NONARCHIMEDEAN DYNAMICAL SYSTEMS AND FORMAL GROUPS

by

Laurent Berger

Abstract. — We prove two theorems that confirm an observation of Lubin concerning families of $p$-adic power series that commute under composition: under certain conditions, there is a formal group such that the power series in the family are either endomorphisms of this group, or semi-conjugate to endomorphisms of this group.

Introduction

Let $K$ be a finite extension of $\mathbb{Q}_p$, and let $\mathcal{O}_K$ be its ring of integers and $\mathfrak{m}_K$ the maximal ideal of $\mathcal{O}_K$. In [Lub94], Lubin studied nonarchimedean dynamical systems, namely families of elements of $X \cdot \mathcal{O}_K[X]$ that commute under composition, and remarked (page 341 of ibid.) that “experimental evidence seems to suggest that for an invertible series to commute with a noninvertible series, there must be a formal group somehow in the background”. Various results in that direction have been obtained (by Hsia, Laubie, Li, Movahhedi, Salinier, Sarkis, Specter, ...; see for instance [Li96], [Li97a], [Li97b], [LMS02], [Sar05], [Sar10], [SS13], [HL16], [Ber17], [Spe18]), using either $p$-adic analysis, the theory of the field of norms or, more recently, $p$-adic Hodge theory. The purpose of this article is to prove two theorems that confirm the above observation in many new cases, using only $p$-adic analysis.

If $g(X) \in X \cdot \mathcal{O}_K[X]$, we say that $g$ is invertible if $g'(0) \in \mathcal{O}_K^\times$ and noninvertible if $g'(0) \in \mathfrak{m}_K$. We say that $g$ is stable if $g'(0)$ is neither 0 nor a root of unity. For example, if $S$ is a formal group of finite height over $\mathcal{O}_K$ and if $c \in \mathbb{Z}$ with $p \nmid c$ and $c \neq \pm 1$, then $f(X) = [p](X)$ and $u(X) = [c](X)$ are two stable power series, with $f$ noninvertible and $u$ invertible, having the following properties: the roots of $f$ and all of its iterates are simple, $f \not\equiv 0 \mod \mathfrak{m}_K$ and $f \circ u = u \circ f$. Our first result is a partial converse of this. If

2010 Mathematics Subject Classification. — 11S82 (11S31; 32P05).
Key words and phrases. — Nonarchimedean dynamical system; formal group; $p$-adic analysis.
\( f(X) \in X \cdot \mathcal{O}_K[X] \), let \( U_f \) denote the set of invertible power series \( u(X) \in X \cdot \mathcal{O}_K[X] \) such that \( f \circ u = u \circ f \), and let \( U_f'(0) = \{ u'(0), \ u \in U_f \} \). This is a subgroup of \( \mathcal{O}_K^\times \).

**Theorem A.** — Let \( K \) be a finite extension of \( \mathbb{Q}_p \) such that \( e(K/\mathbb{Q}_p) \leq p - 1 \), and let \( f(X) \in X \cdot \mathcal{O}_K[X] \) be a noninvertible stable series. Suppose that

1. the roots of \( f \) and all of its iterates are simple, and \( f \not\equiv 0 \) mod \( m_K \);
2. there is a subfield \( F \) of \( K \) such that \( f'(0) \in \mathcal{m}_F \) and such that \( U_f'(0) \cap \mathcal{O}_F^\times \) is an open subgroup of \( \mathcal{O}_F^\times \).

Then there is a formal group \( S \) over \( \mathcal{O}_K \) such that \( f \in \text{End}(S) \) and \( U_f \subset \text{End}(S) \).

Condition (1) can be checked using the following criterion (proposition \[ \text{[Lub94]} \]).

**Criterion A.** — If \( f(X) \in X \cdot \mathcal{O}_K[X] \) is a noninvertible stable series with \( f \not\equiv 0 \) mod \( m_K \), and if \( f \) commutes with a stable invertible series \( u(X) \in X \cdot \mathcal{O}_K[X] \), then the roots of \( f \) and all of its iterates are simple if and only if \( f'(X)/f'(0) \in 1 + X \cdot \mathcal{O}_K[X] \).

If \( K = \mathbb{Q}_p \), condition (2) of Theorem A amounts to requiring the existence of a stable invertible series that commutes with \( f \).

