Compositio Mathematica **130:** 75–88, 2002.

p-Typical Dynamical Systems and Formal Groups

HUA-CHIEH LI
Department of Mathematics, National Taiwan Normal University, Taipei, Taiwan, R.O.C.
e-mail: li@math.ntnu.edu.tw

(Received 13 December 1999; accepted in final form 24 October 2000)

Abstract: By using the idea of logarithm, we give an effective method to decide whether a stable series is an endomorphism of a formal group or not. We also give examples that contradict Lubin's conjecture.

Mathematics Subject Classifications (2000). 11S31, 11F85, 11L05.

Key words. stable series, logarithm, *p*-typical dynamical systems, *p*-typical formal groups.

1. Introduction

A one-dimensional formal group law over a ring A is a formal power series in two variables $F(x, y) \in A[[x, y]]$ such that

$$F(x, 0) = x, \qquad F(0, y) = y, \qquad F(x, F(y, z)) = F(F(x, y), z).$$

An endomorphism of $F(x, y)$ is a power series $f(x) \in A[[x]]$ without constant term such that

$$f(F(x, y)) = F(f(x), f(y)).$$

In the theory of formal groups over the ring of integers in a finite extension of the p-adic field $\mathbb{Q}_p$, the field generated by all roots or fixed points of the iterates of an endomorphism is well known due to the efforts of J. Lubin and J. Tate [11] and J-P. Serre [12]. We are interested in finding conditions for a series to be an endomorphism of a formal group. In [5], we give a necessary and sufficient condition for a stable noninvertible series to be an endomorphism of a formal group. The result is not satisfactory, at least for practical purposes, since it involves infinitely many iterations.

Let A be an integral domain and $f(x) \in A[[x]]$. We say that $f(x)$ is *stable* if $f(0) = 0$ and $f'(0)$ is not 0 nor a root of 1. A series $h(x) \in A[[x]]$ without constant term is called *invertible* if there exists a series $g(x) \in A[[x]]$ such that $h(g(x)) = g(h(x)) = x$. A necessary and sufficient condition for $h(x)$ to be invertible is that $h'(0) \in A^*$. Since $h(x)$ is invertible, it and its iterates can have no other roots than 0, but the fixed points of the iterates of $h(x)$ (that is, the periodic points of $h(x)$) are of serious interest. In the other case, if $f(x) \in A[[x]]$ without constant

term and $0 \neq f'(0) \in A \setminus A^*$, then we call $f(x)$ a *noninvertible stable series*. In this case, $f(x)$ can have no other fixed points than 0, but the roots of its iterates, now play a role parallel to the periodic points of an invertible series. These two studies become no longer disjoint in case an invertible series commutes (under composition) with a noninvertible series, a phenomenon familiar enough when all are endomorphisms of a formal group. (Please see [9] for more detail.) In the case of a formal group over the ring of local integers, its endomorphisms form a commuting family (under composition) which contains both stable invertible series and stable noninvertible series. In [9], Lubin conjectures that for a stable invertible series $u(x)$ to commute with a noninvertible series $f(x)$, there must be a formal group somehow in the background. In particular, in this case, if all the iterates of $f(x)$ have only simple roots, Lubin [10] conjectures that $f(x)$ must be an endomorphism of a formal group. The results in [6] and [7] support this conjecture.

In this paper, by using the idea of logarithm, we give a more effective method to decide whether a stable series is an endomorphism of a formal group or not. When $f(x)$ is a stable series over a characteristic zero integral domain A, its *logarithm* is the unique series $L_f(x)$ over the fraction field of A with $L_f'(0) = 1$ and $L_f(f(x)) = f'(0)L_f(x)$. When $f(x)$ is an endomorphism of a formal group $F(x, y)$. The logarithm of $f(x)$ is exactly the logarithm of the formal group. Thus $L_f(x)$ is the unique series such that $L_f'(0) = 1$ and $F(x, y) = L_f^{-1}(L_f(x) + L_f(y))$, where $L_f^{-1}(x)$ is the inverse power series, i.e. $L_f^{-1}(L_f(x)) = L_f(L_f^{-1}(x)) = x$.

Because we are mainly interested in the roots of iterates and periodic points of a stable series and when two stable series commute to each other, they have the same set of roots of iterates and periodic points (see [9, Propositions 2.1, 3.1 and 3.2] for more detail), we naturally have the following definition.

DEFINITION. Let $f(x)$ be a stable series over a characteristic zero integral domain A. Then the dynamical system over A arising from $f(x)$ is the set of all $g(x)$ which are stable series over A with $g(f(x)) = f(g(x))$. In particular, if $f(x)$ is an endomorphism of a formal group over A, then we call the dynamical system over A arising from $f(x)$, a dynamical system arising from a formal group.

Given two systems $\mathcal{S}_1$ and $\mathcal{S}_2$ over A, we say that they are *isomorphic* if there exist $f_1(x) \in \mathcal{S}_1$, $f_2(x) \in \mathcal{S}_2$ and an invertible series $u(x)$ over A such that $u(f_1(x)) = f_2(u(x))$. In addition, if $u'(0) = 1$, then we say these two systems are *strictly isomorphic*. It is easy to check that if $\mathcal{S}_1$ is a system arising from a formal group over A and $\mathcal{S}_1$ is isomorphic to $\mathcal{S}_2$, then $\mathcal{S}_2$ is also a system arising from a formal group over A.

In [9], we know that the relation of commuting is an equivalence relation and $g(f(x)) = f(g(x))$ if and only if $L_f(x) = L_g(x)$. Hence, we can use the logarithm of $f(x)$ to characterize the dynamical system arising from $f(x)$ and call it the *logarithm* of this system. In conformity with the formal group theory in [2], we will

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

call a system p-typical if its logarithm $L(x)$ is of the form

$$L(x) = x + \sum_{n=1}^{\infty} a_n x^{p^n}.$$

If a system arising from a formal group is p-typical, then we will call such a formal group a *p-typical formal group*.

