COMPOSITIO MATHEMATICA

HUA-CHIEH LI

p-adic dynamical systems and formal groups

Compositio Mathematica, tome 104, n° 1 (1996), p. 41-54
<http://www.numdam.org/item?id=CM_1996__104_1_41_0>

Compositio Mathematica **104:** 41–54, 1996.

p-adic dynamical systems and formal groups

HUA-CHIEH LI
Department of Mathematics, National Tsing Hua University, Hsinchu, Taiwan

Received 3 March 1995; accepted in final form 28 August 1995

1. Introduction

Let K be an algebraic extension of $\mathbf{Q}_p$ and let $\mathcal{O}$ be its integer ring with maximal ideal $\mathcal{M}$ and residue field k. If $\overline{K}$ is an algebraic closure of K, we denote by $\overline{\mathcal{O}}$ and $\overline{\mathcal{M}}$ the integral closure of $\mathcal{O}$ in $\overline{K}$ and the maximal ideal of $\overline{\mathcal{O}}$, respectively.

When $f(x) \in \mathcal{O}[[x]]$, but not all coefficients of $f(x)$ are in $\mathcal{M}$, then the lowest degree in which a unit coefficient appears will be called the Weierstrass degree of $f(x)$, denoted wideg(f). According to the Weierstrass Preparation Theorem there exist a unit power series $U(x) \in \mathcal{O}[[x]]$ and a distinguished polynomial $P(x) \in \mathcal{O}[[x]]$ such that $f(x) = P(x)U(x)$ and deg(P) =wideg(f). All roots of $P(x)$ are in $\overline{\mathcal{M}}$. If wideg$(f) = d$, then, counting multiplicity, there are d of them and they exhaust all roots of f that are in $\overline{\mathcal{M}}$.

The set of all power series over $\mathcal{O}$ without constant term is a monoid (non-commutative, associative, with unit) under composition. A series $u(x) \in \mathcal{O}[[x]]$ without constant term is called invertible if there exists a series $w(x) \in \mathcal{O}[[x]]$ such that $u \circ w(x) = x$. A necessary and sufficient condition for $u(x)$ to be invertible is that $u'(0) \in \mathcal{O}^*$. Let $u(x)$ be an invertible series without constant term in $\mathcal{O}[[x]]$. Since wideg$(u) = 1$, $u(x)$ has no other roots than 0 in $\overline{\mathcal{M}}$. We denote $u^{\circ n}(x)$ the n-fold iteration of $u(x)$ with itself. The point $\alpha \in \overline{\mathcal{M}}$ is a fixed point for $u(x)$ if $u(\alpha) = \alpha$. The point α is a periodic point of period n if $u^{\circ n}(\alpha) = \alpha$.

If $f(x) \in \mathcal{O}[[x]]$ without constant term and $f'(0) \in \mathcal{M}$, then we call $f(x)$ a noninvertible series. A noninvertible series can have no other fixed points than 0, but the roots of iterates are of serious interest. In the invertible series case, the periodic points now play a role parallel to the roots of a noninvertible series. These two studies become no longer disjoint in case an invertible series commutes with a noninvertible series (Lubin [6]). In the case that a dynamical system over the ring of local integers $\mathcal{O}$ arises from a formal group, i.e. when we are discussing the properties of the iterates of an endomorphism of a formal group defined over $\mathcal{O}$, the full commuting family contains both invertible and noninvertible series. Lubin conjectures that for an invertible series to commute with a noninvertible series, there must be a formal group somehow in the background. Lubin's Main Theorem

in [6] supports this conjecture, in that it says that the only possible finite Weierstrass degree for such a noninvertible series is a power of p.

We assume that the series $u(x)$ always satisfies $u'(0) \in 1+\mathcal{M}$; finiteness of the residue field guarantees that any invertible series has an iterate with this property. We also assume that $u'(0)$ is not a root of 1. Let $p \nmid m$. It is important to know that if α is a periodic point of period $p^n m$, then it is a periodic point of period p^n (see Li [2, Corollary 2.3.2]). We define the number of fixed points of $u^{\circ p^n}(x)$ (i.e. the number of periodic points of period p^n), counting multiplicity, by $i_n(u)$. Thus $i_n(u) = \text{wideg}(u^{\circ p^n}(x) - x)$. In [3], the main theorem (Theorem 3.9) says that if $u(x)$ commutes with some noninvertible power series, then there exists m such that for all $n > m$,

$$i_n(u) = a + bp^{\lambda} + bp^{2\lambda} + \cdots + bp^{(n-m)\lambda},$$

for some a, b and λ. This theorem gives us an effective method to compute the number of periodic points of these invertible series. It turns out that this computation lends support to the conjecture of Lubin.

When a noninvertible series, $f(x)$, commutes with an invertible series, a root of iterates of $f(x)$ is not always simple (for example in the *condensation* case [3]). However, if $f(x)$ is a noninvertible endomorphism of a formal group, then it's easy to prove that all the roots of iterates of $f(x)$ are simple. Therefore it seems to be the right setting to consider the case which all the roots of iterates are simple.

If $u(x)$ is an automorphism which commutes with $f(x)$, then $i_n(u)$ is a power of p for all n (Li [3, Proposition 2.2]). In this paper, we shall prove the following:

THEOREM. *Let $u(x)$, $f(x)$ be invertible and noninvertible, respectively, in $\mathcal{O}[[x]]$, with $f \circ u = u \circ f$. Suppose further that all the roots of iterates of $f(x)$ are simple. Then every x-coordinate of the vertices of the Newton polygon of $f(x)$ is a power of p. Further more, we have that $i_n(u)$ is a power of p for n sufficiently large.*

By this theorem, we shall prove that many phenomena are the same as endomorphisms of a formal group. We shall use this theorem to find the *absolute* endomorphism ring of a Lubin–Tate formal group.

2. Newton ploygons and Newton copolygons

In this paper, we consider the set of power series $f(x) \in \mathcal{O}[[x]]$ such that $f(0) = 0$ and $f'(0)$ is neither 0 nor any root of 1. We denote it by $\mathcal{S}_0(\mathcal{O})$.

The *Newton polygon* is a natural tool to study the roots of p-adic power series (see Koblitz [1]). If $f(x) = \Sigma_{i=0}^{\infty} a_i x^i \in K[[x]]$, the Newton polygon of $f(x)$, denoted $\mathcal{N}(f)$ is constructed by erecting vertical half lines on all the points of the form $(i, v(a_i))$ in the Cartesian plane, and then taking the convex hull of the union of these lines. The basic property of the Newton polygon is the following:

LEMMA 2.1 *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* $x \in \overline{K}$ *for which* $f(x) = 0$ *and* $v(x) = -\lambda$.

If $f(x) \in \mathcal{O}[[x]]$ and $\text{wideg}(f) < \infty$, then since there are only finitely many roots in $\overline{\mathcal{M}}$, $\mathcal{N}(f)$ only has finitely many segments with negative slope and finite width. In this paper when we talk about Newton polygon we restrict it to the segments of negative slopes.

