ITERATED EXTENSIONS AND RELATIVE LUBIN-TATE GROUPS

by

Laurent Berger

To Glenn Stevens, on the occasion of his 60th birthday

Abstract. — Let K be a finite extension of $\mathbf{Q}_p$ with residue field $\mathbf{F}_q$ and let $P(T) = T^d + a_{d-1}T^{d-1} + \cdots + a_1T$ where d is a power of q and $a_i \in \mathfrak{m}_K$ for all i. Let u_0 be a uniformizer of $\mathcal{O}_K$ and let $\{u_n\}_{n\geqslant 0}$ be a sequence of elements of $\overline{\mathbf{Q}}_p$ such that $P(u_{n+1}) = u_n$ for all $n \geqslant 0$. Let K_∞ be the field generated over K by all the u_n. If K_∞/K is a Galois extension, then it is abelian, and our main result is that it is generated by the torsion points of a relative Lubin-Tate group (a generalization of the usual Lubin-Tate groups). The proof of this involves generalizing the construction of Coleman power series, constructing some p-adic periods in Fontaine's rings, and using local class field theory.

***Résumé* (Extensions itérées et groupes de Lubin-Tate relatifs).** — Soit K une extension finie de $\mathbf{Q}_p$ de corps résiduel $\mathbf{F}_q$ et $P(T) = T^d + a_{d-1}T^{d-1} + \cdots + a_1T$ où d est une puissance de q et $a_i \in \mathfrak{m}_K$ pour tout i. Soit u_0 une uniformisante de $\mathcal{O}_K$ et $\{u_n\}_{n\geqslant 0}$ une suite d'éléments de $\overline{\mathbf{Q}}_p$ telle que $P(u_{n+1}) = u_n$ pour tout $n \geqslant 0$. Soit K_∞ l'extension de K engendrée par les u_n. Si K_∞/K est Galoisienne, alors elle est abélienne, et notre résultat principal est qu'elle est engendrée par les points de torsion d'un groupe de Lubin-Tate relatif (une généralisation des groupes de Lubin-Tate usuels). Pour prouver cela, nous généralisons la construction des séries de Coleman, construisons des périodes p-adiques dans les anneaux de Fontaine et utilisons la théorie du corps de classes local.

Contents

2010 ***Mathematics Subject Classification.*** — 11S05; 11S15; 11S20; 11S31; 11S82; 13F25; 14F30.
Key words and phrases. — Iterated extension; Coleman power series; Field of norms; p-adic dynamical system; p-adic Hodge theory; Local class field theory; Lubin-Tate group; Chebyshev polynomial.

This material is partially based upon work supported by the NSF under Grant No. 0932078 000 while the author was in residence at the MSRI in Berkeley, California, during the Fall 2014 semester.

Introduction

Let K be a field, let $P(T) \in K[T]$ be a polynomial of degree $d \geqslant 1$, choose $u_0 \in K$ and for $n \geqslant 0$, let $u_{n+1} \in \overline{K}$ be such that $P(u_{n+1}) = u_n$. The field K_∞ generated over K by all the u_n is called an *iterated extension* of K. These iterated extensions and the resulting Galois groups have been studied in various contexts, see for instance [**Odo85**], [**Sto92**], [**AHM05**] and [**BJ07**].

In this article, we focus on a special situation: $p \neq 2$ is a prime number, K is a finite extension of $\mathbf{Q}_p$, with ring of integers $\mathcal{O}_K$, whose maximal ideal is $\mathfrak{m}_K$ and whose residue field is k. Let d be a power of $\mathrm{Card}(k)$, and let $P(T) = T^d + a_{d-1}T^{d-1} + \cdots + a_1 T$ be a monic polynomial of degree d with $a_i \in \mathfrak{m}_K$ for $1 \leqslant i \leqslant d-1$. Let u_0 be a uniformizer of $\mathcal{O}_K$ and define a sequence $\{u_n\}_{n \geqslant 0}$ by letting u_{n+1} be a root of $P(T) = u_n$. Let $K_n = K(u_n)$ and $K_\infty = \cup_{n \geqslant 1} K_n$. This iterated extension is called a *Frobenius-iterate extension*, after [**CD14**] (whose definition is a bit more general than ours). The question that we consider in this article is: which *Galois* extensions K_∞/K are Frobenius iterate?

This question is inspired by the observation, made in remark 7.16 of [**CD14**], that it follows from the main results of ibid. and [**Ber14**] that: if K_∞/K is Frobenius-iterate and Galois, then it is necessarily abelian. Here, we prove a much more precise result.

First, let us recall that in [**dS85**], de Shalit gives a generalization of the construction of Lubin-Tate formal groups (for which see [**LT65**]). A *relative Lubin-Tate group* is a formal group S that is attached to an unramified extension E/F and to an element α of F of valuation $[E : F]$. The extension E_∞^{S}/F generated over F by the torsion points of this formal group is the subextension of F^{ab} cut out via local class field theory by the subgroup of $F^\times$ generated by α. If $E = F$, we recover the classical Lubin-Tate groups.

Theorem A. — *Let K be a finite Galois extension of $\mathbf{Q}_p$, and let K_∞/K be a Frobenius-iterate extension. If K_∞/K is Galois, then there exists a subfield F of K, and a relative Lubin-Tate group* S*, relative to the extension $F^{\mathrm{unr}} \cap K$ of F, such that if K_∞^{S} denotes the extension of K generated by the torsion points of* S*, then $K_\infty \subset K_\infty^{\mathrm{S}}$ and $K_\infty^{\mathrm{S}}/K_\infty$ is a finite extension.*

This is theorem 6.4. Conversely, it is easy to see that the extension coming from a relative Lubin-Tate group is Frobenius-iterate after the first layer (see example 2.3). The proof of theorem A is quite indirect. We start with the observation that if K_∞/K is a Frobenius-iterate extension, that is not necessarily Galois, then we can generalize the construction of Coleman's power series (see [**Col79**]). Let $\varprojlim \mathcal{O}_{K_n}$ denote the set of sequences $\{x_n\}_{n \geqslant 0}$ with $x_n \in \mathcal{O}_{K_n}$ and such that $\mathrm{N}_{K_{n+1}/K_n}(x_{n+1}) = x_n$ for all $n \geqslant 0$.

Theorem B. — *We have $\{u_n\}_{n \geqslant 0} \in \varprojlim \mathcal{O}_{K_n}$ and if $\{x_n\}_{n \geqslant 0} \in \varprojlim \mathcal{O}_{K_n}$, then there exists a unique power series $\mathrm{Col}_x(T) \in \mathcal{O}_K[\![T]\!]$ such that $x_n = \mathrm{Col}_x(u_n)$ for all $n \geqslant 0$.*

Suppose now that K_∞/K is Galois, and let $\Gamma = \mathrm{Gal}(K_\infty/K)$. The results of [**CD14**] and [**Ber14**] imply that K_∞/K is abelian, so that K_n/K is Galois for all $n \geqslant 1$. If $g \in \Gamma$, then $\{g(u_n)\}_{n \geqslant 0} \in \varprojlim \mathcal{O}_{K_n}$, so that by theorem B, we get a power series $\mathrm{Col}_g(T) \in \mathcal{O}_K[\![T]\!]$ such that $g(u_n) = \mathrm{Col}_g(u_n)$ for all $n \geqslant 0$. Let $\widetilde{\mathbf{E}}^+ = \varprojlim_{x \mapsto x^d} \mathcal{O}_{\mathbf{C}_p}/p$, let $K_0 = \mathbf{Q}_p^{\mathrm{unr}} \cap K$ and let $\tilde{\mathbf{A}}^+ = \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} W(\widetilde{\mathbf{E}}^+)$ be Fontaine's rings of periods (see [**Fon94**]). The element $\{u_n\}_{n \geqslant 0}$ gives rise to an element $\overline{u} \in \widetilde{\mathbf{E}}^+$.

