A remark on the norm of a formal group over $\mathbf{Z}_p$

By Yoshichika Iizuka

Department of Mathematics, Gakushuin University
1-5-1, Mejiro, Toshima-ku, Tokyo 171-8588
(Communicated by Shigefumi Mori, m. j. a., May 12, 2004)

Abstract: Let $h \geq 2$ be an integer and F a formal group over $\mathbf{Z}_p$ of Honda type $p + X^h$. The aim of this paper is to calculate the index of the image of the norm of F in the local cyclotomic fields by following Kobayashi's method ([1]). Here we use the property of certain subgroups which we call norm subgroups.

Key words: Formal group; norm subgroup.

1. Introduction. In [1], Kobayashi shed new light on the study of Iwasawa theory for elliptic curves at good supersingular primes, by giving another formulation of the main conjecture for such curves. There, the formal groups of height 2 play an important role.

We fix p an odd prime number. For a non-negative integer n, we denote a p^n-th root of unity by ζ_{p^n} which satisfies $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ and $\zeta_{p^0} = 1$. Let $k_0 := \mathbf{Q}_p$, $k_n := \mathbf{Q}_p(\zeta_{p^n})$ for each $n \geq 1$, $\mathfrak{m}_0 := p\mathbf{Z}_p$ and $\mathfrak{m}_n$ the maximal ideal of the integer ring of k_n for each $n \geq 1$. Put $G_n := \mathrm{Gal}(k_n/\mathbf{Q}_p)$.

For an integer $h \geq 2$, we consider a formal group F of Honda type $p + X^h$, whose logarithm is given by

$$\log_F(X) = \sum_{k=0}^{\infty} (-1)^k \frac{(X+1)^{p^{hk}} - 1}{p^k}$$

(cf. [1, §§8.1]). Let $F(\mathfrak{m}_n)$ denote the group defined by the formal group F on the maximal ideal $\mathfrak{m}_n$.

Let $\Delta := \mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$ and $\widehat{\Delta}$ the group of characters from Δ to $\mathbf{Z}_p^\times$. For $\eta \in \widehat{\Delta}$ and a $\mathbf{Z}_p[\Delta]$-module M, we put $M^\eta := \varepsilon_\eta M$, where $\varepsilon_\eta := \frac{1}{|\Delta|} \sum_{\tau \in \Delta} \eta(\tau)\eta^{-1}$.

For $n \geq 0$, $C_F(\mathfrak{m}_n)$ denotes the norm subgroup, which will be defined in Definition 2.5. Let $q_n := \mathrm{rank}_{\mathbf{Z}_p} C_F(\mathfrak{m}_n)$ and $q_n^\eta := \mathrm{rank}_{\mathbf{Z}_p} C_F(\mathfrak{m}_n)^\eta$. The main result in this paper is the following.

Theorem 1.1. *For $n \geq 1$,*

(i) $\dim_{\mathbf{F}_p} F(\mathfrak{m}_{n-1})/N^F_{n/(n-1)}F(\mathfrak{m}_n) = \phi(p^n) - q_n$,

(ii) $\dim_{\mathbf{F}_p} F(\mathfrak{m}_{n-1})^\eta/N^F_{n/(n-1)}F(\mathfrak{m}_n)^\eta = p^{n-1} - q_n^\eta$.

One can calculate the rank q_n of the norm subgroup $C_F(\mathfrak{m}_n)$ as the following.

Proposition 1.2. (i) *Let ϕ be the Euler function. Then $q_0 = 1$, $q_n + \cdots + q_0 = \phi(p^n) + n$ if $1 \leq n \leq h-2$, and $q_n + \cdots + q_{n-h+1} = \phi(p^n) + (h-1)$ for any $n \geq h-1$.*

(ii) *If η is non-trivial, then $q_0^\eta = 0$, $q_n^\eta + \cdots + q_0^\eta = p^{n-1}$ if $1 \leq n \leq h-2$, and $q_n^\eta + \cdots + q_{n-h+1}^\eta = p^{n-1}$ for any $n \geq h-1$.*

(iii) *If η is trivial, then $q_0^1 = 1$, $q_n^1 + \cdots + q_0^1 = p^{n-1} + n$ if $1 \leq n \leq h-2$, and $q_n^1 + \cdots + q_{n-h+1}^1 = p^{n-1} + (h-1)$ for any $n \geq h-1$.*

Kobayashi remarks this main result in the case where $h = 2$ ([1, Remark 8.14], see also [2]). Kuriya also studies about the index of the norm of F in this direction by a different method ([3]).