Let $f(x), g(x) \in \mathcal{O}[[x]]$. If for some $a > 0$ the set $\{\alpha \in \overline{\mathcal{M}} \mid f(\alpha) = 0,\ v(\alpha) > a\}$ is equal to the set $\{\alpha \in \overline{\mathcal{M}} \mid g(\alpha) = 0,\ v(\alpha) > a\}$ (counting multiplicity), then for every segment of $\mathcal{N}(f)$ with slope less than $-a$, there exists a segment of $\mathcal{N}(g)$ with same slope and same width. This implies the following:

LEMMA 2.2 *Let* $f(x)$ *and* $g(x)$ *be power series in* $\mathcal{O}[[x]]$ *such that their roots satisfy the condition described above, and suppose that every segment of* $\mathcal{N}(f)$ *on the left of the vertical line* $x = b$ *is of slope less than* $-a$. *Then* (ξ, η) *is a vertex of* $\mathcal{N}(f)$ *with* $\xi < b$, *if and only if* $(\xi, \eta + v(g'(0)) - v(f'(0)))$ *is a vertex of* $\mathcal{N}(g)$.

Another geometric object, which contains the same information as the Newton polygon, is the *Newton copolygon*. Let $f(x) = \Sigma_{n=1}^{\infty} a_n x^n$. The Newton copolygon of $f(x)$, denoted $\mathcal{N}^*(f)$, is defined to be the intersection in the Cartesian plane of all half planes defined by the inequalities $y \leqslant ix + v(a_i)$. It is easy to see that two power series have the same Newton copolygon if and only if they have the same Newton polygon: indeed, the polygon and copolygon are essentially dual convex bodies. We have the following facts. The detail is available in [4].

LEMMA 2.3 *The vertices of* $\mathcal{N}(f)$ *are in one-to-one correspondence with the segments of* $\mathcal{N}^*(f)$; *if* $(\mathcal{P}, \mathcal{S}^*)$ *is a corresponding pair, the* x*-coordinate of* $\mathcal{P}$ *is the slope of* $\mathcal{S}^*$ *and the* y*-coordinate of* $\mathcal{P}$ *is the* y*-intercept of* $\mathcal{S}^*$.

LEMMA 2.4 *The nonvertical segments of* $\mathcal{N}(f)$ *are in one-to-one correspondence with the vertices of* $\mathcal{N}^*(f)$; *if* $(\mathcal{S}, \mathcal{P}^*)$ *is a corresponding pair, the* x*-coordinate of* $\mathcal{P}^*$ *is the negative of the slope of* $\mathcal{S}$ *and the* y*-coordinate of* $\mathcal{P}^*$ *is the* y*-intercept of* $\mathcal{S}$.

The valuation function of $f(x)$, denoted by $\Psi_f(x)$, is a real-valued polygonal function defined for nonnegative values whose graph is the upper boundary of the Newton copolygon. We know that for any $\alpha \in \overline{\mathcal{M}}$ if $v(\alpha)$ is not the x-coordinate of any vertex of the Newton copolygon, then the relation $v(f(\alpha)) = \Psi_f(v(\alpha))$ holds. It follows that if $g(x)$ is another series without constant term, then

$$\Psi_f \circ \Psi_g = \Psi_{f \circ g}.$$

If $f(x) \in \mathcal{O}[[x]]$, $f(0) = 0$ and $1 < \text{wideg}(f) = d < \infty$, then $\Psi_f(x)$ is a polygonal function with finitely many segments. The leftmost segment is the line $y = dx$ and

the rightmost segment is the line $y = x + v(f'(0))$. Ψ_f is strictly increasing and all the segments of Ψ_f lie entirely above the line $y = x$.

To study the roots of iterates of $f(x)$, we have to study the Newton polygon (or Newton copolygon) of $f^{\circ n}(x)$ for every n. Let $(\xi_0^*, \Psi_f(\xi_0^*))$ be the rightmost vertex of $\mathcal{N}^*(f)$, i.e. $\Psi_f(x) = x + v(f'(0))$ for all $x \geqslant \xi_0^*$. Let ξ_1^* satisfy that $\Psi_f(\xi_1^*) = \xi_0^*$. Then $\Psi_{f^{\circ 2}}(x) = \Psi_f^{\circ 2}(x) = \Psi_f(x) + v(f'(0))$ for all $x \geqslant \xi_1^*$. This means that the graph of $\mathcal{N}^*(f^{\circ 2})$ above the line $y = \xi_0^* + v(f'(0))$ can be obtained by moving the graph of $\mathcal{N}^*(f)$ above the line $y = \xi_0^*$ along the y-axis by $v(f'(0))$ unit-length. By induction, we find ξ_i^* such that $\Psi_{f^{\circ i}}(\xi_i^*) = \Psi_f^{\circ i}(\xi_i^*) = \xi_0^*$ and the graph of $\mathcal{N}^*(f^{\circ i+1})$ above the line $\xi_0^* + v(f'(0))$ is obtained by moving the graph of $\mathcal{N}^*(f^{\circ i})$ above the line $y = \xi_0^*$ along the y-axis by $v(f'(0))$ unit-length.

PROPOSITION 2.5 *Let $f(x) \in \mathcal{S}_0(\mathcal{O})$ be a noninvertible power series. Then there exists A such that for every i the graph of $\mathcal{N}(f^{\circ i+1})$ above the line $y = A + v(f'(0))$ is obtained by moving the graph of $\mathcal{N}(f^{\circ i})$ above the line $y = A$ along the y-axis by $v(f'(0))$ unit-length.*

Proof. By the observation above and by the duality between the Newton polygon and the Newton copolygon (Lemma 2.3 and Lemma 2.4), we have that a part of the graph of $\mathcal{N}(f^{\circ i+1})$ is obtained by moving the part of the graph of $\mathcal{N}(f^{\circ i})$ with segments of y-intercept greater than ξ_0^*. Since every segment of the Newton polygon is of negative slope, our proof is complete by setting $A = \xi_0^*$. □

Remark. By the ξ_i^* constructed above, it implies that if $f^{\circ i+1}(\alpha) = 0$ and $v(\alpha) > \xi_i^*$, then $f^{\circ i}(\alpha) = 0$.

Suppose that there is a segment of $\mathcal{N}^*(f)$ whose slope is not a power of p (this is equivalent to the condition that there is a vertex of $\mathcal{N}(f)$ whose x-coordinate is not a power of p). It is easy to prove that for every A there exists j such that there is a vertex of $\mathcal{N}^*(f^{\circ j})$ above the line $y = A$ whose right hand side segment is of slope not a power of p. For simplicity, we replace $f^{\circ j}$ with f. Let ξ_1^* be an x-coordinate of the vertex of $\mathcal{N}^*(f)$ such that $\Psi_f(\xi_1^*) \geqslant A$ and the right derivative of $\Psi_f(x)$ at ξ_1^* is not a power of p. Let ξ_2^* satisfy that $\Psi_f(\xi_2^*) = \xi_1^*$. Because $\Psi_f \circ \Psi_f = \Psi_{f^{\circ 2}}$, it implies that ξ_2^* is an x-coordinate of the vertex of $\mathcal{N}^*(f^{\circ 2})$ such that the right derivative of $\Psi_{f^{\circ 2}}(x)$ at ξ_2^* is not a power of p. By induction, we can find ξ_i^* which is an x-coordinate of the vertex of $\mathcal{N}^*(f^{\circ i})$ such that the right derivative of $\Psi_{f^{\circ i}}(x)$ at ξ_i^* is not a power of p and $\Psi_{f^{\circ i}}(\xi_i^*) = \Psi_f^{\circ i}(\xi_i^*) = \Psi_f(\xi_1^*)$. This means that for any i, $(\xi_i^*, \Psi_f(\xi_1^*))$ is a vertex of $\mathcal{N}^*(f^{\circ i})$ such that the right derivative of $\Psi_{f^{\circ i}}(x)$ at ξ_i^* is not a power of p.