**Corollary A.** — If \( f(X) \in X \cdot \mathbb{Z}_p[X] \) is a noninvertible stable series such that the roots of \( f \) and all of its iterates are simple and \( f \not\equiv 0 \) mod \( p \), and if \( f \) commutes with a stable invertible series \( u(X) \in X \cdot \mathbb{Z}_p[X] \), then there is a formal group \( S \) over \( \mathbb{Z}_p \) such that \( f \in \text{End}(S) \) and \( U_f \subset \text{End}(S) \).

There are examples of commuting power series where \( f \) does not have simple roots, for instance \( f(X) = 9X + 6X^2 + X^3 \) and \( u(X) = 4X + X^2 \) with \( K = \mathbb{Q}_3 \) (more examples can be constructed following the discussion on page 344 of \[ \text{[Lub94]} \]). It seems reasonable to expect that if \( f \) and \( u \) are two stable noninvertible and invertible power series that commute, with \( f \not\equiv 0 \) mod \( m_K \), then there exists a formal group \( S \), two endomorphisms \( f_S \) and \( u_S \) of \( S \), and a nonzero power series \( h \) such that \( f \circ h = h \circ f_S \) and \( u \circ h = h \circ u_S \). We then say that \( f \) and \( f_S \) are *semi-conjugate*, and \( h \) is an *isogeny* from \( f_S \) to \( f \) (see for instance \[ \text{[Li97a]} \]).

The simplest case where this occurs is when \( m \) is an integer \( \geq 2 \), and the nonzero roots of \( f \) and all of its iterates are of multiplicity \( m \) (for an example of a more complicated case, see remark \[ \text{[3.5]} \]). In this simplest case, we have the following.

**Theorem B.** — Let \( K \) be a finite extension of \( \mathbb{Q}_p \), let \( f(X) \in X \cdot \mathcal{O}_K[X] \) be a noninvertible stable series and take \( m \geq 2 \). Let \( h(X) = X^m \). Suppose that

1. the nonzero roots of \( f \) and all of its iterates are of multiplicity \( m \)
2. \( f \not\equiv 0 \mod m_K \).

Then there exists a finite unramified extension \( L \) of \( K \) and a noninvertible stable series \( f_0(X) \in X \cdot \mathcal{O}_L[[X]] \) with \( f_0 \not\equiv 0 \mod m_K \), such that \( f \circ h = h \circ f_0 \), and the roots of \( f_0 \) and all of its iterates are simple.

If in addition \( u \) is an element of \( U_f \) with \( u'(0) \equiv 1 \mod m_K \), then there exists \( u_0 \in U_{f_0} \) such that \( u \circ h = h \circ u_0 \). Finally, if there is a subfield \( F \) of \( K \) such that \( f'(0) \in m_F \) and such that \( U'_f(0) \cap \mathcal{O}_F^\times \) is an open subgroup of \( \mathcal{O}_F^\times \), then \( (f_0^m)'(0) \in m_F \) and \( U'_0(0) \cap \mathcal{O}_F^\times \) is an open subgroup of \( \mathcal{O}_F^\times \).

Condition (1) can be checked using the following criterion (proposition 3.2).

**Criterion B.** — If \( f(X) \in X \cdot \mathcal{O}_K[[X]] \) is a noninvertible stable series with \( f \not\equiv 0 \mod m_K \), and if \( f \) commutes with a stable invertible series \( u(X) \in X \cdot \mathcal{O}_K[[X]] \), then the nonzero roots of \( f \) and all of its iterates are of multiplicity \( m \) if and only if the nonzero roots of \( f \) are of multiplicity \( m \), and the set of roots of \( f' \) is included in the set of roots of \( f \).

We have the following simple corollary of Theorem B when \( K = \mathbb{Q}_p \).

**Corollary B.** — If \( m \geq 2 \) and \( f(X) \in X \cdot \mathbb{Z}_p[[X]] \) is a noninvertible stable series such that the nonzero roots of \( f \) and all of its iterates are of multiplicity \( m \) and \( f \not\equiv 0 \mod p \), and if \( f \) commutes with a stable invertible series \( u(X) \in X \cdot \mathbb{Z}_p[[X]] \), then there is a unramified extension \( L \) of \( \mathbb{Q}_p \), a formal group \( S \) over \( \mathcal{O}_L \) and \( f_S \in \text{End}(S) \) such that \( f \circ X^m = X^m \circ f_S \).

