FORMAL GROUPS AND RELATIVE KUMMER THEORY

RINTARO KOZUMA

Abstract. We consider "relative" Kummer theory via formal groups, which gives refinement of Kummer theory over local fields.

1. Introduction

Kummer map of group cohomology is an injection

$$\delta : A^G/\phi(A^G) \longrightarrow H^1(G, \ker\phi),$$

where G is a profinite group, A is a G-module (with continuous action) and $\phi \in \mathrm{End}_G(A)$ is surjective. Let G be a Galois group $\mathrm{Gal}(\overline{K}/K)$ of a fixed separable closure $\overline{K}$ over a perfect field K. In the case where A is the multiplicative group $\overline{K}^*$ and ϕ is the multiplication by n map, the map δ is well-known as classical Kummer theory. In the case where A is the group $E(\overline{K})$ of rational points on an elliptic curve E defined over a field K and ϕ is an isogeny, the map δ gives rise to Kummer (descent) theory for elliptic curves. In the case where A is a group of units of a ring of integers in a field $\overline{K}$ and ϕ is the multiplication by n map, the map δ induces Kummer (descent) theory for groups of units. For each case, if K is a local field then A^G has a subgroup isomorphic to a formal group over the ring $\mathcal{O}_K$ of integers of K. In the present paper, we consider in general the case where A is a one-dimensional commutative formal group $\mathcal{F}$ over the ring $\mathcal{O}_K$ of integers of a local field K, $G = \mathrm{Gal}(\overline{K}/K)$ and ϕ is an isogeny over $\mathcal{O}_K$. This enables us to uniformly consider Kummer theory for certain subgroup of various A. Especially we focus on the system $\{(\mathcal{F}/\phi^m(\mathcal{F}))^i\}_{i,m}$ varying i, m through positive integers, where $(\mathcal{F}/\phi^m(\mathcal{F}))^i$ is the i-th module associated with the filtration of $\mathcal{F}$ (§4). The group structures of K^*, $E(K)$ and $\mathcal{O}_K^*$ over local fields are well-known (the case of elliptic curves is originally due to E. Lutz [7]). However, the algebraic connection among $\{(\mathcal{F}/\phi^m(\mathcal{F}))^i\}_{i,m}$ seems to have been not inquired in the literature. Here we give an answer, which provides precise information of the layer structure of the system $\{(\mathcal{F}/\phi^m(\mathcal{F}))^i \hookrightarrow H^1(G, \ker\phi^m))\}_{i,m}$ relatively and has an important application to Selmer groups ([4]).

This paper is organized as follows: Our main result is Theorem 4.1 in §4. We first set up notation used throughout the paper in §2. In §3, the valuation of division points on formal groups is determined, which plays an essential role in the proof of the main result.

2. General setting

Let K be a finite extension over the p-adic number field $\mathbb{Q}_p$, $\mathcal{O}_K$ the ring of integers of K with maximal ideal $\mathfrak{M}_K$ generated by a uniformizer π_K, $k_K = \mathcal{O}_K/\mathfrak{M}_K$ the residue field, and let $v_K : \overline{K} \to \mathbb{Q} \cup \{\infty\}$ be a normalized valuation on an algebraic closure $\overline{K}$ so that $v_K(\pi_K) = 1$.

Let $\mathcal{F}$ denote a one-dimensional commutative formal group over $\mathcal{O}_K$ ([2]). For any finite extension L over K, we can make $\mathfrak{M}_L$ into an abelian group by the law $x +_{\mathcal{F}} y := \mathcal{F}(x, y)$, $x, y \in \mathfrak{M}_L$. We denote this group by $\mathcal{F}(L)$. Since $\mathcal{F}(X, Y) \equiv X + Y \pmod{\deg 2}$, the filtration $\mathfrak{M}_L \supset \mathfrak{M}_L^2 \supset \mathfrak{M}_L^3 \cdots$ induces the filtration $\mathcal{F}(L) \supset \mathcal{F}(L)^2 \supset \mathcal{F}(L)^3 \cdots$, and there are isomorphisms $\mathcal{F}(L)^i/\mathcal{F}(L)^{i+1} \simeq \mathfrak{M}_L^i/\mathfrak{M}_L^{i+1} \simeq k_L$. If $a \in \mathbb{Q}\,(a > 0)$ then $\mathcal{F}(L)^a$ denotes $\mathcal{F}(L)^{\lceil a \rceil}$, where $\lceil a \rceil$ is the smallest integer $\geq a$. We will frequently use the identification $\mathcal{F}(L) \simeq \mathfrak{M}_L$ as underlying sets, and regard $\mathcal{F}(\overline{K})$ as the inductive limit $\varinjlim \mathcal{F}(L)$ of all finite extensions $L_{/K}$. We often write $\mathcal{F}$ instead of $\mathcal{F}(K)$ for simplicity.

Let ϕ denote an isogeny $\mathcal{F} \to \mathcal{G}$ over $\mathcal{O}_K$, where $\mathcal{G}_{/\mathcal{O}_K}$ is a one-dimensional commutative formal group; that is, a non-zero formal power series $\phi(X) = a_1X + a_2X^2 + \cdots \in \mathcal{O}_K[\![X]\!]$ satisfying $\phi(\mathcal{F}(X, Y)) = \mathcal{G}(\phi(X), \phi(Y))$. If $\phi(X) \notin \mathfrak{M}_K[\![x]\!]$ then there exists a non-negative integer h satisfying $\phi(X) \equiv a_{p^h}X^{p^h} + (\text{higher degree term}) \pmod{\mathfrak{M}_K}$ with $a_{p^h} \in \mathcal{O}_K^*$ ([5], [2]-I-§3). We denote the integer h by $ht(\phi)$, which is called the height of ϕ, and let $ht(\phi) = \infty$ in the case where $\phi(X) \in \mathfrak{M}_K[\![x]\!]$ (but we do not treat this case here). Let

$$c(\phi) := \frac{d\phi}{dX}(0) \quad (= a_1),$$

which plays an important role in the theory of one-dimensional commutative formal groups ([2]-IV-§1, [5]).

3. The valuation of division points on formal groups

In this section, we determine the valuation of the inverse image $\phi^{-1}(\mathcal{G}(K))$ in $\mathcal{F}(\overline{K})$ for an isogeny ϕ whose kernel has exponent p, or equivalently $\ker \phi \subset \ker [p]$, where $[p] \in \mathrm{End}_{\mathcal{O}_K}(\mathcal{F})$ denotes the multiplication by p map. We first show the fundamental properties for height 1 isogenies (§3.1), and use these properties to determine the valuation of the inverse image of isogeny of arbitrary finite height (§3.2). In §3.3, we focus on endomorphisms $\phi^n \in \mathrm{End}_{\mathcal{O}_K}(\mathcal{F})$, where $\phi \in \mathrm{End}_{\mathcal{O}_K}(\mathcal{F})$ and n is any positive integer. Note that the set $\phi^{-1}(y)$ is non-empty for any $y \in \mathcal{G}(K)$ because the map $\phi : \mathcal{F}(\overline{K}) \to \mathcal{G}(\overline{K})$ is surjective ([2]-IV-§2, Theorem 1), and $\ker \phi$ denotes $\phi^{-1}(0)$ in $\mathcal{F}(\overline{K})$.

For a descending filtration $M = M^0 \supseteq M^1 \supseteq \cdots \supseteq M^i \supseteq \cdots$ of modules, let

$$\mathscr{Q}(M)^i := M^i/M^{i+1},$$

which is the i-th factor module of this filtration. If $a \in \mathbb{Q}\,(a > 0)$ then $\mathscr{Q}(M)^a$ denotes $\mathscr{Q}(M)^{\lceil a \rceil}$. Needless to say, a filtration of a module M is not always unique, but throughout this paper, we will consider only one filtration for each module M.

3.1. The case $ht(\phi) = 1$. In this subsection, we assume that $ht(\phi) = 1$. In this case, $\ker\phi \simeq \mathbb{Z}/p\mathbb{Z}$ by Theorem 1 in [2]-IV-§2. Let $t_L := v_L(c(\phi))/(p-1)$, and let C_L denote the subgroup of $\mathcal{F}(L)/\mathcal{F}(L)^{t_L+1}$ generated by $\ker\phi \cap \mathcal{F}(L)$; namely,

$$C_L := (\ker\phi \cap \mathcal{F}(L))/\mathcal{F}(L)^{t_L+1}.$$

Our starting point is the results of V. G. Berkovič [1]. We quote the following two lemmas from the paper [1], which are often used in the present paper.

Lemma 3.1 (Lemma 2.1.1 in [1]). *If $a_1 \mid p$ then $a_1 \mid a_i$ for any positive integer i such that $p \nmid i$.*

Lemma 3.2 (Lemma 1.1.2 in [1]). *If a non-zero element $x \in \mathcal{F}(\overline{L})$ satisfies $\phi(x) = 0$, then $v_L(x) = t_L$. Especially the valuation $v_L(x)$ is independent of the choice of $x \in \ker\phi \setminus \{0\}$.*

From Lemma 3.2, it turns out that C_L is a subgroup of $\mathscr{Q}(\mathcal{F}(L))^{t_L}$, and $C_L = 0$ if $t_L \notin \mathbb{Z}$. For the proof of Lemma 3.4, we shall need the following lemma.

