geq 0} \frac{\delta^n}{\delta X^n} f(x) \cdot y^n \quad \text{in } S. \tag{2.2.2}$$

Proof. Write $f(X+Y) = \sum a_n(X) Y^n$ with $a_n(X) \in R[[X]]$. Applying $\frac{\delta^n}{\delta X^n}$ to both sides and reducing modulo Y, we obtain (*cf.* Remark (2.1), (3))

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

and hence (2.2.1).

The latter half of the Proposition is obvious.

3. Estimate of differents

First we recall Fontaine's numbering of the ramification groups of a local field and some of his results ([4], §1). Throughout 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 lower (resp. upper) filtration $G_{(i)}$ (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 [*Corps locaux*] 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 (3.1). *Let L be a finite Galois extension of K.*
(1) ([4], 1.3) Let $\mathfrak{D}_{L/K}$ be the different of the extension L/K. We have

$$v_K(\mathfrak{D}_{L/K}) = u_{L/K} - i_{L/K}.$$

(2) ([4], 1.5) For a real number $m \geq 0$, consider the following property (P_m) on the extension L/K:

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

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 $m > u_{L/K} - e^{-1}_{L/K}$.

Now we shall refine Fontaine's Proposition 1.7 of [4] as follows. The main point is that it works, *mutatis mutandis*, even in positive characteristics.

PROPOSITION (3.2). *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 $u(\text{mod}.I)$ 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

$$\mathit{Hom}_{\mathfrak{O}_K-\mathrm{alg}}(B, S) \longrightarrow \mathit{Hom}_{\mathfrak{O}_K-\mathrm{alg}}(B, S/I)$$

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 $u \in \mathrm{Hom}_{K-\mathrm{alg}}(B_K, K^{sep})$. 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 we reproduce his proof here for the covenience of the reader.

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

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

i.e., $a 1_h = (q_{li})(a p_{ij})$. (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 [4], 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

$$P_i(u_1+\mu_1, \cdots, u_h+\mu_h) \in aI_2 \quad (1 \leq i \leq h). \tag{3.2.1}$$

If $\mu_j \in I$, we have the Taylor expansion (2.2.2)

$$P_i(u_1+\mu_1, \cdots, u_h+\mu_h) = a\lambda_i + \sum_j \frac{\delta P_i}{\delta X_j}(u_1, \cdots, u_h)\mu_j + R_i \tag{3.2.2}$$

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

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 (2.1), (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 (2.1), (5)). Thus we have

$$R_i \in aI_2. \tag{3.2.3}$$

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

$$\frac{\delta P_i}{\delta X_j}(u_1, \cdots u_h) \cdot \mu_j \equiv aP_{ij}(u_1, \cdots, u_h) \cdot \mu_j \pmod{aI_2}. \tag{3.2.4}$$

Putting (3.2.3) and (3.2.4) into (3.2.2), 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 (3.2.1) 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 (3.2.1) is clear. Moreover $u_j (\mathrm{mod}.I)$, $1 \leq j \leq h$, determine

$\mu_j(\text{mod}.I_2)$, $1 \leq j \leq h$, uniquely, because they determine $\lambda_i \equiv 0$ (mod.I) and $P_{ij}(u_1, \cdots, u_h)$ (mod.I) uniquely and $I^2 \subset I_2$.

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

Proof of (ii): Since B_K is finite over K and $\Omega^1_{B_K/K} = K \otimes_{\mathfrak{O}_K} \Omega^1_{B/\mathfrak{O}_K} = 0$, B_K is étale over K. So we can write $B_K = \prod_{s=1}^t L_s$, where L_s are finte separable extensions of K assumed to be contained in K^{sep}, a fixed separable closure of K. Then L is the composition of the Galois closures in K^{sep} of $L_s/K, s = 1, \cdots, t$. Hence L/K is a Galois extension.

If a is a unit, then $\Omega^1_{B/\mathfrak{O}_K} = 0$, B is étale over $\mathfrak{O}_K$, L/K is unramified, and $u_{L/K} = 0$.

Suppose $a \in \mathfrak{m}_K$. We will show that L/K has the property (P_m) for any $m > v_K(a) + \varepsilon$ with $\varepsilon := \frac{1}{p-1} \cdot \min\{v_K(a), v_K(p)\}$.

Writing $J(E) := \text{Hom}_{\mathfrak{O}_K-\text{alg}}(B, \mathfrak{O}_E)$ for a finite extension E of K, we see that

$$\begin{aligned} J(E) &= \text{Hom}_{K-\text{alg}}(B_K, E) \\ &= \amalg_{s=1}^t \{K - \text{embeddings} : L_s \hookrightarrow E\}. \end{aligned}$$

Here we have $\#\{$ K-embeddings : $L_s \hookrightarrow E\} \leq [L_s : K]$ and the equality holds if and only if E contains a subfield which is K-isomorphic to the Galois closure of L_s/K in K^{sep}. Hence we have

$$\#J(E) \leq \#J(L)$$

and the equality holds if and only if there exists a K-embedding : $L \hookrightarrow E$. So it suffices to show :

If there exists an $\mathfrak{O}_K$-algebra homomorphism

$$\eta : \mathfrak{O}_L \longrightarrow \mathfrak{O}_E/\mathfrak{a}^m_{E/K} \quad \text{with} \quad m > v_K(a) + \varepsilon,$$

then we have $\#J(E) \leq \#J(L)$.