Theorem C. — *There exists $u \in \tilde{\mathbf{A}}^+$ whose image in $\widetilde{\mathbf{E}}^+$ is $\overline{u}$, and such that $\varphi_d(u) = P(u)$. We have $g(u) = \mathrm{Col}_g(u)$ if $g \in \Gamma$.*

The power series $\mathrm{Col}_g(T)$ satisfies the functional equation $\mathrm{Col}_g \circ P(T) = P \circ \mathrm{Col}_g(T)$. The study of p-adic power series that commute under composition was taken up by Lubin in [**Lub94**]. In §6 of ibid., Lubin writes 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". There are a number of results in this direction, see for instance [**LMS02**], [**SS13**] and [**JS14**]. In our setting, the series $\{\mathrm{Col}_g(T)\}_{g \in \Gamma}$ commute with $P(T)$ and theorem A says that indeed, there is a formal group that accounts for this. Let us now return to the proof of theorem A. We first show that $P'(T) \neq 0$. It is then proved in §1 of [**Lub94**] that given such a $P(T)$, a power series $\mathrm{Col}_g(T)$ that commutes with $P(T)$ is determined by $\mathrm{Col}'_g(0)$. If we let $\eta(g) = \mathrm{Col}'_g(0)$, we get the following: the map $\eta : \Gamma \to \mathcal{O}_K^\times$ is an injective character.

In order to finish the proof of theorem A, we use some p-adic Hodge theory. Let $\mathrm{L}_P(T) \in K[\![T]\!]$ be the *logarithm* attached to $P(T)$ and constructed in [**Lub94**]; it converges on the open unit disk, and satisfies $\mathrm{L}_P \circ P(T) = P'(0) \cdot \mathrm{L}_P(T)$ as well as $\mathrm{L}_P \circ \mathrm{Col}_g(T) = \eta(g) \cdot \mathrm{L}_P(T)$ for $g \in \Gamma$. In particular, we can consider $\mathrm{L}_P(u)$ as an element of the ring $\mathbf{B}^+_{\mathrm{cris}}$ (see [**Fon94**] for the rings of periods $\mathbf{B}^+_{\mathrm{cris}}$ and $\mathbf{B}_{\mathrm{dR}}$), which satisfies $g(\mathrm{L}_P(u)) = \eta(g) \cdot \mathrm{L}_P(u)$. More generally, if $\tau \in \mathrm{Gal}(K/\mathbf{Q}_p)$, then we can twist u by τ to get some elements $u_\tau \in \tilde{\mathbf{A}}^+$ and $\mathrm{L}^\tau_P(u_\tau) \in \mathbf{B}^+_{\mathrm{cris}}$, satisfying $g(\mathrm{L}^\tau_P(u_\tau)) = \tau(\eta(g)) \cdot \mathrm{L}^\tau_P(u_\tau)$. The elements $\{\mathrm{L}^\tau_P(u_\tau)\}_\tau$ are crystalline periods for the representation arising from η. Our main technical result concerning these periods is that the set of $\tau \in \mathrm{Gal}(K/\mathbf{Q}_p)$ such that $\mathrm{L}^\tau_P(u_\tau) \in \mathrm{Fil}^1 \mathbf{B}_{\mathrm{dR}}$

is a subgroup of $\mathrm{Gal}(K/\mathbf{Q}_p)$, and therefore cuts out a subfield F of K. This allows us to prove the following.

Theorem D. — *There exists a subfield F of K, a Lubin-Tate character χ_λ attached to a uniformizer λ of K, and an integer $r \geqslant 1$, such that $\eta = \mathrm{N}_{K/F}(\chi_\lambda)^r$.*

Theorem A follows from theorem D by local class field theory: the extensions of K corresponding to $\mathrm{N}_{K/F}(\chi_\lambda)$ are precisely those that come from relative Lubin-Tate groups. At the end of §6, we give an example for which $r = 2$. In this example, the Coleman power series p-adically interpolate Chebyshev polynomials.

1. Relative Lubin-Tate groups

We recall de Shalit's construction (see [**dS85**]) of a family of formal groups that generalize Lubin-Tate groups. Let F be a finite extension of $\mathbf{Q}_p$, with ring of integers $\mathcal{O}_F$ and residue field k_F of cardinality q. Take $h \geqslant 1$ and let E be the unramified extension of F of degree h. Let $\varphi_q : E \to E$ denote the Frobenius map that lifts $[x \mapsto x^q]$. If $f(T) = \sum_{i \geqslant 0} f_i T^i \in E[\![T]\!]$, let $f^{\varphi_q}(T) = \sum_{i \geqslant 0} \varphi_q(f_i) T^i$.

If $\alpha \in \mathcal{O}_F$ is such that $\mathrm{val}_F(\alpha) = h$, let $\mathcal{F}_\alpha$ be the set of power series $f(T) \in \mathcal{O}_E[\![T]\!]$ such that $f(T) = \pi T + \mathrm{O}(T^2)$ with $\mathrm{N}_{E/F}(\pi) = \alpha$ and such that $f(T) \equiv T^q \bmod \mathfrak{m}_E[\![T]\!]$. The set $\mathcal{F}_\alpha$ is nonempty, since $\mathrm{N}_{E/F}(E^\times)$ is the set of elements of $F^\times$ whose valuation is in $h \cdot \mathbf{Z}$. If $\mathrm{N}_{E/F}(\pi) = \alpha$, one can take $f(T) = \pi T + T^q$. The following theorem summarizes some of the results of [**dS85**] (see also §IV of [**Iwa86**]).

Theorem 1.1. — *If $f(T) \in \mathcal{F}_\alpha$, then*

1. *there is a unique formal group law $\mathrm{S}(X, Y) \in \mathcal{O}_E[\![X, Y]\!]$ such that $\mathrm{S}^{\varphi_q} \circ f = f \circ \mathrm{S}$, and the isomorphism class of S depends only on α;*
2. *for all $a \in \mathcal{O}_F$, there exists a unique power series $[a](T) \in \mathcal{O}_E[\![T]\!]$ such that $[a](T) = aT + \mathrm{O}(T^2)$ and $[a](T) \in \mathrm{End}(\mathrm{S})$.*

Let $x_0 = 0$ and for $m \geqslant 0$, let $x_m \in \overline{\mathbf{Q}}_p$ be such that $f^{\varphi_q^m}(x_{m+1}) = x_m$ (with $x_1 \neq 0$). Let $E_m = E(x_m)$ and let $E_\infty^{\mathrm{S}} = \cup_{m \geqslant 1} E_m$.

1. *The fields E_m depend only on α, and not on the choice of $f(T) \in \mathcal{F}_\alpha$;*
2. *The extension E_m/E is Galois, and its Galois group is isomorphic to $(\mathcal{O}_F/\mathfrak{m}_F^m)^\times$;*
3. *$E_\infty^{\mathrm{S}} \subset F^{\mathrm{ab}}$ and E_∞^{S} is the subfield of F^{ab} cut out by $\langle \alpha \rangle \subset F^\times$ via local class field theory.*

Remark 1.2. — If $h = 1$, then we recover the usual Lubin-Tate formal groups of [**LT65**].

2. Frobenius-iterate extensions

Let $p \neq 2$ be a prime number, let K be a finite extension of $\mathbf{Q}_p$, with ring of integers $\mathcal{O}_K$, whose maximal ideal is $\mathfrak{m}_K$ and whose residue field is k. Let $q = \mathrm{Card}(k)$, and let π denote a uniformizer of $\mathcal{O}_K$. Let d be a power of q, and let $P(T) = T^d + a_{d-1}T^{d-1} + \cdots + a_1 T$ be a monic polynomial of degree d with $a_i \in \mathfrak{m}_K$ for $1 \leqslant i \leqslant d-1$.

