Münster J. of Math. **14** (2021), 155–163
DOI 10.17879/59019521586
urn:nbn:de:hbz:6-59019522020

Münster Journal of Mathematics

The Weierstrass preparation theorem and resultants of *p*-adic power series

Laurent Berger

(Communicated by Peter Schneider)

Abstract. We define the resultant of two power series with coefficients in the ring of integers of a p-adic field. In order to do this, we prove a universal version of the Weierstrass preparation theorem.

Introduction

Given two polynomials P and Q with coefficients in a field K, the resultant $\mathrm{Res}(P,Q)$ allows us to determine whether P and Q have a common root in $\overline{K}$. The resultant is a polynomial function of the coefficients of P and Q, and $\mathrm{Res}(P,Q)=0$ if and only if P and Q have a common root.

In this article, we consider a similar question for p-adic power series. Let K be 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 $\mathcal{O}_K$. Let $\mathbf{C}_p$ be the completion of an algebraic closure $\overline{K}$ of K, so that $\mathfrak{m}_{\mathbf{C}_p}$ is the p-adic open unit disk. A power series $f(X)=f_0+f_1X+\cdots\in\mathcal{O}_K[\![X]\!]$ defines a bounded holomorphic function on $\mathfrak{m}_{\mathbf{C}_p}$, and may have roots in this domain. Given two such power series, we would like to know whether they have a common root. The Weierstrass degree $\mathrm{wideg}(f)$ of f is the smallest integer n such that $f_n\in\mathcal{O}_K^\times$, or $+\infty$ if there is no such integer. If $\mathrm{wideg}(f)=n$ is finite, then f has precisely n roots (counting multiplicities) in $\mathfrak{m}_{\mathbf{C}_p}$. Our main result is the following.

Theorem A. *For all $n\geqslant 1$, there exists a power series*

$$\mathrm{Res}_n(\{F_i\}_{i\geqslant 0},\{G_i\}_{i\geqslant 0})\in\mathbf{Z}[F_n,F_n^{-1},\{F_k\}_{k\geqslant n+1},\{G_k\}_{k\geqslant 0}][\![F_0,\dots,F_{n-1}]\!]$$

such that for all power series $f(X)$, $g(X)\in\mathcal{O}_K[\![X]\!]$, with $\mathrm{wideg}(f)=n$, *we have*

$$\prod_{\substack{z\in\mathfrak{m}_{\mathbf{C}_p}\\ f(z)=0}} g(z)=\mathrm{Res}_n(\{f_i\}_{i\geqslant 0},\{g_i\}_{i\geqslant 0}).$$

In particular, $\mathrm{Res}_n(\{f_i\}_{i\geqslant 0}, \{g_i\}_{i\geqslant 0}) = 0$ *if and only if* f *and* g *have a common root in* $\mathfrak{m}_{\mathbf{C}_p}$.

Note that if $\mathrm{wideg}(f) = n$, then $f_0, \dots, f_{n-1} \in \mathfrak{m}_K$ so that the power series $\mathrm{Res}_n(\{f_i\}_{i\geqslant 0}, \{g_i\}_{i\geqslant 0})$ does converge. The main technical tool for proving theorem A is the Weierstrass preparation theorem. We use a version due to O'Malley (see [6]) which allows us to prove the following universal Weierstrass preparation theorem. Recall that if R is a ring and I is an ideal of R, a polynomial is said to be distinguished for I if it is monic and all its non-leading coefficients are in I. If $n \geqslant 1$, let $R_n = \mathbf{Z}[F_n, F_n^{-1}, \{F_k\}_{k\geqslant n+1}][\![F_0, \dots, F_{n-1}]\!]$ and let I_n be the ideal of R_n generated by $F_0, \dots, F_{n-1}$.

Theorem B. *We can write the power series* $F(X) = \sum_{i\geqslant 0} F_i X^i \in R_n[\![X]\!]$ *as* $F(X) = P(X)U(X)$, *where* $U(X) \in R_n[\![X]\!]^\times$ *and* $P(X) = X^n + P_{n-1}X^{n-1} + \dots + P_0 \in R_n[X]$ *is a distinguished polynomial for the ideal* I_n.

In addition, P *and* U *are uniquely determined by* F.

