SUBSTITUTION MAPS IN THE ROBBA RING

by

Laurent Berger

To Bernadette Perrin-Riou, on the occasion of her 65th birthday.

Abstract. — We ask several questions about substitution maps in the Robba ring. These questions are motivated by p-adic Hodge theory and the theory of p-adic dynamical systems. We provide answers to those questions in special cases, thereby generalizing results of Kedlaya, Colmez, and others.

Contents

Introduction and notation

Let p be a prime number. In this article, K is a finite extension of $\mathbf{Q}_p$, or more generally a finite totally ramified extension of $W(k)[1/p]$ where k is a perfect field of characteristic p. Let $\mathcal{O}_K$ denote the integers of K, let $\mathfrak{m}_K$ be the maximal ideal of $\mathcal{O}_K$, let k be the residue field of $\mathcal{O}_K$, and let π be a uniformizer of $\mathcal{O}_K$. We fix a p-adic norm $|\cdot|$ on K.

In p-adic Hodge theory, the theory of p-adic differential equations, and the theory of p-adic dynamical systems, several rings of power series with coefficients in K occur.

2020 ***Mathematics Subject Classification.*** — 11S82; 12H25; 13J07; 46S10.
Key words and phrases. — p-adic analysis; p-adic dynamical system; Robba ring; φ-module.

There is $\mathcal{E}^+ = \mathcal{O}_K[\![X]\!][1/\pi]$, and various completed localizations of that ring, denoted by $\mathcal{E}$ (Fontaine's field), $\mathcal{E}^\dagger$ (the overconvergent elements in $\mathcal{E}$), $\mathcal{R}^+$ (the power series converging on the p-adic open unit disk), and $\mathcal{R}$ (the Robba ring). These rings are often endowed with a substitution map φ of the form $\varphi : f(X) \mapsto f(s(X))$, where $s(X)$ is either a Frobenius lift (for example X^p or $(1+X)^p - 1$ or $\pi X + X^q$ where q is a power of p, in p-adic Hodge theory), or a more general power series (for example the multiplication-by-p map in a formal group, in the theory of p-adic dynamical systems).

When considering certain questions in the above domains, it is necessary to compute $(\operatorname{Frac}\mathcal{R})^{\varphi=\mu}$ for $\mu \in K$ and for certain $s(X)$. This happens for example when considering questions of descent of morphisms for certain φ-modules, or when considering p-adic dynamical systems on annuli. The computation of $(\operatorname{Frac}\mathcal{R})^{\varphi=\mu}$ for $\mu \in K$ is particularly delicate: that computation is carried out (for certain $s(X) \in X \cdot \mathcal{O}_K[\![X]\!]$) in lemma 3.2.4 of [**Ked00**] as well as in lemma 32 of [**MZ02**], but there are mistakes in both proofs. Those mistakes are discussed in remark 5.8 of [**Ked05**] and fixed in §5 of that paper (see also the errata to ibid.).

We compute $(\operatorname{Frac}\mathcal{R})^{\varphi=\mu}$ for all substitutions φ that are of finite height, namely those for which $s(X)$ belongs to $X \cdot \mathcal{O}_K[\![X]\!]$ and is such that $\overline{s}(X) \in k[\![X]\!]$ is nonzero and belongs to $X^2 \cdot k[\![X]\!]$. In particular, we do not assume that $s(X)$ is a Frobenius lift.

If $s'(0) \neq 0$, there exists (see for instance [**Lub94**]) an element $\log_s(X) \in X \cdot \mathcal{R}^+$ such that $\varphi(\log_s) = s'(0) \cdot \log_s$, so that $\log_s^k \in (\mathcal{R}^+)^{\varphi = s'(0)^k}$ if $k \geqslant 1$. The following theorem (theorem 6.8) sums up our main results.

Theorem A. — *If φ is of finite height, then $(\operatorname{Frac}\mathcal{R})^{\varphi=1} = K$. In addition,*

1. $(\operatorname{Frac}\mathcal{R})^{\varphi=s'(0)^k} = K \cdot \log_s^k$ *if $s'(0) \neq 0$ and $k \in \mathbf{Z}$;*
2. $(\operatorname{Frac}\mathcal{R})^{\varphi=\mu} = \{0\}$ *if $\mu \neq 1 \in K$ and if either $s'(0) = 0$ or if $s'(0) \neq 0$ and μ is not of the form $s'(0)^k$ for some $k \in \mathbf{Z}$.*

We propose a conjecture concerning $(\operatorname{Frac}\mathcal{R})^{\varphi=1}$ in a more general setting. We say that the substitution φ is overconvergent if $s(X)$ is in the ring of integers of $\mathcal{E}^\dagger$ and if $\overline{s}(X) \in k(\!(X)\!)$ is nonzero and belongs to $X^2 \cdot k[\![X]\!]$. The following is conjecture 3.1.

Conjecture A. — *If φ is overconvergent, then $(\operatorname{Frac}\mathcal{R})^{\varphi=1} = K$.*

Theorem A implies this conjecture when φ is of finite height. We also prove (corollary 7.4) that if $\mathcal{R}'/\mathcal{R}$ is a finite extension of Robba rings, and if conjecture 3.1 holds for $\mathcal{R}$, then it holds for $\mathcal{R}'$.

Finally, we propose a conjecture about those $h \in \mathcal{R}$ such that $\varphi(h)$ has a large annulus of convergence, when φ is of finite height. Let $\rho(s)$ be the largest norm of a zero of s in the open unit disk. The following is conjecture 8.1, and we prove it in the cyclotomic case, namely when $s(X) = (1+X)^p - 1$ (see proposition 8.2).

Conjecture B. — *If φ is of finite height and $h \in \mathcal{R}$ is such that $\varphi(h)$ is convergent on the annulus $\{z,\ \rho(s) \leqslant |z| < 1\}$, then $h \in \mathcal{R}^+$.*

The definitions and properties of the rings that occur in this article are given in §1. Overconvergent substitutions are introduced in §2, and conjecture 3.1 is discussed in §3. After that, we assume that φ is of finite height; these substitutions are discussed in §4. A generalization of the classical operator ψ is constructed in §5. Theorem A is proved in §6. The stability of conjecture 3.1 under finite extensions is proved in §7, and conjecture 8.1 is discussed in §8.

1. Rings of power series

We start by defining the rings that occur in this article. There is $\mathcal{O}_K[\![X]\!]$, the ring $\mathcal{E}^+ = \mathcal{O}_K[\![X]\!][1/\pi]$, the ring $\mathcal{O}_{\mathcal{E}}$ of power series $\sum_{n \in \mathbf{Z}} a_n X^n$ with $a_n \in \mathcal{O}_K$ and $a_{-n} \to 0$ as $n \to +\infty$, and the field $\mathcal{E} = \mathcal{O}_{\mathcal{E}}[1/\pi]$. If I is a subinterval of $[0;1[$, we have the ring $\mathcal{R}^I$ of power series $a(X) = \sum_{n \in \mathbf{Z}} a_n X^n$ with $a_n \in K$ such that $|a_n| \cdot r^n \to 0$ as $n \to \pm\infty$ for all $r \in I$. We let $\mathcal{R}^+ = \mathcal{R}^{[0;1[}$ be the ring of power series $a(X) = \sum_{n \geqslant 0} a_n X^n$ with $a_n \in K$ such that $|a_n| \cdot r^n \to 0$ as $n \to +\infty$ for all $0 \leqslant r < 1$. Inside $\mathcal{R}^{[r;1[}$ we have the subring $\mathcal{E}^{[r;1[}$ of power series with bounded coefficients. The ring $\mathcal{E}^{[r;1[}$ is contained in $\mathcal{E}$. Finally, we have the field $\mathcal{E}^\dagger = \cup_{r<1} \mathcal{E}^{[r;1[}$ of overconvergent elements of $\mathcal{E}$, and the Robba ring $\mathcal{R} = \cup_{r<1} \mathcal{R}^{[r;1[}$. We have $\mathcal{E}^\dagger \subset \mathcal{E}$ and $\mathcal{E}^\dagger \subset \mathcal{R}$, and $\mathcal{R} = \mathcal{R}^+ + \mathcal{E}^\dagger$ while $\mathcal{R}^+ \cap \mathcal{E}^\dagger = \mathcal{E}^+$.

The rings $\mathcal{R}^I$ are studied in [**Laz62**]. We recall below the results that we use in this article; the proofs can be found in [**Laz62**]. If $I = [r;s]$ is a closed interval, then $\mathcal{R}^I$ is a PID. For $r < 1$, the ring $\mathcal{R}^{[r;1[}$ is a Bezout domain, and $\mathcal{E}^{[r;1[}$ is a PID. In particular, it makes sense to talk about the gcd of two elements of these rings, and to say that two elements are coprime.