PROPOSITION 2.6 *Let $f(x) \in \mathcal{S}_0(\mathcal{O})$ be a noninvertible power series. If there is a vertex of $\mathcal{N}(f)$ whose x-coordinate is not a power of p, then for every A there exists M such that for every sufficiently large n there exists a vertex, (ξ_n, η_n), of $\mathcal{N}(f^{\circ n})$ with $A \leqslant \eta_n \leqslant M$ and ξ_n not a power of p.*

Proof. Without loss of generality, we can assume that $\Psi_f(\xi_1^*) \geqslant A$. Therefore, for every n, $(\xi_n^*, \Psi_f(\xi_1^*))$ is a vertex of $\mathcal{N}^*(f^{\circ n})$ and the right derivative of $\Psi_{f^{\circ n}}$ at ξ_n^* is not a power of p. By the duality between the Newton polygon and the Newton copolygon (Lemma 2.3 and Lemma 2.4), we have that $(\xi_n^*, \Psi_f(\xi_1^*))$ corresponds to a segment of $\mathcal{N}(f^{\circ n})$ with slope $-\xi_n^*$ and y-intercept $\Psi_f(\xi_1^*)$. This segment intersects another segment of $\mathcal{N}(f^{\circ n})$ at the vertex (ξ_n, η_n), where ξ_n is equal to the right derivative of $\Psi_{f^{\circ n}}$ at ξ_n^*. Since the segment is of negative slope, it implies that $\eta_n < \Psi_f(\xi_1^*)$. Therefore our proof is complete by setting $M = \Psi_f(\xi_1^*)$. □

Proposition 2.5 and Proposition 2.6 are true for general noninvertible series (without the assumption that $f(x)$ commutes with an invertible series). For every n, one can argue from the graph of $\mathcal{N}(f)$ to find $\mathcal{N}(f^{\circ n})$ (using the Newton copolygon would be easier). To study the periodic points of an invertible series $u(x)$, we have to study the Newton polygon of $u^{\circ p^n}(x) - x$. Usually, it is almost impossible to find $\mathcal{N}(u^{\circ p^n}(x) - x)$ by just arguing from the graph of $\mathcal{N}(u(x) - x)$. However, if $u(x)$ commutes with $f(x)$, then by using the results in next section, we can find $\mathcal{N}(u^{\circ p^n}(x) - x)$ from $\mathcal{N}(u^{\circ p^{n-1}}(x) - x)$ for n sufficiently large. Here we only need the following properties.

PROPOSITION 2.7 *Let $u(x) \in \mathcal{S}_0(\mathcal{O})$ be an invertible power series with $u'(0) \equiv 1 \pmod{\mathcal{M}}$. Then there exist $B \geqslant e$ such that for sufficiently large n, the graph of $\mathcal{N}(u^{\circ p^n}(x) - x)$ above the line $y = e + B$ can be obtained by moving the graph of $\mathcal{N}(u^{\circ p^{n-1}}(x) - x)$ above the line $y = B$ along the y-axis by e unit-length.*

Proof. This can be obtained by the following elementary observation:

Let π be a prime element in $\mathcal{M}$ and let $w(x) \in \mathcal{O}[[x]]$, with $w(x) = x + \pi^r g(x)$ where $g(x) \in \mathcal{O}[[x]]$. Then $w^{\circ p}(x) \equiv x + p\pi^r g(x) \pmod{\mathcal{M}^{2r}}$. □

3. Counting periodic points

We begin by recalling some of the notations and results from [3]. Recall that K is a field which is complete with respect to a valuation, v. We normalize the valuation v such that $v(\pi) = 1$, where π is a generator of $\mathcal{M}$. There is a unique extension of v to $\overline{K}$, and this will likewise be denoted v. We denote the ramification index $v(p)$ by e.

NOTATION. $u(x) \in \mathcal{S}_0(\mathcal{O})$ is an invertible series with $u'(0) \equiv 1 \pmod{\mathcal{M}}$ which commutes with a noninvertible series $f(x) \in \mathcal{S}_0(\mathcal{O})$. Since we only discuss the case modulo $\mathcal{M}^T$ for a finite number T, after taking some iterates of $u(x)$, we can always suppose that $u'(0) \equiv 1 \pmod{\mathcal{M}^T}$.

Set $m_n(0) = i_n(u) = \text{wideg}(u^{\circ p^n}(x) - x)$ and $m_n(r)$ equal to the lowest degrees of terms of $u^{\circ p^n}$ whose coefficients are in $\mathcal{M}^r \setminus \mathcal{M}^{r+1}$. Thus if $u^{\circ p^n}(x) - x = \Sigma_{i=1}^{\infty} b_i x^i$, then $m_n(r) = \inf\{i \mid v(b_i) = r\}$.

We also set $S_n(r)$ equal to the set of degrees of terms of $f^{\circ n}(x)$ whose coefficients are in $\mathcal{M}^r \setminus \mathcal{M}^{r+1}$. Thus if $f^{\circ n}(x) = \Sigma_{i=1}^{\infty} a_i x^i$, then $S_n(r) = \{i \mid v(a_i) = r\}$. For any $t \in \mathbf{Q}$, define $o(t) \in \mathbf{Z}$ being the order of p at the factorization of t. Suppose that $m = \inf\{o(t) \mid t \in S_n(r)\}$. Let $s_n(r)$ be the smallest number in $S_n(r)$ with $o(s_n(r)) = m$, i.e. $s_n(r) = \inf\{i \mid v(a_i) = r,\ o(i) = m\}$.

Let $\{a_n\}_n, \{b_n\}_n$ be two sequences. Denote $\{a_n\}_n \gg \{b_n\}_n$, if $\liminf_{n\to\infty} a_n/b_n > 1$. Denote $\{a_n\}_n \sim \{b_n\}_n$, if $\liminf_{n\to\infty} a_n/b_n = 1$.

LEMMA 3.1 *For every M and r there exists M' such that for every $j \leqslant r$, $o(s_n(j)) > M$ when $n \geqslant M'$.*

Proof. See Li [3] Proposition 3.4. □

Given T, by this lemma, there exists i such that $o(s_i(j)) > T + e$ for all $j \leqslant T$. By replacing f with $f^{\circ i}$, we may assume that $o(s_1(j)) > T + e$ for all $j \leqslant T$. For convenience, we also replace $s_1(j)$ with $s(j)$.

