数理解析研究所講究録
942巻 1996年 14-28

Finite Group Schemes II

Yukiyoshi Nakkajima*

December 5, 1995

1 Introduction

The aim in this report is to explain [R], which is used in proofs in [M]. It is divided into two parts; One is the classification of vector space (over finite fields) schemes over certain bases (with a mild condition) and the application of it. The other is the determination of the Galois action on the determinant of the Tate module of a $p-$divisible group over a strictly henselian discrete valuation ring (e.g. complete discrete valuation ring with algebraically closed residue field) of mixed characteristics. The first result on the classification of finite commutative group schemes is obtained in [OT]. The classification of the commutative group schemes of prime orders is done there. [R] is a generalization of [OT]. The concept of the classification means to capture the finite group schemes over a base scheme by languages about the base. On the other hand Tate [T] showed that an open subgroup of the Galois group of the fraction field of a strictly henselian ring of mixed characteristics acts by some power of a cyclotomic character on the determinant of a $p-$divisible group over the ring. Raynaud proved that the whole Galois group acts in such a way. His proof is based on the deformations of a $p-$divisible groups. In this report I give an outline of a proof of this fact, following [F1]. The key point is that the Tate module of a $p-$divisible group over a discrete valuation ring of mixed characteristics is crystalline. It strengthens a result of the Hodge decomposition of it [T].

*Department of Mathematical Sciences of University of Tokyo, 3-8-1 Komaba Meguro-ku, Tokyo 153, Japan

Is not given classifications from the viewpoint of Cartier-Dieudonné in this report. See [F] for them.

For the reader. The prerequisite knowledge for reading this report is only that explained in [N] except [Sh] §4 Cor.3. (But a result on the calculation of a Galois cohomology [T] is implicitly used.) I use the words explained in [N] freely, without mentioning where they are stated in [N].

Acknowledgment. It is my pleasure to express my gratitude to Professors T. Sekiguchi and N. Suwa for giving me an opportunity for explaining a result of [R]. My thanks goes to A. Shiho for pointing out some mistakes and Y.Taguchi for informing me of the reference [B].

2 Before the explanation of [R]

Let G/S be a finite commutative group scheme of order $m = m_1 m_2$, where m_1 is prime to m_2. Then G has a decomposition $G = G[m_1] \underset{S}{\times} G[m_2]$, where $G[m_i] := \mathrm{Ker}(m_i : G \longrightarrow G)$ is of order m_i for $i = 1, 2$. Hence, if one wants to classify finite commutative group schemes, one has only to do the group schemes of primary order. In [R] they are not completely classified, but vector space (over finite fields) schemes over certain bases are and when the base scheme is the fraction field of a strictly henselian discrete valuation ring, they have a series of Jordan-Hölder whose each quotient is such a scheme stated above.
The classification may seem somewhat complicated, so we take a group scheme of order 2 which is a typical and an educational example. For simplicity, the base scheme is the spectrum of a ring A (commutative, with unit element). Let G be a finite commutative group scheme of order 2. Then G is the spectrum of a ring B, and the augmentation ideal $I = \mathrm{Ker}(B \xrightarrow{\varepsilon} A)$ is a locally free module of rank 1. Here ε is the counit of G. For simplicity, we assume I is a free A-module. Let x be a basis of I. Since I is an ideal, there exists a unique element $a \in A$ such that $x^2 = ax$. Next we consider the element $\Delta(x) \in B \underset{A}{\otimes} B$. A priori, $\Delta(x)$ is written as follows:

$$\Delta(x) = \alpha(x \otimes 1) + \beta(1 \otimes x) + \gamma(x \otimes x) \quad (\alpha, \beta, \gamma \in A).$$

Using the axioms of the structures of the Hopf algebra, we can see

$$\Delta(x) = x \otimes 1 + 1 \otimes x - b(x \otimes x)$$

such that $ab = 2$. Hence we have a map

$$\begin{gathered}\{\text{finite group schemes of order 2 whose} \\ \text{structure sheaves are free } A\text{-modules}\}/\simeq \\ \downarrow \\ \{(a,b) \in A \times A \mid ab = 2\}/\sim .\end{gathered}$$

Here $\sim$ is the following equivalence relation:

$$(a,b) \sim (a',b') \Leftrightarrow \exists u \in A^*,\ a' = au,\ b' = bu^{-1}.$$

The map above is a bijection. In fact we can construct the inverse of it:

$$\begin{array}{lll}(a,b) & \longmapsto & G = \operatorname{Spec} A[X]/(X^2 - aX) \\ & & \Delta(X) = X \otimes 1 + 1 \otimes X - b(X \otimes X) \\ & & \varepsilon(X) = 0 \\ & & A(X) = X\end{array}$$

Here A denotes an antipode. Note that X is a basis of the augmentation ideal. This example teaches us that it is important to look carefully at the augmentation ideal of a finite commutative group scheme.

3 Classification of $\mathbb{F}_q$-vector space schemes

Let p be a prime number and $q = p^f$ be a power of p. Let G/S be a finite commutative group scheme.