We note that if one would like to generalize Kobayashi's result to abelian varieties, one need to study formal groups of higher dimension, instead of the above formal groups.

2. Norm subgroup.

Proposition 2.1. *Let $h \geq 1$ be an integer. Let F be a formal group whose Honda type is $p + X^h$. $[-p] : F \to F$ denotes the multiplication by $-p$ map of the formal group F. Then,*

(i) $[-p](X) \equiv -pX \bmod \deg 2$,

(ii) $[-p](X) \equiv X^{p^h} \bmod p\mathbf{Z}_p[[X]]$.

Proof. The assertion (i) follows from general properties of formal groups. Let us show the assertion (ii).

Let $\mathcal{P}$ be the $\mathbf{Z}_p$-submodule of $\mathbf{Q}_p[[X]]$ consisting of the elements $\sum_{k=1}^\infty a_k X^k$ satisfying $ka_k \in \mathbf{Z}_p$ for all k. We define an endomorphism φ of $\mathcal{P}$ by

$$\varphi\big(f(X)\big) := f\big((X+1)^p - 1\big)$$

2000 Mathematics Subject Classification. Primary 11S31; Secondary 14L05.

for $f \in \mathcal{P}$. We denote the n-iterated composition of the endomorphism φ by $\varphi^{(n)}$.

By the way of construction of the formal group which corresponds to the Honda type $p + X^h$,

$$[-p](X) = \exp_F(-p \cdot \log_F(X)) \in \mathbf{Z}_p[[X]].$$

Since

$$\begin{aligned}\varphi^{(h)} \circ \log_F(X) &= \log_F(\varphi^{(h)}(X)) \\ &= \sum_{k=0}^{\infty}(-1)^k \frac{(X+1)^{p^{h(k+1)}} - 1}{p^k}\end{aligned}$$

and

$$p \cdot \log_F(X) = pX - \sum_{k=0}^{\infty}(-1)^k \frac{(X+1)^{p^{h(k+1)}} - 1}{p^k},$$

we have

$$\begin{aligned}&\exp_F(-p \cdot \log_F(X)) \\ &\quad \equiv \exp_F(\varphi^{(h)} \circ \log_F(X)) \bmod p\mathbf{Z}_p[[X]] \\ &\quad = \exp_F(\log_F(\varphi^{(h)}(X))) \\ &\quad = \varphi^{(h)}(X).\end{aligned}$$

Further, we have

$$\varphi^{(h)}(X) = (X+1)^{p^h} - 1 \equiv X^{p^h} \bmod p\mathbf{Z}_p[[X]].$$

Therefore,

$$[-p](X) \equiv X^{p^h} \bmod p\mathbf{Z}_p[[X]].$$

□

From the Lubin-Tate theory, $F(\mathfrak{m}_n)$ has no torsion point ([1, §§8.3]). Thus, the logarithm $\log_F$ is injective. This implies that for any integers m, n with $0 \le m \le n$, $\log_F F(\mathfrak{m}_n) \cap k_{n-m} = \log_F F(\mathfrak{m}_{n-m})$.

Definition 2.2. Let F be a formal group over $\mathbf{Z}_p$. Let m, n be integers with $0 \le m \le n$. The norm of a formal group F is the homomorphism $N^F_{n/m} : F(\mathfrak{m}_n) \to F(\mathfrak{m}_m)$ defined by

$$N^F_{n/m}(x) := \sum_{\sigma \in \mathrm{Gal}(k_n/k_m)} x^\sigma$$

for $x \in F(\mathfrak{m}_n)$, where $\sum$ denotes the sum by the addition law of F.

Since $\log_F : F(\mathfrak{m}_0) \to \mathfrak{m}_0$ is an isomorphism between groups, there exists a unique element $\varepsilon \in F(\mathfrak{m}_0)$ such that $\log_F(\varepsilon) = p/(p+1)$. Put

$$c_n := \begin{cases} (\zeta_{p^n} - 1) +_F \varepsilon & \text{for } n \ge 1, \\ \varepsilon & \text{for } -h+2 \le n \le 0, \\ [2]\,\varepsilon & \text{for } n = -h+1. \end{cases}$$

Proposition 2.3. $N^F_{n/(n-1)}(c_n) = -_F c_{n-h}$.