Choose T sufficiently large. We make $o(s(j)) > T + e$ for all $j \leqslant T$, so that we can compute the lowest degrees of $f \circ u^{\circ p^n} - f$ and $u^{\circ p^n} \circ f - f \bmod \mathcal{M}^j$ easily. In fact, when $r < e$, because for $v(a) = 0$, $p \nmid t$ and s sufficiently large,

$$(x + \pi g(x) + ax^m)^{tp^s} \equiv x^{tp^s} + ta^{p^s} x^{p^s(t-1)+mp^s} \pmod{\mathcal{M}^{r+1}, \text{ higher degree}},$$

we have that in $f \circ u^{\circ p^n} - f \bmod \mathcal{M}^{r+1}$ the lowest degree contributed by the monomial $a_i x^i$ of $f(x)$ with $v(a_i) \leqslant r$ is $p^{o(i)}(m_n(0) - 1) + i$. By the definition of $s(j)$, the lowest degree of $f \circ u^{\circ p^n} - f \bmod \mathcal{M}^{r+1}$ is $\min\{p^{o(s(j))}(m_n(0) - 1) + s(j);\ j \leqslant r\}$ when $m_n(0)$ is large enough. Therefore if we set

$$d_r = \min\{o(s(j)) \mid j \leqslant r\} \quad \text{and}$$

$$c_r = \min\{s(j) \mid o(s(j)) = d_r,\ j \leqslant r\},$$

then the lowest degree of $f \circ u^{\circ p^n} - f \bmod \mathcal{M}^{r+1}$ is $p^{d_r}(m_n(0) - 1) + c_r$, for sufficiently large $m_n(0)$.

When $e \leqslant r < 2e$, write $r = e + r'$ where $0 \leqslant r' < e$. Because for $v(a) = 0$, $p \nmid t$ and s sufficiently large,

$$(x + \pi g(x) + ax^m)^{tp^s} \equiv x^{tp^s} + tpa^{p^{s-1}} x^{p^s(t-1)+p^{s-1}(p-1)+mp^{s-1}} \pmod{\mathcal{M}^{r+1}, \text{ higher degree}},$$

we have that in $f \circ u^{\circ p^n} - f \bmod \mathcal{M}^{r+1}$ the lowest degree contributed by the monomial $a_i x^i$ of $f(x)$ with $v(a_i) \leqslant r'$ is $p^{o(i)-1}(m_n(0) - 1) + i$ and the lowest degree contributed by the monomial $a_j x^j$ of $f(x)$ with $r' < v(a_j) \leqslant r$ is $p^{o(j)}(m_n(0) - 1) + j$. Therefore if we set

$$d_r = \min\{o(s(i)) - 1, o(s(j)) \mid i \leqslant r',\ r' < j \leqslant r\} \quad \text{and}$$

$$\begin{aligned} c_r &= \min\{s(i),\ s(j) \mid o(s(i)) - 1 = d_r,\ o(s(j)) = d_r, \\ &\qquad \text{for } i \leqslant r',\ r' < j \leqslant r\}, \end{aligned}$$

then the lowest degree of $f \circ u^{\circ p^n} - f \bmod \mathcal{M}^{r+1}$ is $p^{d_r}(m_n(0) - 1) + c_r$, for sufficiently large $m_n(0)$.

Inductively, when $r = 2e + r'$ where $0 \leqslant r' < e$, we set

$$\begin{aligned} d_r &= \min\{o(s(i)) - 2,\ o(s(i')) - 1,\ o(s(j)) \mid i \leqslant r', \\ &\qquad r' < i' \leqslant e + r',\ e + r' < j \leqslant r\}, \\ c_r &= \min\{s(i), s(i'), s(j) \mid o(s(i)) - 2 = o(s(i')) - 1 = o(s(j)) = d_r, \\ &\qquad \text{for } i \leqslant r',\ r' < i' \leqslant e + r',\ e + r' < j \leqslant r\}. \end{aligned}$$

Set d_r and c_r inductively for all $r \leqslant T$. Then we have that the lowest degree of $f \circ u^{\circ p^n} - f \bmod \mathcal{M}^{r+1}$ is $p^{d_r}(m_n(0) - 1) + c_r$, when $m_n(0)$ is sufficiently large. Notice that these d_r's have the properties that $d_r \leqslant d_{r-1}$ and $d_{r+e} \leqslant d_r - 1$.

LEMMA 3.2 *Suppose that $d_r < d_{r-1} = \cdots = d_{r'} < d_{r'-1}$. If $r > j > r'$, then when $m_n(0)$ is sufficiently large the lowest degree of $u^{\circ p^n} \circ f - f \bmod \mathcal{M}^{j+1}$ is $p^{d_0} m_n(r') - (c_{r'} - c_j)$ and we have that $m_n(j) \geqslant m_n(r') - B_{r'}$, where $B_{r'}$ is independent of n.*

When $m_n(0)$ is sufficiently large, the lowest degree of $u^{\circ p^n} \circ f - f \bmod \mathcal{M}^{r+1}$ is $p^{d_0} m_n(r)$ and we have that $\{m_n(r)\}_n \ll \{m_n(j)\}_n$ for every $j < r$.

Proof. This can be proved by using induction on r and by comparing the lowest degrees of $u^{\circ p^n} \circ f - f$ and $f \circ u^{\circ p^n} - f \bmod \mathcal{M}^{r+1}$. See Li [3] Lemma 3.8 for detail. □

Notice that $d_r < d_{r-1}$ if and only if $\{m_n(r)\}_n \ll \{m_n(j)\}_n$ for every $j < r$.

According to Lubin [6] Corollary 4.3.1, we have that if $m_n(0) = \infty$ for some n, then u has only finitely many periodic points in $\overline{\mathcal{M}}$. If u commutes with some noninvertible series, then $u(x)$ has infinitely many periodic points (Lubin [6] Proposition 3.2). Hence $m_n(0) < \infty$ and $\lim_{n\to\infty} m_n(0) = \infty$. It implies that $m_n(0)$ is sufficiently large when n is sufficiently large. Since $f \circ u = u \circ f$ implies $f \circ u^{\circ p^n} - f = u^{\circ p^n} \circ f - f$, by Lemma 3.1 and Lemma 3.2 we have the following.

PROPOSITION 3.3 *Suppose that $r \leqslant T$ and $d_r < d_{r-1}$. Then $p^{d_r}(m_n(0) - 1) + c_r = p^{d_0} m_n(r)$, if n is sufficiently large (or if $m_n(0)$ is sufficiently large).*

Proposition 2.7 is true for general invertible series, *i.e.* without the assumption that $u(x)$ commutes with a noninvertible series. For the next Proposition, we use the assumption that $u(x)$ commutes with a noninvertible series $f(x)$ to find $\mathcal{N}(u^{\circ p^n}(x) - x)$. Keep the notations about d_r and c_r as above. We call d_r a *jump*, if $d_r < d_{r-1}$. From Lemma 3.2, $\{m_n(r)\}_n \ll \{m_n(j)\}_n$ for every $j < r$, if d_r is

a jump. Since $\mathcal{N}(u^{\circ p^n}(x) - x)$ is constructed by erecting vertical half lines on all the points $(m_n(i), i)$ and then taking the convex hull of the union of these lines, we have the following result.

