Rend. Sem. Mat. Univ. Padova 154 (2025), 227–245
DOI 10.4171/RSMUP/161

A criterion for Lubin's conjecture

Léo Poyeton (*)

Abstract – We prove that a formulation of a conjecture of Lubin regarding two power series commuting for the composition is equivalent to a criterion of checking that some extensions generated by the nonarchimedean dynamical system arising from the power series are Galois. As a consequence of this criterion, we obtain a proof of Lubin's conjecture in a new case.

Mathematics Subject Classification 2020 – 11S31 (primary); 11S15, 11S20, 11S82, 13F25, 32P05, 37P05 (secondary).

Keywords – Lubin–Tate group, ramification theory, p-adic Hodge theory, nonarchimedean dynamical systems, local class field theory.

1. Introduction

Let K be a finite extension of $\mathbf{Q}_p$, with ring of integers $\mathcal{O}_K$ and maximal ideal $\mathfrak{m}_K$. Families of power series in $T \cdot \mathcal{O}_K[\![T]\!]$ that commute under composition have been studied by Lubin [16] under the name of nonarchimedean dynamical systems, because of their interpretation as analytic transformations of the p-adic open unit disk. This study led Lubin to remark 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 have been obtained to support Lubin's observation; see for instance the nonexhaustive list [3, 12–15, 17–21].

This observation has led to several versions of what might be called Lubin's conjecture, and these versions have all been proved under very strong assumptions on the nonarchimedean dynamical system considered.

(*) *Indirizzo dell'A.*: Institut de Mathématiques de Bordeaux, Université de Bordeaux, 351, cours de la Libération, 33405 Talence, France; leo.poyeton@math.u-bordeaux.fr

In this note, we consider two power series $P, U \in T \cdot \mathcal{O}_K[\![T]\!]$ such that $P \circ U = U \circ P$, with $P'(0) \in \mathfrak{m}_K$ and $U'(0) \in \mathcal{O}_K^\times$. Our so-called version of Lubin's conjecture is the following:

CONJECTURE 1.1. *Let $P, U \in T \cdot \mathcal{O}_K[\![T]\!]$ such that $P \circ U = U \circ P$, with $P'(0) \in \mathfrak{m}_K$ and $U'(0) \in \mathcal{O}_K^\times$ not a root of unity, and such that $P(T) \neq 0 \bmod \mathfrak{m}_K$. Then there exists a finite extension E of K, a formal group S defined over $\mathcal{O}_E$, endomorphisms of this formal group P_S and U_S and a power series $h(T) \in T \cdot \mathcal{O}_E[\![T]\!]$ such that $P \circ h = h \circ P_S$ and $U \circ h = h \circ U_S$.*

In the conjecture above, we say following Li's terminology [14] that P and P_S are semiconjugate and that h is an isogeny from P_S to P.

In several proven cases of this conjecture [3, 18, 21], the Lubin–Tate formal group is actually defined over $\mathcal{O}_K$. However, this is not true in general.

The goal of this note is to prove the following theorem, which gives a new criterion to prove Lubin's conjecture in some cases:

THEOREM 1.2. *Let (P, U) be a couple of power series in $T \cdot \mathcal{O}_K[\![T]\!]$ such that $P \circ U = U \circ P$, with $P'(0) \in \mathfrak{m}_K$ and $U'(0) \in \mathcal{O}_K^\times$, and we assume that $P(T) \neq 0 \bmod \mathfrak{m}_K$ and that $U'(0)$ is not a root of unity. Then there exists a finite extension E of K, a Lubin–Tate formal group S defined over $\mathcal{O}_L$, where E/L is a finite extension, endomorphisms of this formal group P_S and U_S over $\mathcal{O}_E$, and a power series $h(T) \in T \cdot \mathcal{O}_E[\![T]\!]$ such that $P \circ h = h \circ P_S$ and $U \circ h = h \circ U_S$, if and only if the following two conditions are satisfied:*

(1) *There exists $V \in T \cdot \mathcal{O}_K[\![T]\!]$, commuting with P, and an integer $d \geq 1$ such that $Q(T) = T^{p^d} \bmod \mathfrak{m}_K$, where $Q = V \circ P$.*

(2) *There exists a finite extension E of K and a sequence $(\alpha_n)_{n \in \mathbf{N}}$, where $\alpha_0 \neq 0$ is a root of Q and $Q(\alpha_{n+1}) = \alpha_n$, such that for all $n \geq 1$, the extension $E(\alpha_n)/E$ is Galois.*

The role of the field L in the theorem above may be confusing, but essentially comes from the fact that Lubin–Tate formal groups are a special case of more general formal groups, and that a formal group defined over $\mathcal{O}_E$ arising from a Lubin–Tate formal group over $\mathcal{O}_L$ is usually no longer a Lubin–Tate formal group over $\mathcal{O}_E$.

The proof of this theorem relies mainly on the same tools and strategy used in [17], which are the tools developed by Lubin [16] to study p-adic dynamical systems, the "canonical Cohen ring for norms fields" of Cais and Davis [6] and tools of p-adic Hodge theory following Berger's strategy in [1].

As a corollary of our main theorem, we obtain the following result, which is a new instance of Lubin's conjecture:

THEOREM 1.3. *Assume that $P(T) \in T \cdot \mathcal{O}_K[\![T]\!]$ is such that $P(T) = T^p \bmod \mathfrak{m}_K$ and that there exists $U \in T \cdot \mathcal{O}_K[\![T]\!]$, commuting with P, such that $U'(0)$ is not a root of unity. Then there exists a finite extension E of K, a Lubin–Tate formal group S defined over $\mathcal{O}_L$, where E/L is a finite extension, endomorphisms of this formal group P_S and U_S over $\mathcal{O}_E$, and a power series $h(T) \in T \cdot \mathcal{O}_E[\![T]\!]$ such that $P \circ h = h \circ P_S$ and $U \circ h = h \circ U_S$.*

In order to prove our main theorem, we also need to prove that some extensions are strictly APF, which is a technical condition on the ramification of the extension. Cais and Davis [6] considered what they called "φ-iterate" extensions, and later proved with Lubin that those extensions are strictly APF [7]. Here we show that this result still holds for more general extensions which generalize the φ-iterate extensions of Cais and Davis:

THEOREM 1.4. *Let K_∞/K be an extension generated by a sequence (u_n) of elements of $\overline{\mathbf{Q}}_p$ such that there exists a power series $P(T) \in T \cdot \mathcal{O}_K[\![T]\!]$ with $P(T) = T^d$, where d is a power of the cardinal of k_K, and an element π_0 of $\mathfrak{m}_K$ such that $u_0 = \pi_0$ and $P(u_{n+1}) = u_n$.*

Then K_∞/K is strictly APF.

Organization of the note

The next section recalls the construction and properties of some rings of periods, which are used in the rest of the paper. Then Section 3 is devoted to the proof of Theorem 1.4, using the rings of periods of Section 2 in order to do so. In Section 4 we recall the main result of [16], which explains why "Lubin's conjecture" seems reasonable. In Section 5 we prove that our version of Lubin's conjecture implies that the two conditions of Theorem 1.2 are satisfied. Sections 6 and 7 show how to use p-adic Hodge theory, using the same strategy as in [17], along with results from [16], in order to prove that the infinite extension generated by such a Q-consistent sequence is actually generated by the torsion points of a formal Lubin–Tate group. In Section 8 we show how to use the "canonical Cohen ring for norms fields" of Cais and Davis [6] to prove that there is indeed an isogeny from an endomorphism of a formal Lubin–Tate group to Q. Section 9 is devoted to the proof of Theorem 1.3.

2. Rings of periods

Let K be a finite extension of $\mathbf{Q}_p$, with uniformizer π_K, and let $K_0 = \mathbf{Q}_p^{\mathrm{unr}} \cap K$ denote the maximal unramified extension of $\mathbf{Q}_p$ inside K. Let $q = p^h$ be the cardinality

of k_K, the residue field of K, and let e be the ramification index of K, so that $eh = [K : \mathbf{Q}_p]$. Let v_K denote the p-adic valuation on K normalized so that $v_K(K^\times) = \mathbf{Z}$ and let v_K still denote its extension to $\overline{\mathbf{Q}}_p$. Let $c > 0$ be such that $c \leq v_K(p)/(p-1)$. If F is a subfield of $\mathbf{C}_p$, let $\mathfrak{a}_F^c$ be the set of elements of F such that $v_K(x) \geq c$.