When p is a prime and A is a $\mathbb{Z}_p$-algebra, it is proven by Hazewinkel in [2] that every dynamical system arising from a formal group is strictly isomorphic to a p-typical dynamical system. More precisely, in Proposition 3.2, we will see that if $L(x) = x + \sum_{i=2}^{\infty} a_i x^i$ is the logarithm of a formal group over A, then $l(x) = x + \sum_{n=1}^{\infty} a_{p^n} x^{p^n}$ is also the logarithm of a formal group over A. Furthermore, these two formal group are strictly isomorphic over A.

The main theorem of this paper is the following theorem:

MAIN THEOREM (see Theorem 4.3). *Let A be a $\mathbb{Z}_p$-algebra and $\mathcal{S}$ be a dynamical system over A. Suppose that in $\mathcal{S}$ there exists a stable series $g(x) \in A[[x]]$ with $g'(0) \in \mathbb{Z}_p$ and $g'(0)^p - g'(0) \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$. Then $\mathcal{S}$ is a dynamical system arising from a formal group over A if and only if $\mathcal{S}$ is isomorphic to a p-typical dynamical system.*

In practice, this theorem provides us a much easier method to determine whether a stable series is an endomorphism of a formal group or not. Let $f(x)$ be a stable series over A and let

$$L_f(x) = x + \sum_{i=2}^{\infty} a_i x^i$$

be the logarithm of $f(x)$. We consider

$$l(x) = x + \sum_{n=1}^{\infty} a_{p^n} x^{p^n},$$

or in other words by simply striking out all terms in $L_f(x)$ that should not occur in the logarithm of a p-typical system. We will see later (Lemma 2.1) that if $L_f^{-1}(l(x)) \in A[[x]]$, then the system arising from $f(x)$ is strictly isomorphic to the system with logarithm $l(x)$, which is p-typical. Furthermore, if there exists $g(x) \in A[[x]]$ with $g'(0) = p$ such that $f(g(x)) = g(f(x))$, then $g(x)$ is in the system arising from $f(x)$ and $g'(0)^p - g'(0) = p^p - p \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$. Therefore, by our main theorem, $f(x)$ is an endomorphism of a formal group over A. In fact, combining with Proposition 3.2 mentioned above, our main theorem says that $f(x)$ is an endomorphism of a formal group over A if and only if $L_f^{-1}(l(x)) \in A[[x]]$ and there exists $g(x) \in A[[x]]$ with $g'(0) = p$ such that $f(g(x)) = g(f(x))$.

Since $\mathbb{Z}_p$ is contained in the endomorphism ring of every formal group over $\mathbb{Z}_p$-algebra, the condition in our main theorem is also necessary. In the final, we will supply examples to illustrate that this condition is in fact sharp. We also give

examples that contradict Lubin's conjecture. To my knowledge, these are the first kind of p-adic dynamical systems which we know that contain both stable invertible series and stable noninvertible series but there is no formal group in the background.

2. Basic Tools

In this section, A is an integral domain and K is the fraction field of A. Let $f(x) \in A[[x]]$ be a stable series. In [9], Lubin shows that we can find a unique $L_f(x)$ with $L_f'(0) = 1$ such that $L_f(f(x)) = f'(0)L_f(x)$. Therefore, for any $b \in K$, $g(x) = L_f^{-1}(bL_f(x))$ is the unique power series in $K[[x]]$ with $g'(0) = b$ which commutes with $f(x)$. Lubin also shows that for any stable series $g(x) \in K[[x]]$, $f(g(x)) = g(f(x))$ if and only if $L_f(x) = L_g(x)$. Therefore, given a system $\mathcal{S}$ over A with logarithm $L(x)$, every element of $\mathcal{S}$ is of the form $L^{-1}(aL(x))$ for some $a \in A$ such that $L^{-1}(aL(x)) \in A[[x]]$.

LEMMA 2.1. *Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two systems over A with logarithm $L_1(x)$ and $L_2(x)$ respectively. Then $\mathcal{S}_1$ and $\mathcal{S}_2$ are isomorphic if and only if there exists an invertible series $u(x) \in A[[x]]$ such that $L_2(u(x)) = u'(0)L_1(x)$.*

Proof. Suppose that $\mathcal{S}_1$ and $\mathcal{S}_2$ are isomorphic. Then by definition, there exist $f_1(x) \in \mathcal{S}_1$, $f_2(x) \in \mathcal{S}_2$ and an invertible series $u(x) \in A[[x]]$ such that $u(f_1(x)) = f_2(u(x))$. Consider $u'(0)L_1(u^{-1}(x))$. It satisfies the defining condition for the logarithm of $f_2(x) = u(f_1(u^{-1}(x)))$. By the uniqueness, it must therefore be equal to $L_2(x)$.

Conversely, suppose that $\mathcal{S}_1$ is a system arising from $f_1(x) \in A[[x]]$. Consider $f_2(x) = u(f_1(u^{-1}(x)))$. Because $u(x)$ is an invertible series over A, $f_2(x)$ is a power series over A and $L_2(f_2(x)) = f_2'(0)L_2(x)$. This implies that $f_2(x) \in \mathcal{S}_2$ and hence $\mathcal{S}_1$ and $\mathcal{S}_2$ are isomorphic. □

LEMMA 2.2. *Let $f_1(x)$ and $f_2(x)$ be stable power series with $f_1'(0) = f_2'(0)$. Let $L_1(x)$ and $L_2(x)$ be the logarithm of $f_1(x)$ and $f_2(x)$, respectively. Suppose that $L_1(x) \equiv L_2(x) \pmod{x^n}$. Then $f_1(x) \equiv f_2(x) \pmod{x^n}$.*