Lemma 3.3. *If $t_L \in \mathbb{Z}$ then there is a Galois equivariant bijection*

$$\begin{aligned} \ker\phi \setminus \{0\} &\xrightarrow{\sim} \left\{\xi \in \overline{k_L} \mid a_p\xi^{p-1} + u \equiv 0 \pmod{\pi_L}\right\} \\ x &\longmapsto \pi_L^{-t_L}x \pmod{\pi_L}, \end{aligned}$$

where $u := \pi_L^{-(p-1)t_L}a_1 \in \mathcal{O}_L^*$. In particular, if $L(x) \neq L$ then $L(x)_{/L}$ is an unramified extension of degree $p-1$ for each $x \in \ker\phi \setminus \{0\}$.

Proof. Let $S := \left\{\xi \in \overline{k_L} \mid a_p\xi^{p-1} + u \equiv 0 \pmod{\pi_L}\right\}$. Take any $x \in \ker\phi \setminus \{0\}$. By Lemma 3.2, we can write $a_1 = \pi_L^{(p-1)t_L}u$, $x = \pi_L^{t_L}\xi$, where $u \in \mathcal{O}_L^*$ and $\xi \in \mathcal{O}_{\overline{L}}^*$. Then

$$\begin{aligned} \phi(x) &= a_1(\pi_L^{t_L}\xi) + \cdots + a_p(\pi_L^{t_L}\xi)^p + \cdots \\ &\equiv \pi_L^{pt_L}\xi(a_p\xi^{p-1} + u) \pmod{\pi_L^{pt_L+1}} \\ &\equiv 0 \pmod{\pi_L^{pt_L+1}}, \end{aligned}$$

which leads to the equation $a_p\xi^{p-1} + u \equiv 0 \pmod{\pi_L}$. Here $a_pX^{p-1} + u \in \mathcal{O}_L[X]$ is separable. Thus, the map $\iota : \ker\phi \setminus \{0\} \to S$ is well-defined. Applying Hensel's lemma to the equation $\phi(X) = 0$, we see that ι is surjective, and hence injective by $\#\ker\phi = \#S = p-1$. If $\xi \notin L$ then, by Hensel's lemma, $\xi \pmod{\pi_L} \notin k_L$. Since the multiplication by $p-1$ map on k_L^* has kernel isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$, the polynomial $a_pX^{p-1} + u \in \mathcal{O}_L[X]$ must be irreducible. Hence $L(x)_{/L}$ is an unramified extension of degree $p-1$. □

The following lemma gives the valuation of $\phi(x)$ for any $x \in \mathcal{F}(L)$.

Lemma 3.4. *Let i be any positive integer.*

(i) *If $i < t_L$ then ϕ induces an isomorphism*

$$\mathscr{Q}(\mathcal{F}(L))^i \xrightarrow{\sim} \mathscr{Q}(\mathcal{G}(L))^{pi}.$$

(ii) *If $i = t_L$ then ϕ induces an exact sequence*

$$0 \longrightarrow C_L \longrightarrow \mathscr{Q}(\mathcal{F}(L))^{t_L} \xrightarrow{\overline{\phi}} \mathscr{Q}(\mathcal{G}(L))^{pt_L} \longrightarrow \widehat{C_L} \longrightarrow 0.$$

Here $\widehat{C_L} = 0$ if $\ker\phi \not\subset \mathcal{F}(L)$, or $\widehat{C_L} \simeq \mathbb{Z}/p\mathbb{Z}$ if $\ker\phi \subset \mathcal{F}(L)$.

(iii) *If $i > t_L$ then $\phi(\mathcal{F}(L)^i) = \mathcal{G}(L)^{(p-1)t_L+i}$.*

Especially, for any $x \in \mathcal{F}(L)$ satisfying $\overline{x} = x +_{\mathcal{F}} \mathcal{F}(L)^{t_L+1} \notin C_L \setminus \{0\}$,

$$v_L(\phi(x)) = \begin{cases} pv_L(x) & \text{if } v_L(x) \leq t_L \\ (p-1)t_L + v_L(x) & \text{if } v_L(x) > t_L. \end{cases}$$

Proof. For any $x \in \mathcal{F}(L)^i \backslash \mathcal{F}(L)^{i+1}$, if $i < t_L$ then combining the inequality $v_L(a_1x) > v_L(a_px^p)$ with Lemma 3.1 yields $v_L(\phi(x)) = v_L(a_px^p) = pi$, and if $i > t_L$ then combining the inequality $v_L(a_1x) < v_L(a_px^p)$ with Lemma 3.1 yields $v_L(\phi(x)) = v_L(a_1x) = (p-1)t_L + i$. Moreover if $i = t_L$ then combining the equality $v_L(a_1x) = v_L(a_px^p)$ with Lemma 3.1 yields $v_L(\phi(x)) \geq v_L(a_1x) = pt_L$.

(i) From the above observation, the map ϕ induces a well-defined map $\mathscr{Q}(\mathcal{F}(L))^i \to \mathscr{Q}(\mathcal{G}(L))^{pi}$, which is injective. Since $\#\mathscr{Q}(\mathcal{F}(L))^i = \#\mathscr{Q}(\mathcal{G}(L))^{pi} = \#k_L < \infty$, this map is also surjective.

(ii) The map ϕ induces a well-defined map $\overline{\phi} : \mathscr{Q}(\mathcal{F}(L))^{t_L} \to \mathscr{Q}(\mathcal{G}(L))^{pt_L}$, which leads to the following commutative diagram:

$$\begin{array}{ccc} \mathscr{Q}(\mathcal{F}(L))^{t_L} & \xrightarrow{\overline{\phi}} & \mathscr{Q}(\mathcal{G}(L))^{pt_L} \\ \uparrow & & \downarrow \\ k_L & \xrightarrow{\Phi} & k_L, \end{array}$$

where the vertical arrows are canonical isomorphisms. It is easy to check that the map Φ is given by $\Phi(x) = x(a_px^{p-1} + u)$, where $u := \pi_L^{-(p-1)t_L}a_1 \in \mathcal{O}_L^*$. If $\ker\phi \not\subset \mathcal{F}(L)$ then $a_px^{p-1} + u \neq 0$ for any $x \in k_L$ by Lemma 3.3 and Hensel's lemma, and hence $\ker\Phi = 0$, $\ker\overline{\phi} = 0$. This forces $\operatorname{coker}\overline{\phi} = 0$ by $\#\mathscr{Q}(\mathcal{F}(L))^{t_L} = \#\mathscr{Q}(\mathcal{G}(L))^{pt_L} = \#k_L < \infty$. Assume that $\ker\phi \subset \mathcal{F}(L)$. Then, by Lemma 3.3, $a_p(\pi_L^{-t_L}x)^{p-1} + u \equiv 0 \pmod{\pi_L}$ for any $x \in \ker\phi\backslash\{0\}$, and so $\operatorname{Im}[\ker\Phi \to \mathscr{Q}(\mathcal{F}(L))^{t_L}]$ ($= \ker\overline{\phi}$) is generated by $\ker\phi$. Since $\ker\Phi \simeq \mathbb{Z}/p\mathbb{Z}$, we have $[k_L : \Phi(k_L)] = p$, which gives $\operatorname{coker}\overline{\phi} \simeq \mathbb{Z}/p\mathbb{Z}$.

(iii) Since $\phi(\mathcal{F}(L)^i) \subset \mathcal{G}(L)^{(p-1)t_L+i}$, $\mathcal{F}(L)^i \approx \mathcal{G}(L)^i \approx \mathbb{Z}_p^{\oplus[L:\mathbb{Q}_p]}$ and $[\mathcal{G}(L)^i : \mathcal{G}(L)^{(p-1)t_L+i}] = [\mathscr{M}_L^i : \mathscr{M}_L^{(p-1)t_L+i}] = p^{(p-1)t_Lf}$, where f is the residue degree of $L_{/\mathbb{Q}_p}$, we have $[\mathcal{G}(L)^i : \phi(\mathcal{F}(L)^i)] = p^{(p-1)t_Lf}$. This implies $\phi(\mathcal{F}(L)^i) = \mathcal{G}(L)^{(p-1)t_L+i}$. □

The following lemma characterizes the inverse image $\phi^{-1}(y)$ for any $y \in \mathcal{G}(L)$. Let $L(x)$ denote the field of definition for $x \in \mathcal{F}(\overline{L})$.

Lemma 3.5. *Let i be any positive integer. For any $y \in \mathcal{G}(L)^i \setminus \mathcal{G}(L)^{i+1}$, let x be an element in $\mathcal{F}(\overline{L})$ such that $\phi(x) = y$.*

(i) *If $i < pt_L$ then $v_L(x) = i/p$. Furthermore if $p \mid i$ then there exists $x' \in \mathcal{F}(L)^{i/p} \setminus \mathcal{F}(L)^{i/p+1}$ such that $\phi(x') -_{\mathcal{G}} y \in \mathcal{G}(L)^{i+1}$. If $p \nmid i$ then $L(x)_{/L}$ is a totally ramified extension of degree $[L(x) : L] = p$.*

(ii) *If* $i = pt_L$ *then* $v_L(x) = t_L$ $(= i/p)$*. Furthermore if* $t_L \in \mathbb{Z}$ *then* $L(x)_{/L}$ *is an unramified extension of degree* $[L(x) : L] \mid p$*. If* $t_L \notin \mathbb{Z}$ *then* $L(x)_{/L}$ *is a totally ramified extension of degree* $[L(x) : L] = p$*.*

(iii) *If* $i > pt_L$ *then there exists* $w \in \ker\phi \cap \mathcal{F}(L(x))$ *so that* $v_L(x +_{\mathcal{F}} w) = i-(p-1)t_L$ *and* $L(x +_{\mathcal{F}} w) = L$*.*

Especially, in the cases (i)(ii)*, the valuation* $v_L(x)$ *is independent of the choice of* $x \in \phi^{-1}(y)$*.*