Let $\mathbf{C}$ be the completion of an algebraic closure K^{alg} of K, so that $\mathfrak{m}_{\mathbf{C}}$ is the p-adic open unit disk. If I is a subinterval of $[0;1[$, let $A(I)$ denote the annulus $A(I) = \{z \in \mathbf{C}$ such that $|z| \in I\}$. Special cases include $D = A([0;1[)$, the open unit disk, $D(r) = A([0;r])$, the closed disk of radius r, and $C(r) = A([r;r])$, the circle of radius r. An element of $\mathcal{R}^I$ defines a function on $A(I)$, which can have zeroes.

Lemma 1.1. — *If $h \in \mathcal{R}^I$, then h is invertible if and only if h has no zeroes in $A(I)$.*

If $r \in I$, we have the norm $|\cdot|_r$ on $\mathcal{R}^I$ given by $|a|_r = \sup_{n\in\mathbf{Z}} |a_n| \cdot r^n$. If $r \in |\mathbf{C}|$, then $|a|_r = \sup_{z\in\mathbf{C},\,|z|=r} |a(z)|$. The norm $|\cdot|_r$ is multiplicative: $|ab|_r = |a|_r \cdot |b|_r$. The function $s \mapsto \log |h|_s$ is a log-convex function on I.

Lemma 1.2. — *The family of norms $\{|\cdot|_s\}_{r\leqslant s<1}$ defines a Fréchet structure on $\mathcal{E}^{[r;1[}$, and the Fréchet completion of $\mathcal{E}^{[r;1[}$ is $\mathcal{R}^{[r;1[}$.*

Lemma 1.3. — *If $h \in \mathcal{R}^{[r;1[}$, the following are equivalent:*

1. *$h \in \mathcal{E}^{[r;1[}$;*
2. *h has finitely many zeroes in $A([r;1[)$;*
3. *the function $s \mapsto |h|_s$ is bounded as $s \to 1$.*

In particular, if $h \in \mathcal{R}$ and $h \notin \mathcal{E}^\dagger$, then $s \mapsto |h|_s$ is eventually increasing as $s \to 1$.

Corollary 1.4. — *We have $(\mathcal{R}^+)^\times = (\mathcal{E}^+)^\times$.*

Proof. — This follows from lemmas 1.1 and 1.3. □

Lemma 1.5. — *If $g/h \in \operatorname{Frac}\mathcal{R}^+$ has no poles, then $g/h \in \mathcal{R}^+$.*

Proof. — We can assume that g and h are coprime, so that h has no zeroes. The function h is then invertible in $\mathcal{R}^+$ by lemma 1.1, so that $g/h \in \mathcal{R}^+$. □

Lemma 1.6. — *We have $\operatorname{Frac}\mathcal{R}^+ \cap \mathcal{E}^\dagger = \operatorname{Frac}\mathcal{E}^+$.*

Proof. — Take $g/h \in \operatorname{Frac}\mathcal{R}^+$, and assume that g and h are coprime. If $g/h \in \mathcal{E}^\dagger$, then g and h can only have finitely many zeroes, and hence both lie in $\mathcal{E}^+$ by lemma 1.3. □

Lemma 1.7. — *If $g \in \mathcal{R}$, there exists $g^+ \in \mathcal{R}^+$ and $g^\dagger \in \mathcal{E}^\dagger$ such that $g = g^+ \cdot g^\dagger$.*

Sketch of proof. — Take $g \in \mathcal{R}^{[r;1[}$. There exists $g^+ \in \mathcal{R}^+$ whose divisor (see [**Laz62**]) is that of g, so that g^+ divides g in $\mathcal{R}^{[r;1[}$, and the quotient is in $\mathcal{E}^{[r;1[}$ by lemma 1.3. □

Lemma 1.8. — *The field K is algebraically closed inside* $\operatorname{Frac}\mathcal{R}$.

Proof. — Let F be a finite extension of K. We show that $F \otimes_K \operatorname{Frac}\mathcal{R} \to \operatorname{Frac}(F \otimes_K \mathcal{R})$ is injective. If $f_1, \dots, f_n$ is a basis of F/K, and if $\sum f_i \otimes a_i(X)/b_i(X) = 0$ in $\operatorname{Frac}(F\otimes_K \mathcal{R})$, then let $c_i(X) = \prod_{j\neq i} b_i(X)$. We have $\sum f_i \otimes a_i(X)c_i(X) = 0$ in $\operatorname{Frac}(F \otimes_K \mathcal{R})$ and hence in $F \otimes_K \mathcal{R}$ so that $a_i c_i = 0$ for all i. The map is therefore injective, so that $F \otimes_K \operatorname{Frac}\mathcal{R}$ is a domain. This would not be the case if there was a K-embedding of F in $\operatorname{Frac}\mathcal{R}$. □

Remark 1.9. — The proof of lemma 1.8 shows that $\operatorname{Frac}(F \otimes_K \mathcal{R}) = F \otimes_K \operatorname{Frac}\mathcal{R}$.

The ring $\mathcal{R}^{]0;1[}$ is the ring of power series converging on the punctured open unit disk.

Proposition 1.10. — *If $h(X) \in \mathcal{R}^{]0;1[}$ and $|h|_r$ is bounded as $r \to 0$, then $h \in \mathcal{R}^+$.*

Proof. — Write $h(X) = \sum_{k\in\mathbf{Z}} h_k X^k$. We have $|h|_r = \max_k |h_k| r^k$. If $|h|_r \leqslant C$ for r small enough, then $|h_{-k}| \leqslant C r^k$ as $r \to 0$, so that $h_{-k} = 0$ if $k \geqslant 1$. □

2. Overconvergent substitution maps

If $s(X) \in \mathcal{O}_{\mathcal{E}}$ is such that $\overline{s}(X) \in k(\!(X)\!)$ is nonzero and belongs to $X \cdot k[\![X]\!]$, then $s(X)^{-1} \in \mathcal{O}_{\mathcal{E}}$ and $s(X)^n \to 0$ in $\mathcal{O}_{\mathcal{E}}$ (for the weak topology) as $n \to +\infty$, so that if $f(X) \in \mathcal{E}$, then $f(s(X))$ converges in $\mathcal{E}$. This way, we get a substitution map $\varphi : f \mapsto f \circ s$ that generalizes the Frobenius lifts (corresponding to those $s(X)$ such that $\overline{s}(X) = X^q$ where q is a power of p, such as X^q or $(1+X)^p - 1$ or $X^q + \pi X$). Analogous maps φ are studied in p-adic Hodge theory, and in the theory of p-adic dynamical systems.

Let $\mathcal{O}_{\mathcal{E}}^{\dagger} = \mathcal{O}_{\mathcal{E}} \cap \mathcal{E}^{\dagger}$. In this section, we assume that $s(X) \in \mathcal{O}_{\mathcal{E}}^{\dagger}$ and we study the restriction of φ to $\mathcal{E}^{\dagger}$ and its extension to $\mathcal{R}$.

Lemma 2.1. — *If $h(X) \in \mathcal{O}_{\mathcal{E}}^{\dagger}$, there exists $r_h < 1$ such that $h \in \mathcal{E}^{[r_h;1[}$ and $|\pi h|_r < 1$ for all $r_h \leqslant r < 1$.*

Proof. — Write $h = h^+ + h^-$ (according to positive and negative powers of X). There exists $s < 1$ such that $h^- \in \mathcal{E}^{[s;+\infty[}$. The function $r \mapsto |h^-|_r$ is defined for all $r \geqslant s$ and decreasing and $|h^-|_1 \leqslant 1$ since $h_n \in \mathcal{O}_K$ for all n. Hence there exists $1 > r_h \geqslant s$ such that $|\pi h^-|_r < 1$ for all $r_h \leqslant r < 1$. Since $|\pi h^+|_r \leqslant |\pi|$ for all $r < 1$, the claim follows. □

We now assume that our substitution map is given by a series $s(X) \in \mathcal{O}_{\mathcal{E}}^{\dagger}$ such that $\overline{s}(X) \in k(\!(X)\!)$ is nonzero and belongs to $X^2 \cdot k[\![X]\!]$. The X-adic valuation of $\overline{s}$ is the Weierstrass degree $\mathrm{wideg}(s)$ of s. In other words, we can write $s(X) = s^+(X) + \pi \cdot s^-(X)$ with $s^+ \in X \cdot \mathcal{O}_K[\![X]\!]$ and $\mathrm{wideg}(s^+) = d$ for some $d \geqslant 2$, and $s^- \in \mathcal{O}_{\mathcal{E}}^{\dagger}$. Lemma 2.1 implies that we can write $s(X)/X^d = s_d \cdot (1+g)$ where $g \in \mathcal{O}_{\mathcal{E}}^{\dagger}$ and $s_d \in \mathcal{O}_K^{\times}$ and there exists $r_s < 1$ such that $|g|_r < 1$ for all $r_s \leqslant r < 1$.