Theorem B provides a universal Weierstrass preparation theorem, and the existence part of the classical versions follows by specializing. In particular, Theorem B shows how the coefficients of p and u depend on those of f when we write a power series $f(X) \in \mathcal{O}_K[\![X]\!]$ as the product of a distinguished polynomial p and a unit u.

In Section 3, we give an application of our results to the iteration of power series in characteristic p. We show that such a power series admits a lift to characteristic zero satisfying certain properties, which strengthens a construction of Lubin (see [5]).

We finish this article with a sketch of an analogue of our constructions that singles out the roots of a power series in a circle, instead of in an open disk.

1. A universal Weierstrass preparation theorem

The classical Weierstrass preparation theorem over $\mathcal{O}_K$ (see, for instance, [3, Ch. VII, Section 3, no 8]) says that if $f(X) \in \mathcal{O}_K[\![X]\!]$ and $\mathrm{wideg}(f) = n$, there exists a distinguished (for the ideal $\mathfrak{m}_K$) polynomial $p(X)$ of degree n and a unit $u(X) \in \mathcal{O}_K[\![X]\!]^\times$ such that $f = pu$. In addition, p and u are uniquely determined by f. The coefficients of p and u depend on those of f. In order to make this dependence more explicit, we use the following strengthening of the Weierstrass preparation theorem, which is [6, Thm. 2.10].

Theorem 1.1. *Let* R *be a ring, and take* $f(X) = f_0 + f_1 X + \dots \in R[\![X]\!]$. *Suppose that* $f_n \in R^\times$ *and that* R *is separated and complete for the* $(f_0, \dots, f_{n-1})$*-adic topology.*

There exists a distinguished (*for the ideal* $(f_0, \dots, f_{n-1})$) *polynomial* $p(X)$ *of degree* n *and* $u(X) \in R[\![X]\!]^\times$ *such that* $f = pu$.

In addition, p *and* u *are uniquely determined by* f.

Although we do not need this in the remainder of this article, we point out the following corollary of Theorem 1.1. Note that some even more general versions of the Weierstrass preparation theorem can be found, see, for instance, [4].

Corollary 1.2. *Let R be a ring and let J be an ideal of R such that R is separated and complete for the J-adic topology. Take $f(X) = f_0 + f_1X + \cdots \in R[\![X]\!]$. Suppose that $f_n \in R^\times$ and that $f_0, \dots, f_{n-1} \in J$.*

There exists a distinguished (for the ideal J) polynomial $p(X)$ of degree n and $u(X) \in R[\![X]\!]^\times$ such that $f = pu$.

In addition, p and u are uniquely determined by f.

Proof. This follows from Theorem 1.1, and the following assertion [8, Tag 00M9, Lem. 10.95.8]: if $I \subset J$ are two ideals of a ring R, with I finitely generated, and if R is separated and complete for the J-adic topology, then R is separated and complete for the I-adic topology. $\square$

If $n \geqslant 1$ is fixed, we can consider the variables $\{F_i\}_{i\geqslant 0}$ and we define

$$R_n = \mathbf{Z}[F_n, F_n^{-1}, \{F_k\}_{k\geqslant n+1}][\![F_0, \dots, F_{n-1}]\!].$$

The ring R_n is separated and complete for the $(F_0, \dots, F_{n-1})$-adic topology, and the following result (Theorem B) is an immediate consequence of Theorem 1.1.

Theorem 1.3. *We can write $F(X) = \sum_{i\geqslant 0} F_iX^i \in R_n[\![X]\!]$ as $F(X) = P(X)U(X)$, where $U(X) \in R_n[\![X]\!]^\times$ and $P(X) = X^n + P_{n-1}X^{n-1} + \cdots + P_0 \in R_n[X]$ is a distinguished polynomial for the ideal I_n.*

In addition, P and U are uniquely determined by F.

