ÉCOLE POLYTECHNIQUE
UNIVERSITÉ PARIS-SACLAY

Journal de l'École polytechnique
Mathématiques

Laurent Berger

Lifting the field of norms

Tome 1 (2014), p. 29-38.

<http://jep.cedram.org/item?id=JEP_2014__1__29_0>

Journal de l'École polytechnique
Mathématiques
Tome 1, 2014, p. 29–38 DOI: 10.5802/jep.2

LIFTING THE FIELD OF NORMS

by Laurent Berger

Abstract. — Let K be a finite extension of $\mathbf{Q}_p$. The field of norms of a p-adic Lie extension K_∞/K is a local field of characteristic p which comes equipped with an action of $\mathrm{Gal}(K_\infty/K)$. When can we lift this action to characteristic 0, along with a compatible Frobenius map? In this note, we formulate precisely this question, explain its relevance to the theory of (φ,Γ)-modules, and give a condition for the existence of certain types of lifts.

Résumé (Relèvement du corps des normes). — Soit K une extension finie de $\mathbf{Q}_p$. Le corps des normes d'une extension de Lie p-adique K_∞/K est un corps local de caractéristique p muni d'une action de $\mathrm{Gal}(K_\infty/K)$. Quand peut-on relever cette action en caractéristique nulle, en même temps qu'une application de Frobenius compatible ? Dans cette note, nous formulons de manière précise cette question, expliquons son intérêt pour la théorie des (φ,Γ)-modules et donnons une condition pour l'existence de certains types de relèvements.

Contents

Introduction

Let K be a finite extension of $\mathbf{Q}_p$ and let K_∞/K be a totally ramified Galois extension whose Galois group Γ_K is a p-adic Lie group (or, more generally, a "strictly arithmetically profinite" extension). Let k_K denote the residue field of K. We can attach to K_∞/K its field of norms $X_K(K_\infty)$, a field of characteristic p that is isomorphic to $k_K(\!(\pi)\!)$ and equipped with an action of Γ_K. Let E be a finite extension of $\mathbf{Q}_p$ such that $k_E = k_K$. In this note, we consider the question: when can we lift the action

Mathematical subject classification (2010). — 11S15, 11S20, 11S25, 11S31, 11S82, 13F25.
Keywords. — Field of norms, (φ,Γ)-module, p-adic representation, anticyclotomic extension, Cohen ring, non-Archimedean dynamical system.

of Γ_K on $k_K(\!(\pi)\!)$ to the p-adic completion of $\mathcal{O}_E[\![T]\!][1/T]$, which is a complete ring of characteristic 0 that lifts $X_K(K_\infty)$, along with a compatible $\mathcal{O}_E$-linear Frobenius map φ_q? When it is possible to do so, we say that the action of Γ_K is *liftable*. In this case, Fontaine's construction of (φ,Γ)-modules applies, and we get the following well-known equivalence of categories (where $\mathbf{A}_K$ denotes the p-adic completion of $\mathcal{O}_E[\![T]\!][1/T]$).

Theorem A. — *If the action of Γ_K is liftable, then there is an equivalence of categories*

$$\{(\varphi_q,\Gamma_K)\text{-modules on } \mathbf{A}_K\} \longleftrightarrow \{\mathcal{O}_E\text{-linear representations of } G_K\}.$$

Such a lift is possible when K_∞/K is the cyclotomic extension, or more generally when K_∞ is generated by the torsion points of a Lubin-Tate formal $\mathcal{O}_F$-module for some $F \subset K$. In §4 of this note, we prove the following partial converse.

Theorem B. — *If the action of Γ_K is liftable with $\varphi_q(T) \in \mathcal{O}_E[\![T]\!]$, then Γ_K is abelian, and there is an injective character $\Gamma_K \to \mathcal{O}_E^\times$, whose conjugates by $\mathrm{Emb}(E,\overline{\mathbf{Q}}_p)$ are all de Rham with weights in $\mathbf{Z}_{\geqslant 0}$.*

At the end of §4, we give some examples of constraints on the extension K_∞/K arising from the existence of such a character.

Some preliminary computations suggest that a similar result may hold in certain cases if we assume that $\varphi_q(T)$ is an overconvergent power series in T. However at this point, I do not know for which extensions we can expect the action of Γ_K to be liftable in general.

The initial motivation for thinking about this problem was the question of whether there is a theory of "anticyclotomic (φ,Γ)-modules", that is, a theory of (φ,Γ)-modules where Γ is the Galois group of the anticyclotomic extension K_∞^{ac}/K of $K = \mathbf{Q}_{p^2}$. Theorem B implies that there is no such theory if in addition we require that $\varphi_q(T) \in \mathcal{O}_K[\![T]\!]$.

Acknowledgements. — Thanks to Kâzım Büyükboduk for asking me about universal norms in the anticyclotomic tower, which started this train of thought. Thanks to Jean-Marc Fontaine for some useful discussions on this topic, in particular for a remark that led to Theorem B above. Thanks to Bryden Cais and Christopher Davis for their comments about the first version of this note, to Sandra Rozensztajn for Remark 4.9, and to the two referees for pointing out some inaccuracies and suggesting some improvements.