Theorem A implies conjecture 5.3 of [HL16] for those \( K \) such that \( e(K/\mathbb{Q}_p) \leq p - 1 \). It also provides a new simple proof (that does not use \( p \)-adic Hodge theory) of the main theorem of [Spe18]. Note also that Theorem A holds without the restriction “\( e(K/\mathbb{Q}_p) \leq p - 1 \)” if \( f'(0) \) is a uniformizer of \( \mathcal{O}_K \) (see [Spe17]). This implies “Lubin’s conjecture” formulated at the very end of [Sar10] (this conjecture is proved in [Ber17] using \( p \)-adic Hodge theory, when \( K \) is a finite Galois extension of \( \mathbb{Q}_p \)) as well as “Lubin’s conjecture” on page 131 of [Sar05] over \( \mathbb{Q}_p \) if \( f \not\equiv 0 \mod p \).

The results of [HL16], [Ber17] and [Spe18] are proved under strong additional assumptions on \( \text{wideg}(f) \) (namely that \( \text{wideg}(f) = p \) in [Spe18], or that \( \text{wideg}(f) = p^h \), where \( h \) is the residual degree of \( K \), in [HL16] and [Ber17]). Theorem A is the first general result in this direction that makes no assumption on \( \text{wideg}(f) \), besides assuming that it is finite. It also does not assume that \( f'(0) \) is a uniformizer of \( \mathcal{O}_K \).

Theorem A and its corollary are proved in section §2 and theorem B and its corollary are proved in section §3.
1. Nonarchimedean dynamical systems

Whenever we talk about the roots of a power series, we mean its roots in the $p$-adic open unit disk $\mathcal{O}_p$. Recall that the Weierstrass degree $\text{wideg}(g(X))$ of a series $g(X) = \sum_{i \geq 1} g_i X^i \in X \cdot \mathcal{O}_K[X]$ is the smallest integer $i \leq +\infty$ such that $g_i \in \mathcal{O}_K$. We have $\text{wideg}(g) = +\infty$ if and only if $g \equiv 0 \mod \mathfrak{m}_K$.

If $r < 1$, let $H(r)$ denote the set of power series in $K[[X]]$ that converge on the closed disk $\{z \in \mathcal{O}_p such that |z|_p \leq r\}$. If $h \in H(r)$, let $\|h\|_r = \sup_{|z|_p \leq r} |h(z)|_p$. The space $H(r)$ is complete for the norm $\|\cdot\|_r$. Let $H = \text{proj lim}_{r < 1} H(r)$ be the ring of holomorphic functions on the open unit disk.

Throughout this article, $f(X) \in X \cdot \mathcal{O}_K[X]$ is a stable noninvertible series such that $\text{wideg}(f) < +\infty$, and $U_f$ denotes the set of invertible power series $u(X) \in X \cdot \mathcal{O}_K[X]$ such that $f \circ u = u \circ f$.

Lemma 1.1. — A series $g(X) \in X \cdot K[[X]]$ that commutes with $f$ is determined by $g'(0)$.

Proof. — This is proposition 1.1 of [Lub94].

Proposition 1.2. — If $U_f$ contains a stable invertible series, then there exists a power series $g(X) \in X \cdot \mathcal{O}_K[[X]]$ and an integer $d \geq 1$ such that $f(X) \equiv g(X^{pd}) \mod \mathfrak{m}_K$.

We have $\text{wideg}(f) = pd$ for some $d \geq 1$.

Proof. — This is the main result of [Lub94]. See (the proof of) theorem 6.3 and corollary 6.2.1 of ibid.

Proposition 1.3. — There is a (unique) power series $L(X) \in X + X^2 \cdot K[[X]]$ such that $L \circ f = f'(0) \cdot L$ and $L \circ u = u'(0) \cdot L$ if $u \in U_f$. The series $L(X)$ converges on the open unit disk, and $L(X) = \lim_{n \to +\infty} f^\circ n(X)/f'(0)^n$ in the Fréchet space $\mathcal{H}$.

Proof. — See propositions 1.2, 1.3 and 2.2 of [Lub94].

