ACTA ARITHMETICA
120.1 (2005)

On commuting properties of endomorphisms of formal A-modules over finite fields

by

HUA-CHIEH LI (Taipei)

1. Introduction. There have recently been increasing studies of discrete dynamical systems relevant to p-adic numbers; see, for example, [1, 2, 10]. In [10], Lubin studied the iterations of analytic transformations of the p-adic open unit disk with a fixed point at 0 and found out that two commuting transformations have the same set of pre-periodic points. However, very few interesting commuting examples are known outside endomorphisms of formal groups. In fact, Lubin [10] conjectures that such a phenomenon is exclusive to endomorphisms of formal group laws. There are some dynamical system results built on these ideas (see [5, 7, 9]).

Throughout this paper $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$ with maximal ideal $\mathcal{M}$ and residue field $k = \mathcal{O}/\mathcal{M}$. We call a power series $g(x) \in \mathcal{O}[[x]]$ *stable* if $g(0) = 0$ and $g'(0)$ is neither 0 nor a root of 1. As usual, we write $h(g(x)) = h \circ g(x)$; in a less standard notation, we denote by $g^{\circ n}(x)$ the n-fold composition of $g(x)$ with itself; this makes sense for negative n in case $g(x)$ is invertible.

Suppose $F(x, y)$ is a formal group law over the characteristic 0 ring $\mathcal{O}$. $F(x, y)$ is constructed by means of a series $l(x)$ defined over the field of fractions of $\mathcal{O}$, so that

$$F(x, y) = l^{\circ -1}(l(x) + l(y)).$$

This series, the *logarithm* of $F(x, y)$, plays an important role in formal dynamics over $\mathcal{O}$. For example, for $\alpha \in \mathcal{O}$ set $g(x) = l^{\circ -1}(\alpha \cdot l(x))$. Then $g(x) \in \mathrm{End}_{\mathcal{O}}(F)$ if and only if $g(x) \in \mathcal{O}[[x]]$. Hence, the map c from $\mathrm{End}_{\mathcal{O}}(F)$ to $\mathcal{O}$ given by $g(x) \mapsto g'(0)$ is an injective ring homomorphism and we will denote $g(x)$ by $[\alpha]_F(x)$. Moreover, suppose that $g(x)$ is stable. Then for $h(x) \in \mathcal{O}[[x]]$, $g(h(x)) = h(g(x))$ if and only if $h(x)$ is an endomorphism of $F(x, y)$.

2000 *Mathematics Subject Classification*: Primary 11S31, 16W60; Secondary 14L05, 37C25.

On the other hand, for a formal group over the field k of characteristic p, the situation changes. The logarithm, for example, does not exist under those circumstances and so the map c from $\mathrm{End}_k(F)$ to k given by $g(x) \mapsto g'(0)$ is no longer injective and two endomorphisms are no longer commutative under composition.

Let $F(x,y)$ be any formal group over $\mathcal{O}$. Denote by $\overline{F}(x,y)$ the coefficient-wise reduction of $F(x,y)$ to k. (For $g(x) \in \mathcal{O}[[x]]$, we will also denote by $\overline{g}(x) \in k[[x]]$ the coefficient-wise reduction of $g(x)$ to k.) Then $\overline{F}(x,y)$ is clearly a formal group over k. Additionally, if $F(x,y)$ has finite height, then the reduced map $\mathrm{End}_{\mathcal{O}}(F) \to \mathrm{End}_k(\overline{F})$ is injective. In fact, $\mathrm{End}_k(\overline{F})$ can be a rather larger ring than its characteristic counterpart.

With Lubin's original conjecture in mind, and with some experimental evidence, Sarkis (see [11]) makes the following conjecture:

Conjecture. *Let k be a finite field and let $\mathcal{F}(x,y)$ be a finite-height formal group over k. Let $\mu(x)$ be a non-torsion automorphism of $\mathcal{F}(x,y)$. Suppose that $\omega(x) \in k[[x]]$ and $\mu(\omega(x)) = \omega(\mu(x))$. Then $\omega(x)$ is an endomorphism of $\mathcal{F}(x,y)$.*