Proof. We prove this by induction. Suppose that for $m < n$, $f_1(x) \equiv f_2(x) + cx^m \pmod{x^{m+1}}$. Since $f_1(0) = f_2(0) = 0$ and $L_1(x) \equiv L_2(x) \pmod{x^{m+1}}$, we have that

$$\begin{aligned} f_1'(0)L_1(x) &= L_1(f_1(x)) \\ &\equiv L_2(f_2(x) + cx^m) \pmod{x^{m+1}} \\ &\equiv L_2(f_2(x)) + cx^m \pmod{x^{m+1}} \\ &= f_2'(0)L_2(x) + cx^m. \end{aligned}$$

Because $f_1'(0) = f_2'(0)$, this implies that $c = 0$ and our induction follows. □

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

LEMMA 2.3. *Let $f_1(x)$ and $f_2(x)$ be stable power series with $f_1'(0) = f_2'(0)$. Let $L_1(x)$ and $L_2(x)$ be the logarithm of $f_1(x)$ and $f_2(x)$, respectively. Suppose that*

$$L_1(x) \equiv L_2(x) + cx^n (\mathrm{mod}\ x^{n+1}) \quad \text{and} \quad f_1(x) \equiv f_2(x) + dx^n (\mathrm{mod}\ x^{n+1}).$$

Then

$$c = d/(f_1'(0) - f_1'(0)^n).$$

Proof. We remark first that since $f_1(x)$ is stable, $f_1'(0) - f_1'(0)^n \neq 0$ for all n. Because $L_2'(0) = 1$, we have that

$$\begin{aligned} f_1'(0)L_1(x) &= L_1(f_1(x)) \\ &\equiv L_2(f_2(x) + dx^n) + c(f_2(x) + dx^n)^n (\mathrm{mod}\ x^{n+1}) \\ &\equiv L_2(f_2(x)) + dx^n + cf_2'(0)^n x^n (\mathrm{mod}\ x^{n+1}) \\ &= f_2'(0)L_2(x) + (d + cf_2'(0)^n)x^n \\ &\equiv f_2'(0)L_1(x) + (d + cf_2'(0)^n - cf_2'(0))x^n (\mathrm{mod}\ x^{n+1}). \end{aligned}$$

Since $f_1'(0) = f_2'(0)$, this implies that $c = d/(f_1'(0) - f_1'(0)^n)$. □

In [2], Hazewinkel gives a method of constructing formal groups by means of certain type of recursive procedure. Here, we just list some results which we need later. (Please see [2] for more detail.)

The basic ingredients for the constructions are: a ring B such that $A \subset B$, a prime number p, a principal ideal $\mathcal{P}$ of A such that $p \in \mathcal{P}$, a ring homomorphism $\sigma : B \to B$ such that $\sigma(a) \equiv a^p (\mathrm{mod}\ \mathcal{P})$ for all $a \in A$ and $\{s_1, s_2, \ldots\} \subset B$ such that $s_i\mathcal{P} \subset A$, $i = 1, 2, \ldots$. Now let $g(x) \in A[[x]]$. Given the ingredients above, we construct a new power series $l_g(x) \in B[[x]]$ by means of the recursion formula

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

where $\sigma_*^i l_g(x)$ is the power series obtained from $l_g(x)$ by applying the automorphism σ^i to the coefficients of $l_g(x)$. We remark that the equation above is in fact a recursion formula for the coefficients of $l_g(x)$. Indeed, let

$$g(x) = \sum_{i=1}^{\infty} b_i x^i, \qquad l_g(x) = \sum_{i=1}^{\infty} a_i x^i,$$

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

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

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

LEMMA 2.4. *Let $g(x)$ and $h(x)$ be two power series over A with $g'(0) = 1$ and let $l_g(x)$ and $l_h(x)$ be two power series over B constructed by the recursion formula above. Then we have:*

(i) $F(x, y) = l_g^{-1}(l_g(x) + l_g(y))$ *is a formal group over* A;
(ii) $l_g^{-1}(l_h(x)) \in A[[x]]$.

Let $C_n(x, y) = \varepsilon_n((x + y)^n - x^n - y^n)$, where $\varepsilon_n = 1$, when n is not a prime power and $\varepsilon_n = 1/q$, when n is a power of the prime q. Let $F(x, y)$ and $G(x, y)$ be formal groups over A with $F(x, y) \equiv G(x, y)$ (mod degree n). Then Lazard's comparison lemma [4] says that $F(x, y) \equiv G(x, y) + aC_n(x, y)$ (mod degree $n + 1$) for some $a \in A$.

Denote by $[m]_F(x)$ (resp. $[m]_G(x)$) the unique endomorphism of $F(x, y)$ (resp. $G(x, y)$) such that $[m]'_F(0) = m$ (resp. $[m]'_G(0) = m$).

LEMMA 2.5. *Suppose that $F(x, y)$ and $G(x, y)$ are formal groups over A and $F(x, y) \equiv G(x, y) + aC_n(x, y)$(mod degree $n + 1$). Then for $m \in \mathbb{Z}$, $[m]_F(x) \equiv [m]_G(x) + a\varepsilon_n(m^n - m)x^n$(mod x^{n+1}).*

Proof. Please see [1, III, Lemma 4]. □

3. Universal Formal Group Law

Most of the results in this section can be found in [2]. However, since we concentrate on formal groups over $\mathbb{Z}_p$-algebra, we give here more direct proofs of these results by considering logarithms. In this section A is a $\mathbb{Z}_p$-algebra and K is the fraction field of A.

DEFINITION. A Formal group $F(x, y)$ over a ring $\mathcal{A}$ is universal for formal groups over $\mathbb{Z}_p$-algebras if for every formal group $G(x, y)$ over a $\mathbb{Z}_p$-algebra A, there is a unique ring homomorphism $\phi: \mathcal{A} \to A$ such that $\phi_* F(x, y) = G(x, y)$.