If $h(X) = \sum_{n\in\mathbf{Z}} h_n X^n \in \mathcal{R}^{[r;1[}$ for $r \geqslant r_s$, the series

$$(\Phi) \qquad \sum_{n\in\mathbf{Z}} h_n s_d^n X^{dn} (1+g)^n = \sum_{n\in\mathbf{Z},\, k\geqslant 0} h_n s_d^n X^{dn} \binom{n}{k} g^k$$

converges in $\mathcal{R}^{[r^{1/d};1[}$. We let $\varphi(h)$ denote the sum of the series on the right. If $h \in \mathcal{E}^{[r;1[}$, then $\varphi(h) \in \mathcal{E}^{[r^{1/d};1[} \subset \mathcal{E}$ coincides with $\varphi(h)$ as defined at the beginning of this section.

Proposition 2.2. — *If $r_s < 1$ is as above and if $r \geqslant r_s$, then*

1. $\varphi(\mathcal{R}^{[r;1[}) \subset \mathcal{R}^{[r^{1/d};1[}$
2. *if* $|z| \geqslant r^{1/d}$ *and* $h \in \mathcal{R}^{[r;1[}$*, then* $|s(z)| = |z|^d \geqslant r$*, and* $\varphi(h)(z) = h(s(z))$
3. $|\varphi(h)|_{r^{1/d}} = |h|_r$.

Proof. — This is clear from equation (Φ) and the definition of r_s. □

3. Eigenvalues of φ and $(\operatorname{Frac}\mathcal{R})^{\varphi=1}$

In §6 below, we prove that $(\operatorname{Frac}\mathcal{R})^{\varphi=1} = K$ if we assume that $s(X) \in X \cdot \mathcal{O}_K[\![X]\!]$ (theorem 6.8). We expect this result to hold for a general overconvergent substitution.

Conjecture 3.1. — *We have* $(\operatorname{Frac}\mathcal{R})^{\varphi=1} = K$ *in general.*

In the rest of this section, we give some results related to this conjecture. These results are not used in the rest of the article. We say that $\lambda \in \mathcal{R}$ is an eigenvalue of φ is there exists a nonzero $h \in \mathcal{R}$ such that $\varphi(h) = \lambda \cdot h$. This terminology is not quite correct as φ is only a semilinear map on $\mathcal{R}$.

Proposition 3.2. — *We have* $(\operatorname{Frac}\mathcal{R})^{\varphi=1} = K$ *iff* $\dim_K \mathcal{R}^{\varphi=\lambda} \leqslant 1$ *for all* $\lambda \in \mathcal{R}$.

Proof. — If $g, h \in \mathcal{R}^{\varphi=\lambda}$, then $g/h \in (\operatorname{Frac}\mathcal{R})^{\varphi=1}$. If $(\operatorname{Frac}\mathcal{R})^{\varphi=1} = K$, then $g/h \in K$ so that $\dim_K \mathcal{R}^{\varphi=\lambda} \leqslant 1$. Conversely, take $g/h \in (\operatorname{Frac}\mathcal{R})^{\varphi=1}$, so that $g \cdot \varphi(h) = h \cdot \varphi(g)$. Take $r < 1$ such that $g, h, \varphi(g)$ and $\varphi(h)$ belong to $\mathcal{R}^{[r;1[}$. We can assume that g and h are coprime in $\mathcal{R}^{[r;1[}$, and then g divides $\varphi(g)$ and h divides $\varphi(h)$ in $\mathcal{R}^{[r;1[}$. The common quotient $\lambda \in \mathcal{R}$ is such that $g, h \in \mathcal{R}^{\varphi=\lambda}$. If $\dim_K \mathcal{R}^{\varphi=\lambda} = 1$, then $g/h \in K$. □

Proposition 3.3. — *If* $\lambda \in \mathcal{R}$ *and* $\mathcal{R}^{\varphi=\lambda} \neq \{0\}$*, then* $\lambda \in \mathcal{O}_{\mathcal{E}}^{\dagger}$.

Proof. — Take $h \in \mathcal{R}^{\varphi=\lambda}$. If $h \in \mathcal{E}^{\dagger}$, we can assume that $h \in \mathcal{O}_{\mathcal{E}}^{\times}$ and then $\lambda = \varphi(h)/h \in \mathcal{O}_{\mathcal{E}} \cap \mathcal{E}^{\dagger} = \mathcal{O}_{\mathcal{E}}^{\dagger}$. If $h \notin \mathcal{E}^{\dagger}$, then $r \mapsto |h|_r$ is eventually increasing as $r \to 1$ by lemma 1.3. If $r < 1$ is close enough to 1, then $|\varphi(h)|_r = |h|_{r^d}$ by proposition 2.2, so that $|\lambda|_r = |h|_{r^d}/|h|_r \leqslant 1$. By lemma 1.3, $\lambda \in \mathcal{E}^{\dagger}$. In addition, if we write $\lambda(X) = \sum \lambda_n X^n$, then $|\lambda_n| r^n \leqslant 1$ for all n and all $r < 1$ close to 1, hence $\lambda_n \in \mathcal{O}_K$ for all n. □

Proposition 3.4. — *We have* $\mathcal{R}^{\varphi=1} = K$.

Proof. — Take $g \in \mathcal{R}$ such that $\varphi(g) = g$. Proposition 2.2 implies that $|g|_{s^{1/d}} = |g|_s$ if s is close to 1, so that the function $s \mapsto |g|_s$ is bounded as $s \to 1$. By lemma 1.3, we have $g \in \mathcal{E}^{\dagger}$. Take $r \geqslant r_s$ so that by proposition 2.2, $\varphi(\mathcal{E}^{[r;1[}) \subset \mathcal{E}^{[r^{1/d};1[}$ and if $|y| \geqslant r^{1/d}$ and $h \in \mathcal{E}^{[r;1[}$, then $|s(y)| \geqslant r$, and $\varphi(h)(y) = h(s(y))$. If $|z| \geqslant r$ and $s(y) = z$, then $|y| \geqslant r^{1/d}$. Therefore if $g(z) = 0$, then $g(y) = \varphi(g)(y) = g(z) = 0$. This implies that if

g has a zero in $A([r;1[)$, then it has infinitely many zeroes. By lemma 1.3, this is not possible if $g \in \mathcal{E}^\dagger$.

Pick $z \in A([r;1[) \cap K^{\mathrm{alg}}$. The function $g \mapsto g(z)$, from $(\mathcal{E}^{[r;1[})^{\varphi=1}$ to $K(z)$, is therefore injective, and hence $(\mathcal{E}^{[r;1[})^{\varphi=1}$ is a finite dimensional K-vector space. It is also a domain, and hence a field extension of K. Since K is algebraically closed in $\mathcal{E}^\dagger$, we get that $(\mathcal{E}^{[r;1[})^{\varphi=1} = K$. This is true for all r close to 1, so that $(\mathcal{E}^\dagger)^{\varphi=1} = K$. □

We say that $s(X)$ is a p-power lift if in $k[\![X]\!]$, we have $\overline{s}(X) \in k[\![X^p]\!]$. This is equivalent to saying that $s'(X) \in \pi\mathcal{O}_{\mathcal{E}}^\dagger$. Frobenius lifts are examples of p-power lifts.