We now recall definitions and properties of some rings of periods which will be used afterwards. We refer mainly to [8, 11] for the properties stated here. The slight generalization to the classical rings by tensoring by $\mathcal{O}_K$ over $\mathcal{O}_{K_0}$ can for example be found in [2].

Let

$$\mathcal{O}_{\mathbf{C}_p}^\flat := \varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbf{C}_p}/\mathfrak{a}_{\mathbf{C}_p}^c.$$

This is the tilt of $\mathcal{O}_{\mathbf{C}_p}$ and is a perfect ring of characteristic p, whose fraction field $\widetilde{\mathbf{E}}$ is algebraically closed. It is endowed with a valuation $v_{\mathbf{E}}$ induced by the one on K. We let $W_K(\cdot) = \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} W(\cdot)$ denote the $\mathcal{O}_K$-Witt vectors, and let $\tilde{\mathbf{A}}^+ = W_K(\widetilde{\mathbf{E}}^+)$ and $\tilde{\mathbf{A}} = W_K(\widetilde{\mathbf{E}})$.

Any element of $\tilde{\mathbf{A}}$ (resp. $\tilde{\mathbf{A}}^+$) can be uniquely written as $\sum_{i \geq 0} \pi_K^k[x_i]$ with the $x_i \in \widetilde{\mathbf{E}}$ (resp. $\widetilde{\mathbf{E}}^+$). We let $w_k \colon \tilde{\mathbf{A}} \to \mathbf{R} \cup \{+\infty\}$ be defined by $w_k(x) = \inf_{i \leq k} v_{\mathbf{E}}(x_i)$.

For $r \in \mathbf{R}_+$, we let $\tilde{\mathbf{A}}^{\dagger, r}$ denote the subset of $\tilde{\mathbf{A}}$ of elements x such that $w_k(x) + \frac{pr}{e(p-1)}k$ is ≥ 0 for all k and whose limit when $k \to +\infty$ is $+\infty$. We let $n(r)$ be the smallest integer n such that $r \leq p^{nh-1}(p-1)$.

We also let $\tilde{\mathbf{A}} = \bigcup_{r>0} \tilde{\mathbf{A}}^{\dagger, r}$.

Lemma 2.1. *Let $x \in \tilde{\mathbf{A}}^{\dagger, r} + \pi_K^k \tilde{\mathbf{A}}$. Then $\frac{x}{[\bar{x}]}$ is a unit of $\tilde{\mathbf{A}}^{\dagger, r'} + \pi_K^k \tilde{\mathbf{A}}$, with $r' = r + \frac{(p-1)e}{p} v_{\mathbf{E}}(\bar{x})$.*

Proof. Since $x \in \tilde{\mathbf{A}}^{\dagger, r} + \pi_K^k \tilde{\mathbf{A}}$, we can write $x = \sum_{i=0}^{k-1} \pi_K^i [x_i]$, where $x_0 = \bar{x}$, and $w_i(x) + \frac{pr}{e(p-1)} i \geq 0$ for all i between 0 and $k-1$.

Now we can write $\frac{x}{[\bar{x}]} \in \tilde{\mathbf{A}}$ as $\sum_{i \geq 0} \pi_K^i [y_i]$, where $y_i = \frac{x_i}{\bar{x}}$ for i between 0 and $k-1$. In particular, $y_0 = 1$. Now a direct computation leads to the fact that

$$w_i\left(\frac{x}{[\bar{x}]}\right) + \frac{pr'}{e(p-1)} i \geq 0$$

for all $i \leq k-1$, where $r' = r + \frac{(p-1)e}{p} v_{\mathbf{E}}(\bar{x})$.

Using the fact that $\frac{x}{[\bar{x}]} \in (\tilde{\mathbf{A}}^{\dagger, r'} + \pi_K^k \tilde{\mathbf{A}}) \cap (1 + \pi_K \tilde{\mathbf{A}})$, we obtain that its inverse also lies in $\tilde{\mathbf{A}}^{\dagger, r'} + \pi_K^k \tilde{\mathbf{A}}$. ∎

Let $\varphi_q \colon \widetilde{\mathbf{E}}^+ \to \widetilde{\mathbf{E}}^+$ denote the map $x \mapsto x^q$. This extends to a map $\widetilde{\mathbf{E}} \to \widetilde{\mathbf{E}}$ also given by $x \mapsto x^q$, and by functoriality of Witt vectors those maps extend into maps φ_q on $\tilde{\mathbf{A}}^+$ and $\tilde{\mathbf{A}}$.

Recall that there is a surjective map $\theta\colon \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p}$ which is a morphism of rings. Moreover, if $x \in \tilde{\mathbf{A}}^+$ and $\bar{x} = (x_n) \in \tilde{\mathbf{E}}^+$, then $\theta \circ \varphi_q^{-n}(x) = x_n \bmod \mathfrak{a}^c_{\mathbf{C}_p}$.

Also recall that, for $n \geq n(r)$, the maps $\theta \circ \varphi_q^{-n}\colon \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p}$ extend into surjective maps $\theta \circ \varphi_q^{-n}\colon \tilde{\mathbf{A}}^{\dagger,r} \to \mathcal{O}_{\mathbf{C}_p}$.

3. Strictly APF extensions

Recall that a (slight generalization of what Cais and Davis [6] have called a) φ-iterate extension K_∞/K is an extension generated by a sequence (u_n) of elements of $\bar{\mathbf{Q}}_p$ such that there exists a power series $P(T) \in T \cdot \mathcal{O}_K[\![T]\!]$ with $P(T) = T^d$, where d is a power of the cardinal of k_K, and a uniformizer π_0 of $\mathcal{O}_K$ such that $u_0 = \pi_0$ and $P(u_{n+1}) = u_n$.

The main theorem of [7] gives a necessary and sufficient condition for an infinite algebraic extension L/K to be strictly APF, and in particular implies directly that those φ-iterate extensions are strictly APF.

In this section we will prove that this result remains true if we remove the assumption in the definition above that π_0 is a uniformizer of $\mathcal{O}_K$, and instead just assume that $\pi_0 \in \mathfrak{m}_K$. We even allow π_0 to be equal to 0, which is basically what we will consider when looking at consistent sequences attached to a noninvertible stable power series.

If L is a finite extension of $\mathbf{Q}_p$, we let v_L denote the p-adic valuation on L normalized such that $v_L(L^\times) = \mathbf{Z}$, and we still denote by v_L its extension to $\bar{\mathbf{Q}}_p$. If L/M is a finite extension, we also let $\mathrm{Emb}_M(L, \bar{\mathbf{Q}}_p)$ denote the set of M-linear embeddings of L into $\bar{\mathbf{Q}}_p$.

For the rest of this section, we let $P(T) \in T \cdot \mathcal{O}_K[\![T]\!]$ with $P(T) = T^s$, where s is a power of the cardinal of k_K, we let π_0 be any element of $\mathfrak{m}_K$ and we define a sequence $(v_n)_{n\in\mathbf{N}}$ of elements of $\bar{\mathbf{Q}}_p$ as follows: we let $v_0 = \pi_0$, and for $n \geq 0$, we let v_{n+1} be a root of $P(T) - v_n$. We let $K_n = K(v_n)$ the field generated by v_n over K, and we let $K_\infty = \bigcup_n K_n$. If $v_0 = 0$, then we choose v_1 to be $\neq 0$, so that the null sequence is excluded from our considerations.

Proposition 3.1. *There exists $n_0 \geq 0$ and $d \geq 1$ such that, for all $n \geq n_0$, we have $v_{K_n}(v_n) = d$ and the extension K_{n+1}/K_n is totally ramified of degree s.*

Proof. The fact that the Weierstrass degree of P is greater than 1 along with the Weierstrass preparation theorem shows that the sequence $v_p(v_n)$ is strictly decreasing. In particular, there exists $n_0 \geq 0$ such that for $n \geq 0$, the Newton polygon of $P - v_n$ has only one slope, equal to $\frac{1}{s}v_p(v_n)$. This implies that for $n \geq n_0$, we have $v_p(v_{n+1}) = \frac{1}{s}v_p(v_n)$, and thus $v_{K_n}(v_{n+1}) = \frac{1}{s}v_{K_n}(v_n)$.