Let u_0 be a uniformizer of $\mathcal{O}_K$ and define a sequence $\{u_n\}_{n \geqslant 0}$ by letting u_{n+1} be a root of $P(T) = u_n$. Let $K_n = K(u_n)$.

Lemma 2.1. — *The extension K_n/K is totally ramified of degree d^n, u_n is a uniformizer of $\mathcal{O}_{K_n}$ and $\mathrm{N}_{K_{n+1}/K_n}(u_{n+1}) = u_n$.*

Proof. — The first two assertions follow immediately from the theory of Newton polygons, and the last one from the fact that $P(T) - u_n$ is the minimal polynomial of u_{n+1} over K_n, as well as the fact that d is odd since $p \neq 2$. □

Let $K_\infty = \cup_{n \geqslant 1} K_n$. This is a totally ramified infinite and pro-p extension of K.

Definition 2.2. — We say that an extension K_∞/K is *φ-iterate* if it is of the form above.

This definition is inspired by the similar one that is given in definition 1.1 of [**CD14**]. We require $P(T)$ to be a monic polynomial, instead of a more general power series as in ibid., in order to control the norm of u_n and to ensure the good behavior of K_{n+1}/K_n.

Example 2.3. — (i) If $P(T) = T^q$, then K_∞/K is a φ-iterate extension, which is the Kummer extension of K corresponding to π.

(ii) Let LT be a Lubin-Tate formal $\mathcal{O}_K$-module attached to π, and $K_n = K(\mathrm{LT}[\pi^n])$. The extension K_∞/K_1 is φ-iterate with $P(T) = [\pi](T)$.

(iii) More generally, let S be a relative Lubin-Tate group, relative to an extension E/F and $\alpha \in F$ as in §1. The extension $E_\infty^{\mathrm{S}}/E_1$ is φ-iterate with $P(T) = [\alpha](T)$.

Proof. — Item (ii) follows from applying (iii) with $K = E = F$, and we now prove (iii). We use the notation of theorem 1.1. Since the isomorphism class of S and the extension E_∞^{S}/E only depend on α, we can take $f(T) = \pi T + T^q$ where $\mathrm{N}_{E/F}(\pi) = \alpha$. Let $P(T) = f^{\varphi_q^{h-1}} \circ \cdots \circ f^{\varphi_q} \circ f(T) \in \mathcal{O}_E[T]$, so that $P(T) = [\alpha](T)$. The extension E_{hm+1} is generated by x_{hm+1} over E_1, and we have $P(x_{hm+1}) = x_{(h-1)m+1}$. The claim therefore follows from taking $u_m = x_{hm+1}$ for $m \geqslant 0$, and observing that since $\pi + u_0^{q-1} = 0$, u_0 is a uniformizer of $\mathcal{O}_{E_1}$. □

3. Coleman power series

Let us write $\varprojlim \mathcal{O}_{K_n}$ for the set of sequences $\{x_n\}_{n\geqslant 0}$ such that $x_n \in \mathcal{O}_{K_n}$ and such that $\mathrm{N}_{K_{n+1}/K_n}(x_{n+1}) = x_n$ for $n \geqslant 0$. By lemma 2.1, the sequence $\{u_n\}_{n\geqslant 0}$ belongs to $\varprojlim \mathcal{O}_{K_n}$. The goal of this § is to show the following theorem (theorem B).

Theorem 3.1. — *If $\{x_n\}_{n\geqslant 0} \in \varprojlim \mathcal{O}_{K_n}$, then there exists a uniquely determined power series $\mathrm{Col}_x(T) \in \mathcal{O}_K[\![T]\!]$ such that $x_n = \mathrm{Col}_x(u_n)$ for all $n \geqslant 0$.*

Our proof follows the one that is given in §13 of [**Was97**]. The unicity is a consequence of the following well-known general principle.

Proposition 3.2. — *If $f(T) \in \mathcal{O}_K[\![T]\!]$ is nonzero, then $f(T)$ has only finitely many zeroes in the open unit disk.*

In order to prove the existence part of theorem 3.1, we start by generalizing Coleman's norm map (see [**Col79**] for the original construction, and §2.3 of [**Fon90**] for the generalization that we use). The ring $\mathcal{O}_K[\![T]\!]$ is a free $\mathcal{O}_K[\![P(T)]\!]$-module of rank d. If $f(T) \in \mathcal{O}_K[\![T]\!]$, let $\mathcal{N}_P(f)(T) \in \mathcal{O}_K[\![T]\!]$ be defined by the requirement that $\mathcal{N}_P(f)(P(T)) = \mathrm{N}_{\mathcal{O}_K[\![T]\!]/\mathcal{O}_K[\![P(T)]\!]}(f(T))$. For example, $\mathcal{N}_P(T) = T$ since d is odd.

Proposition 3.3. — *The map $\mathcal{N}_P$ has the following properties.*

1. *If $f(T) \in \mathcal{O}_K[\![T]\!]$, then $\mathcal{N}_P(f)(u_n) = \mathrm{N}_{K_{n+1}/K_n}(f(u_{n+1}))$;*
2. *If $k \geqslant 1$ and $f(T) \in 1 + \pi^k\mathcal{O}_K[\![T]\!]$, then $\mathcal{N}_P(f)(T) \in 1 + \pi^{k+1}\mathcal{O}_K[\![T]\!]$;*
3. *If $f(T) \in \mathcal{O}_K[\![T]\!]$, then $\mathcal{N}_P(f)(T) \equiv f(T) \bmod \pi$;*
4. *If $f(T) \in \mathcal{O}_K[\![T]\!]^\times$, and $k, m \geqslant 0$, then $\mathcal{N}_P^{m+k}(f) \equiv \mathcal{N}_P^k(f) \bmod \pi^{k+1}$.*

Proof. — The determinant of the multiplication-by-$f(T)$ map on the $\mathcal{O}_K[\![P(T)]\!]$-module $\mathcal{O}_K[\![T]\!]$ is $\mathcal{N}_P(f)(P(T))$. By evaluating at $T = u_{n+1}$, we find that the determinant of the multiplication-by-$f(u_{n+1})$ map on the $\mathcal{O}_{K_n}$-module $\mathcal{O}_{K_{n+1}}$ is $\mathcal{N}_P(f)(u_n)$, so that $\mathcal{N}_P(f)(u_n) = \mathrm{N}_{K_{n+1}/K_n}(f(u_{n+1}))$.

We now prove (2). If $f(T) \in \mathcal{O}_K[\![T]\!]$, let $\mathcal{T}_P(f)(T) \in \mathcal{O}_K[\![T]\!]$ be the trace map defined by $\mathcal{T}_P(f)(P(T)) = \mathrm{Tr}_{\mathcal{O}_K[\![T]\!]/\mathcal{O}_K[\![P(T)]\!]}(f(T))$. A straightforward calculation shows that if $h(T) \in \mathcal{O}_K[\![T]\!]$, then $\mathcal{T}_P(h)(T) \in \pi \cdot \mathcal{O}_K[\![T]\!]$. If $f(T) = 1 + \pi^k h(T)$, then $\mathcal{N}_P(f)(T) \equiv 1 + \pi^k \mathcal{T}_P(h)(T) \bmod \pi^{k+1}$, so that $\mathcal{N}_P(f)(T) \in 1 + \pi^{k+1}\mathcal{O}_K[\![T]\!]$.