Example 1.4. We give an explicit formula for $P(X)$ in Theorem 1.3 when $n = 1$. If $n = 1$, then $P(X) = X + P_0$ and $P_0 \in R_1 = \mathbf{Z}[F_1, F_1^{-1}, \{F_k\}_{k\geqslant 2}][\![F_0]\!]$ is given by the following formula ([1, Prop. 2.2]; here $\pi(j,n)$ denotes the set of $i_1, \dots, i_n \in \mathbf{Z}_{\geqslant 0}$ such that $i_1 + i_2 + \cdots + i_n = j$ and $i_1 + 2i_2 + \cdots + ni_n = n$):

$$\begin{aligned} P_0 &= \sum_{n\geqslant 0} F_0^{n+1} \sum_{j=0}^{n} \Big(-\frac{1}{F_1}\Big)^{n+j+1} \sum_{\pi(j,n)} \frac{(n+j)!}{(n+1)!i_1!i_2!\cdots i_n!} F_2^{i_1}F_3^{i_2}\cdots F_{n+1}^{i_n} \\ &= -\frac{F_0}{F_1} - F_0^2 \cdot \frac{F_2}{F_1^3} + F_0^3 \cdot \Big(\frac{F_3}{F_1^4} - \frac{2F_2^2}{F_1^5}\Big) + \mathrm{O}(F_0^4). \end{aligned}$$

(We have $(n+j)!/(n+1)!i_1!i_2!\cdots i_n! \in \mathbf{Z}$ if $i_1 + i_2 + \cdots + i_n = j$ and $i_1 + 2i_2 + \cdots + ni_n = n$; indeed, $(n+j)!/(n+1)!i_1!i_2!\cdots i_n!$ becomes a multinomial coefficient and hence an integer if we replace either $n+1$ by n or i_k by $i_k - 1$ for some k. If ℓ is a prime number, then it cannot divide both $n+1$ and all of the i_k. Hence $(n+j)!/(n+1)!i_1!i_2!\cdots i_n!$ is a rational number that is ℓ-integral for every prime number ℓ, and is therefore an integer).

2. Resultants and discriminants of p-adic power series

By the theory of Newton polygons, a distinguished polynomial $p(X) = X^n + p_{n-1}X^{n-1} + \cdots + p_0 \in \mathcal{O}_K[X]$ of degree n has precisely n roots in $\mathfrak{m}_{\mathbf{C}_p}$ (counting multiplicities). Let $p(X)$ be such a polynomial. If $g(X) = \sum_{i \geqslant 0} g_i X^i \in \mathcal{O}_K[\![X]\!]$, we can consider $\prod_{p(z)=0} g(z)$.

Proposition 2.1. *There exists a power series*

$$\mathrm{ResPol}_n(P_0, \ldots, P_{n-1}, \{G_k\}_{k \geqslant 0}) \in \mathbf{Z}[\{G_k\}_{k \geqslant 0}][\![P_0, \ldots, P_{n-1}]\!]$$

such that for all $g(X) = \sum_{i \geqslant 0} g_i X^i \in \mathcal{O}_K[\![X]\!]$ and all distinguished polynomial $p(X) = X^n + p_{n-1}X^{n-1} + \cdots + p_0 \in \mathcal{O}_K[X]$ of degree n, we have

$$\prod_{p(z)=0} g(z) = \mathrm{ResPol}_n(p_0, \ldots, p_{n-1}, \{g_k\}_{k \geqslant 0}).$$

Proof. Let $Z_1, \ldots, Z_n$ denote n variables. For each n-uple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbf{Z}_{\geqslant 0}$ with $d_1 \leqslant \cdots \leqslant d_n$, let $Z_{\mathbf{d}} = \sum_{(e_1, \ldots, e_n)} Z_1^{e_1} \cdots Z_n^{e_n}$, where $(e_1, \ldots, e_n)$ ranges over all distinct permutations of $(d_1, \ldots, d_n)$. There exists polynomials $S_{\mathbf{d}} \in \mathbf{Z}[\{G_k\}_{k \geqslant 0}]$ for each $\mathbf{d}$, such that

$$\prod_{i=1}^{n} \sum_{k \geqslant 0} G_k Z_i^k = \sum_{\mathbf{d}} S_{\mathbf{d}}(\{G_k\}_{k \geqslant 0}) Z_{\mathbf{d}}.$$