Recall that, if $M/L/\mathbf{Q}_p$ are finite extensions, then we have $[M : L]v_L \geq v_M$, with equality if and only if M/L is totally ramified. Let $d_n := v_{K_n}(v_n)$. Since s is the degree of a nonzero polynomial with coefficients in K_n whose root is v_{n+1}, we know that $[K_{n+1} : K_n] \leq s$. This implies that $sv_{K_n} \geq [K_{n+1} : K_n]v_{K_n} \geq v_{K_{n+1}}$. For $n \geq n_0$, we have $d_n = s \cdot v_{K_n}(v_{n+1}) \geq [K_{n+1} : K_n]v_{K_n}(v_{n+1}) \geq v_{K_{n+1}}(v_{n+1}) = d_{n+1}$, so that the sequence $(d_n)_{n\in\mathbf{N}}$ is decreasing. Since this sequence takes its values in $\mathbf{N}$, it is stationary and therefore there exists $n_1 \geq n_0$ such that, for all $n \geq n_1$, $d_{n+1} = d_n$. In particular, this implies that the inequalities above are all equalities and thus that for $n \geq 1$, $s = [K_{n+1} : K_n]$ and that K_{n+1}/K_n is totally ramified, and we can take $d = d_{n_1}$. ∎

Let us write $d = p^k m$ where m is prime to p.

Since $P(T) = T^s \bmod \mathfrak{m}_K$, the sequence (v_n) gives rise to an element $\bar{v}$ of $\widetilde{\mathbf{E}}^+ = \varprojlim_{x\mapsto x^s} \mathcal{O}_{\mathbf{C}_p}/\pi_K$. We let φ_s denote the s-power Frobenius map on $\widetilde{\mathbf{E}}^+$ and $\tilde{\mathbf{A}}^+$.

Proposition 3.2. *There exists a unique $v \in \tilde{\mathbf{A}}^+$ lifting $\bar{v}$ such that $\varphi_s(v) = v$. Moreover, we have $\theta \circ \varphi_s^{-n}(v) = v_n$.*

Proof. One can use the same argument as in [6, Rem. 7.16] to produce an element in $\tilde{\mathbf{A}}^+$ such that $P(v) = \varphi_s(v)$ and such that $\theta \circ \varphi_s^{-n}(v) = v_n$ (note that one also needs to extend the results from [6, Rem. 7.16] to the case where the Frobenius is replaced by a power of the Frobenius, which is straightforward).

Such an element automatically lifts $\bar{v}$ by definition of the theta map. For the uniqueness, one checks that the map $x \mapsto \varphi_s^{-1}(P(x))$ is a contracting map on the set of elements of $\tilde{\mathbf{A}}^+$ which lift $\bar{v}$, so that $v = \lim_{m\to+\infty} \varphi_s^{-m}(P^{\circ m}([\bar{v}]))$ and is thus unique. ∎

Since $\widetilde{\mathbf{E}}$ is algebraically closed, there exists $\bar{u} \in \widetilde{\mathbf{E}}$ such that $\bar{u}^m = \bar{v}$. Since such a $\bar{u}$ necessarily has positive valuation, it actually belongs to $\widetilde{\mathbf{E}}^+$.

Since $P(T) = T^s \bmod \pi_K$, we can write $P(T) = T^s(1 + \pi h(T))$, with $h(T) \in \frac{1}{T^s-1}\mathcal{O}_K[\![T]\!]$. Let $Q(T) = T^s(1 + \pi_K h(T^m))^{1/m} \in \widehat{\mathcal{O}_K[\![T]\!][1/T]}$, which is well defined because m is prime to p. Note that $Q(T)$ is overconvergent, meaning that it converges on some annulus bounded by the p-adic unit circle.

Proposition 3.3. *There exists $u \in \tilde{\mathbf{A}}^\dagger$, $u^m = v$.*

Proof. We first construct u such that $\varphi_s(u) = Q(u)$. Just as in the proof of Proposition 3.2, the map $x \mapsto \varphi_s^{-1}(Q(x))$ is a contracting map on the set of elements of $\tilde{\mathbf{A}}$ lifting $\bar{u}$, so that $u = \lim_{m\to+\infty} \varphi_s^{-m}(Q^{\circ m}([\bar{u}]))$ and is unique.

Therefore, there exists $u \in \tilde{\mathbf{A}}$ such that $\varphi_s(u) = Q(u)$. Since $\bar{u} \in \widetilde{\mathbf{E}}^+$, we can write $u = [\bar{u}] + \pi_K z_1 \in \tilde{\mathbf{A}}^+ + \pi_K\tilde{\mathbf{A}}$. Let r be such that $\frac{\pi_K}{[\bar{u}]^d} \in \tilde{\mathbf{A}}^{\dagger,r}$ and let $f = \frac{(p-1)e}{p} v_{\mathbf{E}}(\bar{x})$. Let us write $Q(T) = T^s(1 + \frac{\pi_K}{T^s} g(T))^{1/m}$, with $g(T) \in \mathcal{O}_K[\![T]\!]$.

Now assume that there exists some $k \geq 1$ and $r' > 0$ such that $u \in \tilde{\mathbf{A}}^{\dagger,r'} + \pi_K^k \tilde{\mathbf{A}}$. We can thus write $u = u_k + \pi_K^k z_k$, where $u_k \in \tilde{\mathbf{A}}^{\dagger,r'}$ and $z_k \in \tilde{\mathbf{A}}$. We have

$$Q(u) = Q(u_k \pi_K^k z_k) = (u_k \pi_K^k z_k)^s \left(1 + \frac{\pi_K}{(u_k \pi_K^k z_k)^s} g(u_k \pi_K^k z_k)\right)^{1/m}.$$

Using the fact that $\frac{u}{[\bar{u}]}$ is a unit in $\tilde{\mathbf{A}}^{\dagger,r'+f} + \pi_K^k \tilde{\mathbf{A}}$, we obtain that $Q(u) \in \tilde{\mathbf{A}}^{\dagger,r''} + \pi_K^{k+1} \tilde{\mathbf{A}}$, where $r'' = \max(s \times r', r' + f)$.

Since $\varphi_s^{-1}(Q(u)) = u$, this implies that $u \in \tilde{\mathbf{A}}^{\dagger,r''/s} + \pi_K^{k+1} \tilde{\mathbf{A}}$.

By successive approximations, we have $u \in \tilde{\mathbf{A}}^{\dagger}$.

Finally, we compute $\varphi_s(u^m) = \varphi_s(u)^m = Q(u)^m = P(u^m)$ by construction of Q, so that $\varphi_s(u^m) = P(u^m)$. Since u^m lifts $\bar{u}^m = \bar{v}$, we have $u^m = v$ by unicity in Proposition 3.2. ∎

Recall that since $u \in \tilde{\mathbf{A}}^{\dagger}$, there exists some $r > 0$ such that $u \in \tilde{\mathbf{A}}^{\dagger,r}$ and there exists $n(r) \geq 0$ such that, for all $n \geq n(r)$, the element $u_n := \theta \circ \varphi_s^{-1}(u)$ is well defined and belongs to $\mathcal{O}_{\mathbf{C}_p}$. Actually, since $u^m = v$, we have that $u_n^m = v_n$, and in particular we know that $v_K(u_n) \to 0$.

Lemma 3.4. *There exists a constant $c > 0$, independent of n, such that for any $n \geq n(r)$ and for any $g \in \mathcal{G}_{K_n}$ and any $i \geq 1$, we have*

$$v_K(g(u_{n+i}) - u_{n+i}) \geq c.$$

Proof. Let $n \geq n(r)$. We have $u_{n+i}^m = v_{n+i}$, so that

$$v_K(g(u_{n+i})^m - u_{n+i}^m) = v_K(g(v_{n+i} - v_{n+i})).$$

This means that

$$v_K(g(v_{n+i}) - v_{n+i}) = v_K(g(u_{n+i}) - u_{n+i}) + (m-1) v_K(u_{n+i})$$

since m is prime to p.