Noticing that $\mathfrak{a}^m_{E/K}$ is of the form aI with an ideal I of $\mathfrak{O}_E$ which satisfies the assumption of Part (i), we can define, by (a) of (i), a map

$$J(L) \longrightarrow J(E) \quad ; \quad u \longmapsto u^\eta,$$

where u^η is the unique element of $J(E)$ which makes the following diagram commutative:

$$\begin{array}{ccc} B & \xrightarrow{\eta \circ u} & \mathfrak{O}_E/aI \\ {\scriptstyle u^\eta}\downarrow & & \downarrow \\ \mathfrak{O}_E & \longrightarrow & \mathfrak{O}_E/I. \end{array}$$

It suffices now to show that this map is injective.

To see what the kernel I' of the composition

$$\mathfrak{O}_L \xrightarrow{\eta} \mathfrak{O}_E/aI \xrightarrow{\text{canon.}} \mathfrak{O}_E/I$$

is, let K' be the maximum unramified extension of K contained in L. Then there exists a unique K-embedding : $K' \hookrightarrow E$ for which η is an $\mathfrak{O}_K$-algebra homomorphism, because $\mathfrak{O}_{K'}$ is formally étale over $\mathfrak{O}_K$. Let α be a prime element of $\mathfrak{O}_L$ and let P be the monic minimal polynomial of α over $\mathfrak{O}_{K'}$. Since L/K' is totally ramified, P is an Eisenstein polynomial;

$$P(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n,$$

with $a_i \in \mathfrak{O}_{K'}$, $v_K(a_i) \geq 1$, $v_K(a_0) = 1$, and $n = e_{L/K} = [L : K']$. If β is an element of $\mathfrak{O}_E$ with $\beta(\text{mod}.aI) = \eta(\alpha)$, we must have $P(\beta) \in aI$. Comparing the valuations of $P(\beta)$ and its terms, we see $v_K(\beta) = v_K(\alpha) = 1/n$. Thus the kernel I' is $\{x \in \mathfrak{O}_L; v_K(x) \geq m - v_K(a)\}$, which satisfies the assumption of Part (i).

If $u, v \in J(L)$ and $u^\eta = v^\eta$, we have $\eta \circ u \equiv \eta \circ v$ (mod.I) and $u \equiv v$ (mod.I'), from which we obtain $u = v$ by Part (b) of (i). Thus L/K has the property (P_m).

By Proposition (3.1),(2),(ii), we have $m > u_{L/K} - e_{L/K}^{-1}$ if $m > v_K(a) + \varepsilon$. Hence $u_{L/K} \leq v_K(a) + \varepsilon + e_{L/K}^{-1}$.

If $e_{L/K}$ is prime to p, L/K is tamely ramified and

$$u_{L/K} = 1 \leq v_K(a) + \varepsilon.$$

Suppose p divides $e_{L/K}$, and let $G := \text{Gal}(L/K)$. Then $e_{L/K}u_{L/K}$ is an integer divisible by p, because $u_{L/K} = \int_0^{i_{L/K}} (G_{(x)} : 1)dx$, $p|(G_{(x)} : 1)$ if $x \leq i_{L/K}$, and $G_{(x)}$ may "jump" only at points $x \in e_{L/K}^{-1}\mathbb{Z}$. Hence the inequality

$$(p-1)e_{L/K}u_{L/K} \leq (p-1)e_{L/K}v_K(a) + e_{L/K}(p-1)\varepsilon + (p-1),$$

where the terms except $(p-1)$ are integers divisible by p, implies $u_{L/K} \leq v_K(a) + \varepsilon$.

Corollary (3.3). *Let the notation and hypothesis be as in Proposition (3.2), and let $\mathfrak{D}_{L/K}$ be the different of the extension L/K. 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 (Proposition (3.1),(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 (3.4). *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 $\mathfrak{O}_K$ ([7], §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 $G = Gal(K^{sep}/K)$ on $J(K^{sep})$, $L := (K^{sep})^H$, and $\mathfrak{D}_{L/K}$ the different of the extension L/K. Then we have $G^{(u)} \subset H$ for all $u > u_o$, and $v_K(\mathfrak{D}_{L/K}) < u_o$.*

Proof. Replacing K by its maximum unramified extension, we may suppose the residue field k of K is algebraically closed. Then the general theory of group schemes says that 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 Proposition (3.2) and Corollary (3.3) with $a = \pi^n$ and obtain the theorem.

Remark (3.5). 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

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

$$v_K(\mathfrak{D}_{L/K}) = [L:K]\left[\min\{m, v_F(q) + q^{1-m}\} - q^{n-m+1}/(q-1)\right].$$

References

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

[2] V.G. Drinfeld : Elliptic modules II, Math. USSR. Sb. 31(1977), 159 – 170

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

[4] J-M. Fontaine : Il n'y a pas de variété abélienne sur Z, Inv. Math. 81(1985), 515 – 538

[5] 浜畑 芳紀 : Drinfeld 加群 に同伴する Tate 加群 について, (this volume)

[6] Y. Taguchi : Semi-simplicity of the Galois representations attached to Drinfeld modules over fields of "finite characteristics", (to appear in Duke Math. J.)
[7] Y. Taguchi : Semi-simplicity of the Galois representations attached to Drinfeld modules over fields of "infinite characteristics", (preprint)
[8] Yu. Zarhin : Endomorphisms of abelian varieties over fields of finite characteristics, Math. USSR. Izv. 9(1975), 255 – 260

Tokyo Metropolitan University, Hachioji, Tokyo, 192-03 JAPAN