Tohoku Math. J.
66 (2014), 309–320

A GENERALIZATION OF THE THEORY OF COLEMAN POWER SERIES

KAZUTO OTA

(Received March 30, 2012, revised May 7, 2013)

Abstract. Shinichi Kobayashi found a generalization of the Coleman power series theory to formal groups of elliptic curves and applied it to a study of p-adic height pairings. In this paper, we generalize his theory of Coleman power series to general formal groups.

1. Introduction. The theory of Coleman power series [1] says that every norm compatible system is interpolated by a power series. This theory has been generalized in various ways by Perrin-Riou [8] and others, and they play important roles in Iwasawa theory. On the other hand, Kobayashi [6] found a generalization to formal groups of elliptic curves. He studied the interpolations of "admissible norm systems" (cf. [6]), which are not norm compatible. Furthermore, he applied it to computations of p-adic height pairings to prove the p-adic Gross-Zagier formula for elliptic curves at supersingular primes. We expect a generalization of his theory will play an important role in proving more general p-adic Gross-Zagier formulas. In this paper, we generalize his theory to general formal groups over unramified rings.

Let ζ_{p^n} be a primitive p^n-th root of unity such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$, $\mathfrak{m}_n$ the maximal ideal of $\boldsymbol{Z}_p[\zeta_{p^n}]$ and $U_n = 1 + \mathfrak{m}_n$. Then the Coleman power series theory [1] says that every $(u_n)_n \in \varprojlim U_n$, where the limit is taken with respect to the norm maps, is interpolated by a power series. Namely, there exists a unique power series $f(T) \in \boldsymbol{Z}_p[[T]]$ such that

$$f(\zeta_{p^n} - 1) = u_n$$

for all $n \geq 1$. In terms of formal groups, every element of $\varprojlim \hat{\boldsymbol{G}}_m(\mathfrak{m}_n)$ can be interpolated.

Let E be an elliptic curve over $\boldsymbol{Q}_p$ with good supersingular reduction and $\hat{E}$ the formal group over $\boldsymbol{Z}_p$ (of height two) associated to E. Then it is known that $\varprojlim \hat{E}(\mathfrak{m}_n)$ is trivial, where the projective limit is taken with respect to the trace maps $\mathrm{Tr}_{m/n} : \hat{E}(\mathfrak{m}_m) \to \hat{E}(\mathfrak{m}_n)$. However, systems $(c_n)_n \in \prod_{n=1}^{\infty} \hat{E}(\mathfrak{m}_n)$ satisfying the equations

$$\mathrm{Tr}_{n+2/n} c_{n+2} - a_p \mathrm{Tr}_{n+1/n} c_{n+1} + p c_n = 0 \tag{1.1}$$

in $\hat{E}(\mathfrak{m}_n)$ for all $n \geq 1$, where $a_p = p + 1 - \#E(\boldsymbol{F}_p)$, are also important (cf. Kobayashi [5], Perrin-Riou [7]). For example, some systems satisfying (1.1) are constructed from certain integral power series and applied to a construction of p-adic height pairings in [7]. In [6],

2010 *Mathematics Subject Classification.* Primary 14L05; Secondary 11S31, 11E95, 13F25.
Key words and phrases. Coleman power series, formal group, Dieudonné module.

Kobayashi studied the interpolations of systems $(c_n)_n \in \prod_{n=0}^{\infty} \hat{E}(\mathfrak{m}_n)$ satisfying (1.1) and found a generalization of the Coleman power series theory. By his theory, a system of Heegner points, which satisfies (1.1), can be interpolated by a power series. Thus, he applied the system to computations of the p-adic height of Heegner points. This computation played an important role in his proof of the p-adic Gross-Zagier formula, which relates the p-adic height of a Heegner point to the first derivative of a p-adic L-function of E.

Here, we explain our main theorem for odd primes (see Theorem 4.6 for the general case). Let $\mathcal{G}$ be a d-dimensional, commutative formal group over $\boldsymbol{Z}_p$ of finite height h. We fix an isomorphism $\mathcal{G} \cong \mathrm{Spf}(\boldsymbol{Z}_p[[X_1, X_2, \ldots, X_d]])$ between formal schemes over $\boldsymbol{Z}_p$. Then, we can identify $\mathcal{G}(\boldsymbol{Z}_p[[T]])$ with the subset $(p, T)^{\oplus d}$ of $\boldsymbol{Z}_p[[T]]^{\oplus d}$ and $\mathcal{G}(\mathfrak{m}_n)$ with $\mathfrak{m}_n^{\oplus d}$ not as $\boldsymbol{Z}_p$-modules but as sets (cf. Section 2). We denote by M the Dieudonné module of $\mathcal{G}$, which is a free $\boldsymbol{Z}_p$-module of rank h. Then, M has operators Frobenius F and Verschiebung V. Let $\det(t - V) = t^h + b_{h-1}t^{h-1} + \cdots + b_0 \in \boldsymbol{Z}_p[t]$, ℓ the logarithm $\log_{\mathcal{G}}$ of $\mathcal{G}$ and $\mathrm{tr}_{m/n} : \boldsymbol{Q}_p(\zeta_{p^m}) \to \boldsymbol{Q}_p(\zeta_{p^n})$ the usual trace map. Our main theorem is the following:

THEOREM 1.1 (cf. Theorem 4.6). *For each system $(c_n)_n \in \prod_{n=1}^{\infty} \mathcal{G}(\mathfrak{m}_n)$ satisfying*

$$\mathrm{tr}_{n+h/n}\ell(c_{n+h}) + b_{h-1}\mathrm{tr}_{n+h-1/n}\ell(c_{n+h-1}) + \cdots + b_0\ell(c_n) = 0 \tag{1.2}$$

in $\boldsymbol{Q}_p(\zeta_{p^n})$ for all $n \geq 1$, the following conditions are equivalent:

(a) *There exists a power series $f(T) \in \mathcal{G}(\boldsymbol{Z}_p[[T]])$ such that*

$$f(\zeta_{p^n} - 1) = c_n$$

for all $n \geq 1$;

(b) $c_{n+1}^p \equiv c_n \mod p\boldsymbol{Z}_p[\zeta_{p^{n+1}}]^{\oplus d}$ *for all $n \geq 1$.*

REMARK 1.2. (1) We prove our main theorem for formal groups over unramified rings.