1. Lifting the field of norms

Let K be a finite extension of $\mathbf{Q}_p$ and let K_∞ be an infinite and totally ramified Galois extension of K that is "strictly arithmetically profinite" (see §1.2.1 of [Win83] for the definition, which we don't use; *arithmetically profinite* means that the ramification subgroups Γ_K^u of Γ_K are open and strictness is an additional condition). Note that if $\Gamma_K = \mathrm{Gal}(K_\infty/K)$ is a p-adic Lie group, then as recalled in §1.2.2 of [Win83], it follows from the main theorem of [Sen72] that K_∞/K is strictly arithmetically profinite.

We can apply to K_∞/K the "field of norms" construction of [FW79a, FW79b] and [Win83], which we now recall. Let $\mathcal{F}$ denote the set of finite extensions F of K that are contained in K_∞, and let $X_K(K_\infty)$ denote the set of sequences $(x_F)_{F\in\mathcal{F}}$ such that $\mathrm{N}_{F_2/F_1}(x_{F_2}) = x_{F_1}$ whenever $F_1 \subset F_2$. By the results of §2 of [Win83], one can endow $X_K(K_\infty)$ with the structure of a field, a field embedding of $k_K = k_{K_\infty}$ in $X_K(K_\infty)$, and a valuation $\mathrm{val}(\cdot)$ (where $\mathrm{val}(x)$ is the common value of the $\mathrm{val}_F(x_F)$ for $F \in \mathcal{F}$). We then have the following theorem (theorem 2.1.3 of [Win83]).

Theorem 1.1. — *The field $X_K(K_\infty)$ is a complete valued field with residue field k_K.*

If π_K denotes a uniformizer of $X_K(K_\infty)$, then $X_K(K_\infty) = k_K(\!(\pi_K)\!)$. The group Γ_K acts on $X_K(K_\infty)$. If $q = \mathrm{Card}(k_K)$, then we have the k_K-linear Frobenius map $\varphi_q : X_K(K_\infty) \to X_K(K_\infty)$ given by $x \mapsto x^q$, and it commutes with the action of Γ_K.

Let E be a finite extension of $\mathbf{Q}_p$ such that $k_E = k_K$, let ϖ_E be a uniformizer of E and let $\mathbf{A}_K$ denote the ϖ_E-adic completion of $\mathcal{O}_E[\![T]\!][1/T]$. The ring $\mathbf{A}_K$ is a ϖ_E-Cohen ring for $X_K(K_\infty)$, that is a complete discrete valuation ring whose maximal ideal is generated by ϖ_E and whose residue field is $X_K(K_\infty)$. The question that we want to ask is: when can we lift the action of Γ_K on $X_K(K_\infty)$ to an $\mathcal{O}_E$-linear action on $\mathbf{A}_K$, along with a compatible $\mathcal{O}_E$-linear Frobenius lift?

Question 1.2. — *Do there exist power series $\{F_g(T)\}_{g\in\Gamma_K}$ and $P(T)$ in $\mathbf{A}_K$, such that*

(1) $\overline{F}_g(\pi_K) = g(\pi_K)$ *and* $\overline{P}(\pi_K) = \pi_K^q$ *in* $k_K(\!(\pi_K)\!)$,

(2) $F_g \circ P = P \circ F_g$ *and* $F_h \circ F_g = F_{gh}$ *whenever* $g, h \in \Gamma_K$*?*

If the answer to this question is "yes", then we say that the action of Γ_K is liftable.

If K is unramified over $\mathbf{Q}_p$ and $K_\infty = K(\mu_{p^\infty})$ is the cyclotomic extension, then the action of Γ_K is liftable, since for the uniformizer $\pi_K = ((\zeta_{p^n} - 1)_{K(\zeta_{p^n})})_{n\geqslant 1}$ we can take $P(T) = (1+T)^p - 1$ and $F_g(T) = (1+T)^{\chi_{\mathrm{cyc}}(g)} - 1$. More generally, if K_∞/K is the extension generated by the torsion points of a Lubin-Tate formal $\mathcal{O}_F$-module, with K/F unramified, then the action of Γ_K is liftable with $P(T) = [\varpi_F](T)$ and $F_g(T) = [g](T)$ in appropriate coordinates.

Write $\mathbf{E}_K$ for the field $X_K(K_\infty)$ (this notation is somewhat standard, but unfortunate considering the fact that $\mathbf{E}_K$ depends on K_∞ but not on K). Recall that every finite separable extension of $\mathbf{E}_K$ is of the form $\mathbf{E}_L$, where L is a finite extension of K (§3.2 of [Win83]), and that there corresponds to the extension $\mathbf{E}_L/\mathbf{E}_K$ a unique étale extension of ϖ_E-rings $\mathbf{A}_L/\mathbf{A}_K$. Indeed, if $\mathbf{E}_L = \mathbf{E}_K[X]/Q(X)$ we can take $\mathbf{A}_L = \mathbf{A}_K[X]/\widetilde{Q}(X)$, where $\widetilde{Q}$ is a unitary polynomial that lifts Q, and the resulting ring depends only on $Q(X)$ by Hensel's lemma.