Item (3) follows from a straightfoward calculation in $k[\![T]\!]$ using the fact that $P(T) = T^d$ in $k[\![T]\!]$. Finally, let us prove (4). If $f(T) \in \mathcal{O}_K[\![T]\!]^\times$, then $\mathcal{N}_P(f)/f \equiv 1 \bmod \pi$ by (3), so that $\mathcal{N}_P^m(f)/f \equiv 1 \bmod \pi$ as well. Item (2) now implies that $\mathcal{N}_P^{m+k}(f) \equiv \mathcal{N}_P^k(f) \bmod \pi^{k+1}$. $\square$

of theorem 3.1. — The power series $\mathrm{Col}_x(T)$ is unique by lemma 3.2, and we now show its existence. If x_n is not a unit of $\mathcal{O}_{K_n}$, then there exists $e \geqslant 1$ such that $x_n = u_n^e x_n^*$ where $x_n^* \in \mathcal{O}_{K_n}^\times$ for all n, and then $\mathrm{Col}_x(T) = T^e \cdot \mathrm{Col}_{x^*}(T)$. We can therefore assume that x_n is a unit of $\mathcal{O}_{K_n}$. For all $j \geqslant 1$, we have $\mathcal{O}_{K_j} = \mathcal{O}_K[u_j]$, so that there exists $g_j(T) \in \mathcal{O}_K[T]$ such that $x_j = g_j(u_j)$. Let $f_j(T) = \mathcal{N}_P^j(g_{2j})$. By proposition 3.3, we have $x_n \equiv f_j(u_n) \bmod \pi^{j+1}$ for all $n \leqslant j$. The space $\mathcal{O}_K[\![T]\!]$ is compact; let $f(T)$ be a limit point of $\{f_j\}_{j \geqslant 1}$. We have $x_n = f(u_n)$ for all n by continuity, so that we can take $\mathrm{Col}_x(T) = f(T)$. □

Remark 3.4. — We have $\mathcal{N}_P(\mathrm{Col}_x)(T) = \mathrm{Col}_x(T)$.

Proof. — The power series $\mathcal{N}_P(\mathrm{Col}_x)(T) - \mathrm{Col}_x(T)$ is zero at $T = u_n$ for all $n \geqslant 0$ by proposition 3.3, so that $\mathcal{N}_P(\mathrm{Col}_x)(T) = \mathrm{Col}_x(T)$ by lemma 3.2. □

4. Lifting the field of norms

In this §, we assume that K_∞/K is a Galois extension, and let $\Gamma = \mathrm{Gal}(K_\infty/K)$. We recall some results of [**CD14**] and [**Ber14**], and give a more precise formulation of some of them in our specific situation.

Proposition 4.1. — *If K_∞/K is Galois, then K_n/K is Galois for all $n \geqslant 1$.*

Proof. — It follows from the main results of [**CD14**] and of [**Ber14**] (see remark 7.16 of [**CD14**]) that if K_∞/K is a φ-iterate extension that is Galois, then it is abelian. This implies the proposition (it would be more satisfying to find a direct proof). □

If $g \in \Gamma$, proposition 4.1 and theorem 3.1 imply that there is a unique power series $\mathrm{Col}_g(T) \in \mathcal{O}_K[\![T]\!]$ such that $g(u_n) = \mathrm{Col}_g(u_n)$ for all $n \geqslant 0$. In the sequel, we need some ramification-theoretic properties of K_∞/K. They are summarized in the theorem below.

Theorem 4.2. — *There exists a constant $c = c(K_\infty/K) > 0$ such that for any $E \subset F$, finite extensions of K contained in K_∞, and $x \in \mathcal{O}_F$, we have*

$$\mathrm{val}_K\left(\frac{\mathrm{N}_{F/E}(x)}{x^{[F:E]}} - 1\right) \geqslant c.$$

Proof. — By the main result of [**CDL14**], the extension K_∞/K is *strictly APF*, so that if we denote by $c(K_\infty/K)$ the constant defined in 1.2.1 of [**Win83**], then $c(K_\infty/K) > 0$. By 4.2.2.1 of ibid., we have

$$\mathrm{val}_E\left(\frac{\mathrm{N}_{F/E}(x)}{x^{[F:E]}} - 1\right) \geqslant c(F/E),$$

By 1.2.3 of ibid., $c(F/E) \geqslant c(K_\infty/E)$ and (see for instance the proof of 4.5 of [**CD14**] or page 83 of [**Win83**]) $c(K_\infty/E) \geqslant c(K_\infty/K) \cdot [E:K]$. This proves the theorem. $\square$

Let c be the constant afforded by theorem 4.2. We can always assume that $c \leqslant \mathrm{val}_K(p)/(p-1)$. If E is some subfield of $\mathbf{C}_p$, let $\mathfrak{a}_E^c$ denote the set of elements x of E such that $\mathrm{val}_K(x) \geqslant c$. Let $\widetilde{\mathbf{E}}^+ = \varprojlim_{x \mapsto x^d} \mathcal{O}_{\mathbf{C}_p}/\mathfrak{a}_{\mathbf{C}_p}^c$. The sequence $\{u_n\}_{n \geqslant 0}$ gives rise to an element $\overline{u} \in \widetilde{\mathbf{E}}^+$. Recall that by §2.1 and §4.2 of [**Win83**], there is an embedding $\iota : \varprojlim \mathcal{O}_{K_n} \to \widetilde{\mathbf{E}}^+$, which is an isomorphism onto $\varprojlim_{x \mapsto x^d} \mathcal{O}_{K_n}/\mathfrak{a}_{K_n}^c$, which is also isomorphic to $k[\![\overline{u}]\!]$. Let $K_0 = \mathbf{Q}_p^{\mathrm{unr}} \cap K$ and $\tilde{\mathbf{A}}^+ = \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} W(\widetilde{\mathbf{E}}^+)$. Recall (see [**Fon94**]) that we have a map $\theta : \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p}$. If $x \in \tilde{\mathbf{A}}^+$ and $\overline{x} = (x_n)_{n \geqslant 0}$ in $\widetilde{\mathbf{E}}^+$, then $\theta \circ \varphi_d^{-n}(x) = x_n$ in $\mathcal{O}_{\mathbf{C}_p}/\mathfrak{a}_{\mathbf{C}_p}^c$.

Theorem 4.3. — *There exists a unique $u \in \tilde{\mathbf{A}}^+$ whose image in $\widetilde{\mathbf{E}}^+$ is $\overline{u}$, and such that $\varphi_d(u) = P(u)$. Moreover:*

(i) *If $n \geqslant 0$, then $\theta \circ \varphi_d^{-n}(u) = u_n$;*
(ii) *$\mathcal{O}_K[\![u]\!] = \{x \in \tilde{\mathbf{A}}^+,\ \theta \circ \varphi_d^{-n}(x) \in \mathcal{O}_{K_n}$ for all $n \geqslant 1\}$;*
(iii) *$g(u) = \mathrm{Col}_g(u)$ if $g \in \Gamma$.*

Proof. — The existence of u and item (i) are proved in lemma 9.3 of [**Col02**], where it is shown that $u = \lim_{n \to +\infty} P^{\circ n}(\varphi_d^{-n}([\overline{u}]))$.

Let $R = \{x \in \tilde{\mathbf{A}}^+$ such that $\theta \circ \varphi_d^{-n}(x) \in \mathcal{O}_{K_n}$ for all $n \geqslant 1\}$. If $x \in R$, then its image in $\widetilde{\mathbf{E}}^+$ lies in $\varprojlim_{x \mapsto x^d} \mathcal{O}_{K_n}/\mathfrak{a}_{K_n}^c = k[\![\overline{u}]\!]$. We have $u \in R$ by proposition 4.3, so that the map $R/\pi R \to k[\![\overline{u}]\!]$ is surjective. We then have $R = \mathcal{O}_K[\![u]\!]$, since R is separated and complete for the π-adic topology, which proves (ii).