Lemma 1.4. — If $f(X) \in X \cdot \mathcal{O}_K[[X]]$ is a noninvertible stable series and if $f$ commutes with a stable invertible series $u$, then every root of $f'$ is a root of $f^\circ n$ for some $n \gg 0$.

Proof. — This is corollary 3.2.1 of [Lub94].

Proposition 1.5. — If $f(X) \in X \cdot \mathcal{O}_K[[X]]$ is a noninvertible stable series with $f \not\equiv 0 \mod \mathfrak{m}_K$, and if $f$ commutes with a stable invertible series $u$, then the roots of $f$ and all of its iterates are simple if and only if $f'(X)/f'(0) \in 1 + X \cdot \mathcal{O}_K[X]$. 
Lemma 2.1. — We have \((f^on)'(X) = f'(f^{on-1}(X)) \cdots f'(f(X)) \cdot f'(X)\). If \(f'(X)/f'(0) \in 1 + X \cdot \mathcal{O}_K[X]\), then the derivative of \(f^{on}(X)\) belongs to \(f'(0)^n \cdot (1 + X \cdot \mathcal{O}_K[X])\) and hence has no roots. The roots of \(f^{on}(X)\) are therefore simple.

By lemma [4], any root of \(f'(X)\) is also a root of \(f^{on}\) for some \(n \geq 0\). If the roots of \(f^{on}(X)\) are simple for all \(n \geq 1\), then \(f'(X)\) cannot have any root, and hence \(f'(X)/f'(0) \in 1 + XO_K[X]\).

\[\square\]

2. Formal groups

We now prove theorem A. Let \(S(X, Y) = L^{0-1}(L(X) + L(Y)) \in K[[X, Y]]\). By proposition [3], \(S\) is a formal group law over \(K\) such that \(f\) and all \(u \in U_f\) are endomorphisms of \(S\). In order to prove theorem A, we show that \(S(X, Y) \in \mathcal{O}_K[[X, Y]]\). Write \(S(X, Y) = \sum_{j \geq 0} s_j(X)Y^j\).

Lemma 2.2. — If \(L'(X) \in \mathcal{O}_K[[X]]\), then \(s_j(X) \in j!^{-1} \cdot \mathcal{O}_K[[X]]\) for all \(j \geq 0\).

Proof. — This is lemma 3.2 of [Li96].

\[\square\]

Lemma 2.2. — If the roots of \(f^{on}(X)\) are simple for all \(n \geq 1\), then \(L'(X) \in \mathcal{O}_K[[X]]\).

Proof. — This is sketched in the proof of theorem 3.6 of [Li96]. We give a complete argument for the convenience of the reader.

We have \((f^on)'(X) = f'(f^{on-1}(X)) \cdots f'(f(X)) \cdot f'(X)\), and by proposition [3], \(f'(X)/f'(0) \in 1 + XO_K[[X]]\). We have \(L(X) = \lim_{n \to +\infty} f^{on}(X)/f'(0)^n\) by proposition [3] so that

\[L'(X) = \lim_{n \to +\infty} \frac{(f^on)'(X)}{f'(0)^n} = \lim_{n \to +\infty} \frac{f'(f^{on-1}(X))}{f'(0)} \cdots \frac{f'(f(X))}{f'(0)} \cdot \frac{f'(X)}{f'(0)},\]

and hence \(L'(X) \in 1 + XO_K[[X]]\).

\[\square\]

Theorem 2.3. — If \(e(K/Q_p) \leq p - 1\), then \(s_j(X) \in \mathcal{O}_K[[X]]\) for all \(j \geq 0\).

Proof. — For all \(n \geq 1\), the power series \(u_n(X) = S(X, f^{on}(X))\) belongs to \(X \cdot K[X]\) and satisfies \(u_n \circ f = f \circ u_n\). Since \(U'_f(0) \cap \mathcal{O}_F^\times\) is an open subgroup of \(\mathcal{O}_F^\times\), there exists \(n_0\) such that if \(n \geq n_0\), then \(u_n'(0) = 1 + f'(0)^n \in U'_f(0)\). We then have \(u_n \in U_f\) by lemma [1].