Proposition 3.5. — *If $s(X)$ is a p-power lift, and $\lambda \in \mathcal{O}_{\mathcal{E}}^\dagger$, then $\dim_K \mathcal{R}^{\varphi=\lambda} \leqslant n(\lambda) - 1$ where $n(\lambda) \in \mathbf{Z}$ is such that $n(\lambda) > 2 \cdot \mathrm{val}(\lambda)/\mathrm{val}(s') + 1$.*

Proof. — Take $f \in \mathcal{R}^{\varphi=\lambda}$, so that $f(s(X)) = \lambda(X) \cdot f(X)$. We have

$$f'(s(X)) \cdot s'(X) = \lambda(X) \cdot f'(X) + \lambda'(X) \cdot f(X)$$

and hence $\varphi(f') \in f' \cdot \lambda/s' + \mathcal{R} \cdot f$. Likewise for all $m \geqslant 1$,

$$\varphi(f^{(m)}) \in f^{(m)} \cdot \lambda/(s')^m + \mathcal{R} \cdot f + \mathcal{R} \cdot f' + \cdots + \mathcal{R} \cdot f^{(m-1)}.$$

Given n elements $f_1, \ldots, f_n$ of $\mathcal{R}$, let $W(f_1, \ldots, f_n)$ denote their Wronskian

$$W(f_1, \ldots, f_n) = \det \begin{pmatrix} f_1 & \cdots & f_n \\ f_1' & \cdots & f_n' \\ \vdots & & \vdots \\ f_1^{(n-1)} & \cdots & f_n^{(n-1)} \end{pmatrix}$$

If $f_1, \ldots, f_n \in \mathcal{R}^{\varphi=\lambda}$, then $W(f_1, \ldots, f_n)$ belongs to $\mathcal{R}^{\varphi=\lambda^n/(s')^{n(n-1)/2}}$ by the above. Take $n = n(\lambda) \in \mathbf{Z}$ such that $n > 2 \cdot \mathrm{val}(\lambda)/\mathrm{val}(s') + 1$. By proposition 3.3, $\mathcal{R}^{\varphi=\lambda^n/(s')^{n(n-1)/2}} = \{0\}$, and hence $W(f_1, \ldots, f_n) = 0$, so that $f_1, \ldots, f_n$ are linearly dependent over K.

Therefore, $\dim_K \mathcal{R}^{\varphi=\lambda} \leqslant n(\lambda) - 1$. □

Remark 3.6. — If $s(X)$ is a p-power lift, and $\lambda = 1$, we can take $n(\lambda) = 2$, and we get a new proof that $\mathcal{R}^{\varphi=1} = K$ in this case.

Proposition 3.7. — *If there exists $C \in \mathbf{Z}_{\geqslant 1}$ such that $\dim_K \mathcal{R}^{\varphi=\lambda} \leqslant C$ for all $\lambda \in \mathcal{O}_{\mathcal{E}}^\dagger$, then $\dim_K \mathcal{R}^{\varphi=\lambda} \leqslant 1$ for all $\lambda \in \mathcal{O}_{\mathcal{E}}^\dagger$.*

Proof. — Take $g, h \in \mathcal{R}^{\varphi=\lambda}$, and $m \geqslant 1$. The $m+1$ functions $\{g^i h^{m-i}\}_{0 \leqslant i \leqslant m}$ all belong to $\mathcal{R}^{\varphi=\lambda^m}$. If $m \geqslant C$, they are linearly dependent over K. Hence g/h is algebraic over K in $\operatorname{Frac} \mathcal{R}$. Therefore, $g/h \in K$ by lemma 1.8. □

We finish this section with some additional motivation for conjecture 3.1. Suppose that $s(X) \in X \cdot \mathcal{O}_K[\![X]\!]$ with $s'(0) \neq 0$, and that $u(X) \in X \cdot \mathcal{O}_K[\![X]\!]$ is such that $u \circ s = s \circ u$. Let $\tilde{u} \in \mathcal{R}^+$ be the Lie logarithm of u, as defined in §4 of [**Lub94**]. We have (lemma 4.4.2 of ibid.) $\tilde{u} \circ s = s' \cdot \tilde{u}$. Hence $\tilde{u}$ is an eigenvector of φ for the eigenvalue s'. If $v(X) \in X \cdot \mathcal{O}_K[\![X]\!]$ is another series such that $v \circ s = s \circ v$, then $\tilde{u}$ and $\tilde{v}$ are both eigenvectors of φ for the eigenvalue s', and conjecture 3.1 (which holds, by theorem 6.8, if $s(X) \in X \cdot \mathcal{O}_K[\![X]\!]$) along with proposition 3.2 then implies that $\tilde{v} = c \cdot \tilde{u}$ for some $c \in K$. We can use this to show that u and v commute with each other for composition. If $s(X) \in X \cdot \mathcal{O}_K[\![X]\!]$ with $s'(0) \neq 0$, there is a much simpler proof of this, but knowing conjecture 3.1 in greater generality would allow us to prove similar results for p-adic dynamical systems on annuli, where they are currently not known.

4. Substitutions of finite height

In this section (and in the rest of this article), we assume that $s(X)$ is of finite height, namely that it belongs to $\mathcal{O}_K[\![X]\!]$, and that $s(0) = 0$. Recall that $\mathrm{wideg}(s) = d$ is finite and that $d \geqslant 2$. In other words, $s(X) = \sum_{k \geqslant 1} s_k X^k$ with $s_1, \dots, s_{d-1} \in \mathfrak{m}_K$ and $s_d \in \mathcal{O}_K^\times$.

Remark 4.1. — If $s(X) \in \mathcal{O}_K[\![X]\!]$ and $\mathrm{wideg}(s) = d \geqslant 2$, there exists $a \in \mathfrak{m}_K$ such that $s(a) = a$, so that $s(X)$ is conjugate to the power series $s_a(X) = s(X + a) - a$ which is such that $\mathrm{wideg}(s_a) = d$ and $s_a(X) = 0$. Hence the condition that $s(0) = 0$ can be achieved by a simple conjugation.

Proof. — Let $\mathrm{val}(\cdot) = -\log_p |\cdot|$. Since $\mathrm{wideg}(s) \geqslant 2$, the Newton polygon of $s(X) - X$ starts with a segment of length 1 and slope $-\mathrm{val}(s(0))$, which gives us such an a with $\mathrm{val}(a) = \mathrm{val}(s(0))$. □

Recall that if $r < 1$, $D(r)$ is the closed disk of radius r and $C(r)$ is the circle of radius r. Define a function $\lambda : [0;1] \to [0;1]$ by $\lambda(r) = \max_k |s_k| r^k$.

Lemma 4.2. — *We have $\lambda(r) = r^d$ if r is close enough to 1, $\lambda(r) < r$ for all $r > 0$, and $\lambda(r) \leqslant |\pi| r$ if r is close enough to 0.*

Proof. — These all follow easily from the formula $\lambda(r) = \max_k |s_k| r^k$. □

Proposition 4.3. — *If $r < 1$, then $s(D(r)) = D(\lambda(r))$ and $s(C(r))$ contains $C(\lambda(r))$.*

Proof. — That $s(D(r)) \subset D(\lambda(r))$ follows from the definition $\lambda(r) = \max_k |s_k| r^k$. For the second assertion, it is better to use valuations. Let $\mathrm{val}(\cdot) = -\log_p |\cdot|$. Define $\lambda^*(v) = \min_k \mathrm{val}(s_k) + kv$. If $\mathrm{val}(z) = \lambda^*(v)$, choose an index j such that $\mathrm{val}(z) = \mathrm{val}(s_j) + jv$.

The line with equation $y = \mathrm{val}(s_j) + v \cdot (j - x)$ passes through $(0, \mathrm{val}(z))$, lies below the Newton polygon of s, and touches it at the point $(j, \mathrm{val}(s_j))$. Hence the equation $s(X) - z$ has a root of valuation v. □

Corollary 4.4. — *If $h(X) \in \mathcal{R}^+$, then $|\varphi(h)|_r = |h|_{\lambda(r)}$ for all $r < 1$.*

Proposition 4.5. — *We have $(\mathcal{R}^+)^{\varphi=1} = K$.*

Proof. — Take $g \in \mathcal{R}^+$ such that $\varphi(g) = g$. We have $g(z) = g(s(z))$ for all $z \in D$. Since $s^{\circ n}(z) \to 0$ as $n \to +\infty$, we have $g(z) = g(0)$ for all $z \in D$ and hence $g \in K$. □

Proposition 4.6. — *If $\mu \in K$, and $f \in (\mathrm{Frac}\,\mathcal{R}^+)^{\varphi=\mu}$, then $f^{\pm 1} \in \mathcal{R}^+$.*

Proof. — Write $f = g/h \in (\mathrm{Frac}\,\mathcal{R}^+)^{\varphi=\mu}$. Let z be a nonzero zero (or pole) of g/h. We have $\mu \cdot (g/h)(z) = \varphi(g/h)(z) = (g/h)(s(z))$ so that $s(z)$ is itself a zero (or pole) of g/h. Likewise $s^{\circ n}(z)$ is a zero (or pole) of g/h for all $n \geqslant 0$. Since $|s(x)| < |x|$ if $x \neq 0$, and since the zeroes and poles of g/h cannot accumulate towards 0, we must have $s^{\circ n}(z) = 0$ for $n \gg 0$. Therefore 0 is a zero (or pole) of g/h. Consequently, either 0 is a zero of g/h and g/h only has zeroes, or 0 is a pole of g/h and g/h only has poles. By lemma 1.5, either g/h or h/g belongs to $\mathcal{R}^+$. □

Corollary 4.7. — *We have $(\mathrm{Frac}\,\mathcal{R}^+)^{\varphi=1} = K$.*

Proof. — This follows from propositions 4.6 and 4.5. □

Remark 4.8. — We have $\varphi(\mathcal{R}^+) \subset \mathcal{R}^+$ and $\varphi(\mathcal{R}^{[r;1[}) \subset \mathcal{R}^{[r^{1/d};1[}$ if $r \geqslant r_s$.