The ring $\mathcal{O}_K[\![u]\!]$ is stable under the action of G_K by (ii). If $g \in \Gamma$, there exists $F_g(T) \in \mathcal{O}_K[\![T]\!]$ such that $g(u) = F_g(u)$. We have $g(u_n) = g(\theta \circ \varphi_d^{-n}(u)) = \theta \circ \varphi_d^{-n}(F_g(u)) = F_g(u_n)$ by (i), so that $g(u_n) = F_g(u_n)$ for all n. This implies that $F_g(T) = \mathrm{Col}_g(T)$. $\square$

Remark 4.4. — In the terminology of [**Win83**], $\varprojlim \mathcal{O}_{K_n}$ is the ring of integers of the field of norms $X(K_\infty)$ of the extension K_∞/K, and theorem 4.3 shows that we can lift $X(K_\infty)$ to characteristic zero, along with the Frobenius map φ_d and the action of Γ.

If $g \in \Gamma$, then $\mathrm{Col}_g \circ P(T) = P \circ \mathrm{Col}_g(T)$ since the two series have the same value at u_n for all $n \geqslant 1$. Let $\eta(g) = \mathrm{Col}_g'(0)$, so that $g \mapsto \eta(g)$ is a character $\eta : \Gamma \to \mathcal{O}_K^\times$

Proposition 4.5. — *If $F(T) \in T \cdot \mathcal{O}_K[\![T]\!]$ is such that $F'(0) \in 1 + p\mathcal{O}_K$, and if $A(T) \in T \cdot \mathcal{O}_K[\![T]\!]$ vanishes at order $k \geqslant 2$ at 0, and satisifes $A \circ F(T) = F \circ A(T)$, then $F(T) = T$.*

Proof. — Write $F(T) = f_1 T + \mathrm{O}(T^2)$, and $A(T) = a_k T^k + \mathrm{O}(T^{k+1})$ with $a_k \neq 0$. The equation $F \circ A(T) = A \circ F(T)$ implies that $f_1 a_k = a_k f_1^k$ so that if $k \neq 1$, then $f_1^{k-1} = 1$. Since $f_1 \in 1 + p\mathcal{O}_K$ and $p \neq 2$, this implies that $f_1 = 1$. If $F(T) \neq T$, we can write $F(T) = T + T^i h(T)$ for some $i \geqslant 2$ with $h(0) \neq 0$. The equation $F \circ A(T) = A \circ F(T)$ and the equality $A(T + T^i h(T)) = \sum_{j \geqslant 0} (T^i h(T))^j A^{(j)}(T)/j!$ imply that $A(T) + A(T)^i h(A(T)) = A(T) + T^i h(T) A'(T) + \mathrm{O}(T^{2i+k-2})$, so that $A(T)^i h(A(T)) = T^i h(T) A'(T) + \mathrm{O}(T^{2i+k-2})$. The term of lowest degree of the LHS is of degree ki, while on the RHS it is of degree $i + k - 1$. We therefore have $ki = i + k - 1$, so that $(k-1)(i-1) = 0$ and hence $k = 1$. □

Corollary 4.6. — *We have $P'(0) \neq 0$.*

Proof. — This follows from proposition 4.5, since $\mathrm{Col}_g'(0) \in 1 + p\mathcal{O}_K$ if g is close enough to 1, and $\mathrm{Col}_g(T) = T$ if and only if $g = 1$ (compare with lemma 4.5 of [**Ber14**]). □

Corollary 4.7. — *The character $\eta : \Gamma \to \mathcal{O}_K^\times$ is injective.*

Proof. — This follows from proposition 1.1 of [**Lub94**], which says that if $P'(0) \in \mathfrak{m}_K \setminus \{0\}$, then a power series $F(T) \in T \cdot \mathcal{O}_K[\![T]\!]$ that commutes with $P(T)$ is determined by $F'(0)$. This implies that $\mathrm{Col}_g(T)$ is determined by $\eta(g)$, and then g itself is determined by $\mathrm{Col}_g(T)$, since $g(u_n) = \mathrm{Col}_g(u_n)$ for all n. □

We therefore have a character $\eta : \mathrm{Gal}(\overline{\mathbf{Q}}_p/K) \to \mathcal{O}_K^\times$, such that $K_\infty = \overline{\mathbf{Q}}_p^{\ker \eta}$.

5. p-adic Hodge theory

We now assume that $K/\mathbf{Q}_p$ is Galois (for simplicity), and we keep assuming that K_∞/K is Galois. We use the element u above, and Lubin's logarithm (proposition 5.1 below), to construct crystalline periods for η.

Proposition 5.1. — *There exists a power series $\mathrm{L}_P(T) \in K[\![T]\!]$ that is holomorphic on the open unit disk, and satisfies*

1. $\mathrm{L}_P(T) = T + \mathrm{O}(T^2)$;
2. $\mathrm{L}_P \circ P(T) = P'(0) \cdot \mathrm{L}_P(T)$;
3. $\mathrm{L}_P \circ \mathrm{Col}_g(T) = \eta(g) \cdot \mathrm{L}_P(T)$ *if* $g \in \Gamma$.

If we write $P(T) = T \cdot Q(T)$, then

$$\mathrm{L}_P(T) = \lim_{n \to +\infty} \frac{P^{\circ n}(T)}{P'(0)^n} = T \cdot \prod_{n \geqslant 0} \frac{Q(P^{\circ n}(T))}{Q(0)}.$$

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

Let $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ denote the Fréchet completion of $\tilde{\mathbf{A}}^+[1/\pi]$, so that our $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ is $K \otimes_{K_0}$ the "usual" $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ (for which see [**Ber02**]). If $u \in \tilde{\mathbf{A}}^+$ is the element afforded by proposition 4.3, then $\mathrm{L}_P(u)$ converges in $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$. We have $g(\mathrm{L}_P(u)) = \eta(g) \cdot \mathrm{L}_P(u)$ by proposition 5.1. If $\tau \in \mathrm{Gal}(K/\mathbf{Q}_p)$, then let $n(\tau)$ be some $n \in \mathbf{Z}$ such that $\tau = \varphi^n$ on k_K, and let $u_\tau = (\tau \otimes \varphi^{n(\tau)})(u) \in \tilde{\mathbf{A}}^+$.

If $F(T) = \sum_{i \geqslant 0} f_i T^i \in K[\![T]\!]$, let $F^\tau(T) = \sum_{i \geqslant 0} \tau(f_i) T^i$. We have $g(\mathrm{L}^\tau_P(u_\tau)) = \tau(\eta(g)) \cdot \mathrm{L}^\tau_P(u_\tau)$ in $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$. This implies the following result, which is a slight improvement of theorem 4.1 of [**Ber14**].

Proposition 5.2. — *The character $\eta : \Gamma \to \mathcal{O}_K^\times$ is crystalline, with weights in $\mathbf{Z}_{\geqslant 0}$.*

Proof. — The fact that $g(\mathrm{L}^\tau_P(u_\tau)) = \tau(\eta(g)) \cdot \mathrm{L}^\tau_P(u_\tau)$ for all $\tau \in \mathrm{Gal}(K/\mathbf{Q}_p)$ implies that η gives rise to a $K \otimes_{K_0} \mathbf{B}_{\mathrm{cris}}$-admissible representation. If V is any p-adic representation of G_K, then

$$\Big((K \otimes_{K_0} \mathbf{B}_{\mathrm{cris}}) \otimes_{\mathbf{Q}_p} V\Big)^{G_K} = K \otimes_{K_0} (\mathbf{B}_{\mathrm{cris}} \otimes_{\mathbf{Q}_p} V)^{G_K}.$$

This implies that a $K \otimes_{K_0} \mathbf{B}_{\mathrm{cris}}$-admissible representation is crystalline. The weights of η are $\geqslant 0$ because $\mathrm{L}^\tau_P(u_\tau) \in \mathbf{B}^+_{\mathrm{dR}}$ for all τ. □

Lemma 5.3. — *We have $\theta \circ \varphi_d^{-n}(u_\tau) = \lim_{k \to +\infty} (P^\tau)^{\circ k}(u_{n+k}^{p^{n(\tau)}})$.*

Proof. — The element $u_\tau \in \tilde{\mathbf{A}}^+$ has the property that its image in $\widetilde{\mathbf{E}}^+$ is $\varphi^{n(\tau)}(\overline{u}) = \overline{u}^{p^{n(\tau)}}$, and that $\varphi_d(u_\tau) = P^\tau(u_\tau)$. The lemma then follows from lemma 9.3 of [**Col02**]. □

For simplicity, write $u^n_\tau = \theta \circ \varphi_d^{-n}(u_\tau)$ and $u^{n,k}_\tau = (P^\tau)^{\circ k}(u_{n+k}^{p^{n(\tau)}})$.