Now we take

$$\mathcal{A} = \mathbb{Z}[V_2, V_3, V_4, \ldots], \qquad \mathcal{B} = \mathbb{Q}[V_2, V_3, V_4, \ldots], \qquad \mathcal{P} = p\mathcal{A}, \quad \sigma: \mathcal{B} \to \mathcal{B}$$

raise each V_i to its pth power, $s_i = p^{-1}V_{p^i}$ for all $i = 1, 2, \ldots$, and

$$g(x) = x + \sum_{n=2}^{\infty} V_n x^n - \sum_{i=1}^{\infty} V_{p^i} x^{p^i} \quad \text{and} \quad h(x) = x.$$

We construct power series $l_g(x)$ and $l_h(x)$ by means of Hazewinkel's recursion formula in previous section. We define $F_g(x, y) = l_g^{-1}(l_g(x) + l_g(y))$ and $F_h(x, y) = l_h^{-1}(l_h(x) + l_h(y))$. An application of part (i) of Lemma 2.4 shows that both $F_g(x, y)$ and $F_h(x, y)$ are formal group over $\mathcal{A}$.

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

We write

$$l_g(x) = x + \sum_{n=2}^{\infty} b_n x^n \quad \text{and} \quad l_h(x) = x + \sum_{n=2}^{\infty} c_n x^n,$$

then according to the recursion formula, we have that

$$b_n = \Phi_n(V_2, \ldots, V_{n-1}) + \lambda_n V_n,$$

where $\Phi_n(V_2, \ldots, V_{n-1}) \in \mathbb{Q}[V_2, \ldots, V_{n-1}]$ and $\lambda_n = 1$ if n is not a power of p and $\lambda_n = 1/p$ if n is a power of p. We also have that $c_n = 0$ if n is not a power of p and $c_n = b_n$ if n is a power of p. In fact,

$$c_{p^i} = b_{p^i} = \Psi_i(V_p, ..V_{p^{i-1}}) + V_{p^i}/p,$$

where $\Psi_i(V_p, \ldots, V_{p^{i-1}}) \in \mathbb{Q}[V_p, \ldots, V_{p^{i-1}}]$.

PROPOSITION 3.1. *$F_g(x, y)$ is a universal formal group for formal groups over $\mathbb{Z}_p$-algebras.*

Proof. For any formal group $F(x, y)$ over A with logarithm $L(x)$, we claim that there exists a unique ring homomorphism $\phi: \mathcal{A} \to A$ which tensoring with $\mathbb{Q}$ gives us a homomorphism (also denoted ϕ) $\phi: \mathcal{B} \to K$ such that $\phi_* l_g(x) = L(x)$. We remark that since $l_g'(0) = 1$, this implies that $l_g^{-1}(x) \in \mathcal{B}[[x]]$. Therefore, we have $\phi_* l_g^{-1}(x) = L^{-1}(x)$ and, hence, $\phi_* F_g(x, y) = F(x, y)$.

For the proof of the claim, we use induction. Suppose that there exist $a_2, \ldots, a_{n-1} \in A$ such that

$$x + \sum_{i=2}^{n-1} (\Phi_i(a_2, \ldots, a_{i-1}) + \lambda_i a_i) x^i \equiv L(x) \,(\mathrm{mod}\ x^n).$$

Consider $\varphi: \mathcal{A} \to A$ the $\mathbb{Z}$-homomorphism defined by $\varphi(V_i) = a_i$ for $i \leqslant n-1$ and $\varphi(V_j) = 0$ for $j \geqslant n$. Since $\varphi_* l_g(x)$ is a logarithm of a formal group $F_n(x, y)$ over A. By Lazard's comparison lemma and Lemma 2.5, we have that

$$[p]_{F_n}(x) \equiv [p]_F(x) + a\varepsilon_n(p^n - p)x^n \,(\mathrm{mod}\ x^{n+1})$$

for some $a \in A$. By Lemma 2.3, this says that

$$\varphi_* l_g(x) \equiv L(x) - a\varepsilon_n x^{p^n} (\mathrm{mod}\ x^{n+1}).$$

Recall that $\varepsilon_n \in A$ and $\lambda_n = 1$ if n is not a power of p and $\varepsilon_n = \lambda_n = 1/p$ if n is a power of p. Hence we can uniquely choose $a_n = a\varepsilon_n/\lambda_n \in A$ such that for the $\mathbb{Z}$-homomorphism $\psi: \mathcal{A} \to A$ defined by $\psi(V_i) = a_i$ for $i \leqslant n$ and $\psi(V_j) = 0$ for $j > n$, we have $\psi_* l_g(x) \equiv L(x) (\mathrm{mod}\ x^{n+1})$. Our claim follows. □

PROPOSITION 3.2. *Let A be a $\mathbb{Z}_p$-algebra. Then every formal group over A is strictly isomorphic to a p-typical formal group over A.*

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

In particular, suppose that $L(x) = x + \sum_{i=2}^{\infty} a_i x^i$ *is the logarithm of a formal group over A. Then* $l(x) = x + \sum_{n=1}^{\infty} a_{p^n} x^{p^n}$ *is also the logarithm of a formal group over A. Furthermore, these two formal group are strictly isomorphic over A.*

Proof. By Lemma 2.1, we only need to prove that $L^{-1}(l(x)) \in A[[x]]$. Since $l_g(x)$ is the logarithm of the universal formal group $F_g(x, y)$, there exists a ring homomorphism $\phi: \mathcal{A} \to A$ which tensoring with $\mathbb{Q}$ gives us $\phi_* l_g(x) = L(x)$. Recall that we get $l_h(x)$ by striking out all terms in $l_g(x)$ that its degree is not a power of p. Hence, we have $\phi_* l_h(x) = l(x)$. An application of part (ii) of Lemma 2.4 shows that $l_g^{-1}(l_h(x)) \in \mathcal{A}[[x]]$. Our claim follows by applying ϕ to the coefficients of $l_g^{-1}(x)$, $l_h(x)$ and $l_g^{-1}(l_h(x))$.