In order to prove the theorem, we therefore prove that if \(S(X, f^{on}(X)) \in \mathcal{O}_K[[X]]\) for all \(n \geq n_0\), then \(s_i(X) \in \mathcal{O}_K[[X]]\) for all \(i \geq 0\). If \(j \geq 1\), let

\[a_j(X) = f^{on}(X) \sum_{i \geq 0} s_{j+i}(X)f^{on}(X)^i = s_j(X)f^{on}(X) + s_{j+1}(X)f^{on}(X)^2 + \cdots.\]
We prove by induction on $j$ that $s_0(X), \ldots, s_{j-1}(X)$ as well as $a_j(X)$ belong to $\mathcal{O}_K[X]$. This holds for $j = 1$; suppose that it holds for $j$.

We claim that if $h \in \mathcal{H}(r)$ and $\|h\|_r < p^{-1/(p-1)}$, then $\sum_{i \geq 0} s_{j+i}(X)h(X)^i$ converges in $\mathcal{H}(r)$. Indeed, if $s_p(j+i)$ denotes the sum of the digits of $j+i$ in base $p$, then

$$\text{val}_p(j+i) = \frac{j+i-s_p(j+i)}{p-1} < \frac{i}{p-1} + \frac{j}{p-1}.$$  

Let $\pi$ be a uniformizer of $\mathcal{O}_K$ and let $e = e(K/\mathbb{Q}_p)$ so that $|\pi|_p = p^{-1/e}$. By proposition 1.2 we have

$$f^{\circ n}(X) \in \pi X \cdot \mathcal{O}_K[[X]] + X^{q^n} \cdot \mathcal{O}_K[[X^{q^n}]],$$  

where $q = p^d = \text{width}(f)$, so that $\|f^{\circ n}(X)\|_r \leq \max(rp^{-1/e}, r^{q^n})$. If $\rho_n = p^{-1/(e(q^n-1))}$, then

$$\|f^{\circ n}(X)\|_{\rho_n} \leq p^{-q^n/(e(q^n-1))} < p^{-1/e} \leq p^{-1/(p-1)}$$  

and the series $\sum_{i \geq 0} s_{j+i}(X)f^{\circ n}(X)^i$ therefore converges in $\mathcal{H}(\rho_n)$.

We have $f^{\circ n}(X) \in \pi X \cdot \mathcal{O}_K[[X]] + X^{q^n} \cdot \mathcal{O}_K[[X^{q^n}]]$, as well as $\text{width}(f^{\circ n}) = q^n$. By the theory of Newton polygons, all the zeroes $z$ of $f^{\circ n}(X)$ satisfy $\text{val}_p(z) \geq 1/(e(q^n-1))$, and hence $|z|_p \leq \rho_n$. The equation $a_j(X) = f^{\circ n}(X)\sum_{i \geq 0} s_{j+i}(X)f^{\circ n}(X)^i$ holds in $\mathcal{H}(\rho_n)$, and this implies that $a_j(z) = 0$ for all $z$ such that $f^{\circ n}(z) = 0$. Since all the zeroes of $f^{\circ n}(X)$ are simple and $f^{\circ n}(X) \not\equiv 0 \mod \pi$, the Weierstrass preparation theorem implies that $f^{\circ n}(X)$ divides $a_j(X)$ in $\mathcal{O}_K[[X]]$, and hence that

$$s_j(X) + s_{j+1}(X)f^{\circ n}(X) + s_{j+2}(X)f^{\circ n}(X)^2 + \cdots \in \mathcal{O}_K[[X]].$$  

Choose some $0 < \rho < 1$ and take $n \geq n_0$ such that $\rho_n \geq \rho$. We have

$$f^{\circ n}(X) = f(f^{\circ (n-1)}(X)) \in \pi f^{\circ (n-1)}(X) \cdot \mathcal{O}_K[[X]] + f^{\circ (n-1)}(X)^q \cdot \mathcal{O}_K[[X]].$$  

Therefore $\|f^{\circ n}(X)\|_{\rho} \to 0$ as $n \to +\infty$, and $\|s_{j+1}(X)f^{\circ n}(X) + s_{j+2}(X)f^{\circ n}(X)^2 + \cdots\|_{\rho} \to 0$ as $n \to +\infty$. The series $s_j(X)$ is therefore in the closure of $\mathcal{O}_K[[X]]$ inside $\mathcal{H}(\rho)$ for $\|\cdot\|_{\rho}$, which is $\mathcal{O}_K[[X]]$.