1. If the only zero of s in D is 0, then $\varphi(\mathcal{R}^{[r;1[}) \subset \mathcal{R}^{[r^{1/d};1[}$ for all $0 \leqslant r < 1$.
2. It is not true in general that φ preserves $\mathcal{R}^{]0;1[}$. For example, $1/X \in \mathcal{R}^{]0;1[}$ but $\varphi(1/X) = 1/s(X)$, and that series belongs to $\mathcal{R}^{[r;1[}$ only if r is larger than the norm of all the zeroes of $s(X)$. See §8 for a precise conjecture regarding this.

Proof. — We prove (1). An element of $\mathcal{R}^{[r;1[}$ is the sum of an element of $\mathcal{R}^+$ and of $\sum_{n \geqslant 1} h_n/X^n$ where $|h_n| r^{-n} \to 0$. We have $s(X) = s_d X^d \cdot u(X)$ with $u(X) \in 1 + X\mathcal{O}_K[\![X]\!]$ and $s_d \in \mathcal{O}_K^\times$. The claim now follows since $1/s(X)^n = 1/X^{nd} \cdot u(X)^{-n}$ and $u(X)^{-n} \in 1 + X\mathcal{O}_K[\![X]\!]$, and since $\varphi(\mathcal{R}^+) \subset \mathcal{R}^+$. □

Proposition 4.9. — *If $a(X) \in \mathcal{E}^+$ and $a(0) = 1$, the product $\prod_{i=0}^{\infty} a(s^{\circ i}(X))$ converges in $\mathcal{R}^+$ to an element $m_a(X) \in \mathcal{R}^+$ such that $\varphi(m_a) \cdot a = m_a$.*

If in addition $a(X) \in 1 + X \cdot \mathcal{O}_K[\![X]\!]$, then $m_a(X) \in 1 + X \cdot \mathcal{O}_K[\![X]\!]$ as well.

Proof. — The second claim follows from the first, since $a(s^{\circ i}(X)) \in 1 + X \cdot \mathcal{O}_K[\![X]\!]$ for all i in this case. The first claim follows from lemma 1.2 and the fact that for a given $r < 1$, we have $|a(s^{\circ i}(X)) - 1|_r \to 0$ as $i \to +\infty$. □

Remark 4.10. — Compare with remark 4.5 of [**Ked05**].

5. The operator ψ

We have $\mathcal{O}_\mathcal{E}/\pi\mathcal{O}_\mathcal{E} = k(\!(X)\!)$. Since $\mathrm{wideg}(s) = d$, $k(\!(X)\!)$ is a free $k(\!(s(X))\!)$-vector space of dimension d. Hence $\mathcal{O}_\mathcal{E}$ is a free $\varphi(\mathcal{O}_\mathcal{E})$-module of rank d, and we get a "trace" map $\psi : \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ defined on $\mathcal{O}_\mathcal{E}$ by $\varphi(\psi(h)) = \mathrm{Tr}_{\mathcal{O}_\mathcal{E}/\varphi(\mathcal{O}_\mathcal{E})} h(X)$. This map extends to $\mathcal{E}$. We have $\psi(1) = d$ and $\psi(f \cdot \varphi(g)) = \psi(f) \cdot g$.

Remark 5.1. — In p-adic Hodge theory, the operator ψ is usually defined as either $1/d$ or $1/\pi$ times our ψ defined above. See for instance §I.2 of [**Col10**].

In the rest of this section, we assume that $s(X)$ is of finite height. The ring $k[\![X]\!]$ is a free $k[\![s(X)]\!]$-module of rank d. Hence $\mathcal{O}_K[\![X]\!]$ is a free $\varphi(\mathcal{O}_K[\![X]\!])$-module of rank d, and if $h(X) \in \mathcal{O}_K[\![X]\!]$, then $\varphi(\psi(h)) = \mathrm{Tr}_{\mathcal{O}_K[\![X]\!]/\varphi(\mathcal{O}_K[\![X]\!])} h(X)$. This shows that ψ preserves $\mathcal{E}^+$. We next study the restriction of ψ to $\mathcal{E}^\dagger$.

Lemma 5.2. — *If $0 < r < 1$ and $n \geqslant 1$, then $\psi(1/X^n) \in \mathcal{E}^{[\lambda(r);1[}$, and $|\psi(1/X^n)|_{\lambda(r)} \leqslant r^{1-n}/\lambda(r)$.*

Proof. — Let $q(X) = s(X)/X = s_1 + s_2X + \cdots \in \mathcal{O}_K[\![X]\!]$. The formula
$$\psi\left(\frac{1}{X^n}\right) = \psi\left(\frac{q(X)^n}{s(X)^n}\right) = \frac{\psi(q(X)^n)}{X^n}$$
shows that $\psi(1/X^n) \in \mathcal{E}^+[1/X] \subset \mathcal{E}^{[\lambda(r);1[}$. We now prove the bound on $|\psi(1/X^n)|_{\lambda(r)}$.

By corollary 4.4, we have $\max_k |s_k|r^k = |s|_r = |X|_{\lambda(r)}$. This implies that $|s_j/X|_{\lambda(r)} \leqslant r^{-j}$ for all $j \geqslant 1$. In addition, $|s/X \cdot \psi(X^k)|_{\lambda(r)} \leqslant 1/\lambda(r)$ for all $s \in \mathcal{O}_K$ and $k \geqslant 0$.

We can write
$$\psi\left(\frac{1}{X^n}\right) = \psi\left(\frac{q(X)}{s(X)X^{n-1}}\right) = \frac{1}{X}\psi\left(\frac{1}{X^{n-1}}(s_1 + s_2X + \cdots)\right) = \sum_{j \geqslant 1} \frac{s_j}{X}\psi\left(\frac{1}{X^{n-j}}\right).$$

If $n = 1$, this formula and the above observations imply that $|\psi(1/X)|_{\lambda(r)} \leqslant 1/\lambda(r)$. If $n \geqslant 2$ and $1 \leqslant j \leqslant n-1$, then by induction, we get
$$\left|\frac{s_j}{X}\psi\left(\frac{1}{X^{n-j}}\right)\right|_{\lambda(r)} \leqslant r^{-j} \cdot r^{1-n+j}/\lambda(r) \leqslant r^{1-n}/\lambda(r).$$
If $j \geqslant n$, then $|s_j/X \cdot \psi(X^{j-n})|_{\lambda(r)} \leqslant 1/\lambda(r) \leqslant r^{1-n}/\lambda(r)$. This implies the claim. □

Remark 5.3. — Slightly different estimates for certain r are proved in lemma I.9 of [**Col10**] for $s(X) = (1+X)^p - 1$ and in proposition 2.2 of [**FX13**] for $s(X) = \pi \cdot X + X^q$.

Proposition 5.4. — *We have $\psi(\mathcal{E}^{[r;1[}) \subset \mathcal{E}^{[\lambda(r);1[}$ for $r < 1$.*

Proof. — An element of $\mathcal{E}^{[r;1[}$ is the sum of an element of $\mathcal{E}^+$ and of $\sum_{n \geqslant 1} h_n/X^n$ where $|h_n| r^{-n} \to 0$. We have $\psi(\mathcal{E}^+) \subset \mathcal{E}^+$, and $|\psi(h_n/X^n)|_{\lambda(r)} \to 0$ as $n \to +\infty$ by lemma 5.2. The claim follows. □

Remark 5.5. — Since $\psi(\varphi(h)) = d \cdot h$, we recover, when $s(X)$ is a Frobenius lift, the (unproved) corollary 5.3 of [**Ked05**].

We now show that ψ extends from $\mathcal{E}^+$ to $\mathcal{R}^+$. Recall (lemma 1.2) that the family of norms $\{|\cdot|_r\}_{r<1}$ defines a Fréchet structure on $\mathcal{E}^+$, and that the completion of $\mathcal{E}^+$ is $\mathcal{R}^+$.

Proposition 5.6. — *The map $\psi : \mathcal{E}^+ \to \mathcal{E}^+$ is uniformly continuous for the family of norms $\{|\cdot|_r\}_{r<1}$, and extends to a map $\psi : \mathcal{R}^+ \to \mathcal{R}^+$.*

Proof. — We have $\mathcal{O}_K[\![X]\!] = \oplus_{j=0}^{d-1} \mathcal{O}_K[\![s(X)]\!] \cdot X^j$. If $h(X) \in \mathcal{E}^+$, we can therefore write it as $h(X) = \sum_{i \geqslant 0} \sum_{j=0}^{d-1} h_{i,j} s(X)^i X^j$ with $\{h_{i,j}\}$ a bounded sequence of K.