Proof. Let e denote the ramification index of the extension $L(x)_{/L}$, and let $s := v_{L(x)}(x)$. Since $ht(\phi) = 1$, by the p-adic Weierstrass preparation theorem ([2]-I-§1, Theorem 3) and Lemma 3.1, we can write the polynomial $\phi(X) - y \in \mathcal{O}_L[\![X]\!]$ as

$$\phi(X) - y = (b_0 + b_1X + \cdots + b_{p-1}X^{p-1} + X^p) \cdot u(X)$$

for some unit $u(X) \in \mathcal{O}_L[\![X]\!]^*$. Letting $X = x$ yields $b_0 + b_1x + \cdots + b_{p-1}x^{p-1} + x^p = 0$. It thus turns out that the extension degree $[L(x) : L] \leq p$.
(i) In Lemma 3.4, replacing L, i by $L(x)$, $v_{L(x)}(x)$ respectively, we can easily deduce that $v_{L(x)}(x) < t_{L(x)}$, where $t_{L(x)} = et_L$ by definition. Thus, again using Lemma 3.4 yields $pv_{L(x)}(x) = ei$, and hence $v_L(x) = i/p$. Assume that $p \nmid i$. Since $v_L(x) = s/e$, we have $ei = ps$. This gives $p \mid e$. Combining the inequality $[L(x) : L] \leq p$ with $p \mid e \mid [L(x) : L]$, we have $[L(x) : L] = e = p$. We next assume $p \mid i$. Let $i_0 := i/p \in \mathbb{Z}$. Write $a_1 = \pi_L^{(p-1)t_L}u$, $y = \pi_L^i\eta$, where u, $\eta \in \mathcal{O}_L^*$. Since $v_L(a_p) = 0$ and $v_L(p) > 0$, there exists some $z \in \mathcal{O}_L^*$ such that $a_pz^p \equiv \eta \pmod{\pi}$. Let $\epsilon := \phi(\pi_L^{i_0}z) -_{\mathcal{G}} y \in \mathcal{G}(L)$. Then

$$\begin{aligned}
\phi(\pi_L^{i_0}z) &= y +_{\mathcal{G}} \epsilon \\
&\equiv y + \epsilon \pmod{\pi_L^{i+v_L(\epsilon)}}, \\
\phi(\pi_L^{i_0}z) &= a_1(\pi_L^{i_0}z) + \cdots + a_p(\pi_L^{i_0}z)^p + \cdots \\
&\equiv \pi_L^{pi_0}(a_pz^p + \pi_L^{(p-1)(t_L-i_0)}uz) \pmod{\pi^{pi_0+1}} \quad \text{(by Lemma 3.1)} \\
&\equiv \pi_L^i a_pz^p \pmod{\pi_L^{i+1}} \\
&\equiv \pi_L^i\eta \pmod{\pi_L^{i+1}}.
\end{aligned}$$

We thus have $y + \epsilon \equiv \pi_L^i\eta \pmod{\pi_L^{i+1}}$, and so $\epsilon \equiv 0 \pmod{\pi_L^{i+1}}$; namely, $v_L(\epsilon) > i$. Let $x' := \pi_L^{i_0}z \in \mathcal{F}(L)^{i/p} \backslash \mathcal{F}(L)^{i/p+1}$. The element x' satisfies $v_L(\phi(x')) = v_L(y +_{\mathcal{G}} \epsilon) = i$ and $\phi(x') -_{\mathcal{G}} y = \epsilon \in \mathcal{G}(L)^{i+1}$. Therefore x' is a required element in the statement of the lemma.
(ii) In Lemma 3.4, replacing L, i by $L(x)$, $v_{L(x)}(x)$ respectively, we can easily deduce that $v_{L(x)}(x) = t_{L(x)}$, where $t_{L(x)} = et_L$ by definition. Thus, $v_L(x) = t_L$ $(= i/p)$. Assume that $t_L \in \mathbb{Z}$. Write $a_1 = \pi_L^{(p-1)t_L}u$, $x = \pi_L^{t_L}\xi$, $y = \pi_L^i\eta$, where u, $\eta \in \mathcal{O}_L^*$ and $\xi \in \mathcal{O}_{L(x)}^*$. Then

$$\begin{aligned}
\phi(x) &= a_1(\pi_L^{t_L}\xi) + \cdots + a_p(\pi_L^{t_L}\xi)^p + \cdots \\
&\equiv \pi_L^{pt_L}(a_p\xi^p + u\xi) \pmod{\pi_L^{pt_L+1}} \\
&\equiv \pi_L^i\eta \pmod{\pi_L^{pt_L+1}},
\end{aligned}$$

which leads to the equation $a_p\xi^p + u\xi \equiv \eta \pmod{\pi_L}$. If $x \notin L$ then, by Hensel's lemma, $\xi \pmod{\pi_L} \notin k_L$, and hence $L(x)_{/L}$ is an unramified extension of degree p. Assume that $t_L \notin \mathbb{Z}$. Since $v_L(x) = s/e$, we have $ei = ps$. This gives $p \mid e$. Combining the inequality $[L(x) : L] \leq p$ with $p \mid e \mid [L(x) : L]$, we have $[L(x) : L] = e = p$.
(iii) In Lemma 3.4, replacing L, i by $L(x)$, $v_{L(x)}(x)$ respectively, we can easily deduce that $v_{L(x)}(x) \geq t_{L(x)}$ and $\overline{x} \in C_{L(x)}$. Then, by the definition of $C_{L(x)}$, there exists $w \in \ker\phi \cap \mathcal{F}(L(x))$ so that $v_{L(x)}(x +_{\mathcal{F}} w) > t_{L(x)}$. Again using Lemma 3.4 yields $\phi(\mathcal{F}(L(x))^{j-(p-1)t_{L(x)}}) = \mathcal{G}(L(x))^j$ for any integer $j \geq ei\,(> pt_{L(x)})$, which implies $v_L(x +_{\mathcal{F}} w) = i - (p-1)t_L$. Assume that $x_w := x +_{\mathcal{F}} w \notin \mathcal{F}(L)$. There exists an embedding $\sigma : L(x_w) \to \overline{L}$ fixing any $a \in L$ such that $x_w^\sigma \neq x_w$. Let $z := x_w^\sigma -_{\mathcal{F}} x_w$. Then $\phi(z) = 0$, $z \neq 0$, and hence $v_L(z) = t_L$ from Lemma 3.2. Since $v_L(x_w) - v_L(z) = i - pt_L > 0$, we have $v_L(x_w^\sigma) = v_L(x_w +_{\mathcal{F}} z) = v_L(z) = t_L$. However $i - (p-1)t_L = v_L(x_w) = v_L(x_w^\sigma) = t_L$; that is, $i = pt_L$. This is a contradiction. Therefore $x_w \in \mathcal{F}(L)$. □

3.2. The case $ht(\phi) = h$.

From now on, we consider the arbitrary height cases. Let $h := ht(\phi)$ be any positive integer. We assume that the exponent of $\ker\phi$ is p. Recall from Theorem 1 in [2]-IV-§2 that $\ker\phi$ is an $\mathbb{F}_p$-vector space of dimension h.

Lemma 3.6. *Let $\mathcal{F}'$ be any one-dimensional commutative formal group over $\mathcal{O}_L$. For any finite subgroup $C = \langle\eta_1\rangle \oplus \langle\eta_2\rangle \oplus \cdots \oplus \langle\eta_k\rangle \subset \mathcal{F}'(L)$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus k}$ (i.e. an $\mathbb{F}_p$-vector space of dimension k), where k is an integer (≥ 1), there exist a one-dimensional commutative formal group $\mathcal{F}''$ and a height 1 isogeny $\psi : \mathcal{F}' \to \mathcal{F}''$, both defined over $\mathcal{O}_L$ satisfying the conditions*:

(i) $\ker\psi = \langle\eta_0\rangle \simeq \mathbb{Z}/p\mathbb{Z}$, *where* $\eta_0 \in C$ *and* $v_L(\eta_0) = \max\{v_L(\eta) \mid \eta \in C \setminus \{0\}\}$.
(ii) $\psi(C) \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus(k-1)}$.
(iii) $v_L(\psi(\eta)) = pv_L(\eta) \leq pv_L(\eta_0)$ *for any* $\eta \in C \setminus \ker\psi$.
(iv) *For any isogeny* $\Psi : \mathcal{F}' \to \mathcal{F}'''$ *over* $\mathcal{O}_L$ *with* $\ker\Psi \supset \ker\psi$, *there exists unique isogeny* $\psi' : \mathcal{F}'' \to \mathcal{F}'''$ *over* $\mathcal{O}_L$ *so that* $\Psi = \psi' \circ \psi$.