(2) In [7], Perrin-Riou constructed systems satisfying (1.2) similarly as in the case $\mathcal{G} = \hat{E}$. See Section 3 for details.

(3) In the case $\mathcal{G} = \hat{E}$, we have $\det(t - V) = t^2 - a_p t + p$ and $\bigcup_n \hat{E}(\mathfrak{m}_n)_{\mathrm{tor}} = 0$. Therefore, we see that (1.2) is equivalent to (1.1) and that our main theorem coincides with Kobayashi's theorem [6, Theorem 3.15]. In this paper, we modify his proof. The key is to use Knospe [4, Proposition 2.1].

Acknowledgment. This paper is based on Master's thesis of the author. He would like to express his sincere gratitude to his adviser Professor Shinichi Kobayashi for suggesting the problem to him and for giving much advice. The author would also like to thank the referee for giving helpful comments.

2. Preliminaries. In this section, we fix notation and recall Dieudonné modules of formal groups over unramified rings.

Let p be a prime number and k a perfect field of characteristic p. We denote by W the ring $W(k)$ of Witt vectors with coefficients in k and by K its fractional field with absolute

Frobenius σ. We fix a prime element π of $\boldsymbol{Z}_p$ and $\varphi(T) \in \boldsymbol{Z}_p[[T]]$ such that

$$\varphi(T) \equiv \pi T \mod T^2 \boldsymbol{Z}_p[[T]], \quad \varphi(T) \equiv T^p \mod \pi \boldsymbol{Z}_p[[T]].$$

As is well known, φ induces a Lubin-Tate formal group $\mathcal{F}$ over $\boldsymbol{Z}_p$ whose multiplication-by-π map $[\pi]_{\mathcal{F}}$ is given by $\varphi(T)$. For $n \geq 0$, we denote by $\mathcal{F}[\pi^n]$ the kernel of the endomorphism $[\pi^n]_{\mathcal{F}}$ of $\mathcal{F}$ and put $K_n = K(\mathcal{F}[\pi^n])$. We denote by $\mathfrak{m}_n$ the maximal ideal of the valuation ring $\mathcal{O}_{K_n}$ of K_n. We fix a system $(\pi_n) \in \prod_{n=1}^{\infty} \mathcal{F}[\pi^n] \setminus \mathcal{F}[\pi^{n-1}]$ such that $[\pi]_{\mathcal{F}}(\pi_{n+1}) = \pi_n$. Let $\mathcal{G}$ be a d-dimensional, commutative formal group over W of finite height h. We also fix an isomorphism $\mathcal{G} \cong \mathrm{Spf}(W[[X]])$ between formal schemes over W, where $W[[X]] = W[[X_1, \ldots, X_d]]$, and denote by $X \oplus Y \in W[[X, Y]]^{\oplus d}$ the d-dimensional formal group law. Then, for a commutative W-algebra A which is complete under the topology induced by an ideal I of A containing p, we can identify $\mathcal{G}(I)$ with the set of W-homomorphisms $f : W[[X]] \to A$ such that $f(X_i) \in I$ for $1 \leq i \leq d$. Thus, we can identify $\mathcal{G}(I)$ with $I^{\oplus d}$ as a set by $f \mapsto (f(X_i))_i$. In other words, we identify $\mathcal{G}(I)$ with the $\boldsymbol{Z}_p$-module $I^{\oplus d}$ whose addition is induced by the formal group law $X \oplus Y$.

In order to define Dieudonné modules, we recall the formal differential module of $W[[X]]$ over W. We denote by $\mathcal{D}$ the space of derivations of $W[[X]]$ over W and by $\mathcal{D}^*$ the dual $W[[X]]$-module of $\mathcal{D}$. Then, we have $\mathcal{D}^* = \bigoplus_{1 \leq i \leq d} W[[X]] dX_i$. Here we denote by dg the map $\mathcal{D} \to W[[X]]$ defined by $D \mapsto Dg$ for $g \in W[[X]]$. We say that $\omega \in \mathcal{D}^*$ is an exact form if $\omega = df = \sum_{1 \leq i \leq d} (\partial f / \partial X_i) dX_i$ for some $f \in K[[X]]$. For an exact form ω, we denote by $F_\omega \in K[[X]]$ a unique power series such that $\omega = dF_\omega$ and $F_\omega(0) = 0$. We put

$$Z = \{\omega \in \mathcal{D}^* ;\ \omega \text{ is exact},\ F_\omega(X \oplus Y) - F_\omega(X) - F_\omega(Y) \in pW[[X, Y]]\},$$
$$B = \{df \in \mathcal{D}^* ;\ f \in pW[[X]]\},$$
$$L = \{\omega \in \mathcal{D}^* ;\ F_\omega(X \oplus Y) = F_\omega(X) + F_\omega(Y)\}.$$