Theorem 1.3. — *Let L be a finite extension of K and let $L_\infty = LK_\infty$. If the action of Γ_K on $\mathbf{E}_K$ is liftable, then the action of Γ_L on $\mathbf{E}_L$ is liftable.*

Proof. — Note that Γ_L injects into Γ_K. Since $\mathbf{A}_L/\mathbf{A}_K$ is étale, the Frobenius map φ_q and the action of $g \in \Gamma_K$ extend to $\mathbf{A}_L$ (for example, if $x \in \mathbf{A}_L$ satisfies $Q(x) = 0$ with $Q(X) \in \mathbf{A}_K[X]$ unitary, then $(gQ)(g(x)) = 0$ has a solution in $\mathbf{A}_L$ by Hensel's lemma). There exists an element $T_L \in \mathbf{A}_L$ lifting π_L such that $\mathbf{A}_L$ is the ϖ_E-adic completion of $\mathcal{O}_E[\![T_L]\!][1/T_L]$. We can take $F_g(T_L) = g(T_L)$ and $P(T_L) = \varphi_q(T_L)$. Note that if L_∞/K_∞ is not totally ramified, then we may need to replace E by a larger unramified extension of degree d, and φ_q by φ_q^d accordingly. □

Even in the case of cyclotomic extensions, the series $F_g(T)$ and $P(T)$ can be quite complicated if L/K is ramified. For example, suppose that $\pi_L = \pi_K^{1/n}$ with $p \nmid n$ (this corresponds to a tamely ramified extension L/K). We can then take $T_L = T_K^{1/n}$ and

$$\varphi(T_L) = ((1+T_K)^p - 1)^{1/n} = T_L^p \cdot \Big(1 + \frac{p}{T_L^n} + \cdots + \frac{p}{T_L^{n(p-1)}}\Big)^{1/n},$$

so that $P(T_L)$ is overconvergent but does not belong to $\mathcal{O}_E[\![T_L]\!]$.

Theorem 1.4. — *Let $F_\infty \subset K_\infty$ be a Galois subextension such that K_∞/F_∞ is finite, and let $\Gamma_F = \mathrm{Gal}(F_\infty/K)$. If the action of Γ_K on $\mathbf{E}_K$ is liftable, then the action of Γ_F on $\mathbf{E}_F$ is liftable.*

Proof. — We check that the action of Γ_F lifts to $\mathbf{A}_F = \mathbf{A}_K^{\mathrm{Gal}(K_\infty/F_\infty)}$. The ring $\mathbf{A}_F$ is stable under Γ_F and φ_q by construction, and its image in $\mathbf{E}_K$ is $\mathbf{E}_F$ since $\mathbf{A}_F$ contains both $\mathcal{O}_E$ and $\mathrm{N}_{K_\infty/F_\infty}(T)$. □

2. Application to (φ, Γ)-modules

One reason for asking Question 1.2 is that it is relevant to the theory of (φ, Γ)-modules for $\mathcal{O}_E$-representations of G_K. This theory has been developed in [Fon90] when $K_\infty = K(\mu_{p^\infty})$, but it can easily be generalized to other extensions K_∞/K for which the action of Γ_K is liftable, as was observed for example in §2.1 of [Sch06]. For instance, the generalization to Lubin-Tate extensions is explicitly carried out in §1 of [KR09] and is further discussed in [FX13] and [CE14]. Let $\mathbf{A}$ be the ϖ_E-adic completion of $\varinjlim_L \mathbf{A}_L$, where L runs through the set of finite extensions of K. Let $H_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K_\infty)$.

Theorem 2.1. — *If the action of Γ_K is liftable, then there is an equivalence of categories*

$$\{(\varphi_q, \Gamma_K)\text{-modules on } \mathbf{A}_K\} \longleftrightarrow \{\mathcal{O}_E\text{-linear representations of } G_K\},$$

given by the mutually inverse functors $\mathrm{D} \mapsto (\mathbf{A} \otimes_{\mathbf{A}_K} \mathrm{D})^{\varphi_q=1}$ *and* $V \mapsto (\mathbf{A} \otimes_{\mathcal{O}_E} V)^{H_K}$.

Proof. — The proof follows §A.1.2 and §A.3.4 of [Fon90] as well as §2.1 of [Sch06], and we sketch it here. Note that $\mathbf{A}^{\varphi_q=1} = \mathcal{O}_E$ since $q = \mathrm{Card}(k_E)$. Let $\mathbf{E} = \mathbf{E}_K^{\mathrm{sep}}$, so that $\mathbf{A}/\varpi_E\mathbf{A} = \mathbf{E}$.

The theory of φ-modules tells us that if M is a φ_q-module over $\mathbf{E}$, then $M = \mathbf{E} \otimes_{k_E} M^{\varphi_q=1}$ and that $1 - \varphi_q : M \to M$ is surjective. These two facts imply that if D is a φ_q-module over $\mathbf{A}_K$, then $\mathbf{A} \otimes_{\mathbf{A}_K} D = \mathbf{A} \otimes_{\mathcal{O}_E} V(D)$ with $V(D) = (\mathbf{A} \otimes_{\mathbf{A}_K} D)^{\varphi_q=1}$.