Since m is fixed and $v_K(u_n) \to 0$, it suffices to prove that there exists $c > 0$ independent of n such that $v_K(g(v_{n+i}) - v_{n+i}) \geq c$ for all $g \in \mathcal{G}_{K_n}$.

Since $P(T) = T^s \bmod \mathfrak{m}_K$, and since $P^{\circ j}(v_{n+i}) = v_n$, we already know that for all $n \geq 0$ and for all $g \in \mathcal{G}_{K_n}$, we have $v_K(g(v_{n+i}) - v_{n+i}) \geq 1$, so that $v_K(\frac{g(v_{n+i})}{v_{n+i}} - 1) \geq 1 - v_K(v_{n+i}) \geq 1 - v_K(v_n)$. The statement follows from the fact that $v_K(v_n) \to 0$ when $n \to +\infty$. ∎

Recall that $d = p^k m$, where d is such that $v_{K_n}(v_n) = d$ for $n \gg 0$. Recall also that s is a power of p, and let $j \geq 0$ be such that $s^j \geq p^k > s^{j-1}$. Let $f \geq 0$ be such that $p^{-f} s^j = p^k$. In particular, we have

$$v_{K_n}(u_{n+i}^{p^f}) = p^f s^{-j} v_{K_n}(u_n) = \frac{1}{mp^k} v_{K_n}(v_n) = \frac{d}{d} = 1.$$

We let $E_\infty = \bigcup_{n\geq 0} K(u_n)$, and $F = \mathbf{Q}_p^{\mathrm{unr}} \cap E_\infty$ be the maximal unramified extension of $\mathbf{Q}_p$ inside E_∞. Finally, we let $F^{(m)}$ denote the unramified extension of F generated by the elements $[x^{1/m}]$, $x \in k_F$.

For $n \geq n_0$, let π_n denote a uniformizer of $\mathcal{O}_{K_n}$. Since for all $n \geq n_0$ the extensions K_{n+1}/K_n are totally ramified, the minimal polynomial of π_{n+1} over K_n is an Eisenstein polynomial, and we choose the π_n so that $N_{K_{n+1}/K_n}(\pi_{n+1}) = \pi_n$ for all $n \geq n_0$.

Lemma 3.5. *For any $n \geq n(r)$, we can write $\pi_n = [h] \cdot u_{n+j}^{p^f}(1 + x)$, with $x \in \mathcal{O}_{K_{n+j}}$ and $h \in k_{F^{(m)}}$.*

Proof. Note that $v_{K_n}(\pi_n^m) = v_{K_n}(v_{n+j}^{p^f})$ and that both elements belong to $\mathcal{O}_{K_{n+j}}$, so that we can write

$$\frac{\pi_n^m}{v_{n+j}^{p^f}} = [h_0] + \pi_{n+j}(\cdots),$$

with $h_0 \in k_F$. Taking the mth root, this implies that there exists $h_1 \in k_{F^{(m)}}$ such that

$$\frac{\pi_n}{u_{n+j}^{p^f}} = [h_1](1 + \pi_{n+j}(\cdots)),$$

where the coefficients belong to $\mathcal{O}_{K_{n+j}}$ and $h_1 \in k_{F^{(m)}}$. ∎

Theorem 3.6. *The extension K_∞/K is strictly APF.*

Proof. In order to prove the theorem, it suffices by [22, Prop. 1.2.3] to prove that the extension $F^{(m)} \cdot K_\infty / F^{(m)} \cdot K_{n_0}$ is strictly APF.

To prove that $F^{(m)} \cdot K_\infty / F^{(m)} \cdot K$ is strictly APF, it suffices to prove that the v_K valuations of the nonconstant and nonleading coefficients of the Eisenstein polynomial of π_{n+1} over $F^{(m)} \cdot K_n$, for $n \geq n_0$, are bounded below by a positive constant independent of n, so that $F^{(m)} \cdot K_\infty / F^{(m)} \cdot K_{n_0}$ satisfies the criterion of the main theorem (Thm. 1.1) of [7]. Let $n \geq n_0$.

By Lemma 3.5 and by induction, we can write

$$\pi_{n+1} = u_{n+j+1}^{p^f}([h_0] + u_{n+1+2j}^{p^f}([h_1] + \cdots)),$$

where the h_i belong to $k_{F^{(m)}}$.

Let $g \in \mathcal{G}_{F^{(m)}\cdot K_n}$. We have

$$g(\pi_{n+1}) - \pi_{n+1} = g(u_{n+j+1}^{p^f})([h_0]) - u_{n+j+1}^{p^f}([h_0]) + \cdots,$$

where all the terms on the right-hand side have v_K-valuation at least equal to $c > 0$ by Lemma 3.4, so that $v_K(g(\pi_{n+1}) - \pi_{n+1}) \geq c > 0$.

The conjugates of π_{n+1} over K_n are the elements $g(\pi_{n+1})$, for $g \in \mathcal{G}_{K_n}$, and satisfy the conditions $v_K(g(\pi_{n+1}) - \pi_{n+1}) \geq c > 0$, which ensures that the v_K valuations of the nonconstant and nonleading coefficients of the Eisenstein polynomial of π_{n+1} over $F^{(m)} \cdot K_n$ are bounded below by a positive constant independent of n, which is what we wanted. ∎

4. Nonarchimedean dynamical systems

Let K be a finite extension of $\mathbf{Q}_p$, with ring of integers $\mathcal{O}_K$, uniformizer π, maximal ideal $\mathfrak{m}_K$ and residual field k of cardinal $q = p^h$. We let $K_0 = K \cap \mathbf{Q}_p^{\mathrm{unr}}$ be the maximal unramified extension of $\mathbf{Q}_p$ inside K and we let $\mathcal{O}_{K_0}$ denote its ring of integers. We let $\mathbf{C}_p$ denote the p-adic completion of $\overline{\mathbf{Q}}_p$. Let $P, U \in T \cdot \mathcal{O}_K[\![T]\!]$ be such that $P \circ U = U \circ P$, with $P'(0) \in \mathfrak{m}_K$ and $U'(0) \in \mathcal{O}_K^\times$. In this note, we assume that the situation is "interesting", namely that $P(T) \neq 0 \bmod \mathfrak{m}_K$ and that $U'(0)$ is not a root of unity.

Proposition 4.1. *There exists a power series $H(T) \in T \cdot k[\![T]\!]$ and an integer $d \geq 1$ such that $H'(0) \in k^\times$ and $P(T) = H(T^{p^d}) \bmod \mathfrak{m}_K$.*

Proof. This is [16, Thm. 6.3 and Cor. 6.2.1]. ∎

Near the end of his paper [16], Lubin remarked 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." This has led some authors to prove some cases (see for instance [3, 13–15, 18–21]) of this Lubin "conjecture". The various results obtained in this direction can be thought of as cases of the following conjecture:

Conjecture 4.2. *Let $P, U \in T \cdot \mathcal{O}_K[\![T]\!]$ be such that $P \circ U = U \circ P$, with $P'(0) \in \mathfrak{m}_K$ and $U'(0) \in \mathcal{O}_K^\times$ not a root of unity, and such that $P(T) \neq 0 \bmod \mathfrak{m}_K$. Then there exists a finite extension E of K, a formal group S defined over $\mathcal{O}_E$, endomorphisms of this formal group P_S and U_S, and a power series $h(T) \in T \cdot \mathcal{O}_E[\![T]\!]$ such that $P \circ h = h \circ P_S$ and $U \circ h = h \circ U_S$.*

Remark 4.3. While in many instances of the cases where this conjecture is proven, the formal group is actually defined over $\mathcal{O}_K$ [3, 18, 21], one can produce instances where the formal group is defined over the ring of integers of a finite unramified extension of $\mathcal{O}_K$ [4, §3]. The author does not know of a case where the extension E that the formal group is defined over is ramified over K, so it might be possible that the assumption that E is an unramified extension of K can be enforced.