Proof. Take $\eta_0 \in C$ so that $v_L(\eta_0) = \max\{v_L(\eta) \mid \eta \in C \setminus \{0\}\}$. By the result [6] of Lubin, there exists a height 1 isogeny $\psi : \mathcal{F}' \to \mathcal{F}''$ over $\mathcal{O}_L$ whose kernel is $\langle\eta_0\rangle \simeq \mathbb{Z}/p\mathbb{Z}$, and the isogeny ψ has the universal property (iv). For any $\eta \in C \setminus \ker\psi$, if $v_L(\eta) < v_L(\eta_0)$ then, by Lemma 3.2, 3.4 we have $v_L(\psi(\eta)) = pv_L(\eta) < pv_L(\eta_0)$. If $v_L(\eta) = v_L(\eta_0)$ then, since $v_L(\eta -_{\mathcal{F}'} \eta_0') = v_L(\eta_0)$ for any $\eta_0' \in \ker\psi$, using Lemma 3.2, 3.4 yields $v_L(\psi(\eta)) = pv_L(\eta_0) = pv_L(\eta)$. □

Let $L' := L(\ker\phi)$. Repeated application of Lemma 3.6 to $\ker\phi \subset \mathcal{F}(L')$ enables us to decompose ϕ into the following height 1 isogenies defined over $\mathcal{O}_{L'}$:

$$\phi_i : \mathcal{F}_{i-1} \longrightarrow \mathcal{F}_i \quad (1 \leq i \leq h).$$

Here $\mathcal{F}_0 := \mathcal{F}$, $\mathcal{F}_h := \mathcal{G}$, $\phi = \phi_h \circ \cdots \circ \phi_1$ and $v_L(\eta_{i+1}) \leq pv_L(\eta_i)$, where $\ker\phi_i = \langle\eta_i\rangle \simeq \mathbb{Z}/p\mathbb{Z}$ for some $\eta_i \in \mathcal{F}_{i-1}(L')$. Since $\ker\phi_i \subset \phi_{i-1} \circ \cdots \circ \phi_1(\ker\phi)$, we can find some $\mathbb{F}_p$-basis $\{w_1, w_2, \cdots, w_h\}$ of $\ker\phi$ so that

$$\ker\phi_i = \langle\phi_{i-1} \circ \cdots \circ \phi_1(w_i)\rangle \quad (= \langle\eta_i\rangle).$$

Let $t_L^{(i)} := v_L(c(\phi_i))/(p-1)$. From Lemma 3.2, $v_L(\eta_i) = v_L(\phi_{i-1} \circ \cdots \circ \phi_1(w_i)) = t_L^{(i)}$, and hence $t_L^{(i+1)} \leq p t_L^{(i)}$.

The following lemma is a generalization of Lemma 3.2 to arbitrary height cases.

Lemma 3.7. *If $x \in \mathcal{F}(\overline{L})$ satisfies $\phi_i \circ \cdots \circ \phi_1(x) = 0$, $\phi_{i-1} \circ \cdots \circ \phi_1(x) \neq 0$ for some positive integer $i\,(\leq h)$, then $v_L(x) = t_L^{(i)}/p^{i-1}$. Especially the valuation $v_L(x)$ is independent of the choice of $x \in \ker(\phi_i \circ \cdots \circ \phi_1) \setminus \ker(\phi_{i-1} \circ \cdots \circ \phi_1)$, and so $v_L(w_i) = t_L^{(i)}/p^{i-1}$, $v_L(w_{i+1}) \leq v_L(w_i)$.*

Proof. Let us show $v_L(\phi_{i-j} \circ \cdots \circ \phi_1(x)) = t_L^{(i)}/p^{j-1}$ for any positive integer $j\,(\leq i)$. By induction. The case $j = 1$ follows directly from Lemma 3.2. Assume that this holds for $j-1$. Then $v_L(\phi_{i-(j-1)} \circ \cdots \circ \phi_1(x)) = t_L^{(i)}/p^{j-2} \leq p t_L^{(i-j+1)}$. It thus follows from Lemma 3.5 that $v_L(\phi_{i-j} \circ \cdots \circ \phi_1(x)) = t_L^{(i)}/p^{j-1}$, which gives the desired conclusion. The latter statement immediately follows from this. □

From Lemma 3.7, we have the decreasing sequence

$$v_L(w_1) \geq v_L(w_2) \geq v_L(w_3) \geq \cdots \geq v_L(w_h).$$

For any positive integer $m\,(\leq h)$, there exist unique integers m_0, m_1 $(1 \leq m_0 \leq m \leq m_1 \leq h)$ so that

$$v_L(w_{m_0-1}) > v_L(w_{m_0}) = \cdots = v_L(w_m) = \cdots = v_L(w_{m_1}) > v_L(w_{m_1+1}).$$

Let $C_L^{(m)}$ denote the subgroup of $\mathscr{Q}(\mathcal{F}(L))^{v_L(w_m)}$ generated by the subgroup

$$\langle w_{m_0}, w_{m_0+1}, \cdots, w_{m_1} \rangle \cap \mathcal{F}(L) \subset \mathcal{F}(L)^{v_L(w_m)};$$

namely,

$$C_L^{(m)} := (\langle w_i \mid v_L(w_i) = v_L(w_m) \rangle \cap \mathcal{F}(L))/\mathcal{F}(L)^{v_L(w_m)+1}.$$

Note that $C_L^{(m)} = 0$ if $v_L(w_m) \notin \mathbb{Z}$, and for the case $h = 1$ this definition is equivalent to the definition for C_L in §3.1.

Lemma 3.8. *For any finite extension $M_{/L}$, let $\iota : \mathscr{Q}(\mathcal{F}(L))^{v_L(w_m)} \to \mathscr{Q}(\mathcal{F}(M))^{v_M(w_m)}$ be a canonical embedding. If $M_{/L}$ is a Galois extension then $(\mathscr{Q}(\mathcal{F}(M))^{v_M(w_m)})^{\mathrm{Gal}(M/L)} = \mathrm{Im}\,\iota$ and $\iota^{-1}(C_M^{(m)}) = C_L^{(m)}$.*

Proof. There is a commutative diagram

$$\begin{array}{ccc} \mathscr{Q}(\mathcal{F}(M))^{v_M(w_m)} & \xrightarrow{\sim} & k_M \\ {\scriptstyle\iota}\uparrow & & \uparrow \\ \mathscr{Q}(\mathcal{F}(L))^{v_L(w_m)} & \xrightarrow{\sim} & k_L, \end{array}$$

where the vertical arrows are canonical embeddings and $\mathscr{Q}(\mathcal{F}(M))^{v_M(w_m)} \simeq k_M$ as $\mathrm{Gal}(M/L)$-modules. We thus have $(\mathscr{Q}(\mathcal{F}(M))^{v_M(w_m)})^{\mathrm{Gal}(M/L)} = \mathrm{Im}\,\iota$, by $k_M^{\mathrm{Gal}(k_M/k_L)} \simeq k_L$. Since $C_M^{(m)}$ is a $\mathrm{Gal}(M/L)$-submodule of $\mathscr{Q}(\mathcal{F}(M))^{v_M(w_m)}$, we see that $(C_M^{(m)})^{\mathrm{Gal}(M/L)} \subset \mathrm{Im}\,\iota$, which implies $(C_M^{(m)})^{\mathrm{Gal}(M/L)} \subset \iota(C_L^{(m)})$?. By definition, the inverse inclusion

$(C_M^{(m)})^{\mathrm{Gal}(M/L)} \supset \iota(C_L^{(m)})$ holds clearly. Therefore $(C_M^{(m)})^{\mathrm{Gal}(M/L)} = \iota(C_L^{(m)})$, and hence $\iota^{-1}(C_M^{(m)}) = C_L^{(m)}$?. $\square$

The following proposition gives the valuation of $\phi(x)$ for any $x \in \mathcal{F}(L)$. Let

$$T_L^{(m)} := \begin{cases} \displaystyle\sum_{l=m+1}^{h} t_L^{(l)} & (0 \le m < h) \\ 0 & (m = h). \end{cases}$$

Proposition 3.9. *Let i be any positive integer.*

(i) *If $i < v_L(w_h)$ then ϕ induces an isomorphism*

$$\mathscr{Q}(\mathcal{F}(L))^i \xrightarrow{\sim} \mathscr{Q}(\mathcal{G}(L))^{p^h i}.$$

(ii) *If $v_L(w_{m+1}) < i < v_L(w_m)$ for some integer $m\,(1 \le m < h)$ then ϕ induces an isomorphism*

$$\mathscr{Q}(\mathcal{F}(L))^i \xrightarrow{\sim} \mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+p^m i}.$$

(iii) *If $i = v_L(w_m)$ for some integer $m\,(1 \le m \le h)$ then ϕ induces an exact sequence*

$$0 \longrightarrow C_L^{(m)} \longrightarrow \mathscr{Q}(\mathcal{F}(L))^i \xrightarrow{\phi} \mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+pt_L^{(m)}} \longrightarrow \widehat{C_L}^{(m)} \longrightarrow 0.$$

Here $\widehat{C_L}^{(m)}$ is an $\mathbb{F}_p$-vector space isomorphic to $C_L^{(m)}$.

(iv) *If $i > v_L(w_1)$ then $\phi(\mathcal{F}(L)^i) = \mathcal{G}(L)^{(p-1)T_L^{(0)}+i}$.*

Especially, for any $x \in \mathcal{F}(L)$ satisfying $\overline{x} \notin C_L^{(m)} \backslash \{0\}$ for every integer $m\,(1 \le m \le h)$,

$$v_L(\phi(x)) = \begin{cases} p^h v_L(x) & \text{if } v_L(x) \le v_L(w_h) \\ (p-1)T_L^{(m)} + p^m v_L(x) & \text{if } v_L(w_{m+1}) < v_L(x) \le v_L(w_m)\,(1 \le m < h) \\ (p-1)T_L^{(0)} + v_L(x) & \text{if } v_L(x) \ge v_L(w_1). \end{cases}$$

Proof. We begin by proving the proposition over L'. Let (i)$'\cdots$(iv)$'$ denote the statement of the theorem over L' for (i)$\cdots$(iv), respectively. First of all, we recall from Lemma 3.7 that $v_{L'}(w_l) = t_{L'}^{(l)}/p^{l-1}$ for each positive integer $l\,(\le h)$.