We remark that the assumption of $\mu(x)$ being a non-torsion automorphism is essential ([11]). There are some partial results supporting this conjecture. Let A be the ring of integers of some finite unramified extension of $\mathbb{Q}_p$. We can apply results in [3, Section 21.8] to show that if $\mathcal{F}(x,y)$ is a formal A-module and $\omega(x)$ commutes with all the endomorphisms of $\mathcal{F}(x,y)$ which correspond to A (i.e. if $\varrho_{\mathcal{F}} : A \to \mathrm{End}(\mathcal{F})$ is the A-module structure on $\mathcal{F}(x,y)$, then $\omega \circ \varrho_{\mathcal{F}}(\alpha) = \varrho_{\mathcal{F}}(\alpha) \circ \omega$ for all $\alpha \in A$), then $\omega(x)$ is an endomorphism of $\mathcal{F}(x,y)$. In [11, Theorem 46], Sarkis shows that if $\mu(x)$ is a unit of $\mathbb{Z}_p$ in the endomorphism ring of $\mathcal{F}(x,y)$ (i.e. $\mu(x) = [\alpha]_{\mathcal{F}}(x)$ with $\alpha \in \mathbb{Z}_p^*$), then the conjecture is true.

Definition 1.1. Let $\mathcal{O}$ be the ring of integers of some finite extension of $\mathbb{Q}_p$. For an element $\alpha \in \mathcal{O}^*$, suppose that $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = [\mathbb{F}_p(\overline{\alpha}) : \mathbb{F}_p] = n$. Then we call α a *primitive unramified element* of degree n.

Note that every unit in $\mathbb{Z}_p$ is a primitive unramified element.

Our main aim is to state a generalization of Sarkis' theorem [11, Theorem 46] and Hazewinkel's results.

Main Theorem (Theorem 3.2). *Let α be a primitive unramified element which is not a root of 1 and let $A = \mathbb{Z}[\alpha]$. Suppose that $(\mathcal{F}(x,y), \varrho_{\mathcal{F}})$ is a finite-height formal A-module over k. If $\omega(x) \in k[[x]]$ satisfies*

$$\varrho_{\mathcal{F}}(\alpha) \circ \omega = \omega \circ \varrho_{\mathcal{F}}(\alpha),$$

then $\omega(x)$ is an endomorphism of $\mathcal{F}(x,y)$.

Our approach uses a "not quite commutative" method developed by Honda [4]. In Section 2, we will describe some preliminary results about Honda's method and about Hazewinkel's functional equation lemma for constructing formal groups. Then in Section 3, we will give a detailed proof of the Main Theorem.

2. Preliminaries on formal groups over finite fields. In this section, we provide some necessary background for studying formal groups over the finite field $k = \mathbb{F}_q$ where $q = p^h$ for some prime number p. For simplicity, we only give results which will be needed later; see [3] for more details.

Let K be the unramified extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$ and maximal ideal $\mathcal{M}$ such that the residue field $\mathcal{O}/\mathcal{M}$ is k. Let A be a subring of $\mathcal{O}$ and let $\mathcal{F}(x, y)$ be a formal A-module over k. By the existence of a universal formal A-module (see [3]), there exists a formal A-module $F(x, y)$ over $\mathcal{O}$ that reduces modulo $\mathcal{M}$ to $\mathcal{F}(x, y)$. Hence, throughout this section, we use the following setting: K is the unramified extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$ and maximal ideal $\mathcal{M}$ such that $\mathcal{O}/\mathcal{M} = k$, and $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ is the Frobenius automorphism of K over $\mathbb{Q}_p$.

In [3], Hazewinkel gives a method of constructing formal groups by means of a certain recursive procedure. In our case, every formal group law $F(x, y)$ over $\mathcal{O}$ is a functional equation formal group law ([3, Proposition 20.1.3]). In other words, there exists $\{s_1, s_2, \ldots\} \subset \mathcal{O}$ such that the logarithm $l(x) \in K[[x]]$ of $F(x, y)$ satisfies the recursion formula

$$l(x) = g(x) + \frac{1}{p} \sum_{i=1}^{\infty} s_i \sigma_*^i l(x^{p^i}),$$

where $g(x) \in \mathcal{O}[[x]]$ and $\sigma_*^i l(x)$ is the power series obtained from $l(x)$ by applying the automorphism σ^i to the coefficients of $l(x)$. We remark that the equation above is in fact a recursion formula for the coefficients of $l(x)$. Indeed, let

$$g(x) = \sum_{i=1}^{\infty} c_i x^i \quad \text{and} \quad l(x) = \sum_{i=1}^{\infty} a_i x^i.$$