If we write $\prod_{i=1}^{n}(X - Z_i) = X^n + P_{n-1}X^{n-1} + \cdots + P_0$, then by the fundamental theorem of symmetric polynomials, each $Z_{\mathbf{d}}$ belongs to $\mathbf{Z}[P_0, \ldots, P_{n-1}]$. We set

$$\mathrm{ResPol}_n = \sum_{\mathbf{d}} S_{\mathbf{d}}(\{G_k\}_{k \geqslant 0}) Z_{\mathbf{d}} \in \mathbf{Z}[\{G_k\}_{k \geqslant 0}][\![P_0, \ldots, P_{n-1}]\!].$$

Note that the total degree of $Z_{\mathbf{d}}$ is $d_1 + \cdots + d_n$ so that the degree of $Z_{\mathbf{d}}$ as an element of $\mathbf{Z}[P_0, \ldots, P_{n-1}]$ is at least $(d_1 + \cdots + d_n)/n$. Therefore, the above sum converges for the $(P_0, \ldots, P_{n-1})$-adic topology. The proposition follows by specializing. ☐

We can now prove Theorem A.

Theorem 2.2. *There exists a power series*

$$\mathrm{Res}_n(\{F_i\}_{i \geqslant 0}, \{G_i\}_{i \geqslant 0}) \in \mathbf{Z}[F_n, F_n^{-1}, \{F_k\}_{k \geqslant n+1}, \{G_k\}_{k \geqslant 0}][\![F_0, \ldots, F_{n-1}]\!]$$

such that for all power series $f(X)$, $g(X) \in \mathcal{O}_K[\![X]\!]$ with $\mathrm{wideg}(f) = n$, *we have*

$$\prod_{\substack{z \in \mathfrak{m}_{\mathbf{C}_p} \\ f(z)=0}} g(z) = \mathrm{Res}_n(\{f_i\}_{i \geqslant 0}, \{g_i\}_{i \geqslant 0}).$$

Proof. By Theorem 1.3, we can write the power series $F(X) = \sum_{i \geqslant 0} F_i X^i$ as $F(X) = P(X)U(X)$ with $P(X) = X^n + P_{n-1}X^{n-1} + \cdots + P_0$, where each P_i

belongs to the ideal $(F_0,\ldots,F_{n-1})$ of $\mathbf{Z}[F_n,F_n^{-1},\{F_k\}_{k\geqslant n+1}][\![F_0,\ldots,F_{n-1}]\!]$. The result follows from Proposition 2.1, by setting

$$\mathrm{Res}_n=\mathrm{ResPol}_n(P_0,\ldots,P_{n-1},\{G_k\}_{k\geqslant 0}). \qquad \square$$

If $f,g\in\mathcal{O}_K[\![X]\!]$ and $\mathrm{wideg}(f)=n$, we write $\mathrm{Res}_n(f,g)$ instead of the more cumbersome $\mathrm{Res}_n(\{f_i\}_{i\geqslant 0},\{g_i\}_{i\geqslant 0})$.

Remark 2.3. We have $\mathrm{Res}_n(f,gh)=\mathrm{Res}_n(f,g)\,\mathrm{Res}_n(f,h)$.

Definition 2.4. We define Disc_n to be the power series

$$\mathrm{Disc}_n(\{F_i\}_{i\geqslant 0})=\mathrm{Res}_n(F,F')\in\mathbf{Z}[F_n,F_n^{-1},\{F_k\}_{k\geqslant n+1}][\![F_0,\ldots,F_{n-1}]\!],$$

and likewise write $\mathrm{Disc}_n(f)$ instead of $\mathrm{Disc}_n(\{f_i\}_{i\geqslant 0})$.

By Theorem 2.2, a power series $f(X)\in\mathcal{O}_K[\![X]\!]$ with $\mathrm{wideg}(f)=n$ has only simple roots in $\mathfrak{m}_{\mathbf{C}_p}$ if and only if $\mathrm{Disc}_n(f)\neq 0$.

Proposition 2.5. *The set of elements of $\mathcal{O}_K[\![X]\!]$ having only simple roots in $\mathfrak{m}_{\mathbf{C}_p}$ is open in the p-adic topology.*

Proof. Take $f(X)\in\mathcal{O}_K[\![X]\!]$ having only simple roots in $\mathfrak{m}_{\mathbf{C}_p}$. We can divide f by an appropriate power of π and assume that $\mathrm{wideg}(f)$ is finite. Let $n=\mathrm{wideg}(f)$ and $v=\mathrm{val}_\pi\,\mathrm{Disc}_n(f)$.