By lemma 4.2, there exists $r_0 < 1$ such that if $r_0 \leqslant r < 1$, then $|s|_r = r^d$. In this case, $|h|_r = \max_{i,j} |h_{i,j}| r^{di+j}$. We then have $\psi(h) = \sum_{j=0}^{d-1} \psi(X^j) \sum_{i \geqslant 0} h_{i,j} X^i$. This implies that if $r \geqslant r_0$, there exists a constant $C(r)$ such that $|\psi(h)|_{r^d} \leqslant C(r) \cdot |h|_r$. The map ψ is therefore uniformly continuous, and extends from $\mathcal{E}^+$ to $\mathcal{R}^+$. □

Since ψ is defined on $\mathcal{E}^\dagger$ and on $\mathcal{R}^+$, it extends to $\psi : \mathcal{R} \to \mathcal{R}$, and we have $\psi(\mathcal{R}^{[r;1[}) \subset \mathcal{R}^{[\lambda(r);1[}$ by proposition 5.4. We finish this section with a few results that are not used in the rest of the paper.

Proposition 5.7. — *Let $e_1, \ldots, e_d$ be a basis of $\mathcal{O}_K[\![X]\!]$ over $\mathcal{O}_K[\![s(X)]\!]$.*

There exists $\delta(X) \neq 0 \in \mathcal{E}^+$ and $e_1^*, \ldots, e_d^* \in \delta(X)^{-1} \cdot \mathcal{E}^+$ such that $\psi(e_i^* e_j) = \delta_{ij}$.

Proof. — Let $\delta(X) = \det(\mathrm{Tr}_{\mathcal{E}^+/\varphi(\mathcal{E}^+)}(e_i e_j))_{i,j} \in \mathcal{E}^+$. The set $e_1, \ldots, e_d$ is a basis of $k(\!(X)\!)$ over $k(\!(s(X))\!)$, and hence of $\mathcal{E}$ over $\varphi(\mathcal{E})$, so that $\mathrm{Tr}_{\mathcal{E}^+/\varphi(\mathcal{E}^+)}(e_i e_j) = \mathrm{Tr}_{\mathcal{E}/\varphi(\mathcal{E})}(e_i e_j)$. The field extension $\mathcal{E}/\varphi(\mathcal{E})$ is separable, hence $\delta(X) \neq 0$. We have $e_i^* = \sum_k \varphi(g_{i,k}) e_k$ where $(g_{i,k})_{i,k} = (\psi(e_m e_n)_{m,n})^{-1}$, so that $e_i^* \in \delta(X)^{-1} \cdot \mathcal{E}^+$. □

Corollary 5.8. — *We have $\mathcal{R}^+ = \oplus_{i=1}^d \varphi(\mathcal{R}^+) \cdot e_i$.*

Proof. — We have $\mathcal{E}^+ = \oplus_{i=1}^d \varphi(\mathcal{E}^+) \cdot e_i$, and if $h = \sum \varphi(h_i) \cdot e_i$, then $h_i = \psi(h e_i^*)$. All the underlying maps extend by uniform continuity to $\mathcal{R}^+$. □

Remark 5.9. — In the cyclotomic and Lubin-Tate cases, $\delta(X) \in (\mathcal{E}^+)^\times$. However, if $s(X) = X^d$, then $\delta(X)$ is a multiple of $X^{d(d-1)}$. In general, the discriminant $\delta(X)$ is equal to $\mathrm{N}_{\mathcal{E}^+/\varphi(\mathcal{E}^+)}\, s'(X)$ since $\mathcal{E} = \varphi(\mathcal{E})[X]$.

Remark 5.10. — Corollary 5.8 cannot be pushed too far. For example, if $s'(0) \neq 0$ (which holds in the cyclotomic and Lubin-Tate cases), then $K[\![X]\!] = K[\![s(X)]\!]$.

6. The space $(\operatorname{Frac} \mathcal{R})^{\varphi=\mu}$

In this section, we prove theorems A and B. Recall that $s(X)$ is of finite height.

Proposition 6.1. — *If $\mu \in K$ and $h \in \mathcal{R}^{\varphi=\mu}$, then $h \in \mathcal{R}^+$.*

Proof. — By applying ψ to $\varphi(h) = \mu \cdot h$, we get $\psi(h) = d/\mu \cdot h$. Repeatedly applying proposition 5.4 shows that $h \in \mathcal{R}^{]0;1[}$. If $g \in \mathcal{R}$, write $g = g^- + g^+$ with $g^- \in 1/X \cdot K[\![1/X]\!]$ and $g^+ \in \mathcal{R}^+$. We have $\psi(h)^- = d/\mu \cdot h^-$. Lemma 5.2 implies that there exists a constant C, depending only on μ/d and K, such that

$$|h^-|_{\lambda(r)} = |\mu/d \cdot \psi(h)^-|_{\lambda(r)} \leqslant C \cdot r/\lambda(r) \cdot |h^-|_r.$$

Iterating this gives $|h^-|_{\lambda^{\circ k}(r)} \leqslant C^k \cdot r/\lambda^{\circ k}(r) \cdot |h^-|_r$. If r is small enough, then $\lambda(r) \leqslant |\pi| r$ by lemma 4.2. Fix such an r. If $n \geqslant 1$, then

$$|X^n h^-|_{\lambda^{\circ k}(r)} \leqslant C^k \cdot r/\lambda^{\circ k}(r) \cdot \lambda^{\circ k}(r)^n / r^n \cdot |X^n h^-|_r \leqslant (C|\pi|^{n-1})^k \cdot |X^n h^-|_r.$$

If $n \geqslant 1$ is large enough so that $C|\pi|^{n-1} \leqslant 1$, proposition 1.10 implies that $X^n h^- \in \mathcal{R}^+$. Hence if $\psi(h) = d/\mu \cdot h$, then $h(X) \in X^{-n} \cdot \mathcal{R}^+$ for some $n \geqslant 0$.

If in addition $\varphi(h) = \mu \cdot h$, then $h(s(X)) \in s(X)^{-n} \cdot \mathcal{R}^+$. If h has a pole at 0, then it has poles at the zeroes of s. So unless $h \in \mathcal{R}^+$, the only zeroes of s are at 0, and 0 is then a zero of order d of s. In this case, if h has a pole of order n at 0, then $\varphi(h)$ has a pole of order dn. We therefore have $h \in \mathcal{R}^+$. □

Remark 6.2. — This gives us another proof that $\mathcal{R}^{\varphi=1} = K$ (proposition 3.4).

Proof. — If $h \in \mathcal{R}^{\varphi=1}$, then $h \in \mathcal{R}^+$ by proposition 6.1, and therefore $h \in K$ by proposition 4.5. □

If $s'(0) \neq 0$, there exists an element $\log_s(X) \in X \cdot \mathcal{R}^+$ such that $\varphi(\log_s) = s'(0) \cdot \log_s$ (see for instance proposition 2.2 of [**Lub94**]; if $r(X) = s(X)/(s'(0) \cdot X)$, and m_r is as in proposition 4.9, then $\log_s(X) = X \cdot m_r(X)$). Therefore $\log_s^k \in (\mathcal{R}^+)^{\varphi = s'(0)^k}$ if $k \geqslant 1$.

Theorem 6.3. — *If $\mu \neq 1 \in K$ and $h \neq 0 \in \mathcal{R}^{\varphi=\mu}$, then $s'(0) \neq 0$, and there exists $k \geqslant 1$ such that $\mu = s'(0)^k$ and $h \in K \cdot \log_s^k$.*

Proof. — If there exists $\mu \neq 1 \in K$ and $h \in \mathcal{R}$ such that $\varphi(h) = \mu h$, then $h \in \mathcal{R}^+$ by proposition 6.1, and $h(0) = \mu h(0)$ so that $h(0) = 0$. If $h(X) = h_k X^k + \mathrm{O}(X^{k+1})$ and $s(X) = s_j X^j + \mathrm{O}(X^{j+1})$, with $h_k, s_j \neq 0$, then the order of vanishing at 0 of μh is k and that of $\varphi(h)$ is jk, so that $j = 1$. This shows that $s'(0) \neq 0$. In this case, $\varphi(h) = \mu h$ implies that $\mu = s_1^k = s'(0)^k$ where s_1, k are as above. Corollary 4.7 now implies that $h = c \cdot \log_s^k$ with $c \in K$. □

Proposition 6.4. — *Take $a, b \in \mathcal{E}^+$ such that $a(0), b(0) \neq 0$.*

If $h \in \mathcal{R}$ is such that $\varphi(h)/h = a/b$, then $h \in \operatorname{Frac} \mathcal{R}^+$.