Then the a_n, $n = 1, 2, \ldots$, are recursively determined as follows. Write $n = p^r m$ where m is such that p does not divide m. Then we have

$$a_n = c_n + \frac{s_1}{p} \sigma(a_{n/p}) + \cdots + \frac{s_r}{p} \sigma^r(a_{n/p^r}).$$

Moreover, $F(x, y)$ is strictly isomorphic to a p-typical formal group law with logarithm $L(x) \in K[[x]]$ satisfying the recursion formula

$$L(x) = x + \frac{1}{p} \sum_{i=1}^{\infty} s_i \sigma_*^i L(x^{p^i}).$$

In this case, $L(x)$ can be written as

$$L(x) = \sum_{i=0}^{\infty} b_i x^{p^i},$$

and we have

$$b_0 = 1, \qquad b_r = \frac{s_1}{p}\,\sigma(b_{r-1}) + \cdots + \frac{s_{r-1}}{p}\,\sigma^{r-1}(b_1) + \frac{s_r}{p}.$$

We let $K_\sigma[[T]]$ be the non-commutative power series ring in one indeterminate T with the multiplication rule $Ta = \sigma(a)T$ for all $a \in K$, and let $\mathcal{O}_\sigma[[T]]$ be the subring of $K_\sigma[[T]]$ with coefficients in $\mathcal{O}$. Let

$$\eta = \sum_{i=0}^{\infty} c_i T^i \in K_\sigma[[T]], \qquad f(x) = \sum_{j=1}^{\infty} a_j x^j \in K[[x]].$$

We define

$$\eta * f(x) = \sum_{i=0}^{\infty} c_i \sum_{j=1}^{\infty} \sigma^i(a_j)(x^{p^i})^j.$$

It is obvious from the definition that for $\eta, \theta \in K_\sigma[[T]]$ and $f(x) \in K[[x]]$,

$$(\eta + \theta) * f(x) = \eta * f(x) + \theta * f(x), \qquad (\eta\theta) * f(x) = \eta * (\theta * f(x)).$$

Now let

$$\eta = p - \sum_{i=1}^{\infty} s_i T^i \in \mathcal{O}_\sigma[[T]].$$

We calculate that the coefficients b_i of $\eta^{-1}p = \sum_{i=0}^{\infty} b_i T^i$ satisfy

$$b_0 = 1, \quad b_r = \frac{s_1}{p}\,\sigma(b_{r-1}) + \cdots + \frac{s_{r-1}}{p}\,\sigma^{r-1}(b_1) + \frac{s_r}{p}.$$

Comparing this with the recursive relation of the functional equation lemma for the logarithm, we have

$$(\eta^{-1}p) * i(x) = L(x), \qquad \text{where } i(x) = x.$$

As mentioned before, the functional equation techniques can be used to study endomorphisms of formal group laws over characteristic 0 rings. For example, $f(x) \in \mathcal{O}[[x]]$ is an endomorphism of a formal group over $\mathcal{O}$ with logarithm $l(x)$ if and only if $l^{\circ -1}(f'(0) \cdot l(x)) \in \mathcal{O}[[x]]$. For endomorphisms of formal group laws over finite fields, Honda [4] gives the following similar results:

Lemma 2.1. *Let $F(x,y)$ be the formal group law over $\mathcal{O}$ with logarithm $l(x)$ satisfying the recursion formula*

$$l(x) = x + \frac{1}{p} \sum_{i=1}^{\infty} s_i \sigma_*^i l(x^{p^i}).$$

Let $\vartheta \in \mathcal{O}_\sigma[[T]]$ *and let*

$$\eta = p - \sum_{i=1}^{\infty} s_i T^i.$$

(1) *Set* $\alpha_\vartheta(x) = l^{\circ -1}((\vartheta * l)(x))$. *Then* $\alpha_\vartheta(x) \in \mathcal{O}[[x]]$ *if and only if there exists an* $\eta_\vartheta \in \mathcal{O}_\sigma[[T]]$ *such that* $\eta_\vartheta \eta = \eta \vartheta$.