The fact that Disc_n belongs to $\mathbf{Z}[F_n,F_n^{-1},\{F_k\}_{k\geqslant n+1}][\![F_0,\ldots,F_{n-1}]\!]$ implies that for every $h(X)\in\mathcal{O}_K[\![X]\!]$, we have $\mathrm{val}_\pi\,\mathrm{Disc}_n(f+\pi^{v+1}h)=v$, so that if $g(X)\in\mathcal{O}_K[\![X]\!]$ is such that $\mathrm{val}_\pi(f-g)\geqslant v+1$, then $g(X)$ has only simple roots in $\mathfrak{m}_{\mathbf{C}_p}$. $\square$

Note that the set of elements of $\mathcal{O}_K[\![X]\!]$ having only simple roots in $\mathfrak{m}_{\mathbf{C}_p}$ is also dense in the p-adic topology. If $f=pu$, with p distinguished having multiple roots, then p can be approached by distinguished polynomials having only simple roots. Indeed, the (usual) discriminant of $p(X)=X^n+p_{n-1}X^{n-1}+\cdots+p_0$ is a polynomial $\Delta(p_0,\ldots,p_{n-1})$ and its zero set is closed with empty interior.

3. Lubin's proof of Sen's theorem on iteration of power series

In this section, we give an application of the above constructions. In his paper [5], Lubin gives a short and very nice proof of Sen's theorem on iteration of power series. We start by recalling Sen's theorem and Lubin's argument. Recall that k is the residue field of $\mathcal{O}_K$. If $w(X)=X+\sum_{i\geqslant 2}w_iX^i\in k[\![X]\!]$, let $i(w)=m-1$, where m is the smallest integer $\geqslant 2$ such that $w_m\neq 0$ (or $+\infty$ if there is no such integer). For $n\geqslant 0$, let $i_n(w)=i(w^{\circ p^n})$. Sen's theorem [7, Thm. 1] says that $i_{n-1}(w)\equiv i_n(w) \bmod p^n$ for all $n\geqslant 1$ (where the congruence holds automatically if one side is $+\infty$).

Lubin's argument is to show that for each $n\geqslant 0$ such that $i_n(w)\neq+\infty$, there exists a finite extension L of K and a power series $f_n(X)\in X\cdot\mathcal{O}_L[\![X]\!]$

such that the image of $f_n(X)$ in $k_L[\![X]\!]$ is $w(X)$ and such that all the roots of $f_n^{\circ p^n}(X)-X$ in $\mathfrak{m}_{\mathbf{C}_p}$ are simple. We then have

$$i_n(w)-i_{n-1}(w)=\operatorname{wideg}\left(\frac{f_n^{\circ p^n}(X)-X}{f_n^{\circ p^{n-1}}(X)-X}\right),$$

so that $i_n(w)-i_{n-1}(w)$ is the number of points of $\mathfrak{m}_{\mathbf{C}_p}$ whose orbit under f_n is of cardinality p^n. This number is clearly divisible by p^n, which implies Sen's theorem.

Using our methods, we can improve Lubin's result. We prove that there is one lift f of w that works for all n, and has coefficients in $\mathcal{O}_K$.

Theorem 3.1. *Take $w(X)=X+\sum_{i\geqslant 2} w_i X^i \in k[\![X]\!]$ and let $N\subset \mathbf{Z}_{\geqslant 0}$ be the set of n such that $i_n(w)$ is finite. There exists $f(X)\in X\cdot\mathcal{O}_K[\![X]\!]$ whose image in $k[\![X]\!]$ is $w(X)$ and such that for all $n\in N$, the roots of $f^{\circ p^n}(X)-X$ in $\mathfrak{m}_{\mathbf{C}_p}$ are simple.*

Proof. Let W be the set of $f(X)\in X\cdot\mathcal{O}_K[\![X]\!]$ whose image in $k[\![X]\!]$ is $w(X)$, and let W_n be the set of elements of W such that the roots of $f^{\circ p^n}(X)-X$ in $\mathfrak{m}_{\mathbf{C}_p}$ are simple. We prove that if $n\in N$, then W_n is open and dense in W for the p-adic topology. Since W is a complete metric space, the theorem follows from this assertion and Baire's theorem, which implies that $\bigcap_{n\in N} W_n$ is dense in W and hence nonempty.