5. Endomorphisms of a formal Lubin–Tate group

Let $P, U \in T \cdot \mathcal{O}_K[\![T]\!]$ be such that $P \circ U = U \circ P$, with $P'(0) \in \mathfrak{m}_K$ and $U'(0) \in \mathcal{O}_K^\times$ not a root of unity, and such that $P(T) \neq 0 \bmod \mathfrak{m}_K$. In this section we assume that there exists a finite extension E of K, a Lubin–Tate formal group S defined over $\mathcal{O}_L$ with E/L finite, a power series $h \in T \cdot \mathcal{O}_E[\![T]\!]$ and an endomorphism P_S of S such that h is an isogeny from P_S to P.

Lemma 5.1. *There exists $V \in T \cdot \mathcal{O}_K[\![T]\!]$, commuting with P, and an integer $d \geq 1$ such that $Q(T) = T^{p^d} \bmod \mathfrak{m}_K$, where $Q = V \circ P$. Moreover, there exists Q_S an endomorphism of S such that h is an isogeny from Q_S to Q.*

Proof. First note that for any V_S invertible series commuting with P_S, there corresponds an invertible power series V commuting with P. Since S is a formal Lubin–Tate group over $\mathcal{O}_L$, P_S corresponds to multiplication by an element $\alpha \in \mathfrak{m}_L$. Let $[\pi_L]$ denote multiplication by π_L on S, a uniformizer of $\mathcal{O}_L$ such that $[\pi_L](T) = T^{\mathrm{Card}(k_L)} \bmod \mathfrak{m}_L$ (we can find such a uniformizer since S is a Lubin–Tate formal group defined over $\mathcal{O}_L$). Since $\alpha \in \mathfrak{m}_L$, there exist $c \in \mathcal{O}_L^\times$ and an integer $d \geq 1$ such that $\alpha = c \cdot \pi_L^d$. In particular, we have $\mathrm{wideg}([\alpha]) = \mathrm{wideg}(P) = \mathrm{wideg}([\pi_L^d]) = \mathrm{Card}(k_L)^d$.

We let V denote the power series commuting with P such that $h \circ [c^{-1}] = V \circ h$. We then have that $h \circ [c^{-1}] \circ [\alpha] = V \circ P \circ h$, and that $h \circ [c^{-1}] \circ [\alpha] = h \circ [\pi_L^d]$, so that h is an isogeny from $[\pi_L^d]$ to $Q := V \circ P$. Reducing modulo $\mathfrak{m}_L$, we get

$$h(T)^{\mathrm{Card}(k_L)^d} = h(T^{\mathrm{Card}(k_L)^d}) = h \circ Q \bmod \mathfrak{m}_L,$$

so that $Q = T^{\mathrm{Card}(k_L)^d} = T^{\mathrm{wideg}(P)} \bmod \mathfrak{m}_L$. ∎

Let $(u_n)_{n \in \mathbf{N}}$ be a sequence of elements of $\bar{\mathbf{Q}}_p$ such that $u_0 \neq 0$ is a root of Q_S, and $Q_S(u_{n+1}) = u_n$. In Lubin's terminology (see the definition on [16, p. 329]), the sequence (v_n) is called a Q_S-consistent sequence. Let $E_n = E(u_n)$ and let $E_\infty = \bigcup_n E_n$. Then for all $n \geq 1$, the extensions E_n/E are Galois.

Let Q be as in Lemma 5.1 and let $v_n := h(u_n)$.

LEMMA 5.2. *The sequence $(v_n)_{n\in\mathbf{N}}$ is Q-consistent, and the extensions $E(v_n)/E$ are Galois for all $n \geq 1$.*

PROOF. We know that E_n/E are Galois abelian extensions. Since $E \subset E(v_n) \subset E_n$, this implies that the extensions $E(v_n)/E$ are Galois. The fact that the sequence $(v_n)_{n\in\mathbf{N}}$ is Q-consistent follows directly from the fact that h is an isogeny from Q_S to Q. ∎

6. Embeddings into rings of periods

Let $L := K_{n_0}$ with n_0 as in Proposition 3.1. Since $P(T) = T^{p^d} \bmod \mathfrak{m}_K$, there exists $m \geq 1$ such that $P^{\circ m}$ acts trivially on k_L, so that the degree r of Q is a power of the cardinal of k_L. From now on we fix such an m. We let $w_0 = v_{n_0}$ and (w_n) be a sequence extracted from (v_n) such that $Q(w_{n+1}) = w_n$. For $n \geq 1$, we let $L_n = L(w_n)$. Let $L' = \mathbf{Q}_p^{\mathrm{unr}} \cap L$ be the maximal unramified extension of $\mathbf{Q}_p$ inside L, and let $\tilde{\mathbf{A}}^+ := \mathcal{O}_L \otimes_{\mathcal{O}_{L'}} W(\widetilde{\mathbf{E}}^+)$.

Since K_∞/L is strictly APF, there exists by [22, Lem. 4.2.2.1] a constant $c = c(K_\infty/L) > 0$ such that for all $F \subset F'$ finite subextensions of K_∞/L, and for all $x \in \mathcal{O}_{F'}$, we have

$$v_L\left(\frac{N_{F'/F}(x)}{x^{[F':F]}} - 1\right) \geq c.$$

We can always assume that $c \leq v_L(p)/(p-1)$ and we do so in what follows. By [22, §2.1 and §4.2], there is a canonical $\mathcal{G}_L$-equivariant embedding $\iota_L : A_L(K_\infty) \hookrightarrow \widetilde{\mathbf{E}}^+$, where $A_L(K_\infty)$ is the ring of integers of $X_L(K_\infty)$, the field of norms of K_∞/L. We can extend this embedding into a $\mathcal{G}_L$-equivariant embedding $X_L(K_\infty) \hookrightarrow \widetilde{\mathbf{E}}$, and we note $\mathbf{E}_K$ its image.

It will also be convenient to have the following interpretation for $\widetilde{\mathbf{E}}^+$:

$$\widetilde{\mathbf{E}}^+ = \varprojlim_{x\to x^p} \mathcal{O}_{\mathbf{C}_p} = \left\{(x^{(0)}, x^{(1)}, \ldots) \in \mathcal{O}_{\mathbf{C}_p}^{\mathbf{N}} \ : (x^{(n+1)})^p = x^{(n)}\right\}.$$

To see that this definition coincides with the one given in Section 2, we refer to [5, Prop. 4.3.1].

Note that, even though $\mathbf{E}_K$ depends on K_∞ rather than on L, it is still sensitive to L:

PROPOSITION 6.1. *Let L' be a finite extension of L contained in K_∞. Let L_t (resp. L'_t) be the maximal tamely ramified extension of K_∞/L (resp. K_∞/L'). Let $\mathbf{E}_{K'}$ denote the image of $X_{L'}(K_\infty)$ in $\widetilde{\mathbf{E}}$ by the embedding given in* [22, §4.2].

Then as a subfield of $\widetilde{\mathbf{E}}$, $\mathbf{E}_{K'}$ is a purely inseparable extension of $\mathbf{E}_K$ of degree $[L'_t : L_t]$. In particular, if $L' = L_t$ then $\mathbf{E}_{K'} = \mathbf{E}_K$.

Proof. See [6, Prop. 4.14]. ∎

The sequence (w_n) defines an element $\overline{w} \in \widetilde{\mathbf{E}}^+$.

Proposition 6.2. *There exists a unique $w \in \tilde{\mathbf{A}}^+$ lifting $\overline{w}$ such that $Q(w) = \varphi_r(w)$. Moreover, we have that $\theta \circ \varphi_r^{-n}(w) = w_n$.*

Proof. This is the same as the proof for Proposition 3.2. ∎

For all $k \geq 0$, we let

$$R_k := \left\{x \in \tilde{\mathbf{A}}^+, \theta \circ \varphi_d^{-n}(x) \in \mathcal{O}_{L_{n+k}} \text{ for all } n \geq 1\right\}.$$

Proposition 6.3. *For all $k \geq 0$, there exists $z_k \in R_k$ such that $R_k = \mathcal{O}_L[\![z_k]\!]$.*

Proof. Note that for all $k \geq 0$, R_k is an $\mathcal{O}_L$-algebra, separated and complete for the π_L-adic topology, where π_L is a uniformizer of $\mathcal{O}_L$. If $x \in R_k$, then its image in $\widetilde{\mathbf{E}}^+$ belongs to $\lim_{x \mapsto x^r} \mathcal{O}_{L_{n+k}}/\mathfrak{a}^c_{L_{n+k}}$.