4. *p*-Typical Dynamical Systems

Let K be a totally ramified extension of degree e over $\mathbb{Q}_p$ and let $\mathcal{O}_K$ be its integer ring. Let L be an unramified extension of K with integer ring $\mathcal{O}_L$ and maximal ideal $\mathcal{P}$. We normalize the valuation v of $\mathcal{O}_L$ such that $v(p) = e$. Let $\sigma \in Gal(L/K)$ be the Frobenius automorphism of L over K. Recall that $\sigma(\alpha) \equiv \alpha^p (\mathrm{mod}\ \mathcal{P})$ for all $\alpha \in \mathcal{O}_L$.

THEOREM 4.1. *Let* $\mathcal{S}$ *be a dynamical system over* $\mathcal{O}_L$ *arising from a stable series* $f(x) \in \mathcal{O}_L[[x]]$. *Suppose that in* $\mathcal{S}$ *there exists a stable series* $g(x) \in \mathcal{O}_L[[x]]$ *with* $g'(0) \in \mathcal{O}_K$ *and* $v(g'(0)^p - g'(0)) = 1$. *If* $\mathcal{S}$ *is isomorphic to a p-typical dynamical system, then* $f(x)$ *is an endomorphism of a formal group over* $\mathcal{O}_L$.

Proof. Recall that if $l(x)$ is the logarithm of $f(x)$, then $l(x)$ is also the logarithm of $g(x)$. Without loss of generality, we assume $l(x) = x + \sum_{i=1}^{\infty} a_i x^{p^i}$. Observe that the assumption $v(g'(0)^p - g'(0)) = 1$ implies that $v(g'(0)^{p^n} - g'(0)) = 1$ and since $l(g(x)) = g'(0) l(x)$, by the assumption of $g'(0)$ and by induction, we can easily get $v(a_i) \geqslant -i$. By applying part (i) of Lemma 2.4, we only have to claim that there exist $\{s_1, s_2, \ldots\}$ such that $s_i \mathcal{P} \in \mathcal{O}_L$ and $l(x) = x + \sum_{i=1}^{\infty} s_i \sigma_*^i l(x^{p^i})$. Since σ is the Frobenius automorphism, it is also easy to check that $g(x)^{p^i} \equiv \sigma_*^i g(x^{p^i}) (\mathrm{mod}\ \mathcal{P})$. Hence, we have that $(g(x)^{p^i})^{p^j} \equiv (\sigma_*^i g(x^{p^i}))^{p^j} (\mathrm{mod}\ \mathcal{P}^{j+1})$ and then $\sigma^i(a_j)(g(x)^{p^i})^{p^j} \equiv \sigma^i(a_j)(\sigma_*^i g(x^{p^i}))^{p^j} (\mathrm{mod}\ \mathcal{P})$. Therefore,

$$
\begin{aligned}
\sigma_*^i l(g(x)^{p^i}) &= g(x)^{p^i} + \sum_{j=1}^{\infty} \sigma^i(a_j)(g(x)^{p^i})^{p^j} \\
&\equiv \sigma_*^i g(x^{p^i}) + \sum_{j=1}^{\infty} \sigma^i(a_j)(\sigma_*^i g(x^{p^i}))^{p^j} (\mathrm{mod}\ \mathcal{P}) \\
&\equiv \sigma_*^i l(\sigma_*^i g(x^{p^i})) (\mathrm{mod}\ \mathcal{P}) \\
&= \sigma_*^i (l \circ g)(x^{p^i}) \\
&= \sigma^i(g'(0)) \sigma_*^i l(x^{p^i}).
\end{aligned}
$$

For s_1, we have that $a_1 = s_1$. Since $v(a_1) \geqslant -1$, this implies that $s_1 \mathcal{P} \in \mathcal{O}_L$. Sup-

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

pose our claim is true for $s_1, s_2, \ldots, s_{n-1}$ and $l(x) \equiv x + \sum_{i=1}^{n-1} s_i \sigma_*^i l(x^{p^i}) (\mathrm{mod}\ x^{p^n})$. We choose $s_n \in L$ such that

$$l(x) \equiv x + \sum_{i=1}^{n-1} s_i \sigma_*^i l(x^{p^i}) + s_n x^{p^n} \ (\mathrm{mod}\ x^{p^n+1}).$$

Therefore,

$$\begin{aligned} g'(0)l(x) &= l(g(x)) \\ &\equiv g(x) + \sum_{i=1}^{n-1} s_i \sigma_*^i l(g(x)^{p^i}) + s_n g'(0)^{p^n} x^{p^n} \ (\mathrm{mod}\ \mathcal{O}_L, x^{p^n+1}) \\ &\equiv \sum_{i=1}^{n-1} s_i \sigma^i(g'(0)) \sigma_*^i l(x^{p^i}) + s_n g'(0)^{p^n} x^{p^n} \ (\mathrm{mod}\ \mathcal{O}_L, x^{p^n+1}). \end{aligned}$$

Now, since $g'(0) \in \mathcal{O}_K$, we have that $\sigma^i(g'(0)) = g'(0)$. Hence, the congruences above implies

$$g'(0) s_n x^{p^n} \equiv g'(0)(l(x) - \sum_{i=1}^{n-1} s_i \sigma_*^i l(x^{p^i})) \equiv s_n g'(0)^{p^n} x^{p^n} \ (\mathrm{mod}\ \mathcal{O}_L, x^{p^n+1}).$$

Thus $s_n(g'(0)^{p^n} - g'(0)) \in \mathcal{O}_L$. Since $v(g'(0)^{p^n} - g'(0)) = 1$, we have that $s_n \mathcal{P} \in \mathcal{O}_L$. □

Consider the case $K = \mathbb{Q}_p$. Since $\mathbb{Z}_p$ is contained in the endomorphism ring of every formal group over $\mathcal{O}_L$ (by the embedding $m \mapsto [m](x)$), we have the following corollary:

COROLLARY 4.2. *Suppose that L is a unramified extension of $\mathbb{Q}_p$. Suppose that $\mathcal{S}$ is a dynamical system over $\mathcal{O}_L$. Then $\mathcal{S}$ is a dynamical system arising from a formal group over $\mathcal{O}_L$ if and only if $\mathcal{S}$ is isomorphic to a p-typical dynamical system and in $\mathcal{S}$ there exists a stable series $g(x) \in \mathcal{O}_L[[x]]$ with $g'(0) \in \mathbb{Z}_p$ and $v(g'(0)^p - g'(0)) = v(p)$.*

Corollary 4.2 and the proof of Theorem 4.1 show that every formal group over the integer ring of a unramified extension of $\mathbb{Q}_p$ can be constructed directly by Hazewinkel's recursive formula. In general, this is not always true, so we use another approach to extend the result of Corollary 4.2 to dynamical systems over any $\mathbb{Z}_p$-algebra.

THEOREM 4.3. *Let A be a $\mathbb{Z}_p$-algebra and $\mathcal{S}$ be a dynamical system over A. Suppose that in $\mathcal{S}$ there exists a stable series $g(x) \in A[[x]]$ with $g'(0) \in \mathbb{Z}_p$ and $v(g'(0)^p - g'(0)) = v(p)$. Then $\mathcal{S}$ is a dynamical system arising from a formal group over A if and only if $\mathcal{S}$ is isomorphic to a p-typical dynamical system.*

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

Proof. We only have to prove the 'if' part. Recall that

$$l_h(x) = x + \sum_{i=1}^{\infty} (\Psi_i(V_p, \ldots, V_{p^{i-1}}) + V_{p^i}/p)x^{p^i}$$

where $\Psi_i(V_p, \ldots, V_{p^{i-1}}) \in \mathbb{Q}[V_p, \ldots, V_{p^{i-1}}]$. Without loss of generality, we assume that $\mathcal{S}$ is p-typical. let $L(x)$ be the logarithm of $\mathcal{S}$. We denote $\mathcal{C} = \mathbb{Z}_p[V_p, V_{p^2}, \ldots, V_{p^n}, \ldots]$. Our goal is to find a ring homomorphism $\phi: \mathcal{C} \to A$ which tensoring with $\mathbb{Q}$ gives us $\phi_* l_h(x) = L(x)$.

We use induction. Suppose that there exist $a_1, \ldots, a_{n-1} \in A$ such that

$$x + \sum_{i=1}^{n-1} (\Psi_i(a_1, \ldots, a_{i-1}) + a_i/p)x^{p^i} \equiv L(x) (\mathrm{mod}\ x^{p^n}).$$

Consider $\varphi: \mathcal{C} \to A$ the $\mathbb{Z}$-homomorphism defined by $\varphi(V_{p^i}) = a_i$ for $i \leqslant n-1$ and $\varphi(V_{p^j}) = 0$ for $j \geqslant n$. Since for every formal group over A, its endomorphism ring contains $\mathbb{Z}_p$ and $\varphi_* l_h(x)$ is the logarithm of a formal group over A, there exists a power series $f(x) \in A[[x]]$ with $f'(0) = g'(0)$ such that $\varphi_* l_h(x)$ is the logarithm of $f(x)$. By Lemmas 2.2 and 2.3, we have that

$$\varphi_* l_h(x) \equiv L(x) + d/(f'(0)^{p^n} - f'(0))x^{p^n} (\mathrm{mod}\ x^{p^{n+1}})$$

for some $d \in A$. Hence we can choose

$$a_n = d \cdot p/(f'(0) - f'(0)^{p^n}) \in A$$

such that for the $\mathbb{Z}$-homomorphism $\psi: \mathcal{C} \to A$ defined by $\psi(V_i) = a_i$ for $i \leqslant n$ and $\psi(V_j) = 0$ for $j > n$, we have $\psi_*(l_h)(x) \equiv L(x) (\mathrm{mod}\ x^{p^{n+1}})$. Our induction follows. □

Remark. The proof of Theorem 4.3, shows that $F_h(x, y)$ as a formal group over $\mathcal{C}$ is a universal formal group for p-typical formal groups over $\mathbb{Z}_p$-algebras.

5. Examples

In this section, we give examples to illustrate that the assumption $g'(0) \in \mathbb{Z}_p$ and $v(g'(0)^p - g'(0)) = v(p)$ in Theorem 4.3 is essential.

Let K be an algebraic extension of $\mathbb{Q}_p$ and let $\mathcal{O}_K$ be its integer ring, with maximal ideal $\mathcal{M}_K$. If $\overline{K}$ is an algebraic closure of K, we denote by $\overline{\mathcal{O}}_K$ and $\overline{\mathcal{M}}_K$ the integral closure of $\mathcal{O}_K$ in $\overline{K}$ and the maximal ideal of $\overline{\mathcal{O}}_K$, respectively. There is a unique extension of v to the algebraic closure $\overline{K}$, and this will likewise be denoted v. If $f(x) = \sum_{i=0}^{\infty} a_i x^i$, the *Newton polygon* of $f(x)$ is constructed by erecting vertical half lines on all the points of the form $\big(i, v(a_i)\big)$ in the Cartesian plane, and then taking the convex hull of the union of these lines. The Newton polygon is a natural tool to study the roots of p-adic power series. Here, we just list some results which we need later. Please see Koblitz [3] for more detail.

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

By the vertices of the Newton polygon we mean the points $(i_j, v(a_{i_j}))$ where the slopes change. If a segment joins two vertices (i, m) and (i', m'), where $i < i'$, its slope is $(m' - m)/(i' - i)$; by the *width of the segment* we mean $i' - i$, i.e. the length of the projection of the corresponding segment onto the horizontal axis.

The proof of the following basic property of the Newton polygon can be found in Koblitz [3].