Proof. By direct calculations, we have

$$Tr_{n/(n-1)} \log_F(c_n) = -\log_F(c_{n-h})$$

where $Tr_{n/(n-1)} : k_n \to k_{n-1}$ is the trace map. Since $Tr_{n/(n-1)} \circ \log_F = \log_F \circ N_{n/(n-1)}$ and $\log_F$ is injective, we have the desired formula. □

Proposition 2.4. *Let m be an integer with $1 \le m \le h-1$. Then*

(i) $F(\mathfrak{m}_n)/F(\mathfrak{m}_{n-m}) \cong \mathfrak{m}_n/\mathfrak{m}_{n-m}$.

(ii) $F(\mathfrak{m}_n)/F(\mathfrak{m}_{n-m})$ *is generated by* $\bigcup_{k=n-m+1}^{n}\{c_k^\sigma +_F F(\mathfrak{m}_{n-m}) \mid \sigma \in G_k\}$.

Proof. Since $\log_F$ is injective, $F(\mathfrak{m}_n)$ is isomorphic to $\log_F F(\mathfrak{m}_n)$ for each $n \ge 0$. Therefore, to prove (i), it suffices to show that

$$\log_F F(\mathfrak{m}_n)/\log_F F(\mathfrak{m}_{n-m}) \cong \mathfrak{m}_n/\mathfrak{m}_{n-m}.$$

First, we have

$$\begin{aligned}&\log_F F(\mathfrak{m}_n)/\log_F F(\mathfrak{m}_{n-m}) \\ &\quad = \log_F F(\mathfrak{m}_n)/(\log_F F(\mathfrak{m}_n) \cap k_{n-m}) \\ &\quad \hookrightarrow (\mathfrak{m}_n + k_{n-m})/k_{n-m} \\ &\quad \cong \mathfrak{m}_n/\mathfrak{m}_{n-m},\end{aligned}$$

by sending

$$x +_F \log_F F(\mathfrak{m}_{n-m}) \mapsto x + k_{n-m},$$

and

$$y + k_{n-m} \mapsto y + \mathfrak{m}_{n-m}.$$

Let $c'_n := \log_F(c_n)$. We can see that $c'_n \equiv \zeta_{p^n} - 1 \bmod k_{n-m}$. Hence, we have ${c'_n}^\sigma \equiv \zeta_{p^n}^\sigma - 1 \bmod k_{n-m}$ for each $\sigma \in G_n$.

Since it is well-known that $\mathfrak{m}_n/\mathfrak{m}_{n-m}$ is generated by

$$\{(1-\zeta) + \mathfrak{m}_{n-m} \mid \zeta \text{ is a primitive } p^i\text{-th root of unity } (n-m < i \le n)\},$$

$(\mathfrak{m}_n + k_{n-m})/k_{n-m}$ is generated by

$$\bigcup_{k=n-m+1}^{n}\{{c'_k}^\sigma + k_{n-m} \mid \sigma \in G_k\}.$$

Hence, the above injection

$$\log_F F(\mathfrak{m}_n)/\log_F F(\mathfrak{m}_{n-m}) \hookrightarrow (\mathfrak{m}_n + k_{n-m})/k_{n-m}$$

is surjective, so we have (i). This immediately implies (ii). □

Definition 2.5. For an integer $n \ge 0$, we define the n-th norm subgroup by

$$C_F(\mathfrak{m}_n) := \{x \in F(\mathfrak{m}_n) \mid N^F_{n/m}\, x \in F(\mathfrak{m}_{m-h+1}) \text{ for all } m \equiv n-1 \bmod h,\ 0 \le m \le n\}.$$

Here, we put $F(\mathfrak{m}_k) := F(\mathfrak{m}_0)$ when $k \le 0$.

Proposition 2.6. *For any $n \ge 0$,*

$$F(\mathfrak{m}_n) = C_F(\mathfrak{m}_n) +_F \cdots +_F C_F(\mathfrak{m}_{n-h+1}).$$

Here, we put $C_F(\mathfrak{m}_k) := F(\mathfrak{m}_0)$ for $k < 0$.