Note that the natural map $R_k/\pi_L R_k \to \widetilde{\mathbf{E}}^+$ is injective. To prove this, we need to prove that $\pi_L \tilde{\mathbf{A}}^+ \cap R_k = \pi_L R_k$. Let $x \in R_k \cap \pi_L \tilde{\mathbf{A}}^+$ and let $y \in \tilde{\mathbf{A}}^+$ be such that $x = \pi_L y$. Then since $x \in R_k$ we have that $\theta \circ \varphi_r^{-n}(x) \in \mathcal{O}_{L_{n+k}}$ and thus $\theta \circ \varphi_r^{-n}(y) \in \frac{1}{\pi_L}\mathcal{O}_{L_{n+k}}$. But since $\theta \circ \varphi_r^{-n}$ maps $\tilde{\mathbf{A}}^+$ into $\mathcal{O}_{\mathbf{C}_p}$ we get that $\theta \circ \varphi_r^{-n}(y) \in L_{n+k} \cap \mathcal{O}_{\mathbf{C}_p} = \mathcal{O}_{L_{n+k}}$. Therefore the natural map $R_k/\pi_L R_k \to \widetilde{\mathbf{E}}^+$ is injective.

We know by the theory of fields of norms that $\lim_{x \mapsto x^r} \mathcal{O}_{L_n}/\mathfrak{a}^c_{L_n} \simeq k_L[\![\bar{v}]\!]$ for some $\bar{v} \in \widetilde{\mathbf{E}}^+$, so that the valuation induced by v_L on $\widetilde{\mathbf{E}}^+$ is discrete on $R/\pi_L R$. Let $\bar{u} \in R/\pi_L R$ be an element of minimal valuation within

$$\left\{x \in R/\pi_L R,\ v_L(x) > 0\right\}.$$

Since the valuation on $R/\pi_L R$ is discrete, and since this set is nonempty because it contains the image of the element w given by Proposition 6.2, such an element $\bar{u}$ exists, and we have $R/\pi_L R = k_L[\![\bar{u}]\!]$, so that $R = \mathcal{O}_L[\![u]\!]$ for $u \in R$ lifting $\bar{u}$ since R is separated and complete for the π_L-adic topology. ∎

Proposition 6.4. *There exists $k_0 \geq 0$ such that, for all $k \geq k_0$, we can take $z_{k+1} = \varphi_r^{-1}(z_k)$ and we let $z = z_{k_0}$.*

Proof. The proof of Proposition 6.3 shows that the quotient $R_k/\pi_L R_k$ injects into

$$\varprojlim_{x \mapsto x^r} \mathcal{O}_{L_{n+k}}/\mathfrak{a}^c_{L_{n+k}}.$$

By [22, Prop. 4.2.1],

$$\varprojlim_{x \mapsto x^r} \mathcal{O}_{L_{n+k}}/\mathfrak{a}^c_{L_{n+k}}$$

is the image of ring of integers of the field of norms of L_∞/L_k inside $\tilde{\mathbf{E}}$ by the embedding ι_L, and we will denote

$$\varprojlim_{x \mapsto x^r} \mathcal{O}_{L_{n+k}}/\mathfrak{a}^c_{L_{n+k}}$$

by Y_k. We normalize the valuation of Y_k so that $v_{Y_k}(Y_k) = \mathbf{Z}$. By Proposition 6.1, we get that for $k \geq n_0$, we have $Y_{k+1} = \varphi_r^{-1}(Y_k)$ and thus the valuation $v_{Y_{k+1}}$ is equal to $r v_{Y_k}$.

Now let $v(k) := v_{Y_k}(\overline{z_k})$ for $k \geq 0$. We know by definition of the sets R_k that $\varphi_r^{-1}(z_k) \in R_{k+1}$ for all $k \geq 1$ and thus $v_{Y_{k+1}}(\overline{z_{k+1}}) \leq r v_{Y_k}(\varphi_r^{-1}(\overline{z_k}))$ by construction of the z_k. This implies that the sequence $(v(k))_{k \geq n_0}$ is nonincreasing, and since it is bounded below by 1, this implies that there exists some $k_0 \geq n_0$ such that, for all $k \geq k_0$, we have $v(k) = v(k_0) > 0$. Thus for all $k \geq k_0$ we have $v_{Y_{k+1}}(\overline{z_{k+1}}) = v_{Y_k}(\overline{z_k})$ and by construction of the z_k this implies that we can take $z_{k+1} = \varphi_r^{-1}(z_k)$ which concludes the proof. ∎

We now let k_0 be as in Proposition 6.4. Note that in particular, for all $k \geq k_0$, we have $R_k = \varphi_r^{k_0-k}(\mathcal{O}_E[\![w]\!]) = \mathcal{O}_E[\![\varphi_r^{k_0-k}(w)]\!]$.

Lemma 6.5. *The ring $\mathcal{O}_L[\![z]\!]$ is stable by φ_r. Moreover, there exists $a \in \mathfrak{m}_L$ such that if $z' = z - a$ then there exists $S(T) \in T \cdot \mathcal{O}_L[\![T]\!]$ such that $S(z') = \varphi_r(z')$ and $S(T) \equiv T^r \bmod \mathfrak{m}_L$.*

Proof. The set

$$\left\{x \in \tilde{\mathbf{A}}^+,\ \theta \circ \varphi_r^{-n}(x) \in \mathcal{O}_{L_{n+k_0}} \text{ for all } n \geq 1\right\}$$

is clearly stable by φ_r and equal to $\mathcal{O}_L[\![z]\!]$ by Proposition 6.4, so that $\varphi_r(z) \in \mathcal{O}_L[\![z]\!]$ and so there exists $R \in \mathcal{O}_L[\![T]\!]$ such that $R(z) = \varphi_r(z)$. In particular, we have $\overline{R}(\bar{z}) = \bar{z}^r$ and so $R(T) \equiv T^r \bmod \mathfrak{m}_L$.

Now let $\widetilde{R}(T) = R(T + a)$ with $a \in \mathfrak{m}_L$ and let $z' = z - a$. Then $\varphi_r(z') = \varphi_r(z - a) = R(z) - a = \widetilde{R}(z') - a$ and we let $S(T) = \widetilde{R}(T) - a$ so that $\varphi_r(z') = S(z')$. For $S(0)$ to be 0, it suffices to find $a \in \mathfrak{m}_L$ such that $R(a) = a$. Such an a exists since we have $R(T) \equiv T^r \bmod \mathfrak{m}_L$ so that the Newton polygon of $R(T) - T$ starts with a segment of length 1 and of slope $-v_p(R(0))$.

Now, we have $S(z') = \varphi_r(z')$ and so $\overline{S}(\overline{z'}) = \overline{z'}^r$, so that $S(T) \equiv T^r \bmod \mathfrak{m}_L$. ∎

Lemma 6.5 shows that we can pick $z \in \{x \in \tilde{\mathbf{A}}^+,\ \theta \circ \varphi_r^{-n}(x) \in \mathcal{O}_{L_{n+k_0}} \text{ for all } n \geq 1\}$ such that $\varphi_r(z) = S(z)$ with $S(T) \in T \cdot \mathcal{O}_L[\![T]\!]$, and we will assume in what follows that such a choice has been made.