We define the Dieudonné module M of $\mathcal{G}$ by $M := Z/B$. Since it depends only on the special fiber $\overline{\mathcal{G}}$ of $\mathcal{G}$, we also call it the Dieudonné module of $\overline{\mathcal{G}}$. It is known that M is a free W-module of rank h. Let $W[F, V]$ be the Dieudonné ring. Namely, F and V satisfy the relations

$$FV = VF = p, \quad Fx = x^\sigma F, \quad Vx = x^{\sigma^{-1}} V$$

for $x \in W$. We remark that $W[F, V]$ acts on M as follows: For $\omega \in Z$, we put $F_\omega(X) = \sum_\alpha a_\alpha X^\alpha$. Here α ranges over all $(i_1, \ldots, i_d) \in \boldsymbol{Z}_{\geq 0}^{\oplus d} \setminus \{(0, \ldots, 0)\}$, and X^α denotes the product $X_1^{i_1} \cdots X_d^{i_d}$ for $\alpha = (i_1, \ldots, i_d)$. We make F and V act on M by

$$F(\omega + B) = d\big(F_\omega^\sigma\left(X^p\right)\big) + B = \sum_{1 \leq i \leq d} \frac{\partial}{\partial X_i}\big(F_\omega^\sigma\left(X^p\right)\big) dX_i + B,$$

$$V(\omega + B) = d\Big(\sum_\alpha p a_{p\alpha}^{\sigma^{-1}} X^\alpha\Big) + B = \sum_{1 \leq i \leq d} \frac{\partial}{\partial X_i}\Big(\sum_\alpha p a_{p\alpha}^{\sigma^{-1}} X^\alpha\Big) dX_i + B.$$

Here $p\alpha$ denotes $(pi_1, \ldots, pi_d)$ for $\alpha = (i_1, \ldots, i_d)$. Thus, M is a left $W[F, V]$-module. We call F Frobenius operator and V Verschiebung operator, respectively, on M.

According to Honda [3, Proposition 1.3 and Lemma 1.4], we see that $L \subset Z$. By abuse of notation, we also denote by L the image of L in M. Furthermore, one can show that M is a left $W[F, V]$-module generated by the W-submodule L of M (cf. [3, Lemma 4.3]).

We define a $W[[T]]$-submodule $\mathcal{P}$ of $K[[T]]$ and its quotient $\overline{\mathcal{P}}$ by

$$\mathcal{P} = \left\{ f(T) = \sum_{n=0}^{\infty} a_n T^n \in K[[T]] \,;\; na_n \in W \text{ for } n \geq 0, \quad f(0) \in pW \right\},$$

$$\overline{\mathcal{P}} = \mathcal{P}/pW[[T]]\,.$$

We remark that φ acts on $\mathcal{P}$ by $\varphi(f)(T) = f^{\sigma}(\varphi(T))$. Then, by [3, Lemma 2.1], we see that φ induces Frobenius operator F of $\overline{\mathcal{P}}$, which is defined by

$$F\left(\sum_n a_n T^n + pW[[T]] \right) = \sum_n a_n^{\sigma} T^{pn} + pW[[T]]\,.$$

By an argument similar to that in the proof of [7, Lemme 1.2], one can show that there exists a unique σ^{-1}-linear operator ψ of $\mathcal{P}$ such that $\psi \circ \varphi = p$ and

$$\varphi \circ \psi(f)(T) = \sum_{\eta \in \mathcal{F}[\pi]} f(T \oplus_{\mathcal{F}} \eta)\,,$$

where $\oplus_{\mathcal{F}}$ denotes the addition in $\mathcal{F}$.

PROPOSITION 2.1. *For $f(T) \in \mathcal{P}$ and $n \geq 1$, we have*

(a) $\varphi(f)(\pi_{n+1}) = f^{\sigma}(\pi_n)$;

(b) $\psi(f^{\sigma})(\pi_n) = \mathrm{tr}_{n+1/n}(f(\pi_{n+1}))$.

Here, $\mathrm{tr}_{m/n}$ *is the usual trace map from K_m to K_n for $m \geq n$.*

PROOF. For example, see [7, Lemme 1.4]. □

Moreover, ψ induces Verschiebung operator V of $\overline{\mathcal{P}}$, which is defined by

$$V\left(\sum_n a_n T^n + pW[[T]] \right) = \sum_n p a_{pn}^{\sigma^{-1}} T^n + pW[[T]]\,.$$

Thus, $\overline{\mathcal{P}}$ is a left $W[F, V]$-module. According to Fontaine [2], we have a canonical $\boldsymbol{Z}_p$-linear isomorphism

$$\mathcal{G}(k[[T]]) \cong \mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})\,.$$

In order to construct this isomorphism, we fix some notation.

We denote by $\omega_1, \ldots, \omega_d$ the canonical invariant differentials of $\mathcal{G}$, which is also called the *canonical base* of L in [3]. Here, we recall that we have identified $\mathcal{G}$ with the formal group law $X \oplus Y$ over W through the fixed isomorphism $\mathcal{G} \cong \mathrm{Spf}(W[[X]])$. We denote by $\log_{\mathcal{G}} = (F_{\omega_i}(X)) \in K[[X]]^{\oplus d}$ the logarithm of $\mathcal{G}$, which is also called the *transformer* in [3]. We put $\exp_{\mathcal{G}}(X) = \log_{\mathcal{G}}^{-1} \in K[[X]]^{\oplus d}$. For a local ring A, we denote by $\mathfrak{m}_A$ the maximal ideal.

First, we construct $\mathcal{G}(k[[T]]) \to \mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})$. For $(\overline{f_i}(T)) \in \mathcal{G}(k[[T]]) = \mathfrak{m}_{k[[T]]}^{\oplus d} = Tk[[T]]^{\oplus d}$, we take any lift $(f_i(T))$ in $\mathcal{G}(W[[T]]) = \mathfrak{m}_{W[[T]]}^{\oplus d} = (p, T)^{\oplus d}$ such that $f_i(0) = 0$. We define an element of $\mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})$ by

$$\omega \mapsto F_\omega(f_1(T), \ldots, f_d(T)) \mod pW[[T]]\,.$$

Note that this morphism is independent of the choice of $(f_i(T))$ by [3, Lemma 2.1]. Thus, we have a $\boldsymbol{Z}_p$-morphism

$$\mathcal{G}(k[[T]]) \to \mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})\,.$$

For $v \in \mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})$, we take any lift $F_i(T)$ of $v(\omega_i)$ such that $F_i(0) = 0$. We define an element $\overline{f}(T)$ of $\mathcal{G}(k[[T]])$ by

$$\overline{f}(T) = \exp_{\mathcal{G}}(F_1(T), \ldots, F_d(T)) \mod \mathcal{G}(pW[[T]])\,.$$

Note that the power series $\exp_{\mathcal{G}}(F_1(T), \ldots, F_d(T))$ is an element of $\mathcal{G}(W[[T]])$ by [3, Lemma 2.4]. By [3, Proposition 3.3 and Lemma 4.1], we also see that this is independent of the choice of $(F_i(T))$. Thus, we have the inverse morphism.