Definition 3.1. *G is called $\mathbb{F}_q$-vector space scheme if $G(T)$ is a vector space over $\mathbb{F}_q$ functorially for $T \in (\mathrm{Sch}/S)$.*

We have wanted to classify the finite commutative group schemes of primary order. But this has not yet been solved over a general base. (A different type of classifications from Oort-Tate-Raynaud's can be made when a base scheme is a perfect field of positive characteristic or a complete discrete valuation ring of mixed characteristics with small absolute ramification index ([F], [FL]).) Why we consider $\mathbb{F}_q$-vector space schemes? Because the following holds:

Propositon 3.2 ([R] Prop. (3.2.1)). *Let A be a strictly henselian discrete valuation ring with residue field of characteristic p. Let G be a finite commutative group scheme over* $\operatorname{Frac} A$ *of p−primary order. If G or the Cartier dual G^D is etale, then G has a sequence of Jordan-Hölder whose each quotient is a $\mathbb{F}_{q_i}$-vector space scheme satisfying $(\star)$, where $(\star)$ is explained soon later.*

Note that a finite commutative group scheme over a scheme T is etale if the order is invertible in T ([Sh] §4 Cor.3), hence in particular G and the Cartier dual G^D is etale.

Remark 3.3.

If A is of mixed characteristics and the absolute ramification index is smaller than p, then a finite commutative group scheme over A has a Jordan-Hölder sequence over A ([R]).

The classification of the $\mathbb{F}_q$−vector space schemes have not been made yet for any base scheme. We must explain a base ring and Raynaud have made the classification over a scheme over it. Let μ_{q-1} is the group of the $(q-1)$−th root of 1 of an algebraic closure of $\mathbb{Q}$. Let $\wp$ be a fixed prime of $\mathbb{Z}[\mu_{q-1}]$ over p. By $\wp$ we can embed $\mathbb{Q}(\mu_{q-1})$ in $\overline{\mathbb{Q}}_p$. We put $\Lambda_q := \mathbb{Z}[\mu_{q-1}, \dfrac{1}{p(q-1)}] \cap \overline{\mathbb{Z}}_p$. The intersection is taken in $\overline{\mathbb{Q}}_p$. Λ_q is a Dedekind ring and the set of Λ_q is $\{\wp\} \cup \{$ primes of $\mathbb{Z}[\mu_{q-1}]$ which do not ramify in the extension of $\mathbb{Z}[\mu_{q-1}]/\mathbb{Z}$ and which do not lie over $p\}$. $\Lambda_q = \mathbb{Z}$ for $q = p = 2$, $\mathbb{Z}[\frac{1}{2}]$ for $q = p = 3$, $\mathbb{Z}[i, \dfrac{1}{2(2+1)}]$ for $q = p = 5$. Here i is a square root of -1 and we take $\wp = (2-i)$. $\Lambda_q = \mathbb{Z}[\omega, \frac{1}{3}]$ for $q = 2^2, p = 2$, where ω is a primitive cubic root of 1.
Henceforth the base scheme S is a scheme over Λ_q, e.g. $S = \operatorname{Spec} A$, where A is a local henselian ring whose residue field contains $\mathbb{F}_q$. Let G be a $\mathbb{F}_q$−vector space scheme of rank q and $\mathcal{I}$ be the augmentation ideal of G. We denote by H the set of the characters of $\mathbb{F}_q^*$: $H := \operatorname{Hom}_{\mathrm{gp}}(\mathbb{F}_q^*, \mu_{q-1})$. We put $e_\chi := \dfrac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^*} \chi^{-1}(\lambda)[\lambda]$, $\mathcal{I}_\chi := e_\chi(\mathcal{I})$, where $[\lambda]$ is the endomorphism of $\mathcal{I}$ induced by the action of $\lambda \in \mathbb{F}_q^*$ on G. Then $\mathcal{I}$ has a decomposition: $\mathcal{I} = \bigoplus_{\chi \in H} \mathcal{I}_\chi$. In general $\mathcal{I}_\chi$ is not non-zero. It does not seem beautiful. Hence we make the following assumption:

Assumption ($\star$). $\mathcal{I}_\chi$ is an invertible module for $\forall \chi \in H$. The conditions in the following assure ($\star$).

Propositon 3.4. *If either of the following condition holds, then* ($\star$) *is OK.*
1) ([OT] Lem.2) $q = p$.
2) S *is connected and there is a point* s *of* S *such that* G_s *or the Cartier dual* G_s^D *is etale.*

Next we define a fundamental character to decompose the augmentation ideal of a given $\mathbb{F}_q$−vector space scheme.

Definition 3.5. *Let* $\chi : \mathbb{F}_q^* \longrightarrow \mu_{q-1}$ *be a character.* χ *is called fundamental if* $\mathbb{F}_q \xrightarrow{\chi} \mathbb{Z}[\mu_{q-1}] \overset{\mathrm{mod}\, p}{\longrightarrow} \mathbb{F}_q$ *is additive, i.e. a morphism of fields. Here we define* $\chi(0) = 0$.