Lemma 5.4. — *If $M > 0$, there exists $j \geqslant 0$ such that $\mathrm{val}_K(u^n_\tau - u^{n,j}_\tau) \geqslant M$ for $n \geqslant 1$.*

Proof. — If c is the constant coming from theorem 4.2, then $\mathrm{val}_K(u^n_\tau - u^{n,0}_\tau) \geqslant c$ for all $n \geqslant 1$. We prove the lemma by inductively constructing a sequence $\{c_j\}_{j \geqslant 0}$ such that $\mathrm{val}_K(u^n_\tau - u^{n,j}_\tau) \geqslant c_j$ for all $n \geqslant 1$, and such that $c_j \geqslant M$ for $j \gg 0$. Let $c_0 = c$ and suppose that for some j, we have $\mathrm{val}_K(u^n_\tau - u^{n,j}_\tau) \geqslant c_j$ for all $n \geqslant 1$. We then have

$$\mathrm{val}_K(u^n_\tau - u^{n,j+1}_\tau) = \mathrm{val}_K\left(P^\tau(u^{n+1}_\tau) - P^\tau(u^{n+1,j}_\tau)\right).$$

If $R(T) \in \mathcal{O}_K[T]$ and $x, y \in \mathcal{O}_{\overline{\mathbf{Q}}_p}$, then $R(x) - R(y) = (x-y)R'(y) + (x-y)^2 S(x,y)$ with $S(T,U) \in \mathcal{O}_K[T,U]$. This, and the fact that $P'(T) \in \mathfrak{m}_K[T]$, implies that we can take $c_{j+1} = \min(c_j + 1, 2c_j)$. The lemma follows. □

We now recall a result from [**Lub94**]. If $f(T) \in T \cdot \mathcal{O}_K[\![T]\!]$ is such that $f'(0) \in \mathfrak{m}_K \setminus \{0\}$, let $\Lambda(f)$ be the set of the roots of all iterates of f. If $u(T) \in T \cdot \mathcal{O}_K[\![T]\!]$ is such that

$u'(0) \in \mathcal{O}_K^\times$ and $u'(0)$ is not a root of 1, let $\Lambda(u)$ be the set of the fixed points of all iterates of u.

Lemma 5.5. — *If f and u are as above, and if $u \circ f = f \circ u$, then $\Lambda(f) = \Lambda(u)$.*

Proof. — This is proposition 3.2 of [**Lub94**]. □

For each $\tau \in \mathrm{Gal}(K/\mathbf{Q}_p)$, let r_τ be the weight of η at τ.

Proposition 5.6. — *If $\tau \in \mathrm{Gal}(K/\mathbf{Q}_p)$, then the following are equivalent.*

(i) $r_\tau \geqslant 1$;
(ii) $\mathrm{L}_P^\tau(u_\tau) \in \mathrm{Fil}^1 \mathbf{B}_{\mathrm{dR}}$;
(iii) $\theta(u_\tau) \in \overline{\mathbf{Q}}_p$;
(iv) $\theta(u_\tau) \in \Lambda(P^\tau)$;
(v) $u_\tau \in \cup_{j \geqslant 0}\, \varphi_d^{-j}(\mathcal{O}_K[\![u]\!])$.

Proof. — The equivalence between (i) and (ii) is immediate. We now prove that (ii) implies (iii). If $\mathrm{L}_P^\tau(u_\tau) \in \mathrm{Fil}^1 \mathbf{B}_{\mathrm{dR}}$, then $\mathrm{L}_P^\tau(\theta(u_\tau)) = 0$ so that $\theta(u_\tau) \in \overline{\mathbf{Q}}_p$ since it is a root of a convergent power series with coefficients in K. We next prove that (iii) implies (iv) (it is clear that (iv) implies (iii)). If $x = \theta(u_\tau)$ then $g(x) = \mathrm{Col}_g^\tau(x)$. If $x \in \overline{\mathbf{Q}}_p$ and if g is close enough to 1, then $g(x) = x$ so that $x \in \Lambda(\mathrm{Col}_g^\tau)$, and then $x \in \Lambda(P^\tau)$ by lemma 5.5. Let us prove that (iv) implies (ii). If there exists $n \geqslant 0$ such that $(P^\tau)^{\circ n}(\theta(u_\tau)) = 0$, then $(P^\tau)^{\circ n}(u_\tau) \in \mathrm{Fil}^1 \mathbf{B}_{\mathrm{dR}}$ so that $\mathrm{L}_P^\tau(u_\tau) \in \mathrm{Fil}^1 \mathbf{B}_{\mathrm{dR}}$ as well by proposition 5.1. Conditions (i), (ii), (iii) and (iv) are therefore equivalent. Condition (v) implies (iii) by using theorem 4.3 as well as the fact that $\varphi_d(u_\tau) = P^\tau(u_\tau)$.

It remains to prove that (iii) implies (v). Recall that $u_\tau^n = \theta \circ \varphi_d^{-n}(u_\tau)$. It is enough to show that there exists $j \geqslant 0$ such that $u_\tau^n \in \mathcal{O}_{K_{n+j}}$ for all n, since by theorem 4.3, this implies that $u_\tau \in \varphi_d^{-j}(\mathcal{O}_K[\![u]\!])$. Recall that $u_\tau^{n,k} = (P^\tau)^{\circ k}(u_{n+k}^{p^{n(\tau)}})$. Take $M \geqslant 1 + \mathrm{val}_K((P^\tau)'(u_\tau^n))$ for all $n \gg 0$. By lemma 5.4, there exists $j \geqslant 0$ such that $\mathrm{val}_K(u_\tau^n - u_\tau^{n,j}) \geqslant M$ for all $n \geqslant 1$. The element u_τ^n is a root of $P^\tau(T) = u_\tau^{n-1}$, and therefore $u_\tau^n - u_\tau^{n,j}$ is a root of $P^\tau(u_\tau^{n,j} + T) - u_\tau^{n-1}$. If $u_\tau^{n-1} \in \mathcal{O}_{K_{n+j-1}}$, then the polynomial $R_n(T) = P^\tau(u_\tau^{n,j} + T) - u_\tau^{n-1}$ belongs to $\mathcal{O}_{K_{n+j}}[T]$, and satisfies $\mathrm{val}_K(R_n(0)) \geqslant M + \mathrm{val}_K(R_n'(0))$. By the theory of Newton polygons, $R_n(T)$ has a unique root of slope $\mathrm{val}_K(R_n(0)) - \mathrm{val}_K(R_n'(0)) \geqslant M$, and this root, which is $u_\tau^n - u_\tau^{n,j}$, therefore belongs to K_{n+j}. This implies that $u_\tau^n \in \mathcal{O}_{K_{n+j}}$, which finishes the proof by induction on n. □

If τ satisfies the equivalent conditions of proposition 5.6, then we can write $u_\tau = f_\tau(\varphi_q^{-j_\tau}(u))$ for some $j_\tau \geqslant 0$ and $f_\tau(T) \in \mathcal{O}_K[\![T]\!]$.