Conversely, Hilbert's Theorem 90 says that $H^1(\mathrm{Gal}(\mathbf{E}/\mathbf{E}_K), \mathrm{GL}_d(\mathbf{E}))$ is trivial for all $d \geqslant 1$. The theory of the field of norms gives us an isomorphism between $\mathrm{Gal}(\mathbf{E}/\mathbf{E}_K)$ and H_K (§3.2 of [Win83]). By dévissage, this implies that if V is an $\mathcal{O}_E$-representation of H_K, then $\mathbf{A} \otimes_{\mathcal{O}_E} V = \mathbf{A} \otimes_{\mathbf{A}_K} D(V)$ where $D(V) = (\mathbf{A} \otimes_{\mathcal{O}_E} V)^{H_K}$.

These two facts imply that the functors of the theorem are mutually inverse. □

3. Embeddings into rings of periods

We now explain how to view the different rings whose construction we have recalled as subrings of some of Fontaine's rings of periods (constructed for example in [Fon94a]). Let I be the ideal of elements of $\mathcal{O}_{\mathbf{C}_p}$ with valuation at least $1/p$. Let $\widetilde{\mathbf{E}}$ denote the fraction field of $\widetilde{\mathbf{E}}^+ = \varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbf{C}_p}/I$. Set $\widetilde{\mathbf{E}}_K = \widetilde{\mathbf{E}}^{H_K}$. By §4.2 of [Win83], there is a canonical G_K-equivariant embedding $X_K(K_\infty) \to \widetilde{\mathbf{E}}_K$ and we also denote its image by $\mathbf{E}_K$.

Let $W_E(\cdot) = \mathcal{O}_E \otimes_{\mathcal{O}_{E_0}} W(\cdot)$ denote the ϖ_E-Witt vectors. Let $\widetilde{\mathbf{A}} = W_E(\widetilde{\mathbf{E}})$, and endow it with the $\mathcal{O}_E$-linear Frobenius map φ_q and the $\mathcal{O}_E$-linear action of G_K coming from those on $\widetilde{\mathbf{E}}$. These are well-defined since $E_0 \subset K$. Let $\widetilde{\mathbf{A}}_K = \widetilde{\mathbf{A}}^{H_K}$ so that $\widetilde{\mathbf{A}}_K = W_E(\widetilde{\mathbf{E}}_K)$. If $\mathbf{A}_K$ is equipped with a lift of the action of Γ_K and a commuting Frobenius map φ_q, then there is an embedding $\mathbf{A}_K \to \widetilde{\mathbf{A}}_K$ that is compatible with φ_q, Γ_K-equivariant, and lifts the embedding $\mathbf{E}_K \to \widetilde{\mathbf{E}}_K$. See §A.1.3 of [Fon90] for a proof, or simply remark that since $\mathbf{A}_K$ is the ϖ_E-adic completion of $\mathcal{O}_E[\![T]\!][1/T]$, it is enough to show that there exists one and only one element $v \in \widetilde{\mathbf{A}}_K$ (the image of T) that lifts π_K and satisfies $\varphi_q(v) = P(v)$. This now follows from the fact that if S denotes the set of elements of $\widetilde{\mathbf{A}}_K$ whose image in $\widetilde{\mathbf{E}}_K$ is π_K, then $x \mapsto \varphi_q^{-1}(P(x))$ is a contracting map on S. Let $v \in \widetilde{\mathbf{A}}_K$ be the image of T as above, so that $\varphi_q(v) = P(v)$ and $g(v) = F_g(v)$ for all $g \in \Gamma_K$. Note that $\overline{v} = \pi_K \in \widetilde{\mathbf{E}}^+$. Let $\widetilde{\mathbf{A}}^+ = W_E(\widetilde{\mathbf{E}}^+)$

Lemma 3.1. — *If $P(T) \in \mathcal{O}_E[\![T]\!]$, then $v \in \widetilde{\mathbf{A}}^+$.*

Proof. — We have $v - [\overline{v}] \in \varpi_E \widetilde{\mathbf{A}}$ so that $v \in \widetilde{\mathbf{A}}^+ + \varpi_E \widetilde{\mathbf{A}}$. Suppose that $v \in \widetilde{\mathbf{A}}^+ + \varpi_E^k \widetilde{\mathbf{A}}$ for some $k \geqslant 1$. We have $P(T) \in T^q + \mathfrak{m}_E[\![T]\!]$. This implies that $P(v) \in \widetilde{\mathbf{A}}^+ + \varpi_E^{k+1} \widetilde{\mathbf{A}}$ and hence also $v = \varphi_q^{-1}(P(v)) \in \widetilde{\mathbf{A}}^+ + \varpi_E^{k+1} \widetilde{\mathbf{A}}$. By induction on k, we get $v \in \widetilde{\mathbf{A}}^+$. □

In §4, we use the fact that if L contains K and E, then $\widetilde{\mathbf{A}}^+$ injects into $\mathbf{B}_{\mathrm{dR}}^+$ in a G_L-equivariant way. We also use the following lemma about $\mathbf{B}_{\mathrm{dR}}^+$.