(i)$'$ Since $p^{l-1}i < t_{L'}^{(h)}/p^{h-l} \le t_{L'}^{(l)}$ for any positive integer $l\,(\le h)$, repeated application of Lemma 3.4 yields the statement for this case.

(ii)$'$ Since $p^{l-1}i < t_{L'}^{(m)}/p^{m-l} \le t_{L'}^{(l)}$ for any positive integer $l\,(\le m)$, repeated application of Lemma 3.4 yields the isomorphism $\phi_m \circ \cdots \circ \phi_1 : \mathscr{Q}(\mathcal{F}(L'))^i \simeq \mathscr{Q}(\mathcal{F}_m(L'))^{p^m i}$. Moreover, since $(p-1)(t_{L'}^{(m+1)} + \cdots + t_{L'}^{(l)}) + p^m i > t_{L'}^{(l+1)}$ for any integer $l\,(m \le l < h)$, repeated application of Lemma 3.4 yields the isomorphism $\phi_h \circ \cdots \circ \phi_{m+1} : \mathscr{Q}(\mathcal{F}_m(L'))^{p^m i} \simeq \mathscr{Q}(\mathcal{F}_h(L'))^{(p-1)T_{L'}^{(m)}+p^m i}$. The statement now follows from $\phi = \phi_h \circ \cdots \circ \phi_1$.

(iii)$'$ Let m_0, m_1 be integers so that $1 \le m_0 \le m \le m_1 \le h$ and $v_L(w_{m_0-1}) >$

$v_L(w_{m_0}) = v_L(w_{m_0+1}) = \cdots = v_L(w_m) = \cdots = v_L(w_{m_1}) > v_L(w_{m_1+1})$. From Lemma 3.7, we have

$$p^{l-1}i \begin{cases} < t_{L'}^{(l)} & \text{if } 1 \le l < m_0 \\ = t_{L'}^{(l)} & \text{if } m_0 \le l \le m_1 \\ > t_{L'}^{(l)} & \text{if } m_1 < l \le h. \end{cases}$$

Combining this with repeated application of Lemma 3.4 yields

$$\phi_{m_0-1} \circ \cdots \circ \phi_1 : \mathscr{Q}(\mathcal{F}(L'))^i \xrightarrow{\sim} \mathscr{Q}(\mathcal{F}_{m_0-1}(L'))^{p^{m_0-1}i},$$

$$\begin{aligned} 0 \longrightarrow \phi_{m_0-1} \circ \cdots \circ \phi_1(C_{L'}^{(m)}) \longrightarrow \mathscr{Q}(\mathcal{F}_{m_0-1}(L'))^{p^{m_0-1}i} \stackrel{\phi_{m_1}\circ\cdots\circ\phi_{m_0}}{\longrightarrow} \mathscr{Q}(\mathcal{F}_{m_1}(L'))^{p^{m_1}i} \\ \longrightarrow \operatorname{coker}(\phi_{m_1} \circ \cdots \circ \phi_{m_0}) \longrightarrow 0 \quad \text{(exact sequence)}. \end{aligned}$$

Moreover, since $(p-1)(t_{L'}^{(m_1+1)} + \cdots + t_{L'}^{(l)}) + p^{m_1}i > t_{L'}^{(l+1)}$ for any integer l $(m_1 \le l < h)$, repeated application of Lemma 3.4 yields

$$\phi_h \circ \cdots \circ \phi_{m_1+1} : \mathscr{Q}(\mathcal{F}_{m_1}(L'))^{p^{m_1}i} \xrightarrow{\sim} \mathscr{Q}(\mathcal{F}_h(L'))^{(p-1)T_{L'}^{(m_1)}+p^{m_1}i},$$

where

$$(p-1)\sum_{l=m_1+1}^{h} t_{L'}^{(l)} + p^{m_1}i = (p-1)\sum_{l=m+1}^{h} t_{L'}^{(l)} + p^m i$$

by $i = v_L(w_m) = \cdots = v_L(w_{m_1})$. The statement now follows from $\phi = \phi_h \circ \cdots \circ \phi_1$.
(iv)$'$ Since $(p-1)(t_{L'}^{(1)} + \cdots + t_{L'}^{(l)}) + i > t_{L'}^{(l+1)}$ for any integer l $(0 \le l < h)$, repeated application of Lemma 3.4 yields the statement for this case.

We are now ready to prove the proposition over L. Let e' be the ramification index of $L'_{/L}$.
(i) Since $e'i < t_{L'}^{(h)}/p^{h-1}$, using (i)$'$ yields the following diagram:

$$\begin{array}{ccc} \mathscr{Q}(\mathcal{F}(L'))^{e'i} & \xrightarrow{\phi} & \mathscr{Q}(\mathcal{G}(L'))^{p^h e'i} \\ \uparrow & & \uparrow \\ \mathscr{Q}(\mathcal{F}(L))^i & & \mathscr{Q}(\mathcal{G}(L))^{p^h i}, \end{array}$$

where the vertical arrows are canonical embeddings. Then it is easily seen that

$$\operatorname{Im}[\mathscr{Q}(\mathcal{F}(L))^i \hookrightarrow \mathscr{Q}(\mathcal{F}(L'))^{e'i} \xrightarrow{\phi} \mathscr{Q}(\mathcal{G}(L'))^{p^h e'i}] \subset \operatorname{Im}[\mathscr{Q}(\mathcal{G}(L))^{p^h i} \hookrightarrow \mathscr{Q}(\mathcal{G}(L'))^{p^h e'i}],$$

which implies the map $\phi : \mathscr{Q}(\mathcal{F}(L))^i \to \mathscr{Q}(\mathcal{G}(L))^{p^h i}$ is well-defined and injective. Combining this with $\#\mathscr{Q}(\mathcal{F}(L))^i = \#\mathscr{Q}(\mathcal{G}(L))^{p^h i} = \#k_L < \infty$, the map $\phi : \mathscr{Q}(\mathcal{F}(L))^i \to \mathscr{Q}(\mathcal{G}(L))^{p^h i}$ must be an isomorphism.
(ii) This follows by the same method as in the proof of (i). Since $t_{L'}^{(m+1)}/p^m < e'i < t_{L'}^{(m)}/p^{m-1}$, using (ii)$'$ yields the following diagram:

$$\begin{array}{ccc} \mathscr{Q}(\mathcal{F}(L'))^{e'i} & \xrightarrow{\phi} & \mathscr{Q}(\mathcal{G}(L'))^{(p-1)T_{L'}^{(m)}+p^m e'i} \\ \uparrow & & \uparrow \\ \mathscr{Q}(\mathcal{F}(L))^i & & \mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+p^m i}, \end{array}$$

where the vertical arrows are canonical embeddings. Then it is easily seen that

$$\begin{aligned}\mathrm{Im}\,[\mathscr{Q}(\mathcal{F}(L))^i \hookrightarrow \mathscr{Q}(\mathcal{F}(L'))^{e'i} \xrightarrow{\phi} \mathscr{Q}(\mathcal{G}(L'))^{(p-1)T_{L'}^{(m)}+p^m e'i}]&\\ \subset \mathrm{Im}\,[\mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+p^m i} \hookrightarrow \mathscr{Q}(\mathcal{G}(L'))^{(p-1)T_{L'}^{(m)}+p^m e'i}],&\end{aligned}$$

which implies the map $\phi : \mathscr{Q}(\mathcal{F}(L))^i \to \mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+p^m i}$ is well-defined and injective. Combining this with $\#\mathscr{Q}(\mathcal{F}(L))^i = \#\mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+p^m i} = \#k_L < \infty$, the map $\phi : \mathscr{Q}(\mathcal{F}(L))^i \to \mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+p^m i}$ must be an isomorphism.

(iii) Since $e'i = t_{L'}^{(m)}/p^{m-1}$, using (iii)$'$ yields the following diagram:

$$\begin{array}{ccc}\mathscr{Q}(\mathcal{F}(L'))^{e'i} & \xrightarrow{\phi} & \mathscr{Q}(\mathcal{G}(L'))^{(p-1)T_{L'}^{(m)}+pt_{L'}^{(m)}}\\ {\scriptstyle\iota}\uparrow & & \uparrow\\ \mathscr{Q}(\mathcal{F}(L))^i & & \mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+pt_L^{(m)}},\end{array}$$

where the vertical arrows are canonical embeddings. Then it is easily seen that

$$\begin{aligned}\mathrm{Im}\,[\mathscr{Q}(\mathcal{F}(L))^i \hookrightarrow \mathscr{Q}(\mathcal{F}(L'))^{e'i} \xrightarrow{\phi} \mathscr{Q}(\mathcal{G}(L'))^{(p-1)T_{L'}^{(m)}+pt_{L'}^{(m)}}]&\\ \subset \mathrm{Im}\,[\mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+pt_L^{(m)}} \hookrightarrow \mathscr{Q}(\mathcal{G}(L'))^{(p-1)T_{L'}^{(m)}+pt_{L'}^{(m)}}],&\end{aligned}$$

which implies the map $\phi : \mathscr{Q}(\mathcal{F}(L))^i \to \mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+pt_L^{(m)}}$ is well-defined. Moreover, we have

$$\begin{aligned}\ker\,[\mathscr{Q}(\mathcal{F}(L))^i &\xrightarrow{\phi} \mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+pt_L^{(m)}}]\\ &= \iota^{-1}\left(\ker\,[\mathscr{Q}(\mathcal{F}(L'))^{e't} \xrightarrow{\phi} \mathscr{Q}(\mathcal{G}(L'))^{p^h e't}]\right)\\ &= \iota^{-1}(C_{L'}^{(m)})\\ &= C_L^{(m)}. \quad \text{(by Lemma ???)}\end{aligned}$$

Thus

$$0 \longrightarrow C_L^{(m)} \longrightarrow \mathscr{Q}(\mathcal{F}(L))^i \xrightarrow{\phi} \mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+pt_L^{(m)}} \longrightarrow \mathrm{coker} \longrightarrow 0$$

is an exact sequence of finite $\mathbb{F}_p$-vector spaces, which splits. Combining this with $\#\mathscr{Q}(\mathcal{F}(L))^i = \#\mathscr{Q}(\mathcal{G}(L))^{(p-1)T_L^{(m)}+pt_L^{(m)}} = \#k_L < \infty$ gives $\widehat{C_L}^{(m)} = \mathrm{coker} \simeq C_L$.