Proof. Let m be an integer such that $1 \le m \le h-1$. By Proposition 2.4, $\bigcup_{k=n-m+1}^{n}\{c_k^\sigma + F(\mathfrak{m}_{n-m}) \mid \sigma \in G_k\}$ generates $F(\mathfrak{m}_n)/F(\mathfrak{m}_{n-m})$. Since $\{c_n^\sigma \mid \sigma \in G_n\} \subseteq C_F(\mathfrak{m}_n)$,

$$F(\mathfrak{m}_n) = C_F(\mathfrak{m}_n) +_F \cdots +_F C_F(\mathfrak{m}_{n-m+1}) +_F F(\mathfrak{m}_{n-m}).$$

Therefore, the statement is true for $n = 0, 1, 2, \ldots, h-1$.

Suppose that the statement is true for all integers less than or equal to $n-1$. Then,

$$F(\mathfrak{m}_{n-1}) = C_F(\mathfrak{m}_{n-1}) +_F \cdots +_F C_F(\mathfrak{m}_{n-h}).$$

Hence,

$$\begin{aligned} F(\mathfrak{m}_n) &= C_F(\mathfrak{m}_n) +_F F(\mathfrak{m}_{n-1}) \\ &= C_F(\mathfrak{m}_n) \\ &\quad +_F C_F(\mathfrak{m}_{n-1}) +_F \cdots +_F C_F(\mathfrak{m}_{n-h}). \end{aligned}$$

Since $C_F(\mathfrak{m}_{n-h}) \subseteq C_F(\mathfrak{m}_n)$, we have

$$F(\mathfrak{m}_n) = C_F(\mathfrak{m}_n) +_F \cdots +_F C_F(\mathfrak{m}_{n-h+1}).$$

□

Proposition 2.7. *For any $n \ge 1$ and $1 \le k \le \min\{n, h-1\}$,*

$$\big(C_F(\mathfrak{m}_n) +_F \cdots +_F C_F(\mathfrak{m}_{n-k+1})\big) \cap C_F(\mathfrak{m}_{n-k}) = F(\mathfrak{m}_0).$$

Proof. It suffices to check that the left hand side is contained in the right hand side. Let $x \in \big(C_F(\mathfrak{m}_n) +_F \cdots +_F C_F(\mathfrak{m}_{n-k+1})\big) \cap C_F(\mathfrak{m}_{n-k})$. To show $x \in F(\mathfrak{m}_0)$, we suppose that there exists an integer m such that $x \in F(\mathfrak{m}_m) \setminus F(\mathfrak{m}_{m-1})$ and $1 \le m \le n-k$, and deduce a contradiction.

Let i be an integer with $1 \le i \le h-1$. If $m \equiv n-k-i \bmod h$,

$$[p^{n-(m+i-1)}]x = N^F_{n/(m+i-1)}\, x$$

since $x \in C_F(\mathfrak{m}_m)$. Moreover,

$$\begin{aligned} N^F_{n/(m+i-1)}\, x &= N^F_{(n-k)/(m+i-1)} \circ N^F_{n/(n-k)}\, x \\ &= [p^k]\big(N^F_{(n-k)/(m+i-1)}\, x\big) \end{aligned}$$

is contained in $F(\mathfrak{m}_{m+i-h})$ since $x \in C_F(\mathfrak{m}_{n-k})$ and $m+i-1 \equiv n-k-1 \bmod h$. Therefore, we have

$$[p^{n-(m+i-1)}]x \in F(\mathfrak{m}_{m+i-h}).$$

If $m \equiv n-k \bmod h$, there exist $x_l \in C_F(\mathfrak{m}_l)$ for $n-k+1 \le l \le n$ such that

$$\begin{aligned} [p^{n-m}]x &= N^F_{n/m}\, x \\ &= N^F_{n/m}\, x_n +_F \cdots +_F N^F_{n/m}\, x_{n-k+1} \end{aligned}$$

since $x \in C_F(\mathfrak{m}_n) +_F \cdots +_F C_F(\mathfrak{m}_{n-k+1})$. Moreover, for $j = 0, 1, \ldots, k-1$,

$$\begin{aligned} &N^F_{(m+k-1-j)/m} \circ N^F_{(n-j)/(m+k-1-j)} \circ N^F_{n/(n-j)}\, x_{n-j} \\ &= N^F_{(m+k-1-j)/m} \circ N^F_{(n-j)/(m+k-1-j)} \circ [p^j] x_{n-j} \\ &= N^F_{(m+k-1-j)/m} \circ [p^j] \circ N^F_{(n-j)/(m+k-1-j)}\, x_{n-j} \\ &\in N^F_{(m+k-1-j)/m} \circ [p^j]\big(F(\mathfrak{m}_{m+k-h-j})\big) \\ &\subseteq F(\mathfrak{m}_{m-h}). \end{aligned}$$