Fix an element $\tilde{w}\in W$. We have $W=\{\tilde{w}+h, h\in \pi X\cdot\mathcal{O}_K[\![X]\!]\}$.

If $F(X)=\sum_{j\geqslant 1} F_j X^j$, write $F^{\circ p^n}(X)-X=\sum_{j\geqslant 1} F_j^{(n)} X^j$. Take $n\in N$ and let $i=i_n(w)+1$. Let $F(X)=\sum_{j\geqslant 1}(\tilde{w}_j+H_j)X^j$, where $\{H_j\}_{j\geqslant 1}$ are variables. For all $j\geqslant 1$, $F_j^{(n)}\in\mathcal{O}_K[H_1,\dots,H_j]$. Since $F_i^{(n)}(0)=\tilde{w}_i^{(n)}\in\mathcal{O}_K^\times$, $F_i^{(n)}$ has an inverse $(F_i^{(n)})^{-1}\in\mathcal{O}_K[\![H_1,\dots,H_i]\!]$. If $j\leqslant i-1$, then $\tilde{w}_j^{(n)}\in\mathfrak{m}_K$, and so $F_j^{(n)}$ is in the ideal $(\pi,H_1,\dots,H_j)$ of $\mathcal{O}_K[H_1,\dots,H_j]$. The power series

$$\mathrm{Disc}_i(F^{\circ p^n}(X)-X)\in\mathbf{Z}[F_i^{(n)},(F_i^{(n)})^{-1},\{F_j^{(n)}\}_{j\geqslant i+1}][\![F_1^{(n)},\dots,F_{i-1}^{(n)}]\!]$$

therefore gives rise to an element $D_n(\{H_j\}_{j\geqslant 1})\in\mathcal{O}_K[\{H_j\}_{j\geqslant i+1}][\![H_1,\dots,H_i]\!]$.

Let us first show that W_n is open in W. If $f=\tilde{w}+h\in W_n$, with $h\in\pi X\cdot\mathcal{O}_K[\![X]\!]$, then $D_n(h)\neq 0$ by definition. If $v=\mathrm{val}_\pi(D_n(h))$ and $g(X)$ is in $X\cdot\mathcal{O}_K[\![X]\!]$, then $D_n(h+\pi^{v+1}g)\equiv D_n(h) \bmod \pi^{v+1}$, so that $\mathrm{val}_\pi(D_n(h+\pi^{v+1}g))=v$. Hence $f+h'\in W_n$ for all $h'\in\pi X\cdot\mathcal{O}_K[\![X]\!]$ such that $\mathrm{val}_\pi(h-h')\geqslant v+1$, and therefore W_n is open in W.

We now show that W_n is dense in W. If this is not the case, its complement has nonempty interior. Suppose therefore that there exists $f=\tilde{w}+h\in W$ and $v\geqslant 1$ such that $D_n(h+\pi^v g)=0$ for all $g\in X\cdot\mathcal{O}_K[\![X]\!]$. We can write

$$D_n(\{H_j\}_{j\geqslant 1})=\sum_{\mathbf{d}\in\mathbf{Z}^i_{\geqslant 0}} P_{\mathbf{d}}(\{H_j\}_{j\geqslant i+1})H_1^{d_1}\cdots H_i^{d_i},$$

where $\mathbf{d}=(d_1,\dots,d_i)$ and the $P_{\mathbf{d}}$ are polynomials with coefficients in $\mathcal{O}_K$. The fact that $D_n(h+\pi^v g)=0$ for all $g\in X\cdot\mathcal{O}_K[\![X]\!]$ implies that for all fixed values of $\{g_j\}_{j\geqslant i+1}$, the corresponding power series in $H_1,\dots,H_i$ is zero on the set $(h_1, \dots, h_i) + \pi^v \mathcal{O}_K^i$. It is therefore the zero power series. This in turn implies that for each $\mathbf{d}$, the polynomial $P_{\mathbf{d}}(\{H_j\}_{j \geqslant i+1})$ is zero on the set $\{(h_j + \pi^v \mathcal{O}_K)\}_{j \geqslant i+1}$, and therefore $P_{\mathbf{d}} = 0$.