If χ is fundamental, the fundamental characters are $\{\chi^{p^h} \mid 0 \leq h \leq f-1\}$. Henceforth we fix a fundamental character and we use the following notations:

Notations.

$$\chi_0 := \chi,\ \chi_1 := \chi^p,\ \cdots,\ \chi_{i+1} := \chi_i^p,\ (i \in \mathbb{Z}/f),\ \cdots.$$

The fundamental characters form a "basis" over $\mathbb{F}_p$ of $\{\chi : \mathbb{F}_q^* \longrightarrow \mu_{q-1} :$ a character$\}$: For any nontrivial character χ, χ has the unique expression: $\chi = \prod_{i \in \mathbb{Z}/f} \chi_i^{n_i}$ $(0 \leq n_i \leq p-1)$. If χ is trivial, we can take $n_i = 0$ for all i or $n_i = p-1$ for all i. In this case we take the latter.
To make the classification we prepare some notations. The composite of the multiplication (resp. comultiplication) $m^{n-1} : \mathcal{O}_G^{\otimes n} \longrightarrow \mathcal{O}_G$ (resp. $\Delta^{n-1} : \mathcal{O}_G \longrightarrow \mathcal{O}_G^{\otimes n}$) induces the following

$$m_{\varphi_1,\cdots,\varphi_n} : \mathcal{I}_{\varphi_1} \otimes \cdots \otimes \mathcal{I}_{\varphi_n} \longrightarrow \mathcal{I}_{\varphi_1 \cdots \varphi_n}$$

(resp. $\Delta_{\varphi_1,\cdots,\varphi_n} : \mathcal{I}_{\varphi_1 \cdots \varphi_n} \longrightarrow \mathcal{I}_{\varphi_1} \otimes \cdots \otimes \mathcal{I}_{\varphi_n}$),

where φ_i is an element of H. We consider the composite of $\Delta_{\varphi_1,\cdots,\varphi_n}$ and $m_{\varphi_1,\cdots,\varphi_n}$: $\mathcal{I}_{\varphi_1 \cdots \varphi_n} \xrightarrow{\Delta_{\varphi_1,\cdots,\varphi_n}} \mathcal{I}_{\varphi_1} \otimes \cdots \otimes \mathcal{I}_{\varphi_n} \xrightarrow{m_{\varphi_1,\cdots,\varphi_n}} \mathcal{I}_{\varphi_1 \cdots \varphi_n}$. Since $\mathcal{I}_{\varphi_1 \cdots \varphi_n}$ is an invertible sheaf, the composite defines a global section $w_{\varphi_1,\cdots,\varphi_n} \in \Gamma(S, \mathcal{O}_S)$. It is amazing that $w_{\varphi_1,\cdots,\varphi_n}$ is independent of G:

Propositon 3.6. *1)* $w_{\varphi_1,\cdots,\varphi_n} = \dfrac{1}{q-1}\dfrac{g(\varphi_1^{-1},\psi)\cdots g(\varphi_1^{-1},\psi)}{g((\varphi_1\cdots\varphi_n)^{-1},\psi)} \in \Lambda_q$. *Here* $g(\varphi,\psi)$ *is the Gauss sum defined by*

$$g(\varphi,\psi) := \begin{cases} \sum_{\lambda\in\mathbb{F}_q} \varphi(\lambda)\psi(\lambda), & (\varphi \neq 1) \\ -q, & (\varphi = 1) \end{cases}$$

Here $\psi : (\mathbb{F}_q, +) \longrightarrow \mu_q$ *is a nontrivial character.*
2) $w_{\varphi_1^p,\cdots,\varphi_n^p} = w_{\varphi_1,\cdots,\varphi_n}$, *in particular* $w := w_{\underbrace{\chi_i,\cdots,\chi_i}_{p\text{ pieces}}}$ *is independent of* $1 \leq i \leq f$.
3) $w \equiv p! \bmod p^2$. *In particular* w *is divided exactly by* p.

At last we can state the classification of $\mathbb{F}_q-$vector space schemes over S satisfying $(\star)$.

Theorem 3.7. *There is a bijection between the following two sets:*

$$\{\,\mathbb{F}_q - \textit{vector space schemes over } S \textit{ satsisfying } (\star)\,\}/\simeq,$$

and

$$\{((\mathcal{L}_1,\cdots,\mathcal{L}_f);(a_1,\cdots,a_f);(b_1,\cdots,b_f))\,|\,\mathcal{L}_i : \textit{invertible module},$$
$$a_i \in \mathrm{Hom}(\mathcal{L}_i^{\otimes p},\mathcal{L}_{i+1}),\ b_i \in \mathrm{Hom}(\mathcal{L}_{i+1},\mathcal{L}_i^{\otimes p}),\ a_ib_i = w\,\}/\simeq .$$

The map is as follows:

$$G \longmapsto ((\mathcal{I}_1,\cdots,\mathcal{I}_f);(m_1,\cdots,m_f);(\Delta_1,\cdots,\Delta_f)),$$

where $m_i := m_{\chi_i,\cdots,\chi_i} : \mathcal{I}_{\chi_i}^{\otimes p} \longrightarrow \mathcal{I}_{\chi_{i+1}}$, $\Delta_i := \Delta_{\chi_i,\cdots,\chi_i} : \mathcal{I}_{\chi_{i+1}} \longrightarrow \mathcal{I}_{\chi_i}^{\otimes p}$. *The inverse of it is as follows:*