(2) *If* $\alpha_\vartheta(x) \in \mathcal{O}[[x]]$, *then reducing modulo* $\mathcal{M}$, $\overline{\alpha}_\vartheta(x)$ *is an endomorphism of* $\overline{F}(x,y)$.

(3) *If* $\vartheta_1, \vartheta_2 \in \mathcal{O}_\sigma[[T]]$ *and* $\alpha_{\vartheta_1}, \alpha_{\vartheta_2} \in \mathcal{O}[[x]]$, *then*

$$\overline{\alpha}_{\vartheta_1\vartheta_2}(x) = \overline{\alpha}_{\vartheta_1}(\overline{\alpha}_{\vartheta_2}(x)).$$

(4) *If* $\vartheta \in \mathcal{O}_\sigma[[T]]$ *and* $\alpha_\vartheta \in \mathcal{O}[[x]]$, *then* $\overline{\alpha}_\vartheta(x) = 0$ *if and only if* ϑ *is in the right ideal of* $\mathcal{O}_\sigma[[T]]$ *generated by* η.

(5) *Every element of* $\mathrm{End}_k(\overline{F}(x,y))$ *is of the form* $\overline{\alpha}_\vartheta(x)$ *for some* $\vartheta \in \mathcal{O}_\sigma[[T]]$.

Lemma 2.1 provides us an explicit method to describe endomorphisms of a formal group law over a finite field.

EXAMPLE 2.2. Consider the formal group $F_h(x,y)$ with logarithm

$$l_h(x) = x + \frac{1}{p}\, x^{p^h} + \frac{1}{p^2}\, x^{p^{2h}} + \cdots.$$

Clearly, $F_h(x,y)$ is a formal group of height h defined over $\mathbb{Z}_p$. Let K be the unramified extension of $\mathbb{Q}_p$ of degree h. Considering $\eta = p - T^h \in \mathcal{O}_\sigma[[T]]$, we have $l_h(x) = (\eta^{-1}p) * i(x)$. It is easy to see that for every $\vartheta \in \mathcal{O}_\sigma[[T]]$, $\eta\vartheta = \vartheta\eta$. Therefore, by Lemma 2.1, $\mathrm{End}_{\mathbb{F}_{p^h}}(\overline{F}_h(x,y))$ is isomorphic to the noncommutative ring $\mathcal{O}_\sigma[[T]]/(\eta)$. Let K^{nr} be the maximal unramified extension of K and let $\mathcal{O}^{\mathrm{nr}}$ be the integral closure of $\mathcal{O}$ in K^{nr}. It is easy to see that the only series $\theta \in \mathcal{O}^{\mathrm{nr}}_\sigma[[T]]$ with $\eta_\theta\eta = \eta\theta$ for some $\eta_\theta \in \mathcal{O}^{\mathrm{nr}}_\sigma[[T]]$ are the series in $\mathcal{O}_\sigma[[T]]$. Therefore, by Lemma 2.1 again, we have

$$E_h = \mathrm{End}_{k^{\mathrm{sc}}}(\overline{F}_h(x,y)) = \mathrm{End}_k(\overline{F}_h(x,y)),$$

where k^{sc} is the separable closure of $k = \mathbb{F}_{p^h}$ corresponding to the residue field of $\mathcal{O}^{\mathrm{nr}}$. It can be checked that E_h is a free module of rank h^2 over $\mathbb{Z}_p$. Moreover, if we consider $D_h = E_h \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, then D_h is a central division algebra over $\mathbb{Q}_p$ of invariant equal to h^{-1}.

We remark that we are interested in this example because over a separably closed field of characteristic $p > 0$, the one-dimensional formal group laws are classified by their heights ([6, Theorem IV] or [3, Theorem 19.4.1]). In other words, every one-dimensional formal group law over a separably closed field of characteristic $p > 0$ of height h is isomorphic to $\overline{F}_h(x,y)$.