Hence

$$[p^{n-m}]x \in F(\mathfrak{m}_{m-1}).$$

Therefore, there exists an integer $n_0 \ge 1$ such that

$$[p^{n_0}]x \in F(\mathfrak{m}_{m-1}).$$

Then, for all $\sigma \in \mathrm{Gal}(k_m/k_{m-1})$,

$$[p^{n_0}](x^\sigma -_F x) = 0.$$

Since $F(\mathfrak{m}_n)$ has no p-torsion, we have we have $x^\sigma = x$ for all $\sigma \in \mathrm{Gal}(k_m/k_{m-1})$, so $x \in F(\mathfrak{m}_{m-1})$. □

Proposition 2.8. *$C_F(\mathfrak{m}_n)$ is generated by $\{c_n^\sigma \mid \sigma \in G_n\}$ and $F(\mathfrak{m}_0)$.*

Proof. This statement is proved by induction on n. The statement is clear for $n = 0$ since $C_F(\mathfrak{m}_0) = F(\mathfrak{m}_0)$. Let n be an integer with $n \ge 1$ and let $C'_F(\mathfrak{m}_n)$ the subgroup of $C_F(\mathfrak{m}_n)$ generated by $\{c_n^\sigma \mid \sigma \in G_n\}$ and $F(\mathfrak{m}_0)$. By Proposition 2.4, $F(\mathfrak{m}_n)/F(\mathfrak{m}_{n-1})$ is generated by $\{c_n^\sigma +_F F(\mathfrak{m}_{n-1}) \mid \sigma \in G_n\}$. Hence,

$$F(\mathfrak{m}_n) = C'_F(\mathfrak{m}_n) +_F F(\mathfrak{m}_{n-1}).$$

By Proposition 2.6,

$$F(\mathfrak{m}_n) = C'_F(\mathfrak{m}_n) +_F C_F(\mathfrak{m}_{n-1}) +_F \cdots +_F C_F(\mathfrak{m}_{n-h}).$$

By the assumption of the induction,

$$C'_F(\mathfrak{m}_{n-h}) = C_F(\mathfrak{m}_{n-h}).$$

Moreover, since $c^\sigma_{n-h} = -N^F_{n/(n-1)}\, c^\sigma_n$ by Proposition 2.3,

$$C'_F(\mathfrak{m}_{n-h}) \subseteq C'_F(\mathfrak{m}_n).$$

Hence

$$F(\mathfrak{m}_n) = C'_F(\mathfrak{m}_n) +_F C_F(\mathfrak{m}_{n-1}) \\ +_F \cdots +_F C_F(\mathfrak{m}_{n-h+1}).$$

For $x \in C_F(\mathfrak{m}_n)$,

$$x = x_n +_F y_{n-1} +_F \cdots +_F y_{n-h+1},$$

where $x_n \in C'_F(\mathfrak{m}_n)$ and $y_i \in C_F(\mathfrak{m}_i)$. Then,

$$\begin{aligned} y_{n-h+1} &= (x -_F x_n) -_F y_{n-1} -_F \cdots -_F y_{n-h+2} \\ &\in \big(C_F(\mathfrak{m}_n) +_F C_F(\mathfrak{m}_{n-1}) +_F \cdots \\ &\qquad +_F C_F(\mathfrak{m}_{n-h+2})\big) \cap C_F(\mathfrak{m}_{n-h+1}). \end{aligned}$$

By Proposition 2.7, we have $y_{n-h+1} \in F(\mathfrak{m}_0)$. Then

$$x = x'_n +_F y_{n-1} +_F \cdots +_F y_{n-h+2}$$

where $x'_n \in C'_F(\mathfrak{m}_n)$, $y_i \in C_F(\mathfrak{m}_i)$, and we set $x'_n := x_n + y_{n-h+1}$. Repeating this process, we have successively $y_{n-h+2} \in F(\mathfrak{m}_0), \ldots, y_{n-1} \in F(\mathfrak{m}_0)$, and finally, we have $x \in C'_F(\mathfrak{m}_n)$. Hence $C_F(\mathfrak{m}_n) = C'_F(\mathfrak{m}_n)$. □