$$((\mathcal{L}_1,\cdots,\mathcal{L}_f);(a_1,\cdots,a_f);(b_1,\cdots,b_f)) \longmapsto {}_{\mathcal{L}_1,\cdots,\mathcal{L}_f}G_{a_1,\cdots,a_f}^{b_1,\cdots,b_f},$$

where

$${}_{\mathcal{L}_1,\cdots,\mathcal{L}_f}G_{a_1,\cdots,a_f}^{b_1,\cdots,b_f}(T) = \{(z_1,\cdots,z_f) \in \prod_{i=1}^{f}\Gamma(T,\mathcal{L}_i^{-1}\underset{\mathcal{O}_S}{\otimes}\mathcal{O}_T)\,|$$
$$z_i^{\otimes p} = a_i^*(z_{i+1}),\ 1 \leq i \leq f\}\ (T \in (\mathrm{Sch}/S))$$

and the unit element is $(0,\cdots,0)$, *the antipode* A *is given* $A(z_i) = z_i$ *for* $p = 2$, *and* $-z_i$ *for* $p \neq 2$, *and the group law is given in the* **Appendix** *below. Here* a_i^* *is the* $\mathcal{O}_S-$*dual of* a_i.

Remark 3.8.

1) To state the group law we must prepare some more notations. Strangely, the group law is not important and not used in the rest of the report. The author is very happy if someone explains the reason to him. On the other hand the equation of ${}_{\mathcal{L}_1,\cdots,\mathcal{L}_f}G^{b_1,\cdots,b_f}_{a_1,\cdots,a_f}$ is very important.
2) The Cartier dual of ${}_{\mathcal{L}_1,\cdots,\mathcal{L}_f}G^{b_1,\cdots,b_f}_{a_1,\cdots,a_f}$ is ${}_{\mathcal{L}_1^{-1},\cdots,\mathcal{L}_f^{-1}}G^{a_1,\cdots,a_f}_{b_1,\cdots,b_f}$.

Corollary 3.9. *If* $\operatorname{Pic} S = 0$*, there is a bijection between the following two sets:*

$$\{\,\mathbb{F}_q - \textit{vector space schemes over } S \textit{ satsisfying } (\star)\,\}/\simeq,$$

and

$$\{\,((a_1,\cdots,a_f);(b_1,\cdots,b_f)) \in \prod_{i=1}^{2f} \Gamma(S,\mathcal{O}_S)\,|a_ib_i = w\,\}/\sim,$$

where $\sim$ *is an equivalence relation defined as follows:*

$$(a'_1,\cdots,a'_f;b'_1,\cdots,b'_f) \sim (a_1,\cdots,a_f;b_1,\cdots,b_f)$$

$$\Longleftrightarrow \exists u_i \in \Gamma(S,\mathcal{O}_S)^*\; a'_i = u_i^p a_i u_{i+1}^{-1},\; b'_i = u_i^{-p} b_i u_{i+1}.$$

Corollary 3.10. *If* S *is the spectrum of the strictly henselian discrete valuation ring of mixed characteristic of 0 and p with normalized valuation* v *with* $v(p) = e$*, then there is a bijection between the following two sets:* $\{\,\mathbb{F}_q-$*vector space schemes over* S *satisfying* $(\star)\,\}/\simeq$*, and* $\{\,(n_1,\cdots,n_f) \in \mathbb{Z}^f\,|\,0 \le n_i \le e\,\}$*. The correspondence is given* $(a_1,\cdots,a_f;b_1,\cdots,b_f) \mapsto (v(a_1),\cdots,v(a_f))$ *in the notation of (3.9).*

Remark 3.11.

The inequality $v(a_i) \le e$ is caused by $a_ib_i = w$ and $v(w) = e$ by (3.6) 3).

Remark 3.12. If the base scheme is a perfect field of finite characteristic or complete discrete valuation ring of mixed characteristics with small absolute ramification index, (3.9) should be obtained by Dieudonné theory.

4 Extensions

In this section the base scheme S is Spec A, where A is a henselian discrete valuation ring of mixed characteristic 0 and p with normalized valuation v with $v(p) = e$. Let K be the fraction field of A. By (3.7) and the concept of scheme theoretic closures (which we omit to explain), we have the following:

Theorem 4.1. *1) Case 1: $e < p - 1$.*
a) Let G be a finite commutative group scheme of p-primary order. If G extends to such a scheme over A, i.e. there exists a flat finite commutative group scheme over A whose generic fiber is G, then any extension of G is isomorphic.
b) Let $\mathcal{G}$, $\mathcal{H}$ be finite commutative group schemes over A of p-primary order. Then the followings hold:

$$\mathrm{Hom}_{A-\mathbf{gp}}(\mathcal{G}, \mathcal{H}) = \mathrm{Hom}_{A-\mathbf{gp}}(\mathcal{G} \underset{A}{\otimes} K, \mathcal{H} \underset{A}{\otimes} K),$$

$$\mathrm{Ext}_A(\mathcal{G}, \mathcal{H}) \hookrightarrow \mathrm{Ext}_A(\mathcal{G} \underset{A}{\otimes} K, \mathcal{H} \underset{A}{\otimes} K).$$

2) Case 2: $e = p - 1$.
Let G/K be a $\mathbb{F}_q$-vector space scheme of order q. If G is simple, G extends to a unique group scheme over A or extends in the two way, one of which is etale, and the Cartier dual of the other is etale.