(iv) Since $e'i > t_{L'}^{(1)}$, using (iv)$'$ yields the following diagram:

$$\begin{array}{ccc}\mathcal{F}(L')^{e'i} & \xrightarrow{\phi} & \mathcal{G}(L')^{(p-1)T_{L'}^{(0)}+e'i}\\ \uparrow & & \uparrow\\ \mathcal{F}(L)^i & & \mathcal{G}(L)^{(p-1)T_L^{(0)}+i},\end{array}$$

where the vertical arrows are canonical embeddings. Then it is easily seen that

$$\begin{aligned}\mathrm{Im}\,[\mathcal{F}(L)^i \hookrightarrow \mathcal{F}(L')^{e'i} \xrightarrow{\phi} \mathcal{G}(L')^{(p-1)T_{L'}^{(0)}+e'i}]&\\ \subset \mathrm{Im}\,[\mathcal{G}(L)^{(p-1)T_L^{(0)}+i} \hookrightarrow \mathcal{G}(L')^{(p-1)T_{L'}^{(0)}+e'i}],&\end{aligned}$$

which implies the map $\phi : \mathcal{F}(L)^i \to \mathcal{G}(L)^{(p-1)T_L^{(0)}+i}$ is well-defined and injective.

$\square$

Let $\mathbb{N}$ denote the set of all positive integers. Define a map $\lambda_L : \mathbb{N} \to \mathbb{N}$ by

$$\lambda_L(i) := \begin{cases} (p-1)T_L^{(m)} + pt_L^{(m)} & \text{if } i = v_L(w_m) \in \mathbb{N}\,(1 \leq m \leq h) \\ v_L(\phi(x)) \quad \text{for some} \quad x \in \mathcal{F}(L)^i \setminus \mathcal{F}(L)^{i+1} & \text{otherwise,} \end{cases}$$

which is characterized by

$$\begin{aligned} 0 \longrightarrow C_L^{(m)} \longrightarrow \mathscr{Q}(\mathcal{F}(L))^i \xrightarrow{\overline{\phi}} \mathscr{Q}(\mathcal{F}(L))^{\lambda_L(i)} \longrightarrow \widehat{C_L}^{(m)} \longrightarrow 0 \qquad & \text{if } i = v_L(w_m)\,(1 \leq m \leq h), \\ \overline{\phi} : \mathscr{Q}(\mathcal{F}(L))^i \xrightarrow{\sim} \mathscr{Q}(\mathcal{G}(L))^{\lambda_L(i)} \qquad & \text{otherwise,} \end{aligned}$$

where $\overline{\phi}$ is the map in Proposition 3.9. One can easily check that the map λ_L is injective. From this observation, we shall decompose the set $\mathbb{N}$ into the disjoint union

$$S_0 \cup \bigcup_{m=1}^{h} (S_m \cup \partial S_m),$$

where

$$\begin{aligned} S_h &:= \left\{ i \in \mathbb{N} \;\middle|\; i < pt_L^{(h)} \right\}, \\ S_m &:= \left\{ i \in \mathbb{N} \;\middle|\; t_L^{(m+1)} < i - (p-1)T_L^{(m)} < pt_L^{(m)} \right\} \quad (1 \leq m < h), \\ \partial S_m &:= \left\{ i \in \mathbb{N} \;\middle|\; i = (p-1)T_L^{(m)} + pt_L^{(m)} \right\} \quad (1 \leq m \leq h), \\ S_0 &:= \left\{ i \in \mathbb{N} \;\middle|\; i > (p-1)T_L^{(0)} + t_L^{(1)} \right\}. \end{aligned}$$

It is easily seen that, for any positive integer $m\,(\leq h)$, if $\partial S_m \neq \emptyset$ then $i < j < k$ for any $i \in S_m$, $j \in \partial S_m$, $k \in S_{m-1}$, and if $\partial S_m = \emptyset$ then $i < k$ for any $i \in S_m$, $k \in S_{m-1}$. Then

$$\text{(Ob)} \qquad \begin{aligned} \lambda_L(\{i \in \mathbb{N} \mid i < v_L(w_h)\}) &\subset S_h, \\ \lambda_L(\{i \in \mathbb{N} \mid v_L(w_{m+1}) < i < v_L(w_m)\}) &\subset S_m \quad (1 \leq m < h), \\ \lambda_L(v_L(w_m)) &\in \partial S_m \quad (1 \leq m \leq h,\, v_L(w_m) \in \mathbb{N}), \\ \lambda_L(\{i \in \mathbb{N} \mid i > v_L(w_1)\}) &\subset S_0. \end{aligned}$$

Using Proposition 3.9, we can determine the valuation of the inverse image $\phi^{-1}(y)$ for any $y \in \mathcal{G}(L)$ as follows.

Proposition 3.10. *For any $y \in \mathcal{G}(L)^i \setminus \mathcal{G}(L)^{i+1}$, let x be an element in $\mathcal{F}(\overline{L})$ such that $\phi(x) = y$. There exists an element $w \in \ker\phi \cap \mathcal{F}(L(x))$ so that*

$$v_L(x +_{\mathcal{F}} w) = \begin{cases} \dfrac{i}{p^h} & \text{if } i \in S_h \\ \dfrac{1}{p^m}\left\{ i - (p-1)T_L^{(m)} \right\} & \text{if } i \in S_m \\ v_L(w_m) & \text{if } i \in \partial S_m \\ i - (p-1)T_L^{(0)} & \text{if } i \in S_0. \end{cases}$$

In particular, $v_L(x +_{\mathcal{F}} w) < v_L(\phi(x))$. Furthermore, in the case where $i \in S_h$, the valuation $v_L(x)$ is independent of the choice of $x \in \phi^{-1}(y)$. In the case where $i \notin S_h$, $v_L(x) \geq v_L(w_h)$.

Proof. Let e denote the ramification index of the extension $L(x)_{/L}$. In Proposition 3.9, replacing L, i by $L(x)$, $v_{L(x)}(x)$ respectively, we can easily deduce from the observation (Ob) that

$$\begin{cases} v_{L(x)}(x) < v_{L(x)}(w_h) & \text{if } i \in S_h \\ v_{L(x)}(w_{m+1}) < v_{L(x)}(x +_{\mathcal{F}} w) < v_{L(x)}(w_m) & \text{if } i \in S_m \\ v_{L(x)}(x +_{\mathcal{F}} w) = v_{L(x)}(w_m) & \text{if } i \in \partial S_m \\ v_{L(x)}(x +_{\mathcal{F}} w) > v_{L(x)}(w_1) & \text{if } i \in S_0. \end{cases}$$

Here w is some element in $\ker \phi \cap \mathcal{F}(L(x))$. For the case $v_{L(x)}(x) = v_{L(x)}(w_m)$, we have $v_L(x) = v_L(w_m)$ from $t^{(1)}_{L(x)} = et^{(1)}_L = et$. The remaining cases follow again from Proposition 3.9: For the case $i \in S_h$, we see that $p^h v_{L(x)}(x) = v_{L(x)}(y) = ei$, and hence $v_L(x) = i/p^h$. For the case $i \in S_m$, $(p-1)T^{(m)}_{L(x)} + p^m v_{L(x)}(x) = v_{L(x)}(y) = ei$, and hence $v_L(x) = \{i - (p-1)T^{(m)}_L\}/p^m$. For the case $v_{L(x)}(x) > v_L(w_1)$, since $\phi^n(\mathcal{F}(L(x))^{j-(p-1)T^{(0)}_{L(x)}}) = \mathcal{G}(L(x))^j$ for any integer $j \geq ei\ (> (p-1)T^{(0)}_{L(x)} + t^{(1)}_{L(x)})$, one can verify $v_{L(x)}(x) = ei - (p-1)T^{(0)}_{L(x)}$, and thus $v_L(x) = i - (p-1)T^{(0)}_L$. □

3.3. On endomorphisms $\phi^n : \mathcal{F} \to \mathcal{F}$. In this subsection we will use the same notation as in §3.2, and show lemmas for §4. From now on, we focus on the case $\mathcal{F} = \mathcal{G}$. Let ϕ be a height h isogeny in $\mathrm{End}_{\mathcal{O}_K}(\mathcal{F})$ satisfying $[p](\ker \phi) = 0$ (*i.e.* $\ker \phi \subset \ker [p]$).