3. Main Theorem. Suppose that α is a primitive unramified element and $A = \mathbb{Z}[\alpha]$. Recall that if $(\mathcal{F}(x,y), \varrho_{\mathcal{F}})$ is a finite-height formal A-module over k, then $\mathcal{F}(x,y)$ is actually a reduction of a formal group. More precisely, there exists a field K which is an unramified extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$ and maximal ideal $\mathcal{M}$ such that the residue field $\mathcal{O}/\mathcal{M}$ is k and there exists a formal group law $F(x,y)$ over $\mathcal{O}$ such that $\overline{F}(x,y) = \mathcal{F}(x,y)$ and $\overline{[\alpha]}_F(x) = \varrho_{\mathcal{F}}(\alpha)$.

First we remark that although $\varrho_{\mathcal{F}}(\alpha) \in k[[x]]$ is of the form $\overline{[\alpha]}_F(x)$, if $G(x,y) \in \mathcal{O}[[x,y]]$ is another formal group law such that $\overline{F}(x,y) = \overline{G}(x,y)$, it does not mean that $\varrho_{\mathcal{F}}(\alpha) = \overline{[\alpha]}_G(x)$.

Because all the formal groups over k of the same height are isomorphic over k^{sc}, without loss of generality, we can suppose that $\varrho_{\mathcal{F}}(\alpha) = \overline{[\alpha]}_F(x)$ where $\overline{F}(x,y) = \overline{F}_h(x,y)$. ($F_h(x,y)$ is the formal group defined in Example 2.2.) By the remark above, $\varrho_{\mathcal{F}}(\alpha)$ may not be equal to $\overline{[\alpha]}_{F_h}(x)$. But if we consider $\mathrm{End}(\overline{F}_h(x,y))$ as the maximal order of a central division algebra D over $\mathbb{Q}_p$ of rank h, then $\varrho_{\mathcal{F}}(\alpha)$ and $\overline{[\alpha]}_{F_h}(x)$ are in L_1 and L_2 respectively, where L_1 and L_2 are subfields of D which are unramified of the same degree over $\mathbb{Q}_p$. By the Skolem–Noether theorem, there exists $\gamma \in D$ such that $\gamma^{-1} \cdot \varrho_{\mathcal{F}}(\alpha) \cdot \gamma = \overline{[\alpha]}_{F_h}(x)$. If $\omega(x)$ commutes with $\varrho_{\mathcal{F}}(\alpha)$, then $\gamma^{-1} \cdot \omega(x) \cdot \gamma$ also commutes with $\overline{[\alpha]}_{F_h}(x)$. If we can show that $\gamma^{-1} \cdot \omega(x) \cdot \gamma$ is an endomorphism of $\overline{F}_h(x,y)$ (in other words, $\gamma^{-1} \cdot \omega(x) \cdot \gamma$ is in the maximal order of D), then $\omega(x)$ is also in the maximal order of D and hence is an endomorphism of $\overline{F}(x,y) = \overline{F}_h(x,y)$. Therefore without loss of generality, we assume that $\varrho_{\mathcal{F}}(\alpha) = \overline{[\alpha]}_{F_h}(x)$ and $\varrho_{\mathcal{F}}(\alpha) \circ \omega = \omega \circ \varrho_{\mathcal{F}}(\alpha)$, and claim that $\omega(x)$ is an endomorphism of $\overline{F}_h(x,y)$.

Let $l(x)$ be the logarithm of $F_h(x,y)$. Our goal is to show that there exists $\eta \in \mathcal{O}_\sigma[[T]]$ such that $l^{\circ -1}(\eta * l(x))$ is equal to $\omega(x)$ after reducing modulo $\mathcal{M}$.

LEMMA 3.1. *Let $\mu(x) = \overline{[\alpha]}_{F_h}(x) \in k[[x]]$ where α is primitive unramified of degree s and $k = \mathbb{F}_{p^h}$. Suppose that $f(x) \in k^{\mathrm{sc}}[[x]]$ is such that $f(\mu(x)) = \mu(f(x))$. Then $f(x) \equiv ax^{p^r} \pmod{x^{p^r+1}}$ with $a \in k \setminus \{0\}$ and $r = \lambda s$ for some $\lambda \in \mathbb{N} \cup \{0\}$.*

Proof. By a similar proof to Lubin's [10, Main Theorem 6.3], we see that $f(x) = g(x^{p^r})$ for some $g(x) \in k^{\mathrm{sc}}[[x]]$ with $g'(0) \neq 0$.