This implies that D_n is the zero power series, and therefore that for any extension L/K and any $f(X) \in X \cdot \mathcal{O}_L[\![X]\!]$ such that $\mathrm{wideg}(f^{\circ p^n}(X) - X) = i$, the roots of $f^{\circ p^n}(X) - X$ in $\mathfrak{m}_{\mathbf{C}_p}$ are not simple. This contradicts Lubin's result in [5] (the aforementioned construction of the power series f_n). □

4. A universal Hensel factorization theorem

In this section, we sketch an analogue of our constructions that singles out the roots of a power series in a circle $\{z \in \mathbf{C}_p, |z| = r\}$ instead of in an open disk as in Section 1 and Section 2. Let $\mathcal{O}_K\{X\}$ denote the ring of restricted power series (power series $f(X) = \sum_{n \geqslant 0} f_n X^n$ with $f_n \in \mathcal{O}_K$ and $f_n \to 0$ as $n \to +\infty$). An element of $\mathcal{O}_K\{X\}$ converges on the closed unit disk $\{z \in \mathbf{C}_p, |z| \leqslant 1\}$. We are interested in the roots of f in the unit circle $\{z \in \mathbf{C}_p, |z| = 1\}$. Take $f(X) = \sum_{n \geqslant 0} f_n X^n \in \mathcal{O}_K\{X\}$, one of whose coefficients is in $\mathcal{O}_K^\times$. Let $\mu_{\min}(f) = \min\{i \geqslant 0, f_i \in \mathcal{O}_K^\times\}$ and let $\mu_{\max}(f) = \max\{i \geqslant 0, f_i \in \mathcal{O}_K^\times\}$. If $n = \mu_{\min}(f)$ and $n + d = \mu_{\max}(f)$, we have the factorization $\overline{f} = \overline{p} \cdot \overline{u}$ in $k[X]$, with

$$\overline{p}(X) = \overline{f}_{n+d}^{-1} \cdot (\overline{f}_n + \overline{f}_{n+1} X + \cdots + \overline{f}_{n+d} X^d) \quad \text{and} \quad \overline{u}(X) = \overline{f}_{n+d} \cdot X^n.$$

Hensel's factorization theorem [3, Ch. III, Section 4, no 3] implies that there exist $p(X) \in \mathcal{O}_K[X]$ and $u(X) \in \mathcal{O}_K\{X\}$ such that $f = pu$, the polynomial p is monic of degree d, $p(0) \in \mathcal{O}_K^\times$, and $\mu_{\max}(u) = \mu_{\min}(u)$. This analogue of the Weierstrass preparation theorem, along with the theory of Newton polygons, implies that f has precisely $\mu_{\max}(f) - \mu_{\min}(f)$ roots (counting multiplicities) in the unit circle.

Let $\{F_i\}_{i \geqslant 0}$ be variables, take $n, d \geqslant 0$, and let

$$S_{n,d} = \mathbf{Z}[\{F_{n+j}\}_{0 \leqslant j \leqslant d}, F_n^{-1}, F_{n+d}^{-1}][\![F_0, \dots, F_{n-1}, \{F_{n+d+k}\}_{k \geqslant 1}]\!].$$

Our definition of a power series ring in infinitely many variables is the "large" one (for instance, $\sum_{k \geqslant 0} F_k$ belongs to $S_{n,d}$), see [2, Ch. IV, Section 4]. Let $I_{n,d}$ be the ideal of $S_{n,d}$ generated by $F_0, \dots, F_{n-1}, \{F_{n+d+k}\}_{k \geqslant 1}$. The following result is a universal Hensel factorization theorem.

Theorem 4.1. *We can write the power series $F(X) = \sum_{i \geqslant 0} F_i X^i \in S_{n,d}[\![X]\!]$ as $F(X) = P(X)U(X)$, where $P(X) \in S_{n,d}[X]$ is monic of degree d, $P(0) \in S_{n,d}^\times$, and $U(X) \equiv F_{n+d} X^n \bmod I_{n,d}$.*

In addition, P and U are uniquely determined by F.