Lemma 3.11. *For any positive integer $m\ (< h)$,*

$$pt^{(h)}_K \leq (p-1)T^{(m)}_K + t^{(m+1)}_K \leq (p-1)T^{(m-1)}_K + t^{(m)}_K.$$

Proof. It is easily seen that

$$(p-1)T^{(m)}_K + t^{(m+1)}_K \leq (p-1)T^{(m)}_K + pt^{(m)}_K = (p-1)T^{(m-1)}_K + t^{(m)}_K.$$

Since $(p-1)T^{(h-1)}_K + t^{(h)}_K = pt^{(h)}_K$, the statement follows, by induction. □

Lemma 3.12. *Let n be any positive integer. For any $x \in \mathcal{F}$,*

$$\phi^n(x) \in \begin{cases} \mathcal{F}^{p^{hn} v_K(x)} & \text{if } v_K(x) < v_K(w_h)/(p^h)^{n-1} \\ \mathcal{F}^{pt^{(h)}_K} & \text{if } v_K(x) \geq v_K(w_h)/(p^h)^{n-1}. \end{cases}$$

Proof. Let $i := v_K(x)$. If $i < v_K(w_h)/(p^h)^{n-1}$ then repeated application of Proposition 3.9 yields $v_K(\phi^n(x)) = p^{hn} i$, and hence $\phi^n(x) \in \mathcal{F}^{p^{hn} i}$. Assume that $v_K(x) \geq v_K(w_h)/(p^h)^{n-1}$. Then, repeated application of Proposition 3.9 yields $v_K(\phi^{n-1}(x)) \geq v_K(w_h)$, and hence

$$v_K(\phi^n(x)) \geq (p-1)T^{(m-1)}_K + t^{(m)}_K$$

for some positive integer $m\,(\le h)$. By Lemma 3.11, we have $v_K(\phi^n(x)) \ge pt_K^{(h)}$. Thus, $\phi^n(x) \in \mathcal{F}^{pt_K^{(h)}}$. ☐

Lemma 3.13. *Let n be any positive integer. For any $x \in \mathcal{F}$,*

$$v_K(x) \begin{cases} = \dfrac{v_K(\phi^n(x))}{p^{hn}} & \text{if } v_K(\phi^n(x)) \in S_h \\ \ge \dfrac{v_K(w_h)}{p^{h(n-1)}} \left(= \dfrac{pt_K^{(h)}}{p^{hn}} \right) & \text{if } v_K(\phi^n(x)) \notin S_h. \end{cases}$$

Proof. The statement for the case where $v_K(\phi^n(x)) \in S_h$ follows from repeated application of Proposition 3.10. Assume that $v_K(\phi^n(x)) \notin S_h$. Consider the case $\phi^n(x) \neq 0$. If $v_K(x) \notin S_h$ then $v_K(x) \ge p^h v_K(w_h)$ from the definition of S_h. If $v_K(x) \in S_h$ then, by Proposition 3.9 there exists a positive integer $N\,(\le n)$ so that $v_K(\phi^N(x)) \notin S_h$, $v_K(\phi^{N-1}(x)) \in S_h$, and $v_K(\phi^{N-1}(x)) \ge v_K(w_h)$ by Proposition 3.10. Repeated application of Proposition 3.10 yields $v_K(x) = v_K(\phi^{N-1}(x))/p^{h(N-1)} \ge v_K(w_h)/p^{h(n-1)}$. We next consider the case $\phi^n(x) = 0$. Then, there exist some integers i, $k\,(1 \le i \le h,\ 0 \le k < n)$ so that $\phi_i \circ \cdots \circ \phi_1 \circ \phi^k(x) = 0$ and $\phi_{i-1} \circ \cdots \circ \phi_1 \circ \phi^k(x) \neq 0$. By Lemma 3.7, we have $v_K(\phi^k(x)) = v_K(w_i)$. If $v_K(\phi^k(x)) \in S_h$ then repeated application of Proposition 3.10 yields $v_K(x) = v_K(w_i)/p^{hk} \ge v_K(w_h)/p^{h(n-1)}$. If $v_K(\phi^k(x)) \notin S_h$ then, by the same method as in the case $v_K(\phi^n(x)) \notin S_h$, $\phi^n(x) \neq 0$ above, we have $v_K(x) \ge v_K(w_h)/p^{h(k-1)}$, and hence $v_K(x) > v_K(w_h)/p^{h(n-1)}$. ☐

Lemma 3.14. *If an integer i satisfies $(p-1)T_K^{(m)} + t_K^{(m+1)} < i \le (p-1)T_K^{(m)} + pt_K^{(m)}$ for some integer $m\,(1 \le m < h)$ then $\phi(\mathcal{F}^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}}) \subset \mathcal{G}^i$.*

Proof. Take $x \in \mathcal{F}^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}}$. Let $i_0 := v_K(x) \in \mathbb{Z}$. Then

$$v_K(w_{m+1}) < \frac{1}{p^m}\{i - (p-1)T_K^{(m)}\} \le i_0.$$

If $v_K(w_{m'+1}) < i_0 \le v_K(w_{m'})$ for some integer $m'\,(1 \le m' < h)$ then $m' \le m$, by $v_K(w_{m'+1}) \ge v_K(w_{m+1})$. From Proposition 3.9 and Lemma 3.11, we have

$$\begin{aligned} v_K(\phi(x)) &\ge (p-1)T_K^{(m')} + p^{m'} i_0 \\ &\begin{cases} \ge i & \text{if } m' = m \\ > (p-1)T_K^{(m')} + t_K^{(m'+1)} \ge (p-1)T_K^{(m-1)} + t_K^{(m)} > i & \text{if } m' < m. \end{cases} \end{aligned}$$

If $i_0 > v_K(w_1)$ then from Proposition 3.9 and Lemma 3.11 we have

$$v_K(\phi(x)) \ge (p-1)T_K^{(0)} + t_K^{(1)} \ge (p-1)T_K^{(m-1)} + t_K^{(m)} > i.$$

In each case, we have $\phi(x) \in \mathcal{F}^i$. ☐

4. Relative Kummer theory over local fields

In this section we will use the same notation as in §§3.2, 3.3. Here we establish relative Kummer theory.

For any positive integer n, consider the filtration

$$\mathcal{F}/\phi^n(\mathcal{F}) = \mathcal{F}^1/\phi^n(\mathcal{F}) \cap \mathcal{F}^1 \supseteq \mathcal{F}^2/\phi^n(\mathcal{F}) \cap \mathcal{F}^2 \supseteq \cdots \supseteq \mathcal{F}^i/\phi^n(\mathcal{F}) \cap \mathcal{F}^i \supseteq \cdots .$$

We write $(\mathcal{F}/\phi^n(\mathcal{F}))^i$ for the i-th submodule $\mathcal{F}^i/\phi^n(\mathcal{F}) \cap \mathcal{F}^i$.

The following theorem provides algebraic connection among $\{(\mathcal{F}/\phi^m(\mathcal{F}))^i\}_{i,m}$, relatively. In other words, it can be seen as a dissection of $\mathcal{F}/\phi^n(\mathcal{F})$ to an explicit layer structure.

Theorem 4.1 (Relative Kummer theory)**.** *Let i be any positive integer.*

(i) *If $0 < i \leq pt_K^{(h)}$ then for any integer $k\,(0 \leq k \leq n)$ the sequence*

$$0 \longrightarrow \frac{\ker \phi^k \cap \mathcal{F}^{i/p^{hk}}}{\phi^{n-k}(\ker \phi^n \cap \mathcal{F}) \cap \mathcal{F}^{i/p^{hk}}} \longrightarrow (\mathcal{F}/\phi^{n-k}(\mathcal{F}))^{i/p^{hk}} \xrightarrow{\phi^k} (\mathcal{F}/\phi^n(\mathcal{F}))^i \xrightarrow{\mathrm{id}} (\mathcal{F}/\phi^k(\mathcal{F}))^i \longrightarrow 0$$

is exact.

(ii) *If $(p-1)T_K^{(m)} + t_K^{(m+1)} < i \leq (p-1)T_K^{(m)} + pt_K^{(m)}$ for some integer $m\,(1 \leq m < h)$ then the sequence*

$$0 \longrightarrow \frac{(\ker \phi +_{\mathcal{F}} \phi^{n-1}(\mathcal{F})) \cap \mathcal{F}^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}}}{\phi^{n-1}(\mathcal{F}) \cap \mathcal{F}^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}}} \longrightarrow (\mathcal{F}/\phi^{n-1}(\mathcal{F}))^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}} \xrightarrow{\phi} (\mathcal{F}/\phi^n(\mathcal{F}))^i \xrightarrow{\mathrm{id}} (\mathcal{F}/\phi(\mathcal{F}))^i \longrightarrow 0$$

is exact.

(iii) *If $k(p-1)T_K^{(0)} + t_K^{(1)} < i \leq n(p-1)T_K^{(0)} + t_K^{(1)}$ for some integer $k\,(0 \leq k < n)$ then the sequence*

$$0 \longrightarrow \frac{(\ker \phi^k +_{\mathcal{F}} \phi^{n-k}(\mathcal{F})) \cap \mathcal{F}^{i-k(p-1)T_K^{(0)}}}{\phi^{n-k}(\mathcal{F}) \cap \mathcal{F}^{i-k(p-1)T_K^{(0)}}} \longrightarrow (\mathcal{F}/\phi^{n-k}(\mathcal{F}))^{i-k(p-1)T_K^{(0)}} \xrightarrow{\phi^k} (\mathcal{F}/\phi^n(\mathcal{F}))^i \longrightarrow 0$$

is exact.