LEMMA 6.6. *Assume that there exists $m_0 \geq 0$ such that for all $m \geq m_0$, the extension L_m/L_{m_0} is Galois. Then the ring $\mathcal{O}_L[\![z]\!]$ is stable under the action of $\mathrm{Gal}(K_\infty/L_{m_0})$, and if $g \in \mathrm{Gal}(K_\infty/L_{m_0})$, there exists a power series $H_g(T) \in \mathcal{O}_L[\![T]\!]$ such that $g(z) = H_g(z)$.*

PROOF. Let $f_0 = \max(m_0, k_0)$. Since for all $m \geq m_0$, L_m/L_{m_0} is Galois, the set

$$\{x \in \tilde{\mathbf{A}}^+,\ \theta \circ \varphi_r^{-n}(x) \in \mathcal{O}_{L_{n+f_0}} \text{ for all } n \geq 1\}$$

is stable under the action of $\mathrm{Gal}(K_\infty/L_{m_0})$, and by Proposition 6.4, this set is equal to $\mathcal{O}_L[\![\varphi_r^{k_0-f_0}(z)]\!]$. In particular, if $g \in \mathrm{Gal}(K_\infty/L_{m_0})$, then $g(\varphi_r^{k_0-f_0}(z))$ also belongs to this set and so there exists $H_g(T) \in \mathcal{O}_L[\![T]\!]$ such that $H_g(\varphi_r^{k_0-f_0}(z)) = g(\varphi_r^{k_0-f_0}(z))$, and thus $H_g(z) = g(z)$. ∎

7. *p*-adic Hodge theory

Let us assume that there exists $m_0 \geq 0$ such that for all $m \geq m_0$, the extension L_m/L_{m_0} is Galois. Lemma 6.6 shows that in this case we are in the exact same spot as the situation after [17, Lem. 5.15]. In particular, the exact same techniques apply.

We keep the notation from Section 6 and we let $\kappa\colon \mathrm{Gal}(K_\infty/L_{m_0}) \to \mathcal{O}_L^\times$ denote the character $g \mapsto H_g'(0)$.

PROPOSITION 7.1. *The character $\kappa\colon \mathrm{Gal}(K_\infty/L_{m_0}) \to \mathcal{O}_L^\times$ is injective and crystalline with nonnegative weights.*

PROOF. This is the same as [17, Cor. 5.17 and Prop. 5.19]. ∎

For λ a uniformizer of L_{m_0}, let $(L_{m_0})_\lambda$ be the extension of L_{m_0} attached to λ by local class field theory. This extension is generated by the torsion points of a Lubin–Tate formal group defined over L_{m_0} and attached to λ, and we write

$$\chi_\lambda^{L_{m_0}}\colon \mathrm{Gal}((L_{m_0})_\lambda/L_{m_0}) \to \mathcal{O}_{L_{m_0}}^\times$$

for the corresponding Lubin–Tate character. Since K_∞/L_{m_0} is abelian and totally ramified, there exists λ a uniformizer of $\mathcal{O}_{L_{m_0}}$ such that $K_\infty \subset (L_{m_0})_\lambda$.

PROPOSITION 7.2. *There exists $F \subset L$ and $r \geq 1$ such that $\kappa = N_{L_{m_0}/F}(\chi_\lambda^{L_{m_0}})^r$.*

Proof. Thm. 5.27 of [17] shows that there exists $F \subset L_{m_0}$ and $r \geq 1$ such that $\kappa = N_{L_{m_0}/F}(\chi_\lambda^{L_{m_0}})^r$. The fact that κ takes its values in $\mathcal{O}_L^\times$ shows that F is actually a subfield of L. ∎

Recall that relative Lubin–Tate groups are a generalization of the usual formal Lubin–Tate groups given by de Shalit [10].

Theorem 7.3. *There exists $F \subset L$ and $r \geq 1$ such that $\kappa = N_{L/F}(\chi_\lambda^L)^r$. Moreover, there exists a relative Lubin–Tate group S, relative to the extension $F^{\mathrm{unr}} \cap L$ of F, such that if L_∞^S is the extension of L generated by the torsion points of S, then $L_\infty \subset L_\infty^S$ and L_∞^S/L_∞ is a finite extension.*

Proof. This is the same as [17, Thm. 5.28] using Proposition 7.2 instead of [17, Thm. 5.27]. ∎

8. Isogenies

In the setting of Theorem 7.3, let α be an element of $F^{\mathrm{unr}} \cap L$ such that L_∞^S is the field cut out by $\langle\alpha\rangle$ of F^{ab} by local class field theory, so that the relative Lubin–Tate group S is attached to α. Up to replacing L by a finite extension, we can assume that $L_\infty^S = L_\infty$ and we do so in what follows. We let $u_0 = 0$ and let $(u_n)_{n\in\mathbf{N}}$ be a nontrivial compatible sequence of roots of iterates of $[\alpha]$, the endomorphism of S corresponding to multiplication by α, so that $[\alpha](u_{n+1}) = u_n$ with $u_1 \neq 0$. We let q denote the cardinal of the residue field of $F^{\mathrm{unr}} \cap L$ so that $\mathrm{wideg}([\alpha]) = q$. Let $\bar{u} = (u_0, \ldots) \in \widetilde{\mathbf{E}}^+$. By [9, §9.2], there exists $u \in \tilde{\mathbf{A}}^+$ whose image in $\widetilde{\mathbf{E}}^+$ is $\bar{u}$ and such that $\varphi_q(u) = [\alpha](u)$, $g(w) = [\chi_\alpha(g)](u)$ for $g \in \mathcal{G}_L$.

Recall that Cais and Davis have defined a "canonical ring" attached to L_∞/L, denoted by $\mathbf{A}^+_{L_\infty/L}$, which is a subring of $\tilde{\mathbf{A}}^+$ and is defined via the tower of elementary extensions attached to L_∞/L by ramification theory. The following lemma shows that this canonical ring is related to the ring $\mathcal{O}_L[\![u]\!]$ for the extension L_∞/L:

Lemma 8.1. *There exists $k \geq 0$ such that $\mathbf{A}^+_{L_\infty/L} = \varphi_q^{-k}(\mathcal{O}_L[\![u]\!])$.*

Proof. See [17, Lem. 8.1]. Be mindful that there E and w play, respectively, the roles of L and u here. ∎

Recall that $(w_n)_{n\in\mathbf{N}}$ is a Q-consistent sequence, where Q commutes with P and is such that $Q(T) = T^s \bmod \mathfrak{m}_L$, and that $w \in \tilde{\mathbf{A}}^+$ is such that $\theta \circ \varphi_r^{-n}(w) = w_n$.

Proposition 8.2. *There exists $i \geq 0$ such that $\varphi_r^i(w) \in \mathbf{A}^+_{L_\infty/L}$.*

Proof. The proof is exactly the same as in [17, Prop. 8.2]. ∎

Proposition 8.3. *There exists $d \geq 1$ such that there is an isogeny from $[\alpha^d]$ to Q.*

Proof. Lemma 8.1 and Proposition 8.2 show that there exist $i \geq 0$ and $h(T) \in \mathcal{O}_L[\![T]\!]$ such that $w = h(\varphi_r^{-i}(u))$. Let d be such that $\varphi_r = \varphi_q^{\circ d}$ and let $\tilde{u} = \varphi_r^{-i}(u)$, so that $w = h(\tilde{u})$. For $g \in \mathcal{G}_L$, we have $\varphi_r(w) = Q(w)$ so that $Q(w) = \varphi_r(w) = \varphi_r(h(\tilde{u})) = h(\varphi_r(\tilde{u}))$ and thus $Q \circ h(\tilde{u}) = h \circ [\alpha^d](\tilde{u})$, which means that $Q \circ h = h \circ [\alpha^d]$. ∎

Theorem 8.4. *Let (P, U) be a couple of power series in $T \cdot \mathcal{O}_K[\![T]\!]$ such that $P \circ U = U \circ P$, with $P'(0) \in \mathfrak{m}_K$ and $U'(0) \in \mathcal{O}_K^\times$, and we assume that $P(T) \neq 0 \bmod \mathfrak{m}_K$ and that $U'(0)$ is not a root of unity. Then there exists a finite extension E of K, a Lubin–Tate formal group S defined over $\mathcal{O}_L$, where E/L is a finite extension, endomorphisms of this formal group P_S and U_S over $\mathcal{O}_E$, and a power series $h(T) \in T \cdot \mathcal{O}_E[\![T]\!]$ such that $P \circ h = h \circ P_S$ and $U \circ h = h \circ U_S$ if and only if the following two conditions are satisfied:*

(1) *There exists $V \in T \cdot \mathcal{O}_K[\![T]\!]$, commuting with P, and an integer $d \geq 1$ such that $Q(T) = T^{p^d} \bmod \mathfrak{m}_K$ where $Q = V \circ P$.*

(2) *There exists a finite extension E of K and a sequence $(\alpha_n)_{n \in \mathbf{N}}$ where $\alpha_0 \neq 0$ is a root of Q and $Q(\alpha_{n+1}) = \alpha_n$ such that for all $n \geq 1$, the extension $E(\alpha_n)/E$ is Galois.*

Proof. Lemmas 5.1 and 5.2 of Section 3 imply that if such a Lubin–Tate formal group exists then the two conditions are satisfied.