In the following, we often identify $\mathcal{G}(k[[T]])$ with $\mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})$ by this isomorphism.

3. Construction of systems after Perrin-Riou. In this section, we shall construct systems satisfying a relation similar to (1.2) in the same way as in [7]. First, we recall a lift $\mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}}) \to \mathrm{Hom}_W(M, \mathcal{P})$ constructed in [7]. It plays important roles in this paper. We keep the same notation as in the previous section.

PROPOSITION 3.1. *For each $x \in \mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})$, there exists a unique lift $\hat{x} \in \mathrm{Hom}_W(M, \mathcal{P})$ of x such that*

$$\psi(\varphi(\hat{x}(m)) - \hat{x}(Fm)) = 0 \tag{3.3}$$

for all $m \in M$, or equivalently, $\psi(\hat{x}(m)) = \hat{x}(Vm)$ for all $m \in M$.

PROOF. This is [7, Proposition 3.2]. In [7], only the case where $\varphi(T) = (1+T)^p - 1$ is treated. However, we can also prove this proposition for our φ by the same argument as in [7]. □

We construct systems satisfying a relation similar to (1.2) by using the lift.

Let x be an element of $\mathcal{G}(k[[T]]) \cong \mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})$. In the case $p > 2$, the power series $\exp_{\mathcal{G}} \circ(\hat{x}(\omega_i))$ is an element of $\mathcal{G}(W[[T]]) = \mathfrak{m}_{W[[T]]}^{\oplus d}$ by [3, Lemma 2.4]. Thus, we have a lift

$$\iota : \mathcal{G}(k[[T]]) \to \mathcal{G}(W[[T]]), \quad x \mapsto \exp_{\mathcal{G}} \circ(\hat{x}(\omega_i))\,.$$

Hence, we have

$$\mathcal{G}(W[[T]]) = \iota\,(\mathcal{G}(k[[T]])) \oplus \mathrm{Hom}_W(L,\, pW[[T]])$$

(cf. [7, Théorème 4.1]). For $f(T) = \iota(x) = \exp_{\mathcal{G}} \circ(\hat{x}(\omega_i)) \in \iota\,(\mathcal{G}(k[[T]])) \subsetneqq \mathcal{G}(W[[T]])$, we put

$$c_n = f^{\sigma^{-n}}(\pi_n) = \left(\exp_{\mathcal{G}} \circ(\hat{x}(\omega_i))\right)^{\sigma^{-n}}(\pi_n) \in \mathcal{G}^{\sigma^{-n}}(\mathfrak{m}_n)\,.$$

In the case $p = 2$, we put $c_n = (\exp_{\mathcal{G}} \circ (2\hat{x}(\omega_i)))^{\sigma^{-n}}(\pi_n)$. Note that the constant term of $2\hat{x}(\omega_i)$ is in $4W$ and that $\exp_{\mathcal{G}}$ converges on $4W^{\oplus d}$ (cf. Lemma 4.1). As in the case $p > 2$, we have a lift

$$\iota : \mathcal{G}(k[[T]]) \otimes \boldsymbol{Q}_2 \to \mathcal{G}(W[[T]]) \otimes \boldsymbol{Q}_2, \quad x \mapsto \frac{1}{2}(\exp_{\mathcal{G}} \circ (2\hat{x}(\omega_i)))\,.$$

See [6, Section 3] for a lift without a denominator.

We take a polynomial $Q(t) = t^m + b_{m-1}t^{m-1} + \cdots + b_0 \in W[t]$ such that

$$Q(V)\omega_i = 0 \tag{3.4}$$

for $1 \leq i \leq d$ (e.g. $Q(t) = \det_W(t^\nu - V^\nu | M)$ in the case where k is the finite field $\boldsymbol{F}_{p^\nu}$ of p^ν elements). By Proposition 3.1, we have

$$(\psi^m + b_{m-1}\psi^{m-1} + \cdots + b_0)\hat{x}(\omega_i) = 0$$

for $1 \leq i \leq d$. Therefore, by Proposition 2.1, we have

$$\mathrm{tr}_{n+m/n}\ell_{n+m}(c_{n+m}) + b_{m-1}\mathrm{tr}_{n+m-1/n}\ell_{n+m-1}(c_{n+m-1}) + \cdots + b_0\ell_n(c_n) = 0 \tag{3.5}$$

for all $n \geq 1$, where we denote by ℓ_n the logarithm $\log_{\mathcal{G}}^{\sigma^{-n}}$ of $\mathcal{G}^{\sigma^{-n}}$.

DEFINITION 3.2. Let $Q(t) \in W[T]$ be a polynomial satisfying (3.4). We say that $(c_n)_n \in \prod_{n=1}^{\infty} \mathcal{G}^{\sigma^{-n}}(\mathfrak{m}_n)$ is a Q-norm system if it satisfies (3.5).

REMARK 3.3. (1) We have shown that the map

$$\mathcal{G}(W[[T]]) \to \prod_n \mathcal{G}^{\sigma^{-n}}(\mathfrak{m}_n)\,, \quad f(T) \mapsto (f^{\sigma^{-n}}(\pi_n))_n\,,$$

induces

$$\iota\,(\mathcal{G}(k[[T]])) \to \{Q\text{-norm systems}\}$$

in the case $p > 2$. See Theorem 4.9 for the image.