Proof. — We can replace a by $a/a(0)$ and b by $b/a(0)$ so that $a(0) = 1$. Let $m_a \in \mathcal{R}^+$ be as in proposition 4.9, so that $\varphi(m_a) \cdot a = m_a$. We have $\varphi(hm_a)/(hm_a) = 1/b$, so we only need to prove the claim when $a = 1$.

Assume therefore that $\varphi(h) = h/b$. Recall that $\rho(s)$ is the largest norm of a zero of s in the open unit disk. Fix $r > \rho(s)$ such that $h \in \mathcal{R}^{[r;1[}$. If b has no zero in $A([r;1[)$, then $h/b \in \mathcal{R}^{[r;1[}$ and $\varphi(h/b) = (h/b)/\varphi(b)$. If y is a zero of $\varphi(b)$, then $z = s(y)$ is a zero of b, and we have $|y| \geqslant \min(|z|^{1/d}, |z|/|\pi|)$. We can therefore keep doing this until $\varphi^{\circ n}(b)$ has a zero in $A([r;1[)$. So assume that $\varphi(h) = h/b$ and that b has a zero in $A([r;1[)$. Let c be a full isoclinic factor of b whose zeroes are in $A([r;1[)$ and such that $c(0) = 1$. We have $\varphi(h) \cdot b = h$ so that c divides h in $\mathcal{R}^+$. If $h(z) = 0$ and $s(y) = z$, then $\varphi(h)(y) = 0$. Since $|y| > |z|$ and c is isoclinic, we get that $\varphi(c)$ divides h. By iterating this, we get that, if m_c is the element attached to c by proposition 4.9, then m_c divides h in $\mathcal{R}^+$. We then have $\varphi(h/m_c) \cdot b/c = h/m_c$. This way, we can get rid of all the factors of b corresponding to zeroes in $A([r;1[)$.

By iterating the above two steps, we eventually get that $\varphi(h) \cdot b = h$ where b has no zeroes in D. Indeed, let $N(b) \subset]0;1[$ denote the set of all the norms of the zeroes of b (recall that $b(0) \neq 0$). Each time we divide b by a full isoclinic factor, $\operatorname{card} N(b)$ strictly decreases. And each time we replace b by $\varphi(b)$, the elements of $N(b)$ strictly increase. Past the bound r_s (see proposition 2.2), we have that if $|z| \geqslant r_s$ and $s(y) = z$, then $|y| = |z|^{1/d}$. Therefore, past that point, replacing b by $\varphi(b)$ will not increase $\operatorname{card} N(b)$, while dividing b by a full isoclinic factor will strictly decrease $\operatorname{card} N(b)$. Hence eventually $\operatorname{card} N(b) = 0$.

The resulting element b is therefore of the form $b(0) \cdot c$ where $c \in 1 + X\mathcal{O}_K[\![X]\!]$. Applying proposition 4.9 to c, we get $m_c \in 1 + X\mathcal{O}_K[\![X]\!]$ such that $\varphi(h/m_c) \cdot b(0) = h/m_c$. Proposition 6.1 now implies that $h/m_c \in \mathcal{R}^+$, and we are done. □

Remark 6.5. — If in addition $h \in \mathcal{E}^\dagger$, then $h \in \operatorname{Frac} \mathcal{R}^+ \cap \mathcal{E}^\dagger = \operatorname{Frac} \mathcal{E}^+$ by lemma 1.6.

Now compare proposition 6.4 with lemma 5.4 of [**Ked05**].

Theorem 6.6. — *If* $\mu \in K$ *and* $f \in (\operatorname{Frac}\mathcal{R})^{\varphi=\mu}$, *then* $f^{\pm 1} \in \mathcal{R}^+$.

Proof. — Take $f/g \in (\operatorname{Frac}\mathcal{R})^{\varphi=\mu}$. By lemma 1.7, we can assume that $g = g^+ \in \mathcal{R}^+$ and that $f = f^+h$ with $f^+ \in \mathcal{R}^+$ and $h \in \mathcal{E}^\dagger$. We get

$$\frac{\varphi(h)}{h} = \mu \cdot \frac{f^+ \cdot \varphi(g^+)}{\varphi(f^+) \cdot g^+} \in \operatorname{Frac}\mathcal{R}^+ \cap \mathcal{E}^\dagger = \operatorname{Frac}\mathcal{E}^+$$

where the last equality follows from lemma 1.6. Hence we can write $\varphi(h)/h = a/b$ with $a, b \in \mathcal{E}^+$. In addition, we can divide f^+ and g^+ by powers of X, and assume that $f^+(0), g^+(0) \neq 0$, and then that $a(0), b(0) \neq 0$.

By proposition 6.4, $h \in \operatorname{Frac}\mathcal{R}^+$. Therefore, $f/g = f^+h/g^+$ belongs to $\operatorname{Frac}\mathcal{R}^+$. The claim now follows from proposition 4.6. □

Remark 6.7. — 1. Compare with lemma 5.6 of [**Ked05**] (or rather its corrected version, see the errata to ibid.)

2. In the cyclotomic case, namely when $s(X) = (1+X)^p - 1$, the computations of §3.2 of [**Col14**] give a different proof of the fact that $(\operatorname{Frac}\mathcal{R})^{\varphi=\mu} = (\operatorname{Frac}\mathcal{R}^+)^{\varphi=\mu}$.

We can now state theorem A.

Theorem 6.8. — *If* φ *is of finite height, then* $(\operatorname{Frac}\mathcal{R})^{\varphi=1} = K$. *In addition,*

1. $(\operatorname{Frac}\mathcal{R})^{\varphi=s'(0)^k} = K \cdot \log_s^k$ *if* $s'(0) \neq 0$ *and* $k \in \mathbf{Z}$*;*
2. $(\operatorname{Frac}\mathcal{R})^{\varphi=\mu} = \{0\}$ *if* $\mu \neq 1 \in K$ *and if either* $s'(0) = 0$ *or if* $s'(0) \neq 0$ *and* μ *is not of the form* $s'(0)^k$ *for some* $k \in \mathbf{Z}$.

Proof. — This follows from theorem 6.6, proposition 4.5 and theorem 6.3. □

7. Application to φ-modules

In this section, we assume that $(\operatorname{Frac}\mathcal{R})^{\varphi=1} = K$, and we give some applications to φ-modules. A φ-module over $\operatorname{Frac}\mathcal{R}$ is a finite dimensional $\operatorname{Frac}\mathcal{R}$-vector space, with a semi-linear map $\varphi : \mathrm{M} \to \mathrm{M}$.

Proposition 7.1. — *If* M *is a* φ*-module over* $\operatorname{Frac}\mathcal{R}$, *then* $\mathrm{M}^{\varphi=1} \otimes_K \operatorname{Frac}\mathcal{R} \to \mathrm{M}$ *is injective. In particular,* $\mathrm{M}^{\varphi=1}$ *is a finite dimensional* K*-vector space.*

Proof. — Let $m_1 \otimes f_1 + \cdots + m_r \otimes f_r$ be in the kernel of the map, with r minimal. We can assume that $f_1 = 1$. Applying φ and subtracting gives a shorter relation, which is zero by minimality, so that $\varphi(f_i) = f_i$ for all i. Hence $f_i \in (\operatorname{Frac}\mathcal{R})^{\varphi=1} = K$. □

A φ-module over $\mathcal{R}$ is a free $\mathcal{R}$-module D of finite rank, with a semi-linear map $\varphi : \mathrm{D} \to \mathrm{D}$ (one usually assumes in addition that $\varphi^*(\mathrm{D}) = \mathrm{D}$, but we do not use this).

Corollary 7.2. — *If* D *is a φ-module over $\mathcal{R}$, then $\mathrm{D}^{\varphi=1} \otimes_K \mathcal{R} \to \mathrm{D}$ is injective. In particular, $\mathrm{D}^{\varphi=1}$ is a finite dimensional K-vector space.*

Proof. — This follows from proposition 7.1 applied to $\mathrm{M} = \operatorname{Frac} \mathcal{R} \otimes_{\mathcal{R}} \mathrm{D}$. □

Remark 7.3. — This gives a proof of the unproved assertion "Note that $\mathrm{D}^{\varphi_q=1}$ is finite-dimensional over L" on page 2571 of [**FX13**].