If those two conditions are satisfied, then Proposition 8.3 shows that there exist a finite extension E of K, a subfield F of E, a relative Lubin–Tate group S, relative to the extension $F^{\mathrm{unr}} \cap E$ of F, and an endomorphism Q_S of S such that there exists an isogeny from Q_S to Q. Thus there exists an isogeny from an endomorphism P_S of S to P. In order to conclude, it suffices to notice that a relative Lubin–Tate formal group S, relative to an extension $F^{\mathrm{unr}} \cap E$ of F, is actually isomorphic over $F^{\mathrm{unr}} \cap E$ to a Lubin–Tate formal group S' defined over F. ∎

9. A particular case of Lubin's conjecture

We now apply the results from the previous sections to the particular case where $P(T) = T^p \bmod \mathfrak{m}_K$. Let $P, U \in T \cdot \mathcal{O}_K[\![T]\!]$ be such that $P \circ U = U \circ P$, with $P(T) = T^p \bmod \mathfrak{m}_K$ and $U'(0) \in \mathcal{O}_K^\times$ not a root of unity. We consider as in Section 4

a P-consistent sequence (v_n) and we let $K_n = K(v_n)$ for $n \geq 0$. We let n_0 be as in Proposition 3.1.

PROPOSITION 9.1. *There exists $m_0 \geq 0$ such that for all $m \geq m_0$, the extension K_m/K_{m_0} is Galois.*

PROOF. By [16, Prop. 3.2], the roots of the iterates of P are exactly the fixed points of the iterates of U. Up to replacing U by some power of U, we can assume that $U'(0) = 1 \bmod \mathfrak{m}_K$ and that there exists $n \geq n_0$ such that $U(v_n) = v_n$ but $U(v_{n+1}) \neq v_{n+1}$ (since $U(T) - T$ admits only a finite number of roots in the unit disk).

Since $U(v_n) = v_n$ and U commutes with P, this implies that $U(v_{n+1})$ is also a root of $P(T) - v_n$. The discussion on [16, p. 333] shows that the set $\{U^{\circ k}(v_{n+1})\}_{k\in\mathbf{N}}$ has cardinality a power of p, and is not of cardinal 1 since $U(v_{n+1}) \neq v_{n+1}$ by assumption. Since $P(T) - v_n$ has exactly p roots, this implies that the set $\{U(v_{n+1})\}$ has cardinality p, and thus all the roots of $P(T) - v_n$ are contained in K_{n+1}, so that K_{n+1}/K_n is Galois.

Let $m > n$. The extension K_m/K_n is generated by all the roots of $P^{\circ(m-n)}(T) - v_n = P^{\circ(m-n)}(T) - U(v_n)$. Since U swaps all the roots of $P(T) - v_n$, it is easy to see that the U-orbit $\{U^{\circ k}(v_m)\}_{k\geq 0}$ contains all the roots of $P^{\circ(m-n)}(T) - v_n$, so that K_m/K_n is Galois. This proves the proposition. ∎

We are now in the conditions of our Theorem 8.4, which yields the following:

COROLLARY 9.2. *Lubin's conjecture is true for (P, U).*

ACKNOWLEDGMENTS – I thank the referee for his remarks and careful review.

FUNDING – This work was started when the author was a postdoc in the Department of Mathematics of the Università degli Studi di Padova, and finished after his arrival in Bordeaux.

REFERENCES

[1] L. BERGER, Iterated extensions and relative Lubin–Tate groups. *Ann. Math. Qué.* **40** (2016), no. 1, 17–28. Zbl 1360.11130 MR 3512521

[2] L. BERGER, Multivariable (φ, Γ)-modules and locally analytic vectors. *Duke Math. J.* **165** (2016), no. 18, 3567–3595. Zbl 1395.11084 MR 3577371

[3] L. BERGER, Lubin's conjecture for full p-adic dynamical systems. In *Publications mathématiques de Besançon. Algèbre et théorie des nombres, 2016*, pp. 19–24, Publ. Math. Besançon Algèbre Théorie Nr. 2016, Presses Universitaires Franche-Comté, Besançon, 2017. Zbl 1429.11208 MR 3645058

[4] L. Berger, Nonarchimedean dynamical systems and formal groups. *Proc. Amer. Math. Soc.* **147** (2019), no. 4, 1413–1419. Zbl 1429.11209 MR 3910408

[5] O. Brinon – B. Conrad, CMI summer school notes on p-adic Hodge theory, 2009, https://math.stanford.edu/~conrad/papers/notes.pdf visited on 11 April 2024.

[6] B. Cais – C. Davis, Canonical Cohen rings for norm fields. *Int. Math. Res. Not. IMRN* (2015), no. 14, 5473–5517. Zbl 1342.13028 MR 3384447

[7] B. Cais – C. Davis – J. Lubin, A characterization of strictly APF extensions. *J. Théor. Nombres Bordeaux* **28** (2016), no. 2, 417–430. Zbl 1409.11104 MR 3509717

[8] F. Cherbonnier – P. Colmez, Représentations p-adiques surconvergentes. *Invent. Math.* **133** (1998), no. 3, 581–611. Zbl 0928.11051 MR 1645070

[9] P. Colmez, Espaces de Banach de dimension finie. *J. Inst. Math. Jussieu* **1** (2002), no. 3, 331–439. Zbl 1044.11102 MR 1956055

[10] E. de Shalit, Relative Lubin–Tate groups. *Proc. Amer. Math. Soc.* **95** (1985), no. 1, 1–4. Zbl 0578.12013 MR 0796434

[11] J.-M. Fontaine, Le corps des périodes p-adiques. *Astérisque* (1994), no. 223, 59–102. MR 1293971

[12] F. Laubie – A. Movahhedi – A. Salinier, Systèmes dynamiques non archimédiens et corps des normes. *Compositio Math.* **132** (2002), no. 1, 57–98. Zbl 1101.14057 MR 1914256

[13] H.-C. Li, When is a p-adic power series an endomorphism of a formal group? *Proc. Amer. Math. Soc.* **124** (1996), no. 8, 2325–2329. Zbl 0862.11067 MR 1322933

[14] H.-C. Li, Isogenies between dynamics of formal groups. *J. Number Theory* **62** (1997), no. 2, 284–297. Zbl 0871.11085 MR 1432775

[15] H.-C. Li, p-adic power series which commute under composition. *Trans. Amer. Math. Soc.* **349** (1997), no. 4, 1437–1446. Zbl 0990.11073 MR 1327259

[16] J. Lubin, Nonarchimedean dynamical systems. *Compositio Math.* **94** (1994), no. 3, 321–346. Zbl 0843.58111 MR 1310863

[17] L. Poyeton, Formal groups and lifts of the field of norms. *Algebra Number Theory* **16** (2022), no. 2, 261–290. Zbl 1515.11115 MR 4412573

[18] G. Sarkis, On lifting commutative dynamical systems. *J. Algebra* **293** (2005), no. 1, 130–154. Zbl 1077.14059 MR 2173969

[19] G. Sarkis, Height-one commuting power series over $\mathbb{Z}_p$. *Bull. Lond. Math. Soc.* **42** (2010), no. 3, 381–387. Zbl 1200.11087 MR 2651931

[20] G. Sarkis – J. Specter, Galois extensions of height-one commuting dynamical systems. *J. Théor. Nombres Bordeaux* **25** (2013), no. 1, 163–178. Zbl 1292.37008 MR 3063836

[21] J. Specter, The crystalline period of a height one p-adic dynamical system. *Trans. Amer. Math. Soc.* **370** (2018), no. 5, 3591–3608. Zbl 1428.11202 MR 3766859

[22] J.-P. Wintenberger, Le corps des normes de certaines extensions infinies de corps locaux; applications. *Ann. Sci. École Norm. Sup. (4)* **16** (1983), no. 1, 59–89. Zbl 0516.12015 MR 0719763

Manoscritto pervenuto in redazione il 17 ottobre 2023.