Lemma 3.2. — *Let E be a finite extension of $\mathbf{Q}_p$ and take $f(T) \in E[\![T]\!]$. If $x \in \mathbf{B}_{\mathrm{dR}}^+$, then the series $f(x)$ converges in $\mathbf{B}_{\mathrm{dR}}^+$ if and only if the series $f(\theta(x))$ converges in $\mathbf{C}_p$.*

Proof. — We prove that the series converges in $\mathbf{B}_{\mathrm{dR}}^+/t^k$ for all $k \geqslant 1$. Recall that $\mathbf{B}_{\mathrm{dR}}^+/t^k$ is a Banach space, the unit ball being the image of $\widetilde{\mathbf{A}}^+ \to \mathbf{B}_{\mathrm{dR}}^+/t^k$. We can enlarge E so that it contains an element of valuation $\mathrm{val}_p(\theta(x))$ and it is then enough to prove that if $\theta(x) \in \mathcal{O}_{\mathbf{C}_p}$, then $\{x^n\}_{n\geqslant 0}$ is bounded in $\mathbf{B}_{\mathrm{dR}}^+/t^k$. Let ω be a generator of $\ker(\theta : \widetilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p})$ and let x_0 be an element of $\widetilde{\mathbf{A}}^+$ such that $\theta(x) = \theta(x_0)$. We can write $x = x_0 + \omega y + t^k z$ where $y \in \widetilde{\mathbf{A}}^+[1/p]$ and $z \in \mathbf{B}_{\mathrm{dR}}^+$. We then have

$$x^n = x_0^n + \binom{n}{1} x_0^{n-1}\omega y + \cdots + \binom{n}{k-1} x_0^{n-(k-1)}(\omega y)^{k-1} + t^k z_k,$$

with $z_k \in \mathbf{B}_{\mathrm{dR}}^+$, so that $x^n \in (\widetilde{\mathbf{A}}^+ + y\widetilde{\mathbf{A}}^+ + \cdots + y^{k-1}\widetilde{\mathbf{A}}^+) + t^k\mathbf{B}_{\mathrm{dR}}^+$ for all n. □

4. Lifts of finite height

In this section we prove Theorem B, which we now recall.

Theorem 4.1. — *If the action of Γ_K is liftable with $\varphi_q(T) \in \mathcal{O}_E[\![T]\!]$, then Γ_K is abelian, and there is an injective character $\Gamma_K \to \mathcal{O}_E^\times$, whose conjugates by $\mathrm{Emb}(E, \overline{\mathbf{Q}}_p)$ are all de Rham with weights in $\mathbf{Z}_{\geqslant 0}$.*

Before proving Theorem 4.1, we give a number of intermediate results to the effect that if $P(T) = \varphi_q(T)$ belongs to $\mathcal{O}_E[\![T]\!]$, then one can improve the regularity of the power series $P(T)$ and $F_g(T)$ for $g \in \Gamma_K$.

Proposition 4.2. — *If $P(T) \in \mathcal{O}_E[\![T]\!]$, then $F_g(T) \in T \cdot \mathcal{O}_E[\![T]\!]$ for all $g \in \Gamma_K$.*

Proof. — The ring $\mathbf{A}_K$ is a free $\varphi_q(\mathbf{A}_K)$-module of rank q. As in §2.3 of [Fon90], let $\mathcal{N} : \mathbf{A}_K \to \mathbf{A}_K$ denote the map

$$\mathcal{N} : f(T) \mapsto \varphi_q^{-1} \circ \mathrm{N}_{\mathbf{A}_K/\varphi_q(\mathbf{A}_K)}(f(T)).$$

If $P(T) \in \mathcal{O}_E[\![T]\!]$, then $\mathcal{N}(\mathcal{O}_E[\![T]\!]) \subset \mathcal{O}_E[\![T]\!]$ since the ring $\mathcal{O}_E[\![T]\!]$ is a free $\mathcal{O}_E[\![P(T)]\!]$-module of rank q. Furthermore, we have

$$\mathcal{N}(1 + \varpi_E^k \mathbf{A}_K) \subset 1 + \varpi_E^{k+1}\mathbf{A}_K \quad \text{if } k \geqslant 1$$

(see 2.3.2 of ibid). This implies that if $k \geqslant 1$, then

$$\mathcal{N}(\mathcal{O}_E[\![T]\!]^\times + \varpi_E^k \mathbf{A}_K) \subset \mathcal{O}_E[\![T]\!]^\times + \varpi_E^{k+1}\mathbf{A}_K,$$

and likewise, since $\mathcal{N}(T) = T$ and T is invertible in $\mathbf{A}_K$,

$$\mathcal{N}(T \cdot \mathcal{O}_E[\![T]\!]^\times + \varpi_E^k \mathbf{A}_K) \subset T \cdot \mathcal{O}_E[\![T]\!]^\times + \varpi_E^{k+1}\mathbf{A}_K.$$

This implies, by induction on k, that

$$(T \cdot \mathcal{O}_E[\![T]\!]^\times + \varpi_E \mathbf{A}_K)^{\mathcal{N}(x)=x} \subset T \cdot \mathcal{O}_E[\![T]\!]^\times.$$

We have $F_g(T) \in T \cdot \mathcal{O}_E[\![T]\!]^\times + \varpi_E \mathbf{A}_K$ and since $\mathcal{N}$ commutes with the action of Γ_K, we have $\mathcal{N}(g(T)) = g(T)$ and hence

$$F_g(T) \in (T \cdot \mathcal{O}_E[\![T]\!]^\times + \varpi_E \mathbf{A}_K)^{\mathcal{N}(x)=x} \subset T \cdot \mathcal{O}_E[\![T]\!]^\times.$$ □

Remark 4.3. — The same proof implies that if $P(T)$ is overconvergent, then so is $F_g(T)$.