PROPOSITION 5.1. *If a segment of the Newton polygon of $f(x) \in K[[x]]$ has finite width N and slope λ, then there are, counting multiplicity, precisely N values of $\alpha \in \overline{K}$ for which $f(\alpha) = 0$ and $v(\alpha) = -\lambda$.*

Since we only concern with roots in $\overline{\mathcal{M}}_K$ (i.e. roots with positive valuation), in the following, we only consider those segments of Newton polygon which have negative slopes.

LEMMA 5.2. *Let $f(x)$ be a stable noninvertible series in $\mathcal{O}_K[[x]]$. Suppose that there is only one segment of the Newton polygon of $f(x)$ which has negative slope.*

(i) *Suppose that $g(x) \in \mathcal{O}_K[[x]]$ is a stable noninvertible series such that $f(g(x)) = g(f(x))$. Then $f(x) \mid g(x)$ in $\mathcal{O}_K[[x]]$.*
(ii) *There is no stable series $h(x) \in \mathcal{O}_K[[x]]$ such that $h(h(x)) = f(x)$*

Proof. We first remark that if $\alpha \in \overline{\mathcal{M}}_K$ is a nonzero root of a noninvertible stable series $p(x) \in \mathcal{O}_K[[x]]$, then every root of $p(x) - \alpha$ in $\overline{\mathcal{M}}_K$ has valuation less than $v(\alpha)$.

(i) Suppose that $\alpha \in \overline{\mathcal{M}}_K$ is a nonzero root of $f(x)$. Because every nonzero root of $f(x)$ has the same valuation $v(\alpha)$, by the remark above, we have that every nonzero root of iterates of $f(x)$ has valuation less than or equal to $v(\alpha)$. Because $f(g(x)) = g(f(x))$, the set of roots of iterates of $f(x)$ equals to the set of roots of iterates of $g(x)$ and hence, α must be a root of some iterates of $g(x)$. Now, if $g(\alpha) = \beta \neq 0$, we have that $v(\beta) > v(\alpha)$. However, β is a root of iterates of $g(x)$ and hence a root of iterates of $f(x)$, which contradicts the fact that every nonzero root of iterates of $f(x)$ has valuation less than or equal to $v(\alpha)$. Furthermore, it is easy to check that if $f(g(x)) = g(f(x))$, then every common root of $f(x)$ and $g(x)$ has the same multiplicity. Therefore, Weierstrass preparation theorem shows that $f(x) \mid g(x)$ in $\mathcal{O}_K[[x]]$.

(ii) Suppose that $h(x) \in \mathcal{O}_K[[x]]$ is stable and $h(h(x)) = f(x)$. Let β be a nonzero root of $h(x)$ in $\overline{\mathcal{M}}_K$. Then β is a root of $f(x)$ and so is every root of $h(x) - \beta$ in $\overline{\mathcal{M}}_K$. This contradicts the assumption that every nonzero root of $f(x)$ in $\overline{\mathcal{M}}_K$ has the same valuation. □

Our first example shows that the assumption $g'(0) \in \mathbb{Z}_p$ in Theorem 4.3 is essential. In the following, given the logarithm $l(x)$ of a system, we denote $[a](x)$ the unique power series with $l([a](x)) = al(x)$.

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

EXAMPLE. *Let* $K = \mathbb{Q}_p(\pi)$ *where* $\pi^2 = p$. *Let* $a = (1+\pi)p$. *We have that* $a \notin \mathbb{Z}_p$ *and* $v(a) = v(p)$. *Consider the p-typical system* $\mathcal{S}$ *over* $\mathcal{O}_K$ *with logarithm*

$$l(x) = x + \sum_{i=1}^{\infty} x^{p^i}/a^i.$$

Then $[a](x) \in \mathcal{S}$ *but it is not an endomorphism of a formal group over* $\mathcal{O}_K$.

Proof. We only have to claim that $[a](x) \in \mathcal{O}_K[[x]]$ and $[p](x) \notin \mathcal{O}_K[[x]]$. First, it is easy to check that $[a](x) \equiv ax + (1-a^{p-1})x^p \pmod{x^{p+1}}$. We claim that $[a](x) \equiv x^p \pmod{p\mathcal{O}_K}$ by induction. Suppose that $[a](x) \equiv x^p + cx^n \pmod{p\mathcal{O}_K, x^{n+1}}$ for $n > p$. Then since $l'(x) \in \mathcal{O}_K[[x]]$, we have that $al(x) = l([a](x)) \equiv l(x^p) + cx^n \pmod{p\mathcal{O}_K, x^{n+1}}$. Notice that $l(x^p) = al(x) - ax$. This implies that $c \in p\mathcal{O}_K$.

Now suppose that $[p](x) \in \mathcal{O}_K[[x]]$. Since the Newton polygon of $[a](x)$ has only one segment of negative slope and $[a]([p](x)) = [p]([a](x))$, part (i) of Lemma 5.2 says that $[a](x) \mid [p](x)$ and hence by [8, Theorem 3.4], there exists $h(x) \in \mathcal{O}_K[[x]]$ such that $[p](x) = h([a](x))$. Because

$$h([a]([a](x))) = [p]([a](x)) = [a]([p](x)) = [a](h([a](x)))$$

and $[a](x)$ has no constant term, this implies that $h([a](x)) = [a](h(x))$ and hence $h(x) \in \mathcal{S}$. Comparing the leading coefficients of $[a](x)$ and $[p](x)$ we have that $h'(0) = (1+\pi)^{-1}$. Thus $h^{-1}(x) = [1+\pi](x) \in \mathcal{O}_K[[x]]$. However, by direct computation, we have that

$$[1+\pi](x) = (1+\pi)x + (1-(1+\pi)^{p-1})x^p/p \pmod{x^{p+1}}.$$

Since $v(1-(1+\pi)^{p-1}) = v(\pi) < v(p)$, we get a contradiction. □

In the next example, we show that the assumption $v(g'(0)^p - g'(0)) = v(p)$ in Theorem 4.3 is also essential.