(2) If $\mathcal{G}$ is a formal group over $\boldsymbol{Z}_p$ and if there exist no non-trivial p-torsion points in $\bigcup_{n=1}^{\infty} \mathcal{G}(\mathfrak{m}_n)$, then the relation (3.5) is equivalent to the relation

$$\mathrm{Tr}_{n+m/n}c_{n+m} + b_{m-1}\mathrm{Tr}_{n+m-1/n}c_{n+m-1} + \cdots + b_0c_n = 0\,,$$

where $\mathrm{Tr}_{m/n}$ is the trace map from $\mathcal{G}(\mathfrak{m}_m)$ to $\mathcal{G}(\mathfrak{m}_n)$.

EXAMPLE 3.4 (The case $\mathcal{G} = \hat{\boldsymbol{G}}_m$). Let $\mathcal{G}$ be the multiplicative formal group $\hat{\boldsymbol{G}}_m$. Furthermore, we assume that k is a finite field and that p is odd for simplicity. Our lift ι from $\hat{\boldsymbol{G}}_m(k[[T]])$ to $\hat{\boldsymbol{G}}_m(W[[T]])$ induces a lift

$$1 + \mathfrak{m}_{k[[T]]} \to 1 + \mathfrak{m}_{W[[T]]}\,.$$

One can show that it coincides with the map

$$g \mapsto \mathcal{N}^\infty(\hat{g}) := \lim_{i \to \infty} (\mathcal{N}^i(\hat{g}))^{\sigma^{-i}},$$

where $\mathcal{N} : W[[T]]^\times \to W[[T]]^\times$ is the norm operator defined in [1] and $\hat{g}$ is any lift of g in $W[[T]]^\times$. Hence, we see

$$\iota\big(\hat{\boldsymbol{G}}_m(k[[T]])\big) \cong (1 + \mathfrak{m}_{W[[T]]})^{\mathcal{N}=\sigma} .$$

By the classical theory of Coleman power series, we conclude that

$$\iota\big(\hat{\boldsymbol{G}}_m(k[[T]])\big) \cong \varprojlim \hat{\boldsymbol{G}}_m(\mathfrak{m}_n) ,$$

where the limit is taken with respect to the trace map of $\hat{\boldsymbol{G}}_m$. See [1, 7] for the detail.

4. Proof of the main theorem. In this section, we prove our main theorem. We keep the same notation as in the previous section. First, we show basic properties of formal groups.

LEMMA 4.1. *Let $\mathcal{H}$ be a d-dimensional, commutative formal group over W. As before, we fix a W-isomorphism $\mathcal{H} \cong \mathrm{Spf}(W[[X]])$. Let I be an ideal contained in $\mathfrak{m}_n$.*

(1) *For $A, B \in \mathcal{H}(\mathfrak{m}_n) = \mathfrak{m}_n^{\oplus d}$, the following congruences are equivalent.*
   (a) $A \equiv B \mod I^{\oplus d}$, *where we regard A, B as elements of $\mathfrak{m}_n^{\oplus d}$.*
   (b) $A \equiv B \mod \mathcal{H}(I)$, *where we regard A, B as elements of $\mathcal{H}(\mathfrak{m}_n)$.*

(2) *If I is contained in the ideal $\{x \in K_n \ ; \ v(x) > 1/(p-1)\}$, then $\log_{\mathcal{H}}$ induces a $\boldsymbol{Z}_p$-linear isomorphism*

$$\mathcal{H}(I) \cong I^{\oplus d} .$$

Here, v denotes the valuation of K_n normalized by $v(p) = 1$.

REMARK 4.2. The isomorphism in (2) differs from the identification through the fixed isomorphism $\mathcal{H} \cong \mathrm{Spf}(W[[X]])$.

PROOF. (1) We denote by $X \oplus_{\mathcal{H}} Y$ the formal group law induced by $\mathcal{H} \cong \mathrm{Spf}(W[[X]])$. Since $X \oplus_{\mathcal{H}} Y$ is a formal group law, it satisfies

$$X \oplus_{\mathcal{H}} Y \equiv X + Y \mod \deg 2 ,$$
$$X \oplus_{\mathcal{H}} 0 = X , \quad 0 \oplus_{\mathcal{H}} Y = Y .$$

Suppose that $A \equiv B \mod I^{\oplus d}$, namely, there exists an element C of $I^{\oplus d}$ such that $A = B + C$. According to the congruences above, we have $A = B + C \equiv B \oplus_{\mathcal{H}} C \mod I^{\oplus d}$, which shows that $A \equiv B \mod \mathcal{H}(I)$. Conversely, we suppose that $A \equiv B \mod \mathcal{H}(I)$. Then, there exists an element C of $I^{\oplus d}$ such that $A = B \oplus_{\mathcal{H}} C$, where we regard A, B as elements of $\mathfrak{m}^{\oplus d}$. Hence, we have $A \equiv B + C \mod I^{\oplus d}$, which shows that $A \equiv B \mod I^{\oplus d}$.

(2) By [3, Theorem 2], we may identify $\mathcal{H}$ with the formal group law whose logarithm is of the form

$$X + \sum_{\nu \geq 1} B_\nu X^{p^\nu} \in K[[X_1, \ldots, X_d]]^{\oplus d} ,$$

where $B_\nu \in p^{-\nu} M_d(W)$ for $\nu \geq 1$. Here, we put $X^{p^\nu} = {}^t(X_1^{p^\nu}, \ldots, X_d^{p^\nu})$. For a matrix $D = (d_{i,j})$ with $d_{i,j} \in K_n$, we define the valuation $v(D)$ of D by $v(D) = \inf_{i,j}\{v(d_{i,j})\}$. Then, we have

$$v(B_\nu) \geq -\nu$$

for $\nu \geq 1$. For $x \in \mathfrak{m}_n^{\oplus d}$, we have

$$v(B_\nu x^{p^\nu}) \geq p^\nu v(x) - \nu \to \infty$$

as $\nu \to \infty$. Hence, we see that $\log_{\mathcal{H}}(x)$ is well-defined. Suppose that $v(x) > 1/(p-1)$ in addition. Then, we have