Lemma 4.4. — *If $P(T) \in \mathcal{O}_E[\![T]\!]$, then there exists $a \in \mathfrak{m}_E$ such that if $T' = T - a$, then $\varphi_q(T') = Q(T')$ with $Q(T') \in T' \cdot \mathcal{O}_E[\![T']\!]$.*

Proof. — Let $R(T) = P(T + a)$. We have

$$\varphi_q(T') = \varphi_q(T - a) = P(T) - a = R(T') - a$$

so it is enough to find $a \in \mathfrak{m}_E$ such that $P(a) = a$. The Newton polygon of $P(T) - T$ starts with a segment of length 1 and slope $-\mathrm{val}_p(P(0))$, which gives us such an a with $\mathrm{val}_p(a) = \mathrm{val}_p(P(0))$. □

LEMMA 4.5. — *If $P(T) \in T \cdot \mathcal{O}_E[\![T]\!]$, then $P'(0) \neq 0$.*

Proof. — By proposition 4.2, we have $F_g(T) \in T \cdot \mathcal{O}_E[\![T]\!]$ for all $g \in \Gamma_K$. Write

$$F_g(T) = f_1(g)T + \mathrm{O}(T^2) \quad \text{and} \quad P(T) = \pi_k T^k + \mathrm{O}(T^{k+1})$$

with $\pi_k \neq 0$. Note that $g \mapsto f_1(g)$ is a character $f_1 : \Gamma_K \to \mathcal{O}_E^\times$. The equality $F_g(P(T)) = P(F_g(T))$ implies that $f_1(g)\pi_k = \pi_k f_1(g)^k$ so that if $k \neq 1$, then $f_1(g)^{k-1} = 1$.

In particular, taking g in the open subgroup $f_1^{-1}(1 + 2p\mathcal{O}_E)$ of Γ_K, we must have $f_1(g) = 1$. Take such a $g \in \Gamma_K \smallsetminus \{1\}$; since $\overline{F}_g(T) \neq T$, we can write $F_g(T) = T + T^i h(T)$ for some $i \geqslant 2$ with $h(0) \neq 0$. The equation $F_g(P(T)) = P(F_g(T))$ and the equality

$$P(T + T^i h(T)) = \sum_{j \geqslant 0} (T^i h(T))^j P^{(j)}(T)/j!$$

imply that

$$P(T) + P(T)^i h(P(T)) = P(T) + T^i h(T) P'(T) + \mathrm{O}(T^{2i+k-2}),$$

so that

$$P(T)^i h(P(T)) = T^i h(T) P'(T) + \mathrm{O}(T^{2i+k-2}).$$

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 $k = 1$. □

Proof of Theorem 4.1. — By the preceding results, if $P(T) \in \mathcal{O}_E[\![T]\!]$, then we can make a change of variable so that $P(T) \in T \cdot \mathcal{O}_E[\![T]\!]$ and $F_g(T) \in T \cdot \mathcal{O}_E[\![T]\!]$ for all $g \in \Gamma_K$. Write $P(T) = \sum_{k \geqslant 1} \pi_k T^k$. By lemma 4.5, we have $\pi_1 \neq 0$. If

$$A(T) = \sum_{k \geqslant 1} a_k T^k \in E[\![T]\!] \quad \text{with } a_1 = 1,$$

then the equation $A(P(T)) = \pi_1 \cdot A(T)$ is given by

$$P(T) + a_2 P(T)^2 + \cdots = \pi_1 \cdot (T + a_2 T^2 + \cdots).$$

Looking at the coefficient of T^k in the above equation, we get the equation

$$x_{k,1} a_1 + \cdots + x_{k,k-1} a_{k-1} = a_k(\pi_1 - \pi_1^k),$$

where $x_{k,i}$ is the coefficient of T^k in $P(T)^i$ and hence belongs to $\mathcal{O}_E$. This implies that the equation $A(P(T)) = \pi_1 \cdot A(T)$ has a unique solution in $E[\![T]\!]$, and that

$a_k \in \pi_1^{1-k} \cdot \mathcal{O}_E$. In particular, the power series $A(T)$ belongs to $\mathcal{O}_E[\![T/\pi_1]\!]$ and so has a nonzero radius of convergence. If $g \in \Gamma_K$, then we have

$$A(F_g(P(T))) = A(P(F_g(T))) = \pi_1 \cdot A(F_g(T)).$$

This implies that if $B(T) = f_1(g)^{-1} \cdot A(F_g(T))$, then $b_1 = 1$ and $B(P(T)) = \pi_1 \cdot B(T)$, so that $B(T) = A(T)$ and hence $A(F_g(T)) = f_1(g) \cdot A(T)$ for all $g \in \Gamma_K$. The map $g \mapsto f_1(g)$ is therefore injective, since $f_1(g) = 1$ implies that $F_g(T) = T$ so that $g = 1$.