This proves that $s_j(X)$ as well as $s_{j+1}(X)f^{\circ n}(X) + s_{j+2}(X)f^{\circ n}(X)^2 + \cdots\in \mathcal{O}_K[[X]]$. This finishes the induction and hence the proof of the theorem.

Theorem A now follows: $S$ is a formal group over $\mathcal{O}_K$ such that $f \in \text{End}(S)$. Any power series $u(X) \in X \cdot \mathcal{O}_K[[X]]$ that commutes with $f$ also belongs to $\text{End}(S)$, since $u(X) = [u'(0)](X)$ by lemma 1.1. In particular, $U_f \subset \text{End}(S)$.

To prove corollary A, note that we can replace $u$ by $u^{op-1}$ and therefore assume that $u'(0) \in 1 + p\mathbb{Z}_p$. In this case, $u^{\circ m}$ is defined for all $m \in \mathbb{Z}_p$ by proposition 4.1 of [Lub94] and $U_f'(0)$ is therefore an open subgroup of $\mathbb{Z}_p^\times$. 
3. Semi-conjugation

We now prove theorem B. Assume therefore that the nonzero roots of $f$ and all of its iterates are of multiplicity $m$. Let $h(X) = X^m$.

Since $q = \text{width}(f)$ is finite, we can write $f(X) = X \cdot g(X) \cdot v(X)$ where $g(X) \in \mathcal{O}_K[X]$ is a distinguished polynomial and $v(X) \in \mathcal{O}_K[[X]]$ is a unit. If the roots of $g(X)$ are of multiplicity $m$, then $g(X) = g_0(X)^m$ for some $g_0(X) \in \mathcal{O}_K[X]$. Write $v(X) = [c] \cdot (1 + w(X))$ where $c \in k_K$ (and $[c]$ is its Teichmüller lift) and $w(X) \in (m_K, X)$.

Since $m \cdot \deg(g) = q - 1$, $m$ is prime to $p$ and there exists a unique $w_0(X) \in (m_K, X)$ such that $1 + w(X) = (1 + w_0(X))^m$. If $f_0(X) = [c^{1/m}] \cdot X \cdot g_0(X)^m \cdot (1 + w_0(X))^m = f_0(X)^m = h \circ f_0(X)$.

It is clear that $f_0 \not\equiv 0 \mod m_K$. If we write $f_0^n(X) = X \cdot \prod_m (X - \alpha)^m \cdot v_n(X)$ with $v_n$ a unit of $\mathcal{O}_K[X]$, and where $\alpha$ runs through the nonzero roots of $f_0^n$, then

$$f_0^n(X^m) = X^m \cdot \prod_m (X^m - \alpha^m) \cdot v_n(X^m),$$

so that all the roots of $f_0^n(X^m)$ have multiplicity $m$. Since $f_0^n(X^m) = f_0^n(X^m)$, the roots of $f_0$ and all of its iterates are simple. This finishes the proof of the first part of the theorem, with $L = K([c^{1/m}])$.

If $u \in U_f$ and $u'(0) \in 1 + m_K$, then there is a unique $u_0(X) \in 1 + (m_K, X)$ such that $u_0(X)^m = u(X)^m$. We have $u_0'(0) = u'(0)^{1/m}$ and $(f_0 \circ u_0)^m = (u_0 \circ f_0)^m$ as well as $(f_0 \circ u_0)'(0) = (u_0 \circ f_0)'(0)$, so that $u_0 \in U_{f_0}$. This proves the existence of $u_0$. Since $f(X^m) = f_0(X)^m$, we have $f'(0) = f_0'(0)^m$. We then have $(f_0^m)'(0) = f_0'(0)^m = f'(0) \in m_F$. This finishes the proof of the last claim of theorem B.

Corollary B follows from theorem B in the same way that corollary A followed from theorem A.

**Example 3.1.** — If $p = 3$ and $f(X) = 9X + 6X^2 + X^3$ and $u(X) = 4X + X^2$, so that $f \circ u = u \circ f$, then $f(X) = X(X + 3)^2$ and $f'(X) = 3(X + 3)(X + 1)$. The nonzero roots of $f$ and all of its iterates are therefore of multiplicity 2. We have $f(X^2) = (X(X^2 + 3))^2$ so that $f_0(X) = 3X + X^3$, and the corresponding formal group is $G_m$ (this is a special case of the construction given on page 344 of [Lub94]).