It is better to say how one uses (3.7) for the proof of (4.1). I explain it for (4.1) 1) a) and Case 2 very and very briefly. As I said, the equation of (3.7) is very important. By (3.2), we may assume that G is a $\mathbb{F}_q$-vector space scheme of order q. Let $\mathcal{G}$, $\mathcal{G}'$ be two group schemes whose generic fibers are isomorphic to G. We can write the equation of $\mathcal{G}$ (resp. $\mathcal{G}'$) as $X_i^p = a_i X_{i+1}$ (resp. $(X_i')^p = a_i' X_{i+1}'$) by (3.7). Since $\mathcal{G} \underset{A}{\otimes} K$ is isomorphic to $\mathcal{G}' \underset{A}{\otimes} K$, there exist elements $\alpha_i \in K^*$ such that $a_i' = \alpha_i^p a_i \alpha_{i+1}^{-1}$. As $0 \leq v(a_i), v(a_i') \leq e$, the value $v(\alpha_i)$ is very restricted. In fact, we can show $v(\alpha_i) = 0$ in Case 1) a).

Remark 4.2.

The spectrum of a discrete valuation ring of mixed characteristics 0 and p with absolute index e is thought as the disk with radius e. Thinking in this way, we can interpret (4.1) 1) a) as follows: Since the radius is small, the extension is unique, in other words, the uniqueness of the analytic continuation holds.

Exercise. Investigate the extensions (4.1) Case 2. For example, for the case of A is a strictly henselian discrete valuation ring of mixed characteristics. **Answer.** If we consider $\{(n_1, \cdots, n_f) \in \mathbb{Z}^f \,|\, 0 \le n_i \le e\}$ as the group schemes satisfying ($\star$) by (3.10), two distinct elements $(n_1, \cdots, n_f)$, $(n'_1, \cdots, n'_f)$ are isomorphic if and only if one of it is $(0, \cdots, 0)$ and the other is $(p-1, \cdots, p-1)$.

5 Galois actions

Let A be a strictly henselian discrete valuation ring of mixed characteristic 0 and p, K be the fraction field of A. Let π be a uniformizer of A and v be the normalized valuation of A. Let $e := v(p)$ be the absolute index. Then $\mathrm{Gal}(\overline{K}/K)$ is the inertia group of K and we have an exact sequence:

$$1 \longrightarrow I_p \longrightarrow \mathrm{Gal}(\overline{K}/K) \longrightarrow I_t \longrightarrow 1.$$

Here I_p is the pro$-p$ part of $\mathrm{Gal}(\overline{K}/K)$ and I_t is the tame part, which is $\varprojlim_{(d,p)=1} \mathrm{Gal}(K(\pi^{\frac{1}{d}})/K) \xrightarrow{\simeq} \varprojlim_{(d,p)=1} \mu_d(K)$ ([S] Chap.IV Prop.7). Under this identification, let j_q be the natural projection: $I_t \longrightarrow \mu_{q-1}(K)$. Let G/K be a $\mathbb{F}_q-$vector space scheme of order q. Then (3.7) says that G is isomorphic to $\mathrm{Spec}(K[X_i | i \in \mathbb{Z}/f]/(X_i^p - a_i X_{i+1} | i \in \mathbb{Z}/f))$ as a scheme. The fundamental character is an isomorphism $\chi_i : \mathbb{F}_q^* \xrightarrow{\simeq} \mu_{q-1}(K)$, hence we can consider the inverse $\varphi_i := \chi_i^{-1}$. Then $\varphi_i^p = \varphi_{i-1}$.

Theorem 5.1. *Let G/K be as above. Then the Galois action of* $\mathrm{Gal}(\overline{K}/K)$ *on $G(\overline{K}) \simeq \mathbb{F}_q$ is described as follows:*

$$\mathrm{Gal}(\overline{K}/K) \longrightarrow I_t \xrightarrow{j_q} \mu_{q-1}(K) \xrightarrow{\varphi_1^{v(a_0)}\varphi_2^{v(a_1)}\cdots\varphi_{f-1}^{v(a_{f-2})}\varphi_f^{v(a_{f-1})}} \mathbb{F}_q^*.$$

By (3.6) 3), (3.7) and (5.1) we have the following:

Corollary 5.2. *Let G/K be a $\mathbb{F}_q-$vector space scheme of order q which corresponds to a character $\varphi : \mathbb{F}_q^* \longrightarrow \mu_{q-1}(K)$. Then G extends to a flat finite commutative group scheme over A if and only if φ can be written in the following form:*

$$\varphi = \varphi_1^{e_0}\varphi_2^{e_1} \cdots \varphi_{f-1}^{e_{f-2}}\varphi_f^{e_{f-1}} \quad (0 \le e_i \le e).$$

Remark 5.3.

(5.1) is also obtained by Fontaine-Laffaille theory [FL] (cf. [B] for a partial result of (5.1)).

Since $\varphi_i^p = \varphi_{i-1}$, (5.3) below follows:

Corollary 5.4. *If $e \geq p-1$, then any $\mathbb{F}_q-$vector space scheme of order q extends to a flat group scheme over A.*

6 $p-$divisible groups

Let p be a prime number. In this section we define the $p-$divisible group and investigate the Galois action on the Tate module of a $p-$divisible group over a strictly henselian discrete valuation ring of mixed characteristics, following [F1].