Since $\mu'(0) \in k \setminus \{0\}$, by iterating $\mu(x)$ a certain number of times (say m times), we can suppose that $f(x)$ commutes with $\xi(x) = \mu^{\circ m}(x)$ where

$$\xi(x) \equiv x + b_0 x^{p^t} \pmod{x^{p^t+1}} \quad \text{for some } b_0 \in k \text{ and } t \in \mathbb{N},$$

and

$$\xi^{\circ p}(x) \equiv x + b_1 x^{p^{t+h}} \pmod{x^{p^{t+h}+1}} \quad \text{for some } b_1 \in k.$$

(This can be seen by using the fact that $[\alpha]_{F_h}(x)$ is an endomorphism of $F_h(x, y)$ or the fact that $\mathrm{Height}([\alpha]_{F_h}(x)) = h$ as in [8].)

Now write $f(x) \equiv ax^{p^r} \pmod{x^{p^r+1}}$. The coefficient of the leading term of $f(\mu(x))$ is $a\overline{\alpha}^{p^r}$ and the coefficient of the leading term of $\mu(f(x))$ is $a\overline{\alpha}$. This shows that $\alpha \equiv \alpha^{p^r} \pmod{\mathcal{M}}$. Since α is primitive unramified of degree s, it implies that $r = \lambda s$ for some $\lambda \in \mathbb{N} \cup \{0\}$.

Finally, we claim that $a \in k$. Consider the equality $\xi(f(x)) = f(\xi(x))$. Since

$$f(\xi(x)) - f(x) = g((\xi(x))^{p^r}) - g(x^{p^r}) = g'(0) \cdot (b_0 x^{p^t})^{p^r} + \text{higher terms},$$

the coefficient of the leading term of $f(\xi(x)) - f(x)$ is $ab_0^{p^r}$. Since $F_h(x, y) \in \mathbb{Z}_p[[x, y]]$, we have $[\alpha]_{F_h}(x) \in \mathbb{Z}_p[\alpha][[x]]$ and hence $\mu(x) = \overline{[\alpha]}_{F_h}(x) \in \mathbb{F}_{p^s}[[x]]$ (so that $\xi(x) \in \mathbb{F}_{p^s}[[x]]$). In other words,

$$b_0^{p^r} = b_0^{p^{s\lambda}} = b_0.$$

Therefore, the leading coefficient of $f(\xi(x)) - f(x)$ is ab_0. On the other hand, the leading coefficient of $\xi(f(x)) - f(x)$ is $a^{p^t} b_0$. Since

$$f(\xi(x)) - f(x) = \xi(f(x)) - f(x),$$

we have $a^{p^t} = a$. Similarly, by considering

$$f(\xi^{\circ p}(x)) - f(x) = \xi^{\circ p}(f(x)) - f(x),$$

we obtain $a^{p^{t+h}} = a$. Therefore $a^{p^h} = a$, and hence $a \in k$. ∎

Now we have all the ingredients to prove our main theorem.

THEOREM 3.2. *Let $\mathcal{F}(x, y)$ be a finite-height formal group over k and let $\mu(x)$ be a non-torsion automorphism of $\mathcal{F}(x, y)$. Suppose that there exists a formal group $F(x, y) \in \mathcal{O}[[x, y]]$ such that $\overline{F}(x, y) = \mathcal{F}(x, y)$ and $\mu(x) = \overline{[\alpha]}_F(x)$ with α a primitive unramified element. If $\omega(x) \in k^{\mathrm{sc}}[[x]]$ satisfies $\mu(\omega(x)) = \omega(\mu(x))$, then $\omega(x)$ is also an endomorphism of $\mathcal{F}(x, y)$.*

Proof. Suppose that the height of $\mathcal{F}(x, y)$ is h. As mentioned before, without loss of generality, we can assume that $F(x, y) = F_h(x, y)$, $\mathcal{F}(x, y) = \overline{F}_h(x, y)$ and K is unramified over $\mathbb{Q}_p$ of degree h with ring of integers $\mathcal{O}$ and maximal ideal $\mathcal{M}$ such that $\mathcal{O}/\mathcal{M} = k = \mathbb{F}_{p^h}$.