**Proposition 3.2.** — If $f(X) \in X \cdot \mathcal{O}_K[X]$ is a noninvertible stable series with $f \not\equiv 0 \mod m_K$, and if $f$ commutes with a stable invertible series $u(X) \in X \cdot \mathcal{O}_K[[X]]$, then the nonzero roots of $f$ and all of its iterates are of multiplicity $m$ if and only if the nonzero roots of $f$ are of multiplicity $m$ and the set of roots of $f'$ is included in the set of roots of $f$. 


Proof. — If the nonzero roots of $f$ and all of its iterates are of multiplicity $m$, then the nonzero roots of $f$ are of multiplicity $m$. Hence if $\alpha$ is a root of $f^{\circ n}(X)$ with $f(\alpha) \neq 0$, the equation $f(X) = f(\alpha)$ has simple roots. Since $\alpha$ is one of these roots, we have $f'(\alpha) \neq 0$. By lemma 1.4, any root of $f'(X)$ is also a root of $f^{\circ n}$ for some $n \geq 1$. This implies that the set of roots of $f'$ is included in the set of roots of $f$.

Conversely, suppose that the nonzero roots of $f$ are of multiplicity $m$, and that $f'(\beta) \neq 0$ for any $\beta$ that is not a root of $f$. If $\alpha$ is a nonzero root of $f^{\circ n}(X)$ for some $n \geq 1$, then this implies that the equation $f(X) = \alpha$ has simple roots, so that the nonzero roots of $f$ and all of its iterates are of multiplicity $m$.

Remark 3.3. — If $p = 2$ and $f(X) = 4X + X^2$ and $u(X) = 9X + 6X^2 + X^3$, then $f \circ u = u \circ f$. The roots 0 and $-4$ of $f$ are simple, but $f^{\circ 2}(X) = X(X + 4)(X + 2)^2$ has a double root. In this case, $f$ is still semi-conjugate to an endomorphism of $G_m$, but via the more complicated map $h(X) = X^2/(1 + X)$ (see the discussion after corollary 3.2.1 of [Lub94], and example 2 of [Li96]).

References

[Ber17] L. Berger – “Lubin’s conjecture for full $p$-adic dynamical systems”, in Publications mathématiques de Besançon. Algèbre et théorie des nombres, 2016, Publ. Math. Besançon Algèbre Théorie Nr., vol. 2016, Presses Univ. Franche-Comté, Besançon, 2017, p. 19–24.
[HL16] L.-C. Hsia & H.-C. Li – “Ramification filtrations of certain abelian Lie extensions of local fields”, J. Number Theory 168 (2016), p. 135–153.
[Li96] H.-C. Li – “When is a $p$-adic power series an endomorphism of a formal group?”, Proc. Amer. Math. Soc. 124 (1996), no. 8, p. 2325–2329.
[Li97a] , “Isogenies between dynamics of formal groups”, J. Number Theory 62 (1997), no. 2, p. 284–297.
[Li97b] , “$p$-adic power series which commute under composition”, Trans. Amer. Math. Soc. 349 (1997), no. 4, p. 1437–1446.
[LMS02] F. Laubie, A. Movahhedi & A. Salinier – “Systèmes dynamiques non archimédiens et corps des normes”, Compositio Math. 132 (2002), no. 1, p. 57–98.
[Lub94] J. Lubin – “Nonarchimedean dynamical systems”, Compositio Math. 94 (1994), no. 3, p. 321–346.
[Sar05] G. Sarkis – “On lifting commutative dynamical systems”, J. Algebra 293 (2005), no. 1, p. 130–154.
[Sar10] , “Height-one commuting power series over $Z_p$”, Bull. Lond. Math. Soc. 42 (2010), no. 3, p. 381–387.
[Spe17] J. Specter – personal communication, 2017.
[Spe18] , “The crystalline period of a height one $p$-adic dynamical system”, Trans. Amer. Math. Soc. 370 (2018), no. 5, p. 3591–3608.
[SS13] G. Sarkis & J. Specter – “Galois extensions of height-one commuting dynamical systems”, J. Théor. Nombres Bordeaux 25 (2013), no. 1, p. 163–178.