PROPOSITION 3.4 *Let $u(x)$, $f(x) \in \mathcal{S}_0(\mathcal{O})$ be invertible and noninvertible, respectively. Then for n sufficiently large, $(m_n(j), j)$ is a vertex of $\mathcal{N}(u^{\circ p^n}(x) - x)$ only if d_j is a jump.*

Proof. If $(m_n(j), j)$ is a vertex of the Newton polygon of $u^{\circ p^n}(x) - x$ and d_j is not a jump, then we consider the points $(m_n(r), r)$ and $(m_n(t), t)$ where $d_r < d_{r-1} = \cdots = d_j = \cdots = d_t < d_{t-1}$. Since $(m_n(j), j)$ is a vertex, the slope of the segment which connects $(m_n(r), r)$ and $(m_n(t), t)$ must be smaller than the slope of the segment which connects $(m_n(j), j)$ and $(m_n(t), t)$ and $m_n(j) < m_n(t)$. Lemma 3.2 shows that $m_n(r) \ll m_n(t)$ and $m_n(j) \geqslant m_n(t) - C$ of which C is some constant independent of n. The slope of the segment which connects $(m_n(j), j)$ and $(m_n(t), t)$ is smaller than or equal to $-1/C$, but the slope of the segment which connects $(m_n(r), r)$ and $(m_n(t), t)$ tends to 0 as $n \to \infty$, because $m_n(r) \ll m_n(t)$. We get a contradiction. Therefore for n large enough, $(m_n(j), j)$ is not a vertex of $\mathcal{N}(u^{\circ n}(x) - x)$ if d_j is not a jump. See Figure 1 for illustration.

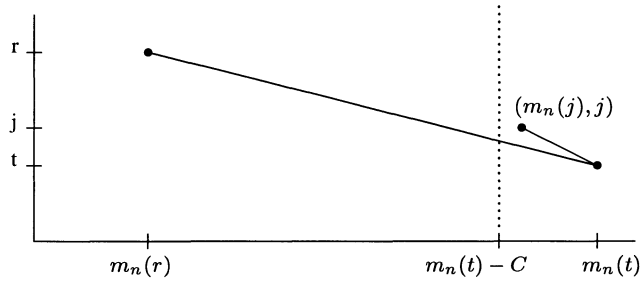

Figure 1.

Remark. By Proposition 3.3 we obtain that if d_r is a jump, then for n sufficiently large

$$\frac{m_{n+1}(r) - m_n(r)}{m_n(r) - m_{n-1}(r)} = \frac{m_{n+1}(0) - m_n(0)}{m_n(0) - m_{n-1}(0)}.$$

Proposition 3.4 combining with the fact that $m_{n+1}(0) - m_n(0) = p^{\lambda}(m_n(0) - m_{n-1}(0))$ for a fixed λ (Li [3, Theorem 3.9]) implies that for n sufficiently large, $(m_n(r), r)$ is a vertex of $\mathcal{N}(u^{\circ p^n}(x) - x)$ if and only if $(m_{n+1}(r), r)$ is a vertex of $\mathcal{N}(u^{\circ p^{n+1}}(x) - x)$.

4. Main theorem

In this Section, we assume that $f(x)$ commutes with an invertible series, $u(x)$, and all the roots of iterates of $f(x)$ are simple. Since $f(x)$ commutes with an invertible

power series, every root of $f'(x)$ is a root of $f^{\circ m}(x)$ for some m (Lubin [6]). $f^{\circ m}(x)$ has only simple roots for all $m \in \mathbf{N}$, so $f'(x)$ has no root in $\overline{\mathcal{M}}$. (In this case it's easy to check that all the roots of iterates of $f(x)$ are simple if and only if $f'(x)$ has no root in $\overline{\mathcal{M}}$.) Hence wideg(f') is either 0 or infinity. Since $f'(0) \in \mathcal{M}$, it implies wideg$(f') = \infty$. Therefore $f'(x) = f'(0) \cdot h(x)$, for some $h(x) \in \mathcal{O}[[x]]$ with wideg$(h) = 0$. Thus $f'(x)/f'(0) \in \mathcal{O}[[x]]$. By the same reasoning we see $(f^{\circ n})'(x)/(f'(0))^n \in \mathcal{O}[[x]]$. Let $f^{\circ n}(x) = \Sigma_{i=1}^{\infty} a_i x^i$. Then we have that

$$v(i) + v(a_i) \geqslant v(a_1) = nv(f'(0)). \qquad (*)$$

Let $(m_i(r), r)$ be a vertex of $\mathcal{N}(u^{\circ p^i}(x) - x)$ with $r \geqslant B$ (B as in Proposition 2.7). We know that the graph of $\mathcal{N}(u^{\circ p^{i+1}}(x) - x)$ above the line $y = r + e$ can be obtained by moving the graph of $\mathcal{N}(u^{\circ p^i}(x) - x)$ above the line $y = r$ along y-axis by e unit-length. If the segment of $\mathcal{N}(u^{\circ p^i}(x) - x)$ on the left of $x = m_i(r)$ which contains the vertex $(m_i(r), r)$ is of slope $-\lambda$, then all the periodic points of $u(x)$ of period p^i with valuation greater than or equal to λ correspond to the segments of $\mathcal{N}(u^{\circ p^i}(x) - x)$ on the left of $x = m_i(r)$. Since for $i' > i$, $\mathcal{N}(u^{\circ p^{i'}}(x) - x)$ on the left of $x = m_i(r)$, has the same shape as $\mathcal{N}(u^{\circ p^i}(x) - x)$ on the left of $x = m_i(r)$, this means that the segments of $\mathcal{N}(u^{\circ p^i}(x) - x)$ on the left of $x = m_i(r)$ correspond to all the periodic points of $u(x)$ with valuation greater than or equal to λ. Since $u(x)$ commutes with $f(x)$, we have that all the periodic points of $u(x)$ are simple (Li [3]) and the set of roots of iterates of $f(x)$ is equal to the set of periodic points of $u(x)$ (Lubin [6]). By Proposition 2.5, all the roots of iterates of $f(x)$ with valuation greater than or equal to λ correspond to some segments of $\mathcal{N}(f^{\circ n})$ for n sufficiently large. By Lemma 2.2, $m_i(r)$ is the x-coordinate of a vertex of $\mathcal{N}(f^{\circ n})$ for all n sufficiently large and there is a one-to-one correspondence between the vertices of $\mathcal{N}(u^{\circ p^i}(x) - x)$ on the left of $x = m_i(r)$ and the vertices of $\mathcal{N}(f^{\circ n})$ on the left of $x = m_i(r)$. Suppose that there exists a sequence $\{n_i\}$ in $\mathbf{N}$ such that $\lim_{i\to\infty} n_i = \infty$ and $\sup_i\{v(m_{n_i}(r))\} \leqslant M < \infty$. For every n_i, there exists n_i' such that $\mathcal{N}(u^{\circ p^{n_i}}(x) - x)$ on the left of $x = m_{n_i}(r)$ is of the same shape as $\mathcal{N}(f^{\circ n_i'})$ on the left of $x = m_{n_i}(r)$. By $(*)$ above, we have that all the vertices of $\mathcal{N}(f^{\circ n_i'})$ on the left of $x = m_{n_i}(r)$ should locate inside the band $\{(x, y) \mid n_i' v(f'(0)) - M \leqslant y \leqslant n_i' v(f'(0))\}$. Only finitely many vertices of Newton polygon can locate inside the band with width M. Because $\lim_{i\to\infty} m_{n_i}(r) = \infty$ and $f(x)$ has infinitely many roots of iterates, we get a contradiction. This means that $\lim_{i\to\infty} o(m_i(r)) = \lim_{i\to\infty} v(m_i(r)) = \infty$.