Definition 6.1. *Let h be a positive integer and S be a scheme. $p-$divisible group of height h over S is a system of pairs $\{(G_n, i_n)\}_{n=1}^{\infty}$ satisfying the followings:*
1) G_n is a finite commutative group scheme of order p^{hn} over S.
2) The following sequence is exact:

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

Remark 6.2.

A $p-$divisible group is not an abstract group which is $p-$divisible. The name is misleading. Grothendieck proposed the name Barsotti-Tate group. But the name $p-$divisible group is usually used today.

Example 6.3.

Let h be a positive integer.
1) $G_n = (\frac{1}{p^n}\mathbb{Z}/\mathbb{Z})^h/S$, and i_n is the natural inclusion.
2) $G_n = \mu_{p^n}^h/S$, and i_n is the natural inclusion.
3) Let $\mathcal{A}/S$ be a semi-abelian scheme, i.e. an extension of an abelian scheme by a torus. Let G_n be Ker$(p^n : \mathcal{A} \longrightarrow \mathcal{A})$, and i_n be the natural inclusion. We get a $p-$divisible group from these.

4) Let B be a complete ring, and $R := B[[X_1, \cdots, X_n]]$ be the ring of formal power series in $n-$variables. Let $\Gamma = \operatorname{Spf} R$ be a commutative group over $\operatorname{Spf} B$, i.e. with a triple of morphisms (m, e, inv) (e.g. $m : \Gamma \underset{\operatorname{Spf} B}{\times} \Gamma \longrightarrow \Gamma$) satisfying the axioms of [N] (2.1) 1) and 2). We assume Γ has a finite height h, i.e. the induced morphism $p^* : R \longrightarrow R$ makes R free over R of rank p^h. Then Γ is called divisible. Let $G_n = \operatorname{Ker}(p^n : \Gamma \longrightarrow \Gamma)$, and i_n be the natural inclusion.
To state a theorem of Tate-Raynaud we need the following:

Theorem 6.4 ([T] (2.2) Prop.1). *Let A be a complete noetherian local ring with residue field of characteristic p. Then the following functor gives an equivalence of the following two categories:*

$$\{ \textit{connected divisible commutative formally smooth group schemes over } A \}$$

$$\ni \Gamma \longmapsto (\operatorname{Ker}(p^n : \Gamma \longrightarrow \Gamma))_n \in \{ \textit{connected } p-\textit{divisible groups} \}.$$

Let G be a $p-$divisible group over a complete noetherian local ring A . Then the dimension of G is by definition is that of the formal group associated to the connected component of $0 \in G$. Here the word "connected" means that each constitute of a $p-$divisible group is connected.

Definition 6.5. *Let A be an integral domain, K be the fraction field of A, and K_s be a separable closure of K. Let $G = \{(G_n, i_n)\}_{n=1}^{\infty}$ be a $p-$divisible group over* $\operatorname{Spec} K$. *Then $T_p(G) := \varprojlim_{p} G_n(K_s)$ is called a Tate module of G.*

Theorem 6.6 (Tate-Raynaud(-Fontaine)). *Let A be a strictly henselian discrete valuation ring of mixed characteristics of* 0 *and p, and $K :=$* $\operatorname{Frac} A$. *Let G be a $p-$divisible group over A of height h and dimension d. Then $h-$th wedge product of $T_p(G)$ over $\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p(d) := (\varprojlim_{p} \mu_{p^n})^{\otimes d}$ as a* $\operatorname{Gal}(\overline{K}/K)$*-module.*

In the rest of the report I give an outline of a proof of (6.6), following [F1]. Let K be a local field, i.e. the fraction field of a complete discrete valuation ring of mixed characteristics with perfect residue field k of characteristic $p > 0$. Let K_0 be $\operatorname{Frac} W(k)$, σ be the Frobenius of K_0. We must use the basic ring B_{crys}. We do not review the definition of B_{crys} ([F2]) here, instead we review the necessary properties of B_{crys}. B_{crys} is a filtered Galois ring, i.e. B_{crys} is a

commutative K_0–algebra with unit element and σ–linear bijective morphism F, and it has a decreasing filtration indexed by $\mathbb{Z}$ on $B_{\mathrm{crys}K} := B_{\mathrm{crys}} \underset{K_0}{\otimes} K$, and has a Galois action of $\mathrm{Gal}(\overline{K}/K)$ which is compatible with the ring structure and the filtration. Moreover B_{crys} has the following properties:
1) There is an injection of filterd modules

$$\widehat{K_0^{\mathrm{nr}}}[T^{\pm 1}] \hookrightarrow B_{\mathrm{crys}} \qquad (T \in \mathrm{Fil}^1(\widehat{K_0^{\mathrm{nr}}}[T^{\pm 1}]) \setminus \mathrm{Fil}^2(\widehat{K_0^{\mathrm{nr}}}[T^{\pm 1}])).$$