Lemma 5.7. — *We have $f_\tau(0)=0$, $f_\tau'(0)\neq 0$, $P^\tau\circ f_\tau(T)=f_\tau\circ P(T)$ and $\mathrm{Col}_g^\tau\circ f_\tau(T)=f_\tau\circ\mathrm{Col}_g(T)$.*

Proof. — If $u_\tau=f_\tau(\varphi_d^{-j}(u))$, then $P^\tau(u_\tau)=P^\tau\circ f_\tau(\varphi_d^{-j}(u))$ and then $\varphi_d(u_\tau)=f_\tau\circ P(\varphi_d^{-j}(u))$ so that $P^\tau\circ f_\tau(T)=f_\tau\circ P(T)$. Likewise, computing $g(u_\tau)$ in two ways shows that $\mathrm{Col}_g^\tau\circ f_\tau(T)=f_\tau\circ\mathrm{Col}_g(T)$. Evaluating $P^\tau\circ f_\tau(T)=f_\tau\circ P(T)$ at $T=0$ gives $P^\tau(f_\tau(0))=f_\tau(0)$ so that $f_\tau(0)$ is a root of $P^\tau(T)=T$. The theory of Newton polygons shows that those roots are 0 and elements of valuation 0. The latter case is excluded because $\theta\circ\varphi_d^{-n}(u_\tau)=f_\tau(u_{n+j})\in\mathfrak{m}_{K_\infty}$, so that $f_\tau(0)\in\mathfrak{m}_K$. We now prove that $f_\tau'(0)\neq 0$. Write $f(T)=f_kT^k+\mathrm{O}(T^{k+1})$ with $f_k\neq 0$. The fact that $P^\tau\circ f_\tau(T)=f_\tau\circ P(T)$ implies that $\tau(P'(0))f_k=f_kP'(0)^k$ so that $\tau(P'(0))=P'(0)^k$. Since $\mathrm{val}_K(P'(0))>0$, this implies that $k=1$. □

Corollary 5.8. — *The set of those $\tau\in\mathrm{Gal}(K/\mathbf{Q}_p)$ such that $r_\tau\geqslant 1$ forms a subgroup of $\mathrm{Gal}(K/\mathbf{Q}_p)$, and if F is the subfield of K cut out by this subgroup, then $\eta(g)\in\mathcal{O}_F^\times$. The weight r_τ is independent of $\tau\in\mathrm{Gal}(K/F)$.*

Proof. — By proposition 4.3, $\tau=\mathrm{Id}$ satisfies condition (iii) of proposition 5.6 above, and therefore condition (i) as well, so that $r_{\mathrm{Id}}\geqslant 1$. If σ,τ satisfy condition (v) of ibid, then we can write $u_\sigma=f_\sigma(\varphi_d^{-j_\sigma}(u))$ and $u_\tau=f_\tau(\varphi_d^{-j_\tau}(u))$ so that $u_{\sigma\tau}=f_\tau^\sigma\circ f_\sigma(\varphi_d^{-(j_\tau+j_\sigma)}(u))$ and therefore $\sigma\tau$ also satisfies condition (v). Since $\mathrm{Gal}(K/\mathbf{Q}_p)$ is a finite group, these two facts imply that the set of $\tau\in\mathrm{Gal}(K/\mathbf{Q}_p)$ such that $r_\tau\geqslant 1$ is a group.

By lemma 5.7, we have $P^\tau\circ f_\tau(T)=f_\tau\circ P(T)$. This implies that $P'(0)\in\mathfrak{m}_F$ and also that $(P^\tau)^{\circ n}\circ f_\tau(T)=f_\tau\circ P^{\circ n}(T)$, so that

$$\frac{1}{P'(0)^n}(P^\tau)^{\circ n}\circ f_\tau(T)=\frac{1}{P'(0)^n}f_\tau\circ P^{\circ n}(T),$$

which implies by passing to the limit that $\mathrm{L}_P^\tau\circ f_\tau(T)=f_\tau'(0)\cdot\mathrm{L}_P(T)$. Since $\mathrm{Col}_g^\tau\circ f_\tau(T)=f_\tau\circ\mathrm{Col}_g(T)$, we have $g(\mathrm{L}_P^\tau\circ f_\tau(u))=\tau(\eta(g))\cdot(\mathrm{L}_P^\tau\circ f_\tau(u))$. Moreover, $\mathrm{L}_P^\tau\circ f_\tau(u)=f_\tau'(0)\cdot\mathrm{L}_P(u)$, and therefore $\tau(\eta(g))=\eta(g)$. This is true for every $\tau\in\mathrm{Gal}(K/F)$, so that $\eta(g)\in\mathcal{O}_F^\times$. The fact that $\eta(g)\in\mathcal{O}_F^\times$ implies that r_τ depends only on $\tau|_F$ and is therefore independent of $\tau\in\mathrm{Gal}(K/F)$. □

6. Local class field theory

We now prove theorem D, and show how local class field theory allows us to derive theorem A from theorem D. We still assume that $K/\mathbf{Q}_p$ is Galois for simplicity. Let λ be a uniformizer of $\mathcal{O}_K$ and let K_λ denote the extension of K attached to λ by local class field theory. This extension is generated over K by the torsion points of a Lubin-Tate formal group defined over K and attached to λ (see for instance [**LT65**] and [**Ser67**]). Let $\chi_\lambda^K : \mathrm{Gal}(K_\lambda/K) \to \mathcal{O}_K^\times$ denote the corresponding Lubin-Tate character.

We still assume that the extension K_∞/K is Galois, so that it is an abelian totally ramified extension. This implies that there is a uniformizer λ of $\mathcal{O}_K$ such that $K_\infty \subset K_\lambda$. Let $\eta : \Gamma \to \mathcal{O}_K^\times$ be the character constructed in §5.

Proposition 6.1. — *We have* $\eta = \prod_{\tau \in \mathrm{Gal}(K/\mathbf{Q}_p)} \tau(\chi_\lambda^K)^{r_\tau}$.

Proof. — The character $\eta : \Gamma \to \mathcal{O}_K^\times$ is crystalline, and its weight at τ is r_τ by definition. The character $\eta_0 = \eta \cdot (\prod_{\tau \in \mathrm{Gal}(K/\mathbf{Q}_p)} \tau(\chi_\lambda^K)^{r_\tau})^{-1}$ of $\mathrm{Gal}(K_\lambda/K)$ is therefore crystalline with weights 0 at all embeddings, so that it is an unramified character of $\mathrm{Gal}(K_\lambda/K)$. Since K_λ/K is totally ramified, we have $\eta_0 = 1$. □

Proposition 6.1 and corollary 5.8 imply the following, which is theorem D.

Theorem 6.2. — *There exists* $F \subset K$ *and* $r \in \mathbf{Z}_{\geqslant 1}$ *such that* $\eta = \mathrm{N}_{K/F}(\chi_\lambda^K)^r$.

We now show how this implies theorem A. If $u \in \mathcal{O}_K^\times$, let μ_u^K denote the unramified character of G_K that sends the Frobenius map of k_K to u. If F is a subfield of K, and $\mathrm{N}_{K/F}(\lambda) = \varpi^h u$ with ϖ a uniformizer of $\mathcal{O}_F$ and some $u \in \mathcal{O}_F^\times$, then $\mathrm{N}_{K/F}(\chi_\lambda^K) = \chi_\varpi^F \cdot \mu_u^K$.