We claim that if $(m_j(t), t)$ is a vertex of $\mathcal{N}(u^{\circ p^j}(x) - x)$ with $t < B$ for j sufficiently large, then we also have that $\lim_{i\to\infty} o(m_i(t)) = \infty$. Define $\Lambda_n(f) = \{z \in \overline{\mathcal{M}} \mid f^{\circ n}(z) = 0 \text{ and } f^{\circ n-1}(z) \neq 0\}$. For any M, since wideg(f) is a power of p, one may argue from the shape of Newton copolygon to get that $o(v(\alpha)) < -M$, $\forall \alpha \in \Lambda_n(f)$ and for n sufficiently large. Suppose that $(m_j(r), r)$ be the lowest vertex of $\mathcal{N}(u^{\circ p^j}(x) - x)$ above or on the line $y = B$ and $(m_j(r'), r')$ be the

highest vertex of $\mathcal{N}(u^{\circ p^j}(x) - x)$ below the line $y = B$. When i is large enough, the roots of $u^{\circ p^i}(x) - x$, which correspond to the segment of $\mathcal{N}(u^{\circ p^i}(x) - x)$ which connects the vertices $(m_i(r), r)$ and $(m_i(r'), r')$, are in $\Lambda_n(f)$ for some n sufficiently large. Therefore, this segment has slope $-l$ with $o(l^{-1})$ very large. Since $m_i(r') = m_i(r) + (r - r')/l$ and $\lim_{i\to\infty} o(m_i(r)) = \infty$, we deduce that $\lim_{i\to\infty} o(m_i(r')) = \infty$. By induction, our claim follows. It also follows that $\lim_{i\to\infty} o(m_i(0)) = \infty$. In summary, we have proved that if $(m_i(r), r)$ is a vertex of $\mathcal{N}(u^{\circ i}(x) - x)$ for i sufficiently large, then $\lim_{i\to\infty} o(m_i(r)) = \infty$.

By Proposition 2.5 and Proposition 2.7, we obtain that there exists C such that the graph of $\mathcal{N}(f^{\circ i})$ (resp. $\mathcal{N}(u^{\circ p^j}(x) - x)$) above the line $y = C + v(f'(0))$ (resp. $y = C + e$) is obtain by moving the graph of $\mathcal{N}(f^{\circ i-1})$ (resp. $\mathcal{N}(u^{\circ p^{j-1}}(x) - x)$) above the line $y = C$ along y-axis (setting $C = \max\{A, B\}$ where A and B as defined in Proposition 2.5 and Proposition 2.7). Now we are ready to prove our main theorem. By Proposition 2.6, our goal is to prove that for any T, there exists a sufficiently large i such that every x-coordinate of the vertices of $\mathcal{N}(f^{\circ i})$ which is under the line $y = T$ and above the line $y = C$ is a power of p.

THEOREM 4.1 *Let $u(x)$, $f(x)$ be invertible and noninvertible, respectively, in $\mathcal{S}_0(\mathcal{O})$ with $f \circ u = u \circ f$. Suppose further that all the roots of iterates of $f(x)$ are simple. Then every x-coordinate of the vertices of the Newton polygon of $f(x)$ is a power of p. Further more, we have that $i_n(u)$ is a power of p for n sufficiently large.*

Proof. Given T, by Lemma 3.1, there exist i such that $o(s_i(t)) > T + e$ for all $t \leqslant T$. We also choose i large enough such that $v((f^{\circ i})'(0)) = iv(f'(0)) = v(u'(0)^{p^j} - 1)$ for a sufficiently large j. (This can be done because $u'(0)$ is not a root of 1.) By replacing f with $f^{\circ i}$, we want to prove that every x-coordinate of the vertices of $\mathcal{N}(f)$ which is under the line $y = T$ and above the line $y = C$ is a power of p.

Since $v(f'(0)) = v(u'(0)^{p^j} - 1)$, by the choice of C and by Lemma 2.2 we obtain that for $\eta \geqslant C$, (ξ, η) is a vertex of $\mathcal{N}(f)$ if and only if it is a vertex of $\mathcal{N}(u^{\circ j}(x) - x)$. If $(\xi, \eta) = (m_j(\eta), \eta)$ is a vertex of $\mathcal{N}(f)$ with $T \geqslant \eta \geqslant C$, then since we choose j large enough, by Proposition 3.4 and by the remark following it, we have that $(m_n(\eta), \eta)$ is a vertex of $\mathcal{N}(u^{\circ n}(x) - x)$ for all $n > j$ and d_η is a jump. Since $\eta \leqslant T$, by using Proposition 3.3 we obtain that $p^{d_\eta}(m_n(0) - 1) + c_\eta = p^{d_0} m_n(\eta)$. Because $\lim_{n\to\infty} o(m_n(\eta)) = \lim_{n\to\infty} o(m_n(0)) = \infty$, it implies that $c_\eta = p^{d_\eta}$. Since (ξ, η) is a vertex of $\mathcal{N}(f)$ we have that $\xi \leqslant c_\eta = p^{d_\eta}$ and by the definition of c_η we have that $o(\xi) \geqslant o(c_\eta) = d_\eta$. This implies that $\xi = p^{d_\eta}$. This proves our first assertion.

For sufficiently large n, let $(m_n(r), r)$ be a vertex of $\mathcal{N}(u^{\circ n}(x) - x)$ with $T \geqslant r \geqslant C$. Then we know that $m_n(r)$ is the x-coordinate of a vertex of $\mathcal{N}(f^{\circ n'})$ for some n'. Therefore $m_n(r)$ is a power of p. Since $p^{d_r}(m_n(0) - 1) + c_r = p^{d_0} m_n(r)$, we conclude that $m_n(0) = i_n(u)$ is a power of p (because d_r is a jump and

$c_r = p^{d_r}$). □

Let $u(x)$ be an automorphism of a formal group with $u'(0) \equiv 1 \pmod{\mathcal{M}}$. Then there exists an endomorphism $f(x)$ such that the set of fixed points of $u(x)$ is equal to the set of roots of $f(x)$. In our case, we have the following:

COROLLARY 4.1.1. *Suppose that* $\operatorname{wideg}(u(x)-x)$ *is large enough and* $v(f'(0)) = v(u'(0)-1)$. *Then* $\operatorname{wideg}(f) = \operatorname{wideg}(u(x)-x)$

Proof. As discussed in the proof of Theorem 4.1, choose $r > C$ such that $(m_0(r), r)$ is a vertex of $\mathcal{N}(u(x)-x)$. Because $(m_0(r), r)$ is also a vertex of $\mathcal{N}(f)$, we have that $m_0(r) = p^{d_r}$. Since $p^{d_r}(m_0(0)-1) + c_r = p^{d_0} m_0(r)$ and $c_r = p^{d_r}$, it implies that $\operatorname{wideg}(u(x)-x) = m_0(0) = p^{d_0} = \operatorname{wideg}(f)$. □

COROLLARY 4.1.2. *Let* $f(x)$ *be a noninvertible power series in* $S_0(\mathcal{O})$ *such that* $\mathcal{N}(f)$ *has only one segment. Suppose that* $f(x)$ *commutes with an invertible series* $u(x)$ *with* $\operatorname{wideg}(u(x)-x)$ *sufficiently large. If* $v(u'(0)-1) = rv(f'(0))$, *then* $\mathcal{N}(f^{\circ r})$ *is the same as* $\mathcal{N}(u(x)-x)$. *Furthermore, for* $\alpha \in \overline{\mathcal{M}}$ $u(\alpha) = \alpha$ *if and only if* $f^{\circ r}(\alpha) = 0$.