$$v(B_\nu x^{p^\nu}) - v(x) \geq p^\nu v(x) - v(x) - \nu > \frac{p^\nu - 1}{p-1} - \nu \geq 0$$

for $\nu \geq 1$. Hence we have

$$v(B_\nu x^{p^\nu}) > v(x) \tag{4.6}$$

for $\nu \geq 1$. Thus, we have $v(x) = v(\log_{\mathcal{H}}(x))$. Hence, we see that $\log_{\mathcal{H}}$ induces an injective $\boldsymbol{Z}_p$-morphism

$$\log_{\mathcal{H}} : \mathcal{H}(I) \to I^{\oplus d}.$$

We put $\mathfrak{m}_n^a = I$. For $b \geq 0$ and $A \in (\mathfrak{m}_n^{a+b})^{\oplus d}$, by (4.6), we have

$$A - \log_{\mathcal{H}}(A) \in (\mathfrak{m}_n^{a+b+1})^{\oplus d}.$$

Namely, the map

$$\log_{\mathcal{H}} : \mathcal{H}(\mathfrak{m}_n^{a+b}) \to (\mathfrak{m}_n^{a+b})^{\oplus d}/(\mathfrak{m}_n^{a+b+1})^{\oplus d}$$

is surjective for all $b \geq 0$. By the completeness of K_n, we conclude that the map $\mathcal{H}(I) \to I^{\oplus d}$ is surjective. □

REMARK 4.3. The assumption that $\mathcal{H}$ is defined over W allows us to use Honda's theory and to simplify the proof. One can show this lemma in more general case (cf. Tate [9, §2]).

Let $|\ |$ denote a p-adic absolute value on $\bigcup_n K_n$. The following proposition plays an important role in the proof of our main theorem:

PROPOSITION 4.4. *Let $P(t) = t^m + d_{m-1}t^{m-1} + \cdots + d_0 \in W[t]$ be a polynomial such that the p-adic absolute value of every root of $P(t)$ is strictly greater than $|p|$. If $(y_n)_n \in \prod_{n=1}^{\infty} \mathcal{O}_{K_n}$ satisfies*

$$\mathrm{tr}_{n+m/n}(y_{n+m}) + d_{m-1}\mathrm{tr}_{n+m-1/n}(y_{n+m-1}) + \cdots + d_0 y_n = 0$$

for all $n \geq 1$, then $y_n = 0$ for all $n \geq 1$.

REMARK 4.5. In the case $k = \boldsymbol{F}_{p^\nu}$, the polynomial $P(t) = \det_W(t^\nu - V^\nu | M)$ satisfies the condition of the proposition since F on M is topologically nilpotent and $FV = VF = p$.

PROOF. This is [4, Proposition 2.1]. In [4] it is assumed that $p > 2$, k is a finite field, $y_n \in \mathfrak{m}_n$ for all $n \geq 1$ and that $\varphi(T) = (1+T)^p - 1$. However, we can prove this proposition for our case by the same argument as in [4]. □

In the following, we fix a polynomial $Q(t) \in W[t]$ satisfying (3.4) and the assumption of Proposition 4.4 about the p-adic absolute values of the roots.

We state our main theorem.

THEOREM 4.6. (1) *Suppose $p > 2$. For each Q-norm system $(c_n)_n \in \prod_{n=1}^{\infty} \mathcal{G}^{\sigma^{-n}}(\mathfrak{m}_n)$, the following conditions are equivalent:*

(a) *There exists a power series $f(T) \in \mathcal{G}(W[[T]]) = \mathfrak{m}_{W[[T]]}^{\oplus d}$ such that*
$$f^{\sigma^{-n}}(\pi_n) = c_n$$
for all $n \geq 1$;

(b) $c_{n+1}^p \equiv c_n \mod p\mathcal{O}_{K_{n+1}}^{\oplus d}$ *for all $n \geq 1$.*

(2) *Suppose $p = 2$. For each Q-norm system $(c_n)_n$, the following conditions are equivalent:*

(a) *There exist $r \geq 0$ and a power series $f(T) \in \mathcal{G}(W[[T]]) = \mathfrak{m}_{W[[T]]}^{\oplus d}$ such that*
$$f^{\sigma^{-n}}(\pi_n) = [2^r]_{\mathcal{G}^{\sigma^{-n}}} c_n$$
for all $n \geq 1$;

(b) *There exists $r \geq 0$ such that* $([2^r]_{\mathcal{G}^{\sigma^{-(n+1)}}} c_{n+1})^2 \equiv [2^r]_{\mathcal{G}^{\sigma^{-n}}} c_n \mod 2\mathcal{O}_{K_{n+1}}^{\oplus d}$ *for all $n \geq 1$.*

REMARK 4.7. In (b), for $c_n \in \mathcal{G}^{\sigma^{-n}}(\mathfrak{m}_n)$, we regard c_n as an element $(c_{i,n})_i$ of $\mathfrak{m}_n^{\oplus d}$ by the identification $\mathcal{G}^{\sigma^{-n}}(\mathfrak{m}_n) = \mathfrak{m}_n^{\oplus d}$ through $\mathcal{G} \cong \mathrm{Spf}(W[[X]])$ and put $c_n^p = (c_{i,n}^p)_i$.

PROOF. We first prove that the condition (a) implies the condition (b). In the case $p > 2$, we suppose that there exists $f(T) \in \mathcal{G}(W[[T]])$ such that
$$f^{\sigma^{-n}}(\pi_n) = c_n$$
for all $n \geq 1$. Note that $\pi_{n+1}^p \equiv \pi_n \mod p\mathcal{O}_{K_{n+1}}$ since $\varphi(\pi_{n+1}) = \pi_n$. Hence, we have
$$c_{n+1}^p = f^{\sigma^{-(n+1)}}(\pi_{n+1})^p \equiv f^{\sigma^{-n}}(\pi_n) = c_n \mod p\mathcal{O}_{K_{n+1}}^{\oplus d}$$
for $n \geq 1$. In the case $p = 2$, we can also prove that the condition (a) implies the condition (b) in the same way as in the case $p > 2$.