We have seen in §3 that there is a map $\mathbf{A}_K \to \widetilde{\mathbf{A}}$ that commutes with φ_q and the action of G_K. Let $v \in \widetilde{\mathbf{A}}$ be the image of T. By lemma 3.1, $v \in \widetilde{\mathbf{A}}^+$. We have

$$\theta(v) \in \mathfrak{m}_{\mathbf{C}_p} \quad \text{and} \quad \theta(\varphi_q^m(v)) = \theta(P \circ \cdots \circ P(v)),$$

and so there exists $m_0 \geqslant 0$ such that $\theta(\varphi_q^m(v))$ belongs to the domain of convergence of $A(T)$ if $m \geqslant m_0$. By lemma 3.2, the series $A(\varphi_q^m(v))$ converges in $(\mathbf{B}_{\mathrm{dR}}^+)^{H_L}$, where $L = KE$, and if $g \in G_L$ we have

$$g(A(\varphi_q^m(v))) = A(F_g(\varphi_q^m(v))) = f_1(g) \cdot A(\varphi_q^m(v)).$$

We now show that $A(\varphi_q^m(v)) \neq 0$ for some $m \geqslant m_0$. If $\theta(\varphi_q^m(v)) = 0$ for some m, then $\varphi_q^m(v) \in \mathrm{Fil}^k \smallsetminus \mathrm{Fil}^{k+1}\mathbf{B}_{\mathrm{dR}}^+$ for some $k \geqslant 1$, and then $A(\varphi_q^m(v)) \in \mathrm{Fil}^k \smallsetminus \mathrm{Fil}^{k+1}\mathbf{B}_{\mathrm{dR}}^+$ as well, so that $A(\varphi_q^m(v)) \neq 0$. If $\theta(\varphi_q^m(v)) \neq 0$ for all $m \geqslant m_0$, then the sequence $\{\theta(\varphi_q^m(v))\}_{m \geqslant m_0}$ converges to zero in $\mathbf{C}_p$ and if $A(\varphi_q^m(v)) = 0$ for all $m \geqslant m_0$, then $A(\theta(\varphi_q^m(v))) = 0$ for all $m \geqslant m_0$ and this implies that $A(T) = 0$ since 0 would not be an isolated zero of $A(T)$. Hence there is some $m \geqslant m_0$ such that $A(\varphi_q^m(v)) \neq 0$, and the equality $g(A(\varphi_q^m(v))) = f_1(g) \cdot A(\varphi_q^m(v))$ if $g \in G_L$ implies that the character $g \mapsto f_1(g)$ is de Rham and that its weight is in $\mathbf{Z}_{\geqslant 0}$.

The conjugates of $g \mapsto f_1(g)$ are treated in the same way. If $h \in \mathrm{Emb}(E, \overline{\mathbf{Q}}_p)$, then choose some $n(h) \in \mathbf{Z}$ such that $h = [x \mapsto x^p]^{n(h)}$ on k_E so that $h = \varphi^{n(h)}$ on $\mathcal{O}_{E_0}$. Define an element $h(v) \in W_{h(E)}(\widetilde{\mathbf{E}}^+)$ by the formula

$$h(e \otimes a) = h(e) \otimes \varphi^{n(h)}(a).$$

If $v \in W_E(\widetilde{\mathbf{E}}^+)$ satisfies $\varphi_q(v) = P(v)$ and $g(v) = F_g(v)$ for $g \in \Gamma_K$, then

$$\varphi_q(h(v)) = P^h(h(v)) \quad \text{and} \quad g(h(v)) = F_g^h(h(v)).$$

The same reasoning as above now implies that the character $g \mapsto h(f_1(g))$ is de Rham and that its weight is in $\mathbf{Z}_{\geqslant 0}$. □

Example 4.6. — If $E = \mathbf{Q}_p$, then Theorem B implies that $K_\infty \subset \mathbf{Q}_p^{\mathrm{ab}} \cdot L$ where L is a finite extension of K. Indeed, every de Rham character $\eta : G_K \to \mathbf{Z}_p^\times$ is of the form $\chi_{\mathrm{cyc}}^r \cdot \mu$ for some $r \in \mathbf{Z}$ and some potentially unramified character μ (see §3.9 of [Fon94b]).

More generally, the condition that there is an injective character $\eta : \Gamma_K \to \mathcal{O}_E^\times$, whose conjugates by $\mathrm{Emb}(E, \overline{\mathbf{Q}}_p)$ are all de Rham with weights in $\mathbf{Z}_{\geqslant 0}$, imposes some constraints on K_∞/K. Here is a simple example (recall that E is a finite extension of $\mathbf{Q}_p$ such that $k_E = k_K$).