Proof. If (ξ, η) is a vertex of $\mathcal{N}(f^{\circ r})$ with $\eta \geqslant C$, we have that $m_0(\eta) = \xi$, by the assumption that $v(u'(0)-1) = rv(f'(0))$. Since $m_0(0) = \operatorname{wideg}(u(x)-x)$ is large enough, by Corollary 4.1.1 we have that $\operatorname{wideg}(f^{\circ r}) = \operatorname{wideg}(u(x)-x) = m_0(0)$. Since $\mathcal{N}(f)$ has only one segment, by arguing from the shape of the Newton copolygon of $f(x)$, it is easy to check that $\forall\, \alpha, \beta \in \Lambda_n(f)$, $v(\alpha) = v(\beta)$ and $v(\alpha_1) \neq v(\alpha_2)$, if $\alpha_1 \in \Lambda_n(f)$ and $\alpha_2 \notin \Lambda_n(f)$. This implies that for $\eta < C$, (ξ, η) is a vertex of $\mathcal{N}(f^{\circ r})$ if and only if $(m_0(\eta), \eta)$ is a vertex of $\mathcal{N}(u(x)-x)$. If (ξ, η) is a vertex of $\mathcal{N}(f^{\circ r})$ with $\eta < C$, then since ξ is a power of p, by Proposition 3.3, we have that $\xi m_0(0) = \operatorname{wideg}(f^{\circ r}) m_0(\eta)$. This implies that $\xi = m_0(\eta)$. Our proof is complete. □

In Li [3, Theorem 3.9], we know that for n sufficiently large, there exists λ such that

$$\frac{i_{n+1}(u) - i_n(u)}{i_n(u) - i_{n-1}(u)} = p^{\lambda}.$$

If $u(x)$ is an automorphism of a formal group $\mathcal{F}(x, y)$ and $f(x)$ is an endomorphism of $\mathcal{F}(x, y)$ with $v(f'(0)) = v(p) = e$, then we have that $\operatorname{wideg}(f) = p^{\lambda}$. In our case, we have the following:

COROLLARY 4.1.3. *If* $f \circ u = u \circ f$ *and* $\operatorname{wideg}(f) = p^l$, *then* $\lambda = el/v(f'(0))$.

Proof. Choose a sufficiently large n such that $v(u'(0)^n - 1) = mv(f'(0))$, for some m (notice the assumption that $u'(0)$ is not a root of 1). By Corollary

4.1.1, it implies that $i_n(u) = m_n(0) = \text{wideg}(f^{\circ m}) = p^{ml}$. Choose another $n' > n$ such that $v(u'(0)^{p^{n'}} - 1) = m'v(f'(0))$, for some m'. We have that $i_{n'}(u) = m_{n'}(0) = \text{wideg}(f^{\circ m'}) = p^{m'l}$. $i_{n+1}(u) = p^{\lambda}(i_n(u) - i_{n-1}(u)) + i_n(u) = p^{\lambda+ml} - p^{\lambda}i_{n-1}(u) + p^{ml}$. Since $i_{n+1}(u)$ and $i_{n-1}(u)$ are powers of p and $i_{n+1}(u) > i_{n-1}(u)$, it implies that $i_{n+1}(u) = p^{\lambda+ml}$. By induction, it follows that $i_{n'}(u) = p^{(n'-n)\lambda+ml}$. This implies $p^{m'l} = p^{(n'-n)\lambda+ml}$, i.e. $(m'-m)l = (n'-n)\lambda$.

When n is large enough, $v(u'(0)^{p^{n'}} - 1) - v(u'(0)^{p^n} - 1) = (n'-n)v(p) = (n'-n)e$. By assumption, we have that $(m'-m)v(f'(0)) = (n'-n)e$. Our claim follows. □

5. Fields of torsion points

Let $f(x)$ be a *Lubin–Tate* power series, i.e. $f(x) \equiv \pi x \,(\text{mod } x^2)$ and $f(x) \equiv x^q (\text{mod } \mathcal{M})$, where π is a generator of $\mathcal{M}$ and $q = \#(k) = \#(\mathcal{O}/\mathcal{M})$. Then there exists a unique formal group law $\mathcal{F}(x,y) \in \mathcal{O}[[x]]$ satisfying the condition $\mathcal{F}(f(x), f(y)) = f(\mathcal{F}(x,y))$. $\mathcal{F}(x,y)$ gives $\overline{\mathcal{M}}$ a formal $\mathcal{O}$-module structure. We denote the field of $f^{\circ n}$-torsion points by $K_n(f) = K(\Lambda_n(f))$. In [7], it says that $K_n(f)$ is a totally ramified abelian extension over K. In this section, we shall get a similar result, if $f(x) \equiv \pi x \ (\text{mod } x^2)$, and the set of noninvertible series which commute with $f(x)$ is sufficiently large.

LEMMA 5.1 *Let $f(x) \in \mathcal{S}_0(\mathcal{O})$. Then for every $a \in K$, there exists a unique power series $h(x) \in K[[x]]$ with $h(0) = 0$, $h'(0) = a$ and $f \circ h = h \circ f$.*

Proof. See Lubin [6, Proposition 1.1]. □

By the Lemma above, for every $a \in K$, we denote $[a]_f(x)$ the unique series in $K[[x]]$ satisfying $[a]_f \circ f = f \circ [a]_f$ whose first-degree coefficient is a.

DEFINITION 5.2 Let $f(x) \in \mathcal{S}_0(\mathcal{O})$. We define $U_f = \{u \in \mathcal{O}^* \mid [u]_f(x) \in \mathcal{O}[[x]]\}$ and $U_f^{(n)} = \{u \in \mathcal{O}^* \mid [u]_f(x) \in \mathcal{O}[[x]] \text{ and } u - 1 \in \mathcal{M}^n\}$.

Remark. U_f is a subgroup of $\mathcal{O}^*$, since for every $u_1, u_2 \in U_f$ $[u_1 \cdot u_2]_f(x) = [u_1]_f \circ [u_2]_f(x) \in \mathcal{O}[[x]]$ and $[u^{-1}]_f(x) = [u]_f^{\circ -1}(x) \in \mathcal{O}[[x]]$. By the same reasoning, $U_f^{(n)}$ is a subgroup of U_f.