Here $\widehat{\ }$ means a completion and $^{\mathrm{nr}}$ a maximal non-ramified extension, and $\widehat{K_0^{\mathrm{nr}}}[T^{\pm 1}] := \widehat{K_0^{\mathrm{nr}}} \underset{\mathbb{Z}_p}{\otimes} \mathrm{Sym}\,\mathbb{Z}_p(1)$.
2) $B_{\mathrm{crys}}^{\mathrm{Gal}(\overline{K}/K)} = K_0$,
3) $B_{\mathrm{crys}}^{F=1} \cap B_{\mathrm{crys}K}^{\mathrm{fil}=0} = \mathbb{Q}_p$.
4) There is an injection $\mathrm{gr}(B_{\mathrm{crys}K}) \hookrightarrow C[T^{\pm 1}]$ which induces the isomorphism $\mathrm{gr}(\widehat{K^{\mathrm{nr}}}[T^{\pm 1}]) \xrightarrow{\simeq} \widehat{K^{\mathrm{nr}}}[T^{\pm 1}]$. Here C is the completion of an algebraic closure of K.
(In [F1] such a ring as above is called a Barsotti-Tate ring.) A p–adic representation is a finite dimensional vector space with continuous Galois action , and a filtered module is a finite dimensional K_0– vector space D with σ–linear bijective morphism F, and with decreasing filtration indexed by $\mathbb{Z}$ on $D \underset{K_0}{\otimes} K$. Using B_{crys} we can construct two fundamental functors:

$$\{\, p - \text{adic representations} \,\} \rightleftarrows \{\, \text{filtered modules} \,\},$$

where $\longrightarrow$ is defined by $D_{\mathrm{crys}}(V) := (B_{\mathrm{crys}} \underset{\mathbb{Q}_p}{\otimes} V)^{\mathrm{Gal}(\overline{K}/K)}$ for a p–adic representation V and $\longleftarrow$ is by $V_{\mathrm{crys}}(D) := (B_{\mathrm{crys}} \underset{K_0}{\otimes} D)^{F=1,\mathrm{fil}=0}$ for a filtered module D. Under these $\mathbb{Q}_p$ corresponds to K_0 by the properties 2) and 3) of B_{crys}. Every p–adic representation is not good, of course:

Definition 6.7. *1) A p–adic representation V is called a crystalline representation if* $\dim_{K_0} D_{\mathrm{crys}}(V) = \dim_{\mathbb{Q}_p} V$.
2) A p–adic representation V is Hodge-Tate if $\sum_{i\in\mathbb{Z}} \dim_K (C \underset{\mathbb{Q}_p}{\otimes} V)\{-i\} = \dim_{\mathbb{Q}_p} V$. *Here* $X\{-i\} := \{x \in X | g \cdot x = \chi^i(g)x, (g \in \mathrm{Gal}(\overline{K}/K)\}$ *for a C–vector space X with C–semi-linear* $\mathrm{Gal}(\overline{K}/K)$*–action. (χ is the cyclotomic character.).*

It is known that crystalline representations (or more generally de Rham representations) are Hodge-Tate [F1].

Remark 6.8.

1) For any $p-$adic representation V there is a natural injection

$$B_{\mathbf{crys}} \underset{K_0}{\otimes} D_{\mathbf{crys}}(V) \hookrightarrow B_{\mathbf{crys}} \underset{\mathbb{Q}_p}{\otimes} V,$$

hence V is cr:'stalline if and only if

$$B_{\mathbf{crys}} \underset{K_0}{\otimes} D_{\mathbf{crys}}(V) \xrightarrow{\simeq} B_{\mathbf{crys}} \underset{\mathbb{Q}_p}{\otimes} V.$$

2) Crystalline representations are stable under sub-object, quotient, direct sum, tensor product, dual and wedge product.
3) $D_{\mathbf{crys}}$ gives an equivalence of the categories of the crystalline representations and the essential images of them. The quasi-inverse is $V_{\mathbf{crys}}$.
4) A $p-$adic representation V is Hodge-Tate if and only if $\underset{i}{\oplus} C \underset{K}{\otimes} (C \underset{\mathbb{Q}_p}{\otimes} V\{-i\}) = C \underset{\mathbb{Q}_p}{\otimes} V$.

The following is quite elementary modulo a calculation of a Galois cohomology in [T]:

Propositon 6.9 ([F1] (3.3.1),(3.3.5)). *Let V be a $p-$adic representation such that the inertia subgroup of* $\mathrm{Gal}\,(\overline{K}/K)$ *acts through a finite quotient. Then V is crystalline if and only if V is unramified, i.e. the inertia group has a trivial action on V.*
2) Let V be a $1-$dimensional $p-$adic representation. Than V is crystalline if and only if there exists an integer i such that $V(-i) := V \underset{\mathbb{Q}_p}{\otimes} \mathbb{Q}_p(-i)$ is unramified. Here $\mathbb{Q}_p(-i) := (\underset{\overleftarrow{p}}{\lim}\mu_{p^n})^{\otimes(-i)} \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p$.

We must review the Dieudonné module of a $p-$divisible group of G of height h over $\mathcal{O}_K$. But we state only the following properties: It is a filtered module of rank h over K_0 whose filtration is as follows: Fil^0 : the whole space, Fil^1 : the dual of the tangent space of the formal group associated to the connected component of G, $\mathrm{Fil}^2 = 0$. [F] is a good reference on Cartier-Dieudonné theory. The following is the key point for the proof of (6.6).