In the following, we prove that the condition (b) implies the condition (a). First, we consider the case where $p > 2$. For $n \geq 1$, we take a polynomial $f_n = (f_{i,n}) \in (p, T)^{\oplus d} \subseteq W[T]^{\oplus d}$ such that
$$f_n^{\sigma^{-n}}(\pi_n) = c_n\,.$$
By (b), we have
$$f_n^{\sigma^{-m}}(\pi_m) \equiv f_n^{\sigma^{-n}}(\pi_n)^{p^{n-m}} \equiv c_n^{p^{n-m}} \equiv c_{n-1}^{p^{n-m-1}} \equiv \cdots \equiv c_m \mod p\mathcal{O}_{K_n}^{\oplus d}$$
for $m \leq n$. Thus, we have
$$f_{i,n+1}(\pi_m) \equiv f_{i,n}(\pi_m) \mod p\mathcal{O}_{K_m} \tag{4.7}$$
for $m \leq n$, $1 \leq i \leq d$. We claim that
$$f_{i,n+1} \equiv f_{i,n} \mod (p, T^{p^n - p^{n-1}})\,. \tag{4.8}$$
In fact, we have
$$[\pi^n]_{\mathcal{F}}(T) = U_n(T)P_n(T)$$

by the p-adic Weierstrass preparation theorem. Here, $U_n(T)$ is a unit of $W[[T]]$, and $P_n(T)$ is a distinguished polynomial of degree p^n since $[\pi^n]_{\mathcal{F}}(T) \equiv T^{p^n} \mod pW[[T]]$. Therefore, we have

$$\Phi_n(T) := [\pi^n]_{\mathcal{F}}(T)/[\pi^{n-1}]_{\mathcal{F}}(T) = U(T)P(T)\,,$$

where $U(T)$ is a unit of $W[[T]]$, and $P(T) = P_n(T)/P_{n-1}(T)$ is a *distinguished polynomial* of degree $\phi(p^n) = p^n - p^{n-1}$. Hence, we have

$$f_{i,n+1} - f_{i,n} = R(T)\Phi_n(T) + a_{\phi(p^n)-1}T^{\phi(p^n)-1} + \cdots + a_0$$

for some $R(T) \in W[[T]]$ and $a_j \in W$ $(0 \le j \le \phi(p^n) - 1)$. If we put $T = \pi_n$, then we have

$$a_{\phi(p^n)-1}\pi_n^{\phi(p^n)-1} + \cdots + a_0 \in p\mathcal{O}_{K_n}$$

by (4.7). Since $\{\pi_n^j\}_{j=0}^{\phi(p^n)-1}$ is free over W, we have $a_j \in pW$ for $0 \le j \le \phi(p^n) - 1$. Thus, we have proved (4.8) as claimed.

By (4.8), we see that $\overline{f}_{i,n}$ converges to an element $\overline{h}_i$ of $k[[T]]$ as $n \to \infty$, where $\overline{f}_{i,n}$ is the image of $f_{i,n}$ in $k[[T]]$. For the lift $h_i \in W[[T]]$ of $\overline{h}_i$ such that $h_i(0) = 0$, we put $h = (h_i)$. Then, we have $h^{\sigma^{-n}}(\pi_n) \equiv c_n \mod p\mathcal{O}_{K_n}^{\oplus d}$ for $n \ge 1$. Thus, by Lemma 4.1, we have

$$(\log_{\mathcal{G}} \circ h)^{\sigma^{-n}}(\pi_n) \equiv \ell_n(c_n) \mod p\mathcal{O}_{K_n}^{\oplus d}.$$

We define $x \in \mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})$ by

$$(x(\omega_i)) = \log_{\mathcal{G}} \circ h + pW[[T]]^{\oplus d}\,.$$

Here, recall that M is generated by L as a left $W[F, V]$-module. We put $z_n = (\hat{x}(\omega_i)^{\sigma^{-n}}(\pi_n)) \in K_n^{\oplus d}$ for $n \ge 1$ (see Proposition 3.1 for the definition of $\hat{x}$). Then we have

$$\begin{aligned} \mathrm{tr}_{n+m/n} z_{n+m} + b_{m-1}\mathrm{tr}_{n+m-1/n} z_{n+m-1} + \cdots + b_0 z_n = 0\,, \\ z_n \equiv (\log_{\mathcal{G}} \circ h)^{\sigma^{-n}}(\pi_n) \equiv \ell_n(c_n) \mod p\mathcal{O}_{K_n}^{\oplus d} \end{aligned}$$

for all $n \ge 1$. If we put $y_n = z_n - \ell_n(c_n) \in p\mathcal{O}_{K_n}^{\oplus d}$, then we have $y_n = 0$ for all $n \ge 1$ by Proposition 4.4. We put $f(T) = \iota(x) = \exp_{\mathcal{G}} \circ(\hat{x}(\omega_i)) \in \mathcal{G}(W[[T]])$. Then, we have

$$\begin{aligned} \ell_n(f^{\sigma^{-n}}(\pi_n)) = z_n = \ell_n(c_n)\,, \\ f^{\sigma^{-n}}(\pi_n) \equiv h^{\sigma^{-n}}(\pi_n) \equiv c_n \mod p\mathcal{O}_{K_n}^{\oplus d} \end{aligned}$$

for all $n \ge 1$. Therefore, we have $f^{\sigma^{-n}}(\pi_n) = c_n$ for all $n \ge 1$ by Lemma 4.1.