We say that $\mathcal{R}'/\mathcal{R}$ is a finite extension of Robba rings if $\mathcal{R}'$ itself is a Robba ring with coefficients in a finite extension L of K, and in a variable Y, and if $\mathcal{R}'$ is a free $\mathcal{R}$-module of finite rank. We also assume that φ extends to $\mathcal{R}'$. These objects occur for instance in p-adic Hodge theory, when $\mathcal{R}$ is attached to a p-adic field F, and we are given a finite extension F'/F. In this case there is a corresponding finite extension $\mathcal{R}'/\mathcal{R}$ of Robba rings as defined above (see for instance §I.2 of [**Ber08**]). For example, take $K = L = \mathbf{Q}_p$ and $s(X) = (1+X)^p - 1$ (the cyclotomic case). If $Y = X^{1/n}$ with $n \geqslant 1$, then $\mathcal{R}'/\mathcal{R}$ is a finite extension of Robba rings of degree n, and if $p \nmid n$ we can set

$$\varphi(Y) = ((1+X)^p - 1)^{1/n} = Y^p \cdot \left(1 + \frac{p}{Y^n} + \cdots + \frac{p}{Y^{n(p-1)}}\right)^{1/n} \in (\mathcal{E}')^\dagger.$$

Corollary 7.4. — *Let $\mathcal{R}'/\mathcal{R}$ be a finite extension of Robba rings, with coefficients in L and K, such that φ extends to $\mathcal{R}'$. If $(\operatorname{Frac} \mathcal{R})^{\varphi=1} = K$, then $(\operatorname{Frac} \mathcal{R}')^{\varphi=1} = L$.*

Proof. — The hypotheses on $\mathcal{R}'/\mathcal{R}$ imply that $\operatorname{Frac} \mathcal{R}'$ is a finite extension of $\operatorname{Frac} \mathcal{R}$, and therefore also a φ-module over $\operatorname{Frac} \mathcal{R}$. By proposition 7.1, $(\operatorname{Frac} \mathcal{R}')^{\varphi=1}$ is a finite dimensional K-vector space. It is also a field extension of L. The corollary now results from lemma 1.8 applied to $\mathcal{R}'$. □

8. Convergence close to the origin

We still assume $s(X)$ to be of finite height. Recall (see remark 4.8) that it is not true in general that φ preserves $\mathcal{R}^{]0;1[}$. For example, $1/X \in \mathcal{R}^{]0;1[}$ but $\varphi(1/X) = 1/s(X)$, that belongs to $\mathcal{R}^{[r;1[}$ only if $r > \rho(s)$. We propose the following conjecture.

Conjecture 8.1. — *If $h \in \mathcal{R}$ is such that $\varphi(h) \in \mathcal{R}^{[\rho(s);1[}$, then $h \in \mathcal{R}^+$.*

Proposition 8.2. — *Conjecture 8.1 is true in the cyclotomic case, namely when $s(X) = (1+X)^p - 1$.*

Lemma 8.3. — *Let S be the set of sequences $\{x_k\}_{k\geqslant 0}$ with $x_k \in K$. Define an operator $T : S \to S$ by the formula $(Tx)_\ell = \sum_{k=0}^{\ell}(-1)^k\binom{\ell}{k}x_k$. If both sequences x and Tx converge to 0, then $x = 0$.*

Proof. — Suppose that x converges to 0, and let $f : \mathbf{Z}_p \to K$ be given by the formula $f(z) = \sum_{k\geqslant 0}(-1)^k\binom{z}{k}x_k$. The function f is continuous and $(Tx)_\ell = f(\ell)$. If $f(\ell) \to 0$ as $\ell \to +\infty$, then $f = 0$ by continuity, and hence $x = 0$. □

Proof of proposition 8.2. — Let ε be a primitive p-th root of 1. Since $s(X) = (1+X)^p - 1$, we have $\rho(s) = \rho = |\varepsilon - 1|$. Take $r > \rho$ and $g(X) = \sum_{n\geqslant 1} g_n/X^n \in \mathcal{E}^{[r;1[}$. We have $g((1+X)\varepsilon - 1) = g(X\varepsilon + \varepsilon - 1) \in \mathcal{E}^{[r;1[}$ and we expand it as follows:

$$\sum_{n\geqslant 1}\frac{g_n}{(X\varepsilon+\varepsilon-1)^n} = \sum_{n\geqslant 1}\frac{g_n}{X^n}\varepsilon^{-n}\left(1+\frac{\varepsilon-1}{X\varepsilon}\right)^{-n} = \sum_{n\geqslant 1}\frac{g_n}{X^n}\varepsilon^{-n}\sum_{j\geqslant 0}\binom{-n}{j}\left(\frac{\varepsilon-1}{X\varepsilon}\right)^j$$

By setting $m = n+j$ and using the fact that $\binom{-n}{j} = (-1)^j\binom{n+j-1}{j}$, we get $g((1+X)\varepsilon-1) = \sum_{m\geqslant 1} b_m/X^m$ where $b_m = \varepsilon^{-m}\sum_{n=1}^{m}(-1)^{n-m}\binom{m-1}{n-1}g_n(\varepsilon-1)^{n-m}$. This gives us an explicit formula for the coefficients of $g((1+X)\varepsilon - 1) \in \mathcal{E}^{[r;1[}$.

We now prove that if $g(X) \in \mathcal{R}^{[\rho;1[}$ is such that $g((1+X)\varepsilon-1) \in \mathcal{R}^{[\rho;1[}$, then $g(X) \in \mathcal{R}^+$. It is enough to prove that the negative part $\sum_{n\geqslant 1} g_n/X^n$ of g is zero, so we assume that $g(X) = \sum_{n\geqslant 1} g_n/X^n$ as above. If we let $x_k = g_{k+1}(\varepsilon-1)^{k+1}$ and $y_\ell = (-1)^\ell\varepsilon^{\ell+1}b_{\ell+1}(\varepsilon - 1)^{\ell+1}$ for $k, \ell \geqslant 0$, then $y_\ell = \sum_{k=0}^{\ell}(-1)^k\binom{\ell}{k}x_k$. The fact that $g(X) \in \mathcal{E}^{[\rho;1[}$ is equivalent to $x_k \to 0$ as $k \to +\infty$, and likewise the fact that $g((1+X)\varepsilon - 1) \in \mathcal{E}^{[\rho;1[}$ is equivalent to $y_\ell \to 0$ as $\ell \to +\infty$. The claim now results from lemma 8.3, applied to $\{x_k\}_{k\geqslant 0}$, since $y = Tx$ in the notation of that lemma.

We now prove the proposition. If $g(X) = \varphi(h)(X) \in \mathcal{R}^{[\rho;1[}$, then $\varphi(h)(X) = \varphi(h)((1+X)\varepsilon-1)$ so that by the above claim $\varphi(h)(X) \in \mathcal{R}^+$. Therefore $h = 1/p\cdot\psi\varphi(h) \in \mathcal{R}^+$. □

Remark 8.4. — The method of proof of proposition 8.2 is reminiscent of the Amice-Fresnel theorem (see [**AF72**], Théorème 1 or [**Rob00**], §4.4 of chapter 6).

References

[AF72] Yvette Amice and Jean Fresnel, *Fonctions zêta p-adiques des corps de nombres abeliens réels*, Acta Arith. **20** (1972), 353–384.

[Ber08] Laurent Berger, *Équations différentielles p-adiques et (φ, N)-modules filtrés*, Astérisque (2008), no. 319, 13–38.

[Col10] Pierre Colmez, *La série principale unitaire de* $\mathrm{GL}_2(\mathbf{Q}_p)$, Astérisque (2010), no. 330, 213–262.

[Col14] Pierre Colmez, *La série principale unitaire de* $\mathrm{GL}_2(\mathbf{Q}_p)$ *: vecteurs localement analytiques*, Automorphic forms and Galois representations. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 414, Cambridge Univ. Press, Cambridge, 2014, pp. 286–358.

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

[Ked00] Kiran Kedlaya, *Descent theorems for overconvergent F-crystals*, Ph.D. thesis, Massachusetts Institute of Technology, 2000.

[Ked05] Kiran Kedlaya, *Frobenius modules and de Jong's theorem*, Math. Res. Lett. **12** (2005), no. 2-3, 303–320.

[Laz62] Michel Lazard, *Les zéros des fonctions analytiques d'une variable sur un corps valué complet*, Inst. Hautes Études Sci. Publ. Math. (1962), no. 14, 47–75.

[Lub94] Jonathan Lubin, *Nonarchimedean dynamical systems*, Compositio Math. **94** (1994), no. 3, 321–346.

[MZ02] William Messing and Thomas Zink, *De Jong's theorem on homomorphisms of p-divisible groups*, preprint, 2002.

[Rob00] Alain Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000.

Laurent Berger