3. Proof of main result.

Proposition 3.1. *Let $h \geq 2$ be an integer. Let F be the formal group which is of Honda type $p + X^h$.*

For $n \geq h-1$, the sequence

$$0 \to \bigoplus_{i=1}^{h-1} F(\mathfrak{m}_0) \xrightarrow{f} \bigoplus_{i=0}^{h-1} C_F(\mathfrak{m}_{n-i}) \xrightarrow{g} F(\mathfrak{m}_n) \to 0$$

is exact, where we define the maps f and g by

$$\begin{aligned} &f(x_{n-1}, x_{n-2}, \ldots, x_{n-h+1}) \\ &\quad := (-_F x_{n-1}, x_{n-1} -_F x_{n-2}, \\ &\qquad \ldots, x_{n-h+2} -_F x_{n-h+1}, x_{n-h+1}), \\ &g(x_n, x_{n-1}, \ldots, x_{n-h+1}) \\ &\quad := \sum_{i=0}^{h-1} x_{n-i}. \end{aligned}$$

Proof. By Proposition 2.6, the sequence

$$0 \to \ker g \xrightarrow{\iota} \bigoplus_{i=0}^{h-1} C_F(\mathfrak{m}_{n-i}) \xrightarrow{g} F(\mathfrak{m}_n) \to 0$$

is exact. If $(x_n, x_{n-1}, \ldots, x_{n-h+1}) \in \ker g$, then

$$\begin{aligned} x_{n-h+1} &= -_F \sum_{i=0}^{h-2} x_{n-i} \in F(\mathfrak{m}_0), \\ x_{n-h+2} + x_{n-h+1} &= -_F \sum_{i=0}^{h-3} x_{n-i} \in F(\mathfrak{m}_0), \\ &\cdots\cdots \\ \sum_{i=1}^{h-1} x_{n-i} &= -_F x_n \in F(\mathfrak{m}_0) \end{aligned}$$

by Proposition 2.7. Therefore, we have a map

$$\begin{aligned} &\ker g \to \bigoplus_{i=1}^{h-1} F(\mathfrak{m}_0), \\ &(x_n, \ldots, x_{n-h+2}, x_{n-h+1}) \\ &\quad \mapsto \left(\sum_{i=1}^{h-1} x_{n-i}, \sum_{i=2}^{h-1} x_{n-i}, \right. \\ &\qquad \left. \ldots, x_{n-h+2} +_F x_{n-h+1}, x_{n-h+1}\right). \end{aligned}$$

We see that this map is an isomorphism because the following map

$$\begin{aligned} &f' : \bigoplus_{i=1}^{h-1} F(\mathfrak{m}_0) \to \ker g, \\ &(y_{n-1}, \ldots, y_{n-h+2}, y_{n-h+1}) \\ &\quad \mapsto (-_F y_{n-1}, y_{n-1} -_F y_{n-2}, \\ &\qquad \ldots, y_{n-h+2} -_F y_{n-h+1}, y_{n-h+1}) \end{aligned}$$

gives the inverse map. Note that this is well-defined since $F(\mathfrak{m}_0) \subseteq C_F(\mathfrak{m}_n)$ for all $n \geq 0$. Hence, by putting $f := \iota \circ f'$, we have the desired exact sequence. □

Remark 3.2. In the same way, we can show that for each $1 \leq n \leq h-2$, the sequence

$$0 \to \bigoplus_{i=1}^{n} F(\mathfrak{m}_0) \xrightarrow{f} \bigoplus_{i=0}^{n} C_F(\mathfrak{m}_{n-i}) \xrightarrow{g} F(\mathfrak{m}_n) \to 0$$

is exact, where we define the maps f and g by

$$\begin{aligned} &f(x_{n-1}, x_{n-2}, \ldots, x_0) \\ &\quad := (-_F x_{n-1}, x_{n-1} -_F x_{n-2}, \\ &\qquad \ldots, x_1 -_F x_0, x_0), \\ &g(x_n, x_{n-1}, \ldots, x_0) \\ &\quad := \sum_{i=0}^{n} x_{n-i}. \end{aligned}$$