Let $l(x)$ be the logarithm of $F_h(x, y)$ and let $u(x) = l^{\circ -1}(\alpha \cdot l(x)) = [\alpha]_{F_h}(x)$. Then we have $\mu(x) = \overline{u}(x)$. Suppose that $\omega(x)$ commutes with $\mu(x)$. To prove our theorem, by Lemma 2.1, it is enough to show that there exists $\theta \in \mathcal{O}_\sigma[[T]]$ such that $f(x) = l^{\circ -1}(\theta * l(x))$ and $\omega(x) = \bar{f}(x)$.

Suppose that α is a primitive unramified element of degree s. Let $\omega(x) \equiv a_0 x^n \pmod{x^{n+1}}$ with $a_0 \neq 0$. Then by Lemma 3.1, we have $a_0 \in k$ and $n = p^{\lambda s}$. Choose any $\alpha_0 \in \mathcal{O}$ such that $a_0 = \overline{\alpha}_0$ and let $\theta_0 = -\alpha_0 T^{\lambda s} \in \mathcal{O}_\sigma[[T]]$. By Example 2.2, we have $l^{\circ -1}(\theta_0 * l(x)) \in \mathcal{O}[[x]]$. Let $\tau_0(x) \in k[[x]]$ be such that $\tau_0(x) = \overline{l^{\circ -1}(\theta_0 * l(x))}$. Consider

$$\omega_1(x) = \mathcal{F}(\omega(x), \tau_0(x)).$$

We have

$$\begin{aligned}\omega_1(\mu(x)) &= \mathcal{F}(\omega(\mu(x)), \tau_0(\mu(x))),\\ \mu(\omega_1(x)) &= \mu(\mathcal{F}(\omega(x), \tau_0(x))) = \mathcal{F}(\mu(\omega(x)), \mu(\tau_0(x))).\end{aligned}$$

Since $\sigma^s(\alpha) = \alpha$, we have

$$\theta_0 \cdot \alpha = -\alpha_0 \sigma^{\lambda s}(\alpha) T^{\lambda s} = -\alpha\alpha_0 T^{\lambda s} = \alpha \cdot \theta_0$$

in $\mathcal{O}_\sigma[[T]]$, and hence Lemma 2.1 says that $\tau_0(\mu(x)) = \mu(\tau_0(x))$. This implies that $\omega_1(\mu(x)) = \mu(\omega_1(x))$. It is clear that the initial degree of $\omega_1(x)$ is greater than the initial degree of ω. The proof is completed by induction. ∎

The series $\mu(x)$ in Theorem 3.2 is a reduction of an endomorphism of a formal group over $\mathcal{O}$. The series $\omega(x)$ may not be a reduction of an endomorphism. However, our next result shows that under a certain condition, $\omega(x)$ does come from an endomorphism over $\mathcal{O}$.

COROLLARY 3.3. *Let K be unramified over $\mathbb{Q}_p$ of degree h. Let $\mathcal{F}(x, y)$ be a formal group over k of height h and let $F(x, y)$ be a formal group over $\mathcal{O}$ such that $\overline{F}(x, y) = \mathcal{F}(x, y)$. Suppose that $\mu(x) = \overline{[\alpha]}_F(x)$ is a non-torsion automorphism of $\mathcal{F}(x, y)$ with α a primitive unramified element of degree h and suppose that $\omega(x) \in k^{\mathrm{sc}}[[x]]$ is such that $\mu(\omega(x)) = \omega(\mu(x))$. Then $\omega(x) = \overline{[\beta]}_F(x)$ for some $\beta \in \mathcal{O}$.*

Proof. Without loss of generality, we can assume that $F(x, y) = F_h(x, y)$ and $\mathcal{F}(x, y) = \overline{F}_h(x, y)$. We use the same notations as in the proof of Theorem 3.2.