In the following, we treat the case $p = 2$. By the congruences in (b) of (2), as in the case $p > 2$, we can take an element $h(T)$ of $W[[T]]^{\oplus d}$ such that $h(0) = 0$ and

$$h^{\sigma^{-n}}(\pi_n) \equiv [2^r]_{\mathcal{G}^{\sigma^{-n}}} c_n \mod 2\mathcal{O}_{K_n}^{\oplus d}$$

for all $n \ge 1$. Therefore, we have

$$\begin{aligned} ([2]_{\mathcal{G}}h)^{\sigma^{-n}}(\pi_n) \equiv [2^{r+1}]_{\mathcal{G}^{\sigma^{-n}}} c_n \mod 4\mathcal{O}_{K_n}^{\oplus d}\,, \\ \ell_n([2]_{\mathcal{G}}h)^{\sigma^{-n}}(\pi_n) \equiv \ell_n([2^{r+1}]_{\mathcal{G}^{\sigma^{-n}}} c_n) \mod 4\mathcal{O}_{K_n}^{\oplus d} \end{aligned}$$

for all $n \geq 1$. We define $x \in \mathrm{Hom}_{W[F,V]}(M, \overline{\mathcal{P}})$ by

$$(x(\omega_i)) = \log_{\mathcal{G}} \circ h + 2W[[T]]^{\oplus d}\,.$$

Then, we have

$$(2\hat{x}(\omega_i)) \equiv 2\log_{\mathcal{G}} \circ h = \log_{\mathcal{G}} \circ([2]_{\mathcal{G}} h) \mod 4W[[T]]^{\oplus d}\,. \tag{4.9}$$

If we put $z_n = (2\hat{x}(\omega_i)^{\sigma^{-n}}(\pi_n)) \in K_n^{\oplus d}$ for $n \geq 1$, then we have $z_n = \ell_n([2^{r+1}]_{\mathcal{G}^{\sigma^{-n}}} c_n)$ for all $n \geq 1$ by Proposition 4.4. We put $f(T) = \exp_{\mathcal{G}} \circ(2\hat{x}(\omega_i)) \in \mathcal{G}(W[[T]])$. By (4.9), we have $f(T) \equiv [2]_{\mathcal{G}} h(T) \mod 4W[[T]]^{\oplus d}$. Therefore, we have

$$\ell_n(f^{\sigma^{-n}}(\pi_n)) = z_n = \ell_n([2^{r+1}]_{\mathcal{G}^{\sigma^{-n}}} c_n)\,,$$
$$f^{\sigma^{-n}}(\pi_n) \equiv [2^{r+1}]_{\mathcal{G}^{\sigma^{-n}}} c_n \mod 4\mathcal{O}_{K_n}^{\oplus d}\,.$$

Hence, we have $f^{\sigma^{-n}}(\pi_n) = [2^{r+1}]_{\mathcal{G}^{\sigma^{-n}}} c_n$ for all $n \geq 1$. □

REMARK 4.8. In the proof of the case $p = 2$, we have also shown that if (c_n) satisfies the condition (b) for some r, then there exists $f \in \mathcal{G}(W[[T]])$ such that $f^{\sigma^{-n}}(\pi_n) = [2^{r+1}]c_n$ for all $n \geq 1$.

We denote by $N\mathcal{G}$ the set of Q-norm systems satisfying (b). In the proof of our main theorem, we have proved the following theorem.

THEOREM 4.9. *In the case $p > 2$, the image of the map*

$$\iota\,(\mathcal{G}(k[[T]])) \to \prod_n \mathcal{G}^{\sigma^{-n}}(\mathfrak{m}_n)\,, \quad f(T) \mapsto (f^{\sigma^{-n}}(\pi_n))_n\,,$$

is $N\mathcal{G}$. In the case $p = 2$, the map $\iota\,(\mathcal{G}(k[[T]]) \otimes \boldsymbol{Q}_2) \to N\mathcal{G} \otimes \boldsymbol{Q}_2$ is surjective.

REMARK 4.10. (1) Since the map $\mathcal{G}(W[[T]]) \to \prod_n \mathcal{G}^{\sigma^{-n}}(\mathfrak{m}_n)$ is injective by the p-adic Weierstrass preparation theorem, we conclude $\iota\,(\mathcal{G}(k[[T]])) \cong N\mathcal{G}$ in the case $p > 2$. In the case $p = 2$, we also conclude $\iota\,(\mathcal{G}(k[[T]]) \otimes \boldsymbol{Q}_2) \cong N\mathcal{G} \otimes \boldsymbol{Q}_2$.

(2) See Example 3.4 for the case $\mathcal{G} = \hat{\boldsymbol{G}}_m$ of Theorem 4.9.

(3) Since these maps are independent of the fixed Q, the set $N\mathcal{G}$ is also independent of the choice of Q. Thus, as in [6], we may call a Q-norm system satisfying (b) an admissible norm system with dropping Q.

REFERENCES

[1] R. COLEMAN, Division values in local fields, Invent. Math. 53 (1979), 91–116.

[2] J.-M. FONTAINE, Groupes p-divisibles sur les corps locaux, Astérisque, No. 47–48, Société Mathématique de France, Paris, 1977.

[3] T. HONDA, On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970), 213–246.

[4] H. KNOSPE, Iwasawa-theory of abelian varieties at primes of non-ordinary reduction, Manuscripta Math. 87 (1995), 225–258.

[5] S. KOBAYASHI, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. 152 (2003), 1–36.

[6] S. KOBAYASHI, The p-adic Gross-Zagier formula for elliptic curves at supersingular primes, Invent. Math. 191 (2013), 527–629.

[7] B. PERRIN-RIOU, Théorie d'Iwasawa p-adique locale et globale, Invent. Math. 99 (1990), 247–292.
[8] B. PERRIN-RIOU, Théorie d'Iwasawa des représentations p-adiques sur un corps local, Invent. Math. 115 (1994), 81–149.
[9] J. TATE, p-divisible groups, Proc. Conf. Local Fields, 158–183, Springer, Berlin, 1967.

MATHEMATICAL INSTITUTE
TOHOKU UNIVERSITY
SENDAI 980–8578
JAPAN

E-mail address: sb0m07@math.tohoku.ac.jp