Proposition 4.7. — *If K is a Galois extension of $\mathbf{Q}_p$ of degree d, where d is a prime number, and if $\eta:\Gamma_K\to\mathcal{O}_E^\times$ is a de Rham character with weights in $\mathbf{Z}_{\geqslant 0}$, then the Lie algebra of the image of η is either $\{0\}$, $\mathbf{Q}_p$ or K.*

Proof. — By local class field theory, Γ_K can be realized as a quotient of $\mathcal{O}_K^\times$ and η can be seen as a character $\eta:\mathcal{O}_K^\times\to\mathcal{O}_E^\times$. This character is then the product of a finite order character by

$$x\longmapsto\prod_{h\in\mathrm{Gal}(K/\mathbf{Q}_p)}h(x)^{a_h},$$

where a_h is the weight of η at the embedding h, so that $a_h\in\mathbf{Z}_{\geqslant 0}$. It is therefore enough to prove that if $f:K\to K$ is defined by $f=\sum_{h\in\mathrm{Gal}(K/\mathbf{Q}_p)}a_h\cdot h$ with $a_h\in\mathbf{Z}_{\geqslant 0}$, then the image of f is either $\{0\}$, $\mathbf{Q}_p$ or K.

Let g be a generator of $\mathrm{Gal}(K/\mathbf{Q}_p)$ and write a_i for a_{g^i} if $i\in\mathbf{Z}/d\mathbf{Z}$. If $\sum_i a_ig^i(x)=0$ for some $x\in K^\times$, then $\sum_i a_{i+j}g^i(x)=0$ for all $j\in\mathbf{Z}/d\mathbf{Z}$. This implies that the circulant matrix $(a_{i+j})_{i,j}$ is singular. Its determinant is

$$\prod_{j=0}^{d-1}\sum_{i=0}^{d-1}\zeta_d^{ij}a_i,$$

where ζ_d is a primitive d-th root of 1. Since d is a prime number and $a_i\in\mathbf{Z}_{\geqslant 0}$ for all i, we can have $\sum_{i=0}^{d-1}\zeta_d^{ij}a_i=0$ for some j if and only if all a_i are equal. In this case, f is equal to $a_0\cdot\mathrm{Tr}_{K/\mathbf{Q}_p}(\cdot)$. Otherwise, $f:K\to K$ is bijective. This proves the proposition. ☐

Corollary 4.8. — *If $K=\mathbf{Q}_{p^2}$ and K_∞ is the anticylotomic extension of K and E is a totally ramified extension of $\mathbf{Q}_{p^2}$, then it is not possible to find a lift for φ_q and Γ_K such that $\varphi_q(T)\in\mathcal{O}_E[\![T]\!]$.*

Remark 4.9. — If d is not a prime number, then the conclusion of proposition 4.7 does not necessarily hold anymore. This is already the case if $\mathrm{Gal}(K/\mathbf{Q}_p)=\mathbf{Z}/4\mathbf{Z}$.

Remark 4.10. — There is some similarity between our methods for proving Theorem B and the constructions of [Lub94]. For example, the power series $A(T)$ constructed in the proof of Theorem B is denoted by $\mathbf{L}_f$ in §1 of ibid. and called the *logarithm*. Theorem B is then consistent with the suggestion on page 341 of ibid. that "for an invertible series to commute with a noninvertible series, there must be a formal group somehow in the background". Indeed, the existence of a de Rham character $\Gamma_K\to\mathcal{O}_E^\times$ with weights in $\mathbf{Z}_{\geqslant 0}$ indicates that the extension K_∞/K must in some sense "come from geometry".

References

[CE14] B. Chiarellotto & F. Esposito – "A note on Fontaine theory using different Lubin-Tate groups", *Kodai Math. J.* **37** (2014), no. 1, p. 196–211.

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

[Fon94a] ———, "Le corps des périodes p-adiques", in *Périodes p-adiques (Bures-sur-Yvette, 1988)*, Astérisque, vol. 223, Société Mathématique de France, 1994, With an appendix by Pierre Colmez, p. 59–111.

[Fon94b] ———, "Représentations p-adiques semi-stables", in *Périodes p-adiques (Bures-sur-Yvette, 1988)*, Astérisque, vol. 223, Société Mathématique de France, 1994, p. 113–184.

[FW79a] J.-M. Fontaine & J.-P. Wintenberger – "Le "corps des normes" de certaines extensions algébriques de corps locaux", *C. R. Acad. Sci. Paris Sér. A-B* **288** (1979), no. 6, p. A367–A370.

[FW79b] ———, "Extensions algébriques et corps des normes des extensions APF des corps locaux", *C. R. Acad. Sci. Paris Sér. A-B* **288** (1979), no. 8, p. A441–A444.

[FX13] L. Fourquaux & B. Xie – "Triangulable $\mathcal{O}_F$-analytic (φ_q, Γ)-modules of rank 2", *Algebra Number Theory* **7** (2013), no. 10, p. 2545–2592.

[KR09] M. Kisin & W. Ren – "Galois representations and Lubin-Tate groups", *Doc. Math.* **14** (2009), p. 441–461.

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

[Sch06] A. J. Scholl – "Higher fields of norms and (φ, Γ)-modules", *Doc. Math.* (2006), p. 685–709, Extra Volume: John H. Coates' Sixtieth Birthday.

[Sen72] S. Sen – "Ramification in p-adic Lie extensions", *Invent. Math.* **17** (1972), p. 44–50.

[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.

Manuscript received October 10, 2013
accepted April 17, 2014

Laurent Berger, UMPA de l'ENS de Lyon, UMR 5669 du CNRS, IUF
46 allée d'Italie, 69007 Lyon, France
E-mail : laurent.berger@ens-lyon.fr
Url : http://perso.ens-lyon.fr/laurent.berger/