PROPOSITION 5.3 *Let $f(x)$ be a power series in $\mathcal{O}[[x]]$ satisfying $f(x) \equiv \pi x$ (mod x^2) and* wideg$(f) = p^l$. *Let $K_n(f) = K(\Lambda_n(f))$ be the field of $f^{\circ n}$-torsion points. For a sufficiently large n, suppose that $\#(U_f/U_f^{(n)}) = p^{l(n-1)}(p^l - 1)$. Then $K_n(f)|K$ is a totally ramified abelian extension, of degree $p^{l(n-1)}(p^l - 1)$ with Galois group*

$$\text{G}(K_n(f)|K) \cong U_f/U_f^{(n)}.$$

Proof. Since $f(x)$ commutes with an invertible series, we have that $f(x) \equiv g(x^{p^l}) \pmod{\mathcal{M}}$ (Lubin [6]). Therefore $\text{wideg}(f') = \infty$. Because $f'(0) = \pi$, $f'(x)$ has no root in $\overline{\mathcal{M}}$. Hence all the roots of iterates of $f(x)$ are simple.

Fix an $\alpha \in \Lambda_n(f)$. Since the Newton polygon of $f(x)$ has only one segment, $[u]_f(\alpha) \in \Lambda_n(f)$ for every $u \in U_f$ (because $f^{\circ n}([u]_f(\alpha)) = [u]_f(f^{\circ n}(\alpha)) = 0$ and $v([u]_f(\alpha)) = v(\alpha)$). Consider the map

$$U_f \to \Lambda_n(f), \qquad u \mapsto [u]_f(\alpha).$$

By Corollary 4.1.2, it induces an injective map $U_f/U_f^{(n)} \to \Lambda_n(f)$, which is also surjective since both sides have same order.

Consider

$$\phi_n(x) = \frac{f^{\circ n}(x)}{f^{\circ n-1}(x)} \in \mathcal{O}[[x]].$$

$\phi_n(0) = \pi$ and $\text{wideg}(\phi_n) = p^{l(n-1)}(p^l - 1)$. According to the Weierstrass Preparation Theorem, $\Lambda_n(f)$ is the set of roots of an Eisenstein polynomial of degree $p^{l(n-1)}(p^l - l)$. Since for every $\beta \in \Lambda_n(f)$ there exists $u \in U_f$ such that $[u]_f(\alpha) = \beta$, our claim follows. □

In fact, we have proved:

PROPOSITION 5.4 *Let $f(x)$ be a power series in $\mathcal{O}[[x]]$ satisfying $f(x) \equiv \pi x \pmod{x^2}$ and $\text{wideg}(f) = p^l$. Then $\#(U_f/U_f^{(n)}) \leqslant p^{l(n-1)}(p^l - 1)$, for n sufficiently large.*

Proof. Since the map $U_f/U_f^{(n)} \to \Lambda_n(f)$ is injective and $\#(\Lambda_n(f))$ is $p^{l(n-1)}(p^l - 1)$, our proof is complete. □

EXAMPLE Let L be an finite unramified extension of K. We denote by $\mathcal{O}_K$ (*resp.* $\mathcal{O}_L$) the integer ring of K (*resp.* L) and U_K (*resp.* U_L) being it's unit. Let $f(x)$ be a Lubin-Tate power series over $\mathcal{O}_K$ and $\mathcal{F}(x, y)$ be it's group law. The set of all $\mathcal{O}_K$-endomorphisms (*resp.* $\mathcal{O}_L$-endomorphisms) of $\mathcal{F}$ is denoted by $\text{End}_{\mathcal{O}_K}(\mathcal{F})$ (*resp.* $\text{End}_{\mathcal{O}_L}(\mathcal{F})$). According to Lubin and Tate [7], $\text{End}_{\mathcal{O}_K}(\mathcal{F})$ is isomorphic to $\mathcal{O}_K$. Thus for every $a \in \mathcal{O}_K$, $[a]_f \in \mathcal{O}_K[[x]]$. We would like to find $\text{End}_{\mathcal{O}_L}(\mathcal{F})$.

Denote by $U_{f,K}$ (*resp.* $U_{f,L}$) the set of $u \in U_K$ (*resp.* U_L) such that $[u]_f \in \mathcal{O}_K[[x]]$ (*resp.* $\mathcal{O}_L[[x]]$). We have that for n large enough,

$$U_K/U_K^{(n)} = U_{f,K}/U_{f,K}^{(n)} \hookrightarrow U_{f,L}/U_{f,L}^{(n)}.$$

Recall that $\text{wideg}(f) = q$, where q is the number of residue field of $\mathcal{O}_K$. By Proposition 5.3, we have that $\#(U_{f,L}/U_{f,L}^{(n)}) \leqslant q^{n-1}(q-1)$. Since $\#(U_K/U_K^{(n)}) = q^{n-1}(q-1)$, it implies that $U_{f,L}/U_{f,L}^{(n)} \cong U_K/U_K^{(n)}$ for all n which is sufficiently large. It follows that $U_{f,L} = U_K$, because both K and L are complete.

If $h(x) \in \mathrm{End}_{\mathcal{O}_L}(\mathcal{F})$, then we have that $h \circ f = f \circ h$. Since the Newton polygon of f has only one segment, according to Li [4, Corollary 3.4.1] for every $h(x) \in \mathrm{End}_{\mathcal{O}_L}(\mathcal{F}), h(x) = [u]_f \circ f^{om}(x)$ for some m and $u \in U_{f,L}$. Because $U_{f,L} = U_K$ and $f \in \mathcal{O}_K[[x]]$, it implies that

$$\mathrm{End}_{\mathcal{O}_L}(\mathcal{F}) = \mathrm{End}_{\mathcal{O}_K}(\mathcal{F}) \cong \mathcal{O}_K.$$

Remark. When L is totally ramified over K, we can use similar argument to prove that $\mathrm{End}_{\mathcal{O}_L}(\mathcal{F}) = \mathrm{End}_{\mathcal{O}_K}(\mathcal{F})$. This says that the *absolute* endomorphism ring of $\mathcal{F}(x, y)$ is isomorphic to $\mathcal{O}_K$. This result can also be proved by using Lubin [8, Theorem 2.3.2].

Acknowledgment

The author would like to thank M. Rosen and J. Lubin for many helpful comments.

References

1. Koblitz, N.: *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, New York, 1977.
2. Li, H.-C.: p-adic Periodic Points and Sen's Theorem, *J. Number Theory* 56, 2 (1996), 309–318.
3. Li, H.-C.: Counting Periodic Points of p-adic Power Series, *Comp. Math.* 100 (1996), 351–364.
4. Li, H.-C.: p-adic Power Series which Commute under Composition, *Trans. of A.M.S.*, to appear.
5. Li, H.-C.: p-adic Dynamical Systems, *Ph. D. Thesis*, Brown University, 1994.
6. Lubin, J.: Nonarchimedean Dynamical System, *Comp. Math.* 94 (1994), 321–346.
7. Lubin, J. and Tate, J.: Formal Complex Multiplication in Local Field, *Ann. Math.* 81 (1965), 380–387.
8. Lubin, J.: One-parameter Formal Lie Groups over p-adic Integer Rings, *Ann. Math.* 80 (1964), 464–484.