Proposition 3.3. *For $n \geq h-1$, the sequence*

$$0 \to \bigoplus_{i=1}^{h-1} \frac{F(\mathfrak{m}_0)}{[p]F(\mathfrak{m}_0)} \xrightarrow{\tilde{f}} \bigoplus_{i=1}^{h-1} \frac{C_F(\mathfrak{m}_{n-i})}{[p]C_F(\mathfrak{m}_{n-i})} \xrightarrow{\tilde{g}} \frac{F(\mathfrak{m}_{n-1})}{N^F_{n/(n-1)}F(\mathfrak{m}_n)} \to 0$$

is exact, where the maps $\widetilde{f}$ and $\widetilde{g}$ are induced by f and g at the exact sequence in Proposition 3.1.

Proof. We define the homomorphism

$$\widetilde{N} : \left(\bigoplus_{i=1}^{h-1} C_F(\mathfrak{m}_{n-i})\right) \oplus C_F(\mathfrak{m}_n) \to \bigoplus_{i=1}^{h} C_F(\mathfrak{m}_{n-i})$$

by

$$\begin{aligned}\widetilde{N}&(x_{n-1}, \dots, x_{n-h+1}, x_n)\\ &:= (N_{n/(n-1)}x_{n-1}, \dots,\\ &\qquad N_{n/(n-1)}x_{n-h+1}, N_{n/(n-1)}x_n)\\ &= ([p]x_{n-1}, \dots, [p]x_{n-h+1}, N_{n/(n-1)}x_n).\end{aligned}$$

Furthermore, we put

$$\begin{aligned}T : \bigoplus_{i=0}^{h-1} C_F(\mathfrak{m}_{n-i}) &\to \left(\bigoplus_{i=1}^{h-1} C_F(\mathfrak{m}_{n-i})\right) \oplus C_F(\mathfrak{m}_n),\\ (x_n, x_{n-1}, \dots, x_{n-h+1}) &\mapsto (x_{n-1}, \dots, x_{n-h+1}, x_n),\end{aligned}$$

and

$$\begin{aligned}T' : \bigoplus_{i=1}^{h-1} F(\mathfrak{m}_0) &\to \bigoplus_{i=1}^{h-1} F(\mathfrak{m}_0),\\ (x_{n-1}, x_{n-2}, \dots, x_{n-h+1}) &\mapsto (x_{n-2} -_F x_{n-1}, x_{n-3} -_F x_{n-1},\\ &\qquad \dots, x_{n-h+1} -_F x_{n-1}, -_F x_{n-1}).\end{aligned}$$

By a direct calculation, we can check

$$f \circ \widetilde{N} \circ T' = \widetilde{N} \circ T \circ f$$

and

$$g \circ \widetilde{N} \circ T = N^F_{n/(n-1)} \circ g.$$

Since T' is an isomorphism,

$$\widetilde{N} \circ T'\left(\bigoplus_{i=1}^{h-1} F(\mathfrak{m}_0)\right) = \widetilde{N}\left(\bigoplus_{i=1}^{h-1} F(\mathfrak{m}_0)\right).$$

Hence

$$\operatorname{coker} \widetilde{N} \circ T' = \bigoplus_{i=1}^{h-1} \frac{F(\mathfrak{m}_0)}{[p]F(\mathfrak{m}_0)}.$$

Since T is an isomorphism,

$$\widetilde{N} \circ T\left(\bigoplus_{i=0}^{h-1} C_F(\mathfrak{m}_{n-i})\right) = \widetilde{N}\left(\bigoplus_{i=0}^{h-1} C_F(\mathfrak{m}_{n-i})\right).$$

If $i \geq 1$, the norm map $N_{n/(n-1)}$ on $C_F(\mathfrak{m}_{n-i})$ is multiplication-by-p map. Furthermore, we have $N^F_{n/(n-1)}C_F(\mathfrak{m}_n) = C_F(\mathfrak{m}_{n-h})$ by Proposition 2.3 and Proposition 2.8. Hence

$$\operatorname{coker} \widetilde{N} \circ T = \bigoplus_{i=1}^{h-1} \frac{C_F(\mathfrak{m}_{n-i})}{[p]C_F(\mathfrak{m}_{n-i})}.$$