Proposition 6.3. — *Let* S *be a relative Lubin-Tate group, attached to an extension* E/F*, and an element* $\alpha = \varpi^h u \in \mathcal{O}_F^\times$*. The action of* $\mathrm{Gal}(\overline{\mathbf{Q}}_p/E)$ *on the torsion points of* S *is given by* $g(x) = [\chi_\varpi^F \cdot \mu_u^E(g)](x)$.

Proof. — See §4 of [**Yos08**]. □

Let F be the subfield of K afforded by theorem 6.2, and let E be the maximal unramified extension of F contained in K.

Theorem 6.4. — *There exists a relative Lubin-Tate group* S*, relative to the extension* E/F*, such that if* K_∞^{S} *denotes the extension of* K *generated by the torsion points of* S*, then* $K_\infty \subset K_\infty^{\mathrm{S}}$ *and* $K_\infty^{\mathrm{S}}/K_\infty$ *is a finite extension.*

Proof. — Let λ be a uniformizer of K such that $K_\infty \subset K_\lambda$ and let $\pi = \mathrm{N}_{K/E}(\lambda)$ and $\alpha = \mathrm{N}_{K/F}(\lambda)$, so that π is a uniformizer of E and $\alpha = \mathrm{N}_{E/F}(\pi)$. Let S be a relative Lubin-Tate group attached to α, and let K_∞^{S} be the extension of K generated by the torsion points of S. If $g \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/K_\infty^{\mathrm{S}})$, then $\mathrm{N}_{K/F}(\chi_K)(g) = 1$ by proposition 6.3 and the observation preceding it, so that $\eta(g) = 1$ by theorem 6.2. This implies that $K_\infty \subset K_\infty^{\mathrm{S}}$. By Galois theory and theorem 6.2,

1. K_∞^{S} is the field cut out by $\{g \in G_K \mid \mathrm{N}_{K/F}(\chi_\lambda^K(g)) = 1\}$;
2. K_∞ is the field cut out by $\{g \in G_K \mid \mathrm{N}_{K/F}(\chi_\lambda^K(g))^r = 1\}$.

This implies that $K_\infty^{\mathrm{S}}/K_\infty$ is a finite Galois extension, whose Galois group injects into $\{x \in \mathcal{O}_F^\times \mid x^r = 1\}$. □

This proves theorem A. We conclude this § with an example of a φ-iterate extension that is Galois, corresponding to a polynomial $P(T) \in \mathbf{Q}_p[T]$ such that $r = 2$ and such that the extension $K_\infty^{\mathrm{S}}/K_\infty$ is of degree 2 in the notation of theorems 6.2 and 6.4.

Theorem 6.5. — *Let $K = \mathbf{Q}_3$, $P(T) = T^3 + 6T^2 + 9T$ and $u_0 = -3$. The corresponding iterated extension K_∞ is $\mathbf{Q}_3(\mu_{3^\infty})^{\{\pm 1\} \subset \mathbf{Z}_3^\times}$, and $\eta = \chi_{\mathrm{cyc}}^2$.*

Proof. — For $k \geqslant 1$, let $C_k(T)$ denote the k-th Chebyshev polynomial, which is characterized by the fact that $C_k(\cos(\theta)) = \cos(k\theta)$. Let $P_k(T) = 2(C_k(T/2+1) - 1)$, so that $P_k(T)$ is a monic polynomial of degree k, and $P_k(2(\cos(\theta) - 1)) = 2(\cos(k\theta) - 1)$. Note that $P(T) = P_3(T)$ and that $u_0 = -3 = 2(\cos(2\pi/3) - 1)$. The element u_n is therefore a conjugate of $2(\cos(2\pi/3^{n+1}) - 1)$. This proves the fact that $K_\infty = \mathbf{Q}_3(\mu_{3^\infty})^{\{\pm 1\} \subset \mathbf{Z}_3^\times}$

If $g \in G_{\mathbf{Q}_3}$, then $g(2(\cos(2\pi/3^n) - 1) = 2(\cos(2\pi\chi_{\mathrm{cyc}}(g)/3^n) - 1)$. This implies that $\mathrm{Col}_g(T) = P_k(T)$ if $\chi_{\mathrm{cyc}}(g) = k \in \mathbf{Z}_{\geqslant 1}$. The formula for η now follows from this, and the well-known fact that $C_k'(1) = k^2$ if $k \geqslant 1$. □

We leave to the reader the generalization of this construction to other p and other Lubin-Tate groups. The results of §2 of [**LMS02**] should be useful for this.

References

[AHM05] W. Aitken, F. Hajir & C. Maire – "Finitely ramified iterated extensions", *Int. Math. Res. Not.* (2005), no. 14, p. 855–880.

[Ber02] L. Berger – "Représentations p-adiques et équations différentielles", *Invent. Math.* **148** (2002), no. 2, p. 219–284.

[Ber14] ———, "Lifting the field of norms", *J. École polytechnique - Math.* **1** (2014), p. 29–38.

[BJ07] N. Boston & R. Jones – "Arboreal Galois representations", *Geom. Dedicata* **124** (2007), p. 27–35.

[CD14] B. Cais & C. Davis – "Canonical Cohen rings for norm fields", *Int. Math. Res. Not. IMRN* (2014), Art. ID: rnu098, 45.

[CDL14] B. Cais, C. Davis & J. Lubin – "A characterization of strictly APF extensions", to appear in the Journal de Théorie des Nombres de Bordeaux, 2014.

[Col79] R. Coleman – "Division values in local fields", *Invent. Math.* **53** (1979), no. 2, p. 91–116.

[Col02] P. Colmez – "Espaces de Banach de dimension finie", *J. Inst. Math. Jussieu* **1** (2002), no. 3, p. 331–439.

[dS85] E. de Shalit – "Relative Lubin-Tate groups", *Proc. Amer. Math. Soc.* **95** (1985), no. 1, p. 1–4.

[Fon90] J.-M. Fontaine – "Représentations p-adiques des corps locaux. I", in *The Grothendieck Festschrift, Vol. II*, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, p. 249–309.

[Fon94] ———, "Le corps des périodes p-adiques", *Astérisque* (1994), no. 223, p. 59–111, With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988).

[Iwa86] K. Iwasawa – *Local class field theory*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1986, Oxford Mathematical Monographs.

[LMS02] F. Laubie, A. Movahhedi & A. Salinier – "Systèmes dynamiques non archimédiens et corps des normes", *Compositio Math.* **132** (2002), no. 1, p. 57–98.

[LT65] J. Lubin & J. Tate – "Formal complex multiplication in local fields", *Ann. of Math. (2)* **81** (1965), p. 380–387.

[Lub94] J. Lubin – "Non-Archimedean dynamical systems", *Compositio Math.* **94** (1994), no. 3, p. 321–346.

[Odo85] R. Odoni – "The Galois theory of iterates and composites of polynomials", *Proc. London Math. Soc. (3)* **51** (1985), no. 3, p. 385–414.

[Ser67] J.-P. Serre – "Local class field theory", in *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, Thompson, Washington, D.C., 1967, p. 128–161.

[SS13] G. Sarkis & J. Specter – "Galois extensions of height-one commuting dynamical systems", *J. Théor. Nombres Bordeaux* **25** (2013), no. 1, p. 163–178.

[JS14] J. Specter – "The crystalline period of a height one p-adic dynamical system", preprint, 2014.

[Sto92] M. Stoll – "Galois groups over $\mathbf{Q}$ of some iterated polynomials", *Arch. Math. (Basel)* **59** (1992), no. 3, p. 239–244.

[Was97] L. Washington – *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[Win83] 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, p. 59–89.

[Yos08] T. Yoshida – "Local class field theory via Lubin-Tate theory", *Ann. Fac. Sci. Toulouse Math. (6)* **17** (2008), no. 2, p. 411–438.

Laurent Berger