From Theorem 3.2, there exists $\theta \in \mathcal{O}_\sigma[[T]]$ such that $f(x) = l^{\circ -1}(\theta * l(x))$ and $\omega(x) = \bar{f}(x)$. The commutativity of $\mu(x)$ and $\omega(x)$ also implies that $\theta \cdot \alpha = \alpha \cdot \theta$ in $\mathcal{O}_\sigma[[T]]$. Suppose that

$$\theta \equiv a_0 + a_1 T + \cdots + a_{h-1} T^{h-1} \pmod{p - T^h}$$

in $\mathcal{O}_\sigma[[T]]$. We have

$$\begin{aligned}\theta \cdot \alpha &\equiv a_0\alpha + a_1\sigma(\alpha)T + \cdots + a_{h-1}\sigma^{h-1}(\alpha)T^{h-1} \pmod{p - T^h},\\ \alpha \cdot \theta &\equiv \alpha a_0 + \alpha a_1 T + \cdots + \alpha a_{h-1} T^{h-1} \pmod{p - T^h}.\end{aligned}$$

The assumption that α is primitive unramified of degree h implies that $\theta \equiv a_0 \pmod{p - T^h}$ and hence by Lemma 2.1,

$$\omega(x) = \bar{f}(x) = \overline{l^{\circ -1}(\theta * l(x))} = \overline{l^{\circ -1}(a_0 \cdot l(x))} = \overline{[a_0]}_F(x). \ ∎$$

REMARK 3.4. Let $A = \mathcal{O}$. In the language of formal A-modules, the condition in Corollary 3.3 says that $\mathcal{F}(x, y)$ is a formal A-module of A-height equal to 1. Therefore, every A-endomorphism actually comes from A.

Finally, we remark that the hypothesis on $\mu(x)$ can be weakened. Consider a non-primitive unramified unit $\alpha = \alpha_0 + p^n\alpha_1$ with $n \in \mathbb{N}$ and α_0, α_1 satisfying the following:

1. α_1 is primitive.
2. α_0 is a unit such that $\alpha_0 \in \mathbb{Z}_p[\alpha_1]$ and $\alpha_0^r \equiv 1 \pmod{p^n}$, where r is the least positive integer such that $\overline{\alpha}_0^r = 1$ in k (i.e. r is the order of $\overline{\alpha}_0$ in k).

Then, for any non-negative integer s, we have $\alpha^{p^s r} = 1 + p^{s+n}\alpha'$, with α' a primitive unramified element of the same degree as α_1. Therefore, by using a similar argument to the proof of Theorem 3.2, we can show that if $\mu(x) = \overline{[\alpha]}_F(x)$ is a non-torsion automorphism of $\mathcal{F}(x, y)$, and $\omega(x) \in k^{\mathrm{sc}}[[x]]$ satisfies $\mu(\omega(x)) = \omega(\mu(x))$, then $\omega(x)$ is also an endomorphism of $\mathcal{F}(x, y)$.

References

[1] D. Bosio and F. Vivaldi, *Round-off errors and p-adic numbers*, Nonlinearity 13 (2000), 309–322.

[2] B. Green and M. Matignon, *Order p automorphisms of the open disk of a p-adic field*, J. Amer. Math. Soc. 12 (1999), 269–303.

[3] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, New York, 1978.

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

[5] F. Laubie, A. Movahhedi et A. Salinier, *Systèmes dynamiques non archimédiens et corps des normes*, Compos. Math. 132 (2002), 57–98.

[6] M. Lazard, *Sur les groupes de Lie formels à un paramètre*, Bull. Soc. Math. France 83 (1955), 251–274.

[7] H.-C. Li, *p-adic dynamical systems and formal groups*, Compos. Math. 104 (1996), 41–54.

[8] —, *On heights of p-adic dynamical systems*, Proc. Amer. Math. Soc. 130 (2002), 379–386.

[9] —, *On dynamics of power series over unramified extensions of* $\mathbb{Q}_p$, J. Reine Angew. Math. 545 (2002), 183–200.

[10] J. Lubin, *Nonarchimedean dynamical systems*, Compos. Math. 94 (1994), 321–346.

[11] G. Sarkis, *Formal groups and p-adic dynamical systems*, doctoral thesis, Brown Univ., 2001.

Department of Mathematics
National Taiwan Normal University
88, Sec. 4, Ting Chou Road
Taipei, Taiwan, R.O.C.
E-mail: li@math.ntnu.edu.tw

Received on 14.12.2004
and in revised form on 17.6.2005 (4904)