Theorem 6.10 ([F2] (6.2)). *Let G be a $p-$divisible group over O_K. Then $V_p(G) := T_p(\Gamma)\underset{\mathbb{Z}_p}{\otimes}\mathbb{Q}_p$ is a crystalline representation. Furthermore $D_{\mathbf{crys}}(V_p(G))$ is isomorphic to the dual of the Dieudonné-module of Γ as a filtered module.*

By completing A and using (6.9) and (6.10), we get (6.6).

Appendix
As we said, we give the group law of ${}_{\mathcal{L}_1,\cdots,\mathcal{L}_f}G^{b_1,\cdots,b_f}_{a_1,\cdots,a_f}$ in the notation of (3.7). For this we must prepare some notations. Let $\chi : \mathbb{F}_q^* :\longrightarrow \mu_{q-1}$ be a character. Then it can be uniquely written in the rule of of §3 Notations as follows:

$$\chi = \prod_{i \in \mathbb{Z}/f} \chi_i^{e_i} \quad 0 \leq e_i \leq p-1.$$

Then we put

$$w_\chi := w_{\underbrace{\chi_1, \cdots, \chi_1}_{e_1 \text{ pieces}}, \cdots, \underbrace{\chi_{f-1}, \cdots, \chi_{f-1}}_{e_f \text{ pieces}}}.$$

It can be shown that w_χ is an invertible element of Λ_q. Let $1 \leq i \leq f$ be an integer. We take the fundamental character and consider $\chi' = \prod \chi_j^{e'_j}$, $\chi'' = \prod \chi_j^{e''_j}$ such that $\chi'\chi'' = \chi_i$. In this case there is a unique integer $1 \leq k \leq f$ such that $e'_{i-k} + e''_{i-k} = p$, $e'_{i-h} + e''_{i-h} = p-1\,(1 \leq h < k)$, $e'_j + e''_j = 0$ otherwise. Let T be a scheme over the base scheme S, and $x = (x_i)$, $y = (y_i) \in {}_{\mathcal{L}_1,\cdots,\mathcal{L}_f}G^{b_1,\cdots,b_f}_{a_1,\cdots,a_f}(T) = \{(z_1, \cdots, z_f) \in \prod_{i=1}^f \Gamma(T, \mathcal{L}_i^{-1} \underset{\mathcal{O}_S}{\otimes} \mathcal{O}_T)\,|z_i^{\otimes p} = a_i^*(z_{i+1}),\, i = 1, \cdots, f\}$. Under these notations the group law of ${}_{\mathcal{L}_1,\cdots,\mathcal{L}_f}G^{b_1,\cdots,b_f}_{a_1,\cdots,a_f}$ is given as follows: The i-th component of $x+y$ is

$$x_i + y_i + \sum_{\chi'\chi'' = \chi_i} \frac{b_{i-k} \otimes \cdots \otimes b_{i-1}}{w_{\chi'} w_{\chi''}} \prod_j x_j^{\otimes e'_j} \otimes y_j^{\otimes e''_j}.$$

Here b_j is considered as a section of $(\mathcal{L}_i^{\otimes p} \otimes \mathcal{L}_{i+1}^{-1})(T)$.

References

[B] P. Berthelot. *Systèmes de Honda des schémas en $\mathbb{F}_q$−vectoriels.* Bull. Soc. Math. Fr. 105 (1979), pp.225-239.

[F] J.-M. Fontaine. *Groupes p−divisibles sur les corps locaux.* Astérisque 47-48, Soc. Math. de France (1977),

[F1] J.-M. Fontaine. *Module galoisiens, modules filtrés et anneaux de Barsotti-Tate.* Dans Journées de Géométrie de Rennes, Astérisque 65, Soc. Math. 115 (1982), pp.3-80.

[F2] J.-M. Fontaine. *Sur certains types de représentations p-adiques du groupe de Galois d'un corps local: construction d'un anneaux de Barsotti-Tate.* Ann. of Math. 115 (1982), pp.529-577.

[FL] J.-M. Fontaine et G.Laffaille. *Construction de représentations p-adiques.* Ann. Scient. Éc. Norm. Sup. 4e série 15 (1982), pp.547-608.

[M] F. Momose. *Q-curves and QM-curves.* In this volume.

[N] Y. Nakkajima. *Finite Group Schemes I.* In this volume.

[OT] F. Oort and J. Tate. *Group schemes of finite order.* Ann. Sci. École Norm. Sup.3, (1970), pp. 1-21.

[R] M. Raynaud. *Schémas en groupes de type $(p, \cdots, p)$.* Bull. Soc. Math. Fr. 102, (1974), pp. 241-280.

[S] J.-P. Serre. *Corps Locaux.* Hermann, Paris (1968).

[Sh] S.S. Shatz. *Group Schemes, Formal Groups, and p-Divisible Groups.* In Arithmetic Geometry edited by G. Cornell and J.H. Silverman, Springer-Verlag, (1986), pp. 29-78.

[T] J. Tate. *p-divisible groups.* Proceedings of a Conference on Local Fields, Driebergen, 1966. Springer-Verlag, (1967), pp. 158-183.