Proof. The ring $S_{n,d}$ is separated and complete for the $I_{n,d}$-adic topology. The polynomials $\overline{P}(X) = F_{n+d}^{-1} \cdot (F_n + F_{n+1} X + \cdots + F_{n+d} X^d)$ and $\overline{U}(X) = F_{n+d} \cdot X^n$ generate the unit ideal in $S_{n,d}/I_{n,d}[X]$, since $F_n, F_{n+d} \in S_{n,d}^\times$. Indeed, a descending induction on $n-1 \geqslant m \geqslant 0$ shows that $X^m \in (\overline{P}, \overline{U})$ by considering $X^m \overline{P}$.

The theorem therefore results from Hensel's factorization theorem (see [3, Ch. III, Section 4, no 3], and the discussion at the beginning of no 5 of ibid). □

We now give an application to the slope factorization of polynomials. Take a nonzero polynomial $P(X) \in K[X]$ and let c be its leading coefficient. We can write $P(X) = c \cdot \prod_r P_r(X)$, where for each r, the polynomial $P_r(X)$ is monic and all of its roots are of valuation $r \in \mathbf{Q}$. By Galois theory, each $P_r(X)$ belongs to $K[X]$. The decomposition $P(X) = c \cdot \prod_r P_r(X)$ is the slope factorization of $P(X)$, and $P_r(X)$ is the slope r factor of $P(X)$.

Corollary 4.2. *Given $F(X) \in \mathcal{O}_K[X]$, one of whose coefficients is in $\mathcal{O}_K^\times$, there are universal formulas, depending only on $\mu_{\min}(F)$, $\mu_{\max}(F)$ and* $\deg(F)$, *for the coefficients of the slope* 0 *factor of F in its slope factorization, in terms of the coefficients of F.*

Proof. Let $F = F_0 F_{\neq 0}$ be the factorization of F as the product of a monic polynomial of slope 0 and of a polynomial of slopes $\neq 0$. The polynomial $F_{\neq 0}$ has no roots in the unit circle, so that if we view F as an element of $\mathcal{O}_K\{X\}$, then $P = F_0$ and $U = F_{\neq 0}$. □

Theorem 4.1 can also be used, as in Section 2, to produce resultant power series $\mathrm{Res}_{n,d}$, that will detect whether two restricted power series f and g, with $\mu_{\min}(f) = n$ and $\mu_{\max}(f) = n + d$, have roots in common in the unit circle.

We end this article with the following question.

Question 4.3. The classical resultant of two polynomials P and Q can be defined using either the product $\prod_{P(z)=0} Q(z)$ or the determinant of the Sylvester matrix. Both approaches give the same formula, after a suitable normalization. In this article, we follow the first approach. Is it possible to view our resultants as the (generalized) determinants of some operators on some p-adic Banach spaces?

Acknowledgements. I thank Sandra Rozensztajn for her help when I was writing the paper, and the referee for several useful remarks.

REFERENCES

[1] D. Birmajer, J. B. Gil, and M. D. Weiner, On Hensel's roots and a factorization formula in $\mathbb{Z}[[X]]$, Integers **14** (2014), Paper No. A47, 18 pp. MR3259300
[2] N. Bourbaki, *Éléments de mathématique. Algèbre.*, Springer-Verlag, Berlin, 2006.
[3] N. Bourbaki, *Éléments de mathématique. Algèbre commutative.*, Springer-Verlag, Berlin, 2006.
[4] J. Elliott, Factoring formal power series over principal ideal domains, Trans. Amer. Math. Soc. **366** (2014), no. 8, 3997–4019. MR3206450
[5] J. Lubin, Sen's theorem on iteration of power series, Proc. Amer. Math. Soc. **123** (1995), no. 1, 63–66. MR1215030
[6] M. O'Malley, On the Weierstrass preparation theorem, Rocky Mountain J. Math. **2** (1972), no. 2, 265–273. MR0289500
[7] S. Sen, On automorphisms of local fields, Ann. of Math. (2) **90** (1969), 33–46. MR0244214
[8] The stacks project authors, Stacks project, 2018.

Received January 27, 2020; accepted March 24, 2020

Laurent Berger
UMPA de l'ENS de Lyon
UMR 5669 du CNRS
Lyon, France
E-mail: laurent.berger@ens-lyon.fr
URL: perso.ens-lyon.fr/laurent.berger/