(iv) *If $i > n(p-1)T_K^{(0)} + t_K^{(1)}$ then $(\mathcal{F}/\phi^n(\mathcal{F}))^i = 0$.*

Proof. (i) This is trivial for the case $k = 0$. Assume that $k > 0$. The canonical identity map id is clearly surjective. By Lemma 3.12, since $\phi^k(\phi^{n-k}(\mathcal{F}) \cap \mathcal{F}^{i/p^{hk}}) \subset \phi^n(\mathcal{F}) \cap \phi^k(\mathcal{F}^{i/p^{hk}}) \subset \phi^n(\mathcal{F}) \cap \mathcal{F}^i$, the map $\phi^k : (\mathcal{F}/\phi^{n-k}(\mathcal{F}))^{i/p^{hk}} \to (\mathcal{F}/\phi^n(\mathcal{F}))^i$ is well-defined. We next show that

$$\operatorname{Im} \phi^k = \ker \left[(\mathcal{F}/\phi^n(\mathcal{F}))^i \xrightarrow{\mathrm{id}} (\mathcal{F}/\phi^k(\mathcal{F}))^i\right] \quad (= (\phi^k(\mathcal{F}) \cap \mathcal{F}^i)/(\phi^n(\mathcal{F}) \cap \mathcal{F}^i)).$$

The inclusion $\operatorname{Im} \phi^k \subset \ker(\mathrm{id})$ is clear. Take any $\overline{\phi^k(x)} \in \ker(\mathrm{id})$, where $x \in \mathcal{F}$, $v_K(\phi^k(x)) = i_0$ for some integer $i_0 \geq i$. From Lemma 3.13, we have $v_K(x) \geq$

$i/p^{hk} \geq \lceil i/p^{hk} \rceil$ by $v_K(x) \in \mathbb{Z}$. Therefore $x \in \mathcal{F}^{i/p^{hk}}$, and so $\mathrm{Im}\,\phi^k \supset \ker(\mathrm{id})$. Finally,

$$\begin{aligned}\ker\phi^k &= \left\{ \overline{x} \in (\mathcal{F}/\phi^{n-k}(\mathcal{F}))^{i/p^{hk}} \;\middle|\; \phi^k(x) \in \phi^n(\mathcal{F}) \cap \mathcal{F}^i \right\} \\ &= \frac{(\ker\phi^k +_{\mathcal{F}} \phi^{n-k}(\mathcal{F})) \cap \mathcal{F}^{i/p^{hk}}}{\phi^{n-k}(\mathcal{F}) \cap \mathcal{F}^{i/p^{hk}}} \\ &= \frac{\ker\phi^k \cap \mathcal{F}^{i/p^{hk}}}{\phi^{n-k}(\mathcal{F}) \cap \mathcal{F}^{i/p^{hk}}} \quad \text{(by Lemma 3.13)} \\ &= \frac{\ker\phi^k \cap \mathcal{F}^{i/p^{hk}}}{\phi^{n-k}(\ker\phi^n \cap \mathcal{F}) \cap \mathcal{F}^{i/p^{hk}}}.\end{aligned}$$

(ii) The canonical identity map id is clearly surjective. By Lemma 3.14, since

$$\phi(\phi^{n-1}(\mathcal{F}) \cap \mathcal{F}^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}}) \subset \phi^n(\mathcal{F}) \cap \phi(\mathcal{F}^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}}) \subset \phi^n(\mathcal{F}) \cap \mathcal{F}^i,$$

the map $\phi : (\mathcal{F}/\phi^{n-1}(\mathcal{F}))^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}} \to (\mathcal{F}/\phi^n(\mathcal{F}))^i$ is well-defined. We next show that

$$\mathrm{Im}\,\phi = \ker\left[(\mathcal{F}/\phi^n(\mathcal{F}))^i \xrightarrow{\mathrm{id}} (\mathcal{F}/\phi(\mathcal{F}))^i \right] \quad (= (\phi(\mathcal{F}) \cap \mathcal{F}^i)/(\phi^n(\mathcal{F}) \cap \mathcal{F}^i)).$$

The inclusion $\mathrm{Im}\,\phi \subset \ker(\mathrm{id})$ is clear. Take any $\overline{\phi(x)} \in \ker(\mathrm{id})$, where $x \in \mathcal{F}$, $v_K(\phi(x)) = i_0$ for some integer $i_0 \geq i$. By Lemma 3.11, since $pt_K^{(h)} \leq (p-1)T_K^{(m)} + t_K^{(m+1)} < i$, we have $i_0 \notin S_h$. If $i_0 \in S_{m'}$ $(1 \leq m' < h)$ then $m' \leq m$, by $i_0 \geq i$. From Proposition 3.10, there exists $w \in \ker \cap \mathcal{F}$ so that

$$\begin{aligned} v_K(x +_{\mathcal{F}} w) &= \frac{1}{p^{m'}}\left\{ i_0 - (p-1)T_K^{(m')} \right\} \\ &\begin{cases} \geq \dfrac{1}{p^m}\left\{ i - (p-1)T_K^{(m)} \right\} & \text{if } m' = m \\ > v_K(w_{m'+1}) \geq v_K(w_m) \geq \dfrac{1}{p^m}\left\{ i - (p-1)T_K^{(m)} \right\} & \text{if } m' < m. \end{cases} \end{aligned}$$

If $i_0 \in \partial S_{m'}$ $(1 \leq m' \leq h)$ then $m' \leq m$, by $i_0 \geq i$. From Proposition 3.10, there exists $w \in \ker \cap \mathcal{F}$ so that

$$v_K(x +_{\mathcal{F}} w) = v_K(w_{m'}) \geq v_K(w_m) \geq \frac{1}{p^m}\left\{ i - (p-1)T_K^{(m)} \right\}.$$

If $i_0 \in S_0$ then by Proposition 3.10 there exists $w \in \ker \cap \mathcal{F}$ so that

$$v_K(x +_{\mathcal{F}} w) = i_0 - (p-1)T_K^{(0)} > v_K(w_1) \geq v_K(w_m) \geq \frac{1}{p^m}\left\{ i - (p-1)T_K^{(m)} \right\}.$$

Consequently, there exists $w \in \ker \cap \mathcal{F}$ so that

$$v_K(x +_{\mathcal{F}} w) \geq \frac{1}{p^m}\left\{ i - (p-1)T_K^{(m)} \right\} \geq \left\lceil \frac{1}{p^m}\left\{ i - (p-1)T_K^{(m)} \right\} \right\rceil$$

by $v_K(x +_{\mathcal{F}} w) \in \mathbb{Z}$. Therefore $\overline{\phi(x)} = \overline{\phi(x +_{\mathcal{F}} w)} \in \operatorname{Im}\phi$, and so $\operatorname{Im}\phi \supset \ker(\mathrm{id})$. Finally,

$$\ker\phi = \left\{ \overline{x} \in (\mathcal{F}/\phi^{n-1}(\mathcal{F}))^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}} \;\middle|\; \phi(x) \in \phi^n(\mathcal{F}) \cap \mathcal{F}^i \right\}$$
$$= \frac{(\ker\phi +_{\mathcal{F}} \phi^{n-1}(\mathcal{F})) \cap \mathcal{F}^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}}}{\phi^{n-1}(\mathcal{F}) \cap \mathcal{F}^{\frac{1}{p^m}\{i-(p-1)T_K^{(m)}\}}}.$$

(iii) This is trivial for the case $k = 0$. Assume that $k > 0$. From Proposition 3.9, $\phi^k(\phi^{n-k}(\mathcal{F}) \cap \mathcal{F}^{i-k(p-1)T_K^{(0)}}) \subset \phi^n(\mathcal{F}) \cap \phi^k(\mathcal{F}^{i-k(p-1)T_K^{(0)}}) = \phi^n(\mathcal{F}) \cap \mathcal{F}^i$, and hence $\phi^k : (\mathcal{F}/\phi^{n-k}(\mathcal{F}))^{i-k(p-1)T_K^{(0)}} \to (\mathcal{F}/\phi^n(\mathcal{F}))^i$ is well-defined. By Proposition 3.9, since $\phi^k(\mathcal{F}^{i-k(p-1)T_L^{(0)}}) = \mathcal{F}^i$, the map ϕ^k is surjective. Finally,

$$\ker\phi^k = \left\{ \overline{x} \in (\mathcal{F}/\phi^{n-k}(\mathcal{F}))^{i-k(p^h-1)t} \;\middle|\; \phi^k(x) \in \phi^n(\mathcal{F}) \cap \mathcal{F}^i \right\}$$
$$= \frac{(\ker\phi^k +_{\mathcal{F}} \phi^{n-k}(\mathcal{F})) \cap \mathcal{F}^{i-k(p^h-1)t}}{\phi^{n-k}(\mathcal{F}) \cap \mathcal{F}^{i-k(p^h-1)t}}.$$

(iv) This follows directly from Proposition 3.9. □

Our important purpose of relative Kummer theory is to understand the relative structure of Selmer groups, which is developed in the forthcoming paper [4].

References

[1] V. G. Berkovič, On the division by an isogeny of the points of an elliptic curve, *Math. USSR Sb.* **22** No.3 (1974), 473–492.

[2] A. Fröhlich, Formal Groups, Lecture Notes in Math. No.74, Springer-Verlag, 1968.

[3] M. Hazewinkel, Formal Groups and Applications, AMS Chelsea, 2012.

[4] R. Kozuma, On the relative structure of Selmer groups, in preparation.

[5] J. Lubin, One-parameter formal Lie groups over p-adic integer rings, *Ann. of Math.* **80** (1964), 464–484.

[6] J. Lubin, Finite subgroups and isogenies of one-parameter formal Lie groups, *Ann. of Math.* **85** (1967), 296–302.

[7] E. Lutz, Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps -adiques, *J. Reine Angew. Math.* **177** (1937), 238–247.

[8] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A* **273** (1971), 238–241.

College of International Management, Ritsumeikan Asia Pacific University, Oita 874-8577, Japan

E-mail address: rintaro@apu.ac.jp