By Proposition 3.1 and the snake lemma, the sequence

$$\bigoplus_{i=1}^{h-1} \frac{F(\mathfrak{m}_0)}{[p]F(\mathfrak{m}_0)} \xrightarrow{\tilde{f}} \bigoplus_{i=1}^{h-1} \frac{C_F(\mathfrak{m}_{n-i})}{[p]C_F(\mathfrak{m}_{n-i})} \xrightarrow{\tilde{g}} \frac{F(\mathfrak{m}_{n-1})}{N^F_{n/(n-1)}F(\mathfrak{m}_n)} \to 0$$

is exact. In order to show that $\widetilde{f}$ is an injection, suppose that $(x_{n-1}, \dots, x_{n-h+1}) +_F \bigoplus_{i=1}^{h-1}[p]F(\mathfrak{m}_0) \in \ker \widetilde{f}$. Since $F(\mathfrak{m}_n)$ has no torsion point, $[p]C_F(\mathfrak{m}_n) \cap F(\mathfrak{m}_0) = [p]F(\mathfrak{m}_0)$ for each integer $n \geq 0$. Therefore,

$$\begin{aligned}&-_F x_{n-1} \in [p]C_F(\mathfrak{m}_{n-1}) \cap F(\mathfrak{m}_0) = [p]F(\mathfrak{m}_0),\\ &x_{n-1} -_F x_{n-2} \in [p]C_F(\mathfrak{m}_{n-2}) \cap F(\mathfrak{m}_0) = [p]F(\mathfrak{m}_0),\\ &\qquad \dots\dots\\ &x_{n-h+2} -_F x_{n-h+1}\\ &\qquad \in [p]C_F(\mathfrak{m}_{n-h+1}) \cap F(\mathfrak{m}_0) = [p]F(\mathfrak{m}_0).\end{aligned}$$

Then we have $x_{n-1} \in [p]F(\mathfrak{m}_0)$, $x_{n-2} \in [p]F(\mathfrak{m}_0), \dots, x_{n-h+1} \in [p]F(\mathfrak{m}_0)$ one after another. Hence $(x_{n-1}, \dots, x_{n-h+1}) \in \bigoplus_{i=1}^{h-1}[p]F(\mathfrak{m}_0)$. This shows that $\widetilde{f}$ is an injection. □

Remark 3.4. In the same way, we can show that for each $1 \leq n \leq h-2$, the sequence

$$0 \to \bigoplus_{i=1}^{n} \frac{F(\mathfrak{m}_0)}{[p]F(\mathfrak{m}_0)} \xrightarrow{\tilde{f}} \bigoplus_{i=1}^{n} \frac{C_F(\mathfrak{m}_{n-i})}{[p]C_F(\mathfrak{m}_{n-i})} \xrightarrow{\tilde{g}} \frac{F(\mathfrak{m}_{n-1})}{N^F_{n/(n-1)}F(\mathfrak{m}_n)} \to 0$$

is exact, where the maps $\widetilde{f}$ and $\widetilde{g}$ are induced by f and g at the exact sequence in Remark 3.2.

Proposition 1.2 follows from Proposition 3.1 and Remark 3.2 immediately.

Proof of Theorem 1.1. Since $F(\mathfrak{m}_n)$ has no torsion, we have

$$\begin{aligned}&\dim_{\mathbf{F}_p} C_F(\mathfrak{m}_{n-i})/[p]C_F(\mathfrak{m}_{n-i}) = \operatorname{rank}_{\mathbf{Z}_p} C_F(\mathfrak{m}_{n-i}),\\ &\dim_{\mathbf{F}_p} F(\mathfrak{m}_0)/[p]F(\mathfrak{m}_0) = \operatorname{rank}_{\mathbf{Z}_p} F(\mathfrak{m}_0).\end{aligned}$$

Then the desired result follows from the exact sequence in Proposition 3.3 and Proposition 1.2. □

Acknowledgements. The author wishes to thank Prof. S. Nakano for his warm encouragement. He is grateful to Dr. Y. Hachimori for his valuable suggestions to complete this study.

References

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

[2] Kurihara, M.: On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I. Invent. Math., **149**, 195–224 (2002).

[3] Kuriya, T.: On the norm maps of formal groups for $\mathbf{Z}_p$-extensions. (Preprint).