EXAMPLE. *Let* $\mathcal{S}$ *be a system over* $\mathbb{Z}_p$ *with logarithm*

$$l(x) = x + \sum_{i=1}^{\infty} x^{p^{2i}}/p^{2i}.$$

Then $[p^2](x) \in \mathcal{S}$ *but it is not an endomorphism of any formal group over* $\mathbb{Z}_p$.

Proof. We first check that

$$[p^2](x) \equiv p^2x + (1-p^{2p^2})x^{p^2} \pmod{x^{p^2+1}}.$$

Using similar argument as above, we can prove that $[p^2](x) \equiv x^{p^2} \bmod p^2\mathbb{Z}_p$. Hence $[p^2](x) \in \mathcal{S}$. Since the Newton polygon of $[p^2](x)$ has only one segment of negative slope, by part (ii) of Lemma 5.2, it is impossible to find a stable power series $h(x) \in \mathbb{Z}_p[[x]]$ such that $h(h(x)) = [p^2](x)$. Because $[p]([p](x)) = [p^2](x)$, it follows that $[p](x) \notin \mathbb{Z}_p[[x]]$. □

https://doi.org/10.1023/A:1013792029235 Published online by Cambridge University Press

When A is a local ring and $f(x) \in A[[x]]$, then the lowest degree in which a unit coefficient appears will be called the Weierstrass degree of $f(x)$. If all coefficients of $f(x)$ are in the maximal ideal, then we will say that the Weierstrass degree of $f(x)$ is infinite.

All noninvertible series in the systems we constructed above have finite Weierstrass degrees. In our next example, we have a system raises from a power series with infinite Weierstrass degree. Surprisingly, this system contains both stable noninvertible series and stable invertible series, but there is no formal group in the background.

EXAMPLE. *Let $\mathcal{S}$ be a system over $\mathbb{Z}_p$ with logarithm $l(x) = x + x^p/p$. Then $\mathcal{S} = \{[a](x) \mid a^p - a \in p^2\mathbb{Z}_p\}$. We remark that both $[p^2](x)$ and $[1 + p^2](x)$ are in $\mathcal{S}$ but $[p](x)$ is not in $\mathcal{S}$. Hence $\mathcal{S}$ is not a system arising from any formal group.*

Proof. We check first that

$$[a](x) \equiv ax + (a - a^p)x^p/p (\mathrm{mod}\ x^{p+1}).$$

Suppose that $a^p - a \in p^2\mathbb{Z}_p$. Then since $l(ax) - al(x) = (a^p - a)x^p/p$, by similar argument as above, we can prove that $[a](x) \equiv ax (\mathrm{mod}\ p\mathbb{Z}_p)$. Hence we have that $\{[a](x) \mid a^p - a \in p^2\mathbb{Z}_p\} \subseteq \mathcal{S}$.

Next we check that

$$[p](x) \equiv px + (1 - p^{p-1})x^p (\mathrm{mod}\ x^{p+1}) \quad .$$

Suppose that $[p](x) \in \mathbb{Z}_p[[x]]$. Then the Weierstrass degree of $[p](x)$ is p. Notice that $[1 + p^2](x) \equiv x (\mathrm{mod}\ p\mathbb{Z}_p)$. In this case, Lubin [9, Corollary 4.3.1] shows that $[1 + p^2](x)$ cannot commute with a noninvertible series over $\mathbb{Z}_p$ of finite Weierstrass degree. We have a contradiction, and hence $[p](x) \notin \mathcal{S}$. We can use similar argument or use Theorem 4.3 to claim that $[a](x) \notin \mathcal{S}$ for all a such that $a^p - a \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$. □

Remark. In this example, we understand that Lubin's conjecture needs some modification. However, in the example, the system has only finite many roots of iterates and periodic points, but in [6] and [7] to support Lubin's conjecture, we do assume that our systems have infinitely many roots of iterates and periodic points. Perhaps Lubin's conjecture can be fixed by somehow expressing the hypothesis that the dynamical system shall have an infinite set of roots of iterates and periodic points.

Acknowledgements

Portions of this work were done while the author was visiting Brown University under the support of NSC 37134F. The author would like to thank everyone at Brown University for their hospitality and, especially, the author would like to thank J. Lubin and M. Rosen for many valuable discussions. In addition, the author wishes to thank the referee, whose suggestions have been very helpful.

References

1. Fröhlich, A.: *Formal Groups*, Lecture Notes in Math. 74, Springer, New York, 1968.
2. Hazewinkel, M.: *Formal Groups and Applications*, Academic Press, New York, 1978.
3. Koblitz, N.: *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, Springer, New York, 1977.
4. Lazard, M.: Sur les groupes de Lie formels à un paramètre, *Bull. Soc. Math. France* **83** (1955), 251–274
5. Li, H.-C.: When is a p-adic power series an endomorphism of a formal group? *Proc. Amer. Math. Soc.* **124** (1996), 2325–2329.
6. Li, H.-C.: Counting periodic points of p-adic power series, *Compositio Math.* **100** (1996), 351–364.
7. Li, H.-C.: p-adic Dynamical systems and formal groups, *Compositio Math.* **104** (1996), 41–54.
8. Li, H.-C.: p-adic power series which commute under composition, *Trans. Amer. Math. Soc.* **349** (1997), 1437–1446.
9. Lubin, J.: Nonarchimedean dynamical systems, *Compositio Math.* **94** (1994), 321–346.
10. Lubin, J.: personal communication.
11. Lubin, J. and Tate, J.: Formal complex multiplication in local field, *Ann. of Math.* **81** (1965), 380–387.
12. Serre, J.-P.: Sur les groupes de Galois attachés aux groupes p-divisibles, *Proc. Conf. Local Fields held at Driebergen*, Springer-Verlag, Berlin, 1967.