Rend. Sem. Mat. Univ. Padova, Vol. 142 (2019), 145–179
DOI 10.4171/RSMUP/35

π-exponentials for generalized twisted ramified Witt vectors

Shigeki Matsuda (*)

Abstract – In this paper, we generalize Hazewinkel's theory of twisted ramified Witt rings and then generalize π-exponentials defined by Pulita using newly defined Witt vectors. As an application, we determine the radii of convergence of some formal group exponentials. We also show that p-typical part of a theorem of R. Richard [Ric15] on the convergence of π-exponentials holds for these series and prove some overconvergence properties of related series.

Mathematics Subject Classification (2010). 11F85, 11S80, 13F35.

Keywords. Twisted ramified Witt ring, π-exponential, overconvergence, formal group, Carlitz module.

Contents

(*) *Indirizzo dell'A.*: Department of Mathematics and Informatics, Graduate School of Science, Chiba University, Nishi-Chiba Campus, 1-33, Yayoi-cho, Inage-ku, Chiba-shi, Chiba, 263-8522 Japan
E-mail: matsu@math.s.chiba-u.ac.jp

Introduction

Exponential functions play important roles in the theory of p-adic analysis. Let p be a prime number and $\mathbb{Q}_p$ a p-adic number field. Let π be an element of an extension of $\mathbb{Q}_p$ such that $\pi^{p-1} = -p$. B. Dwork showed that the series $\exp(\pi(T - T^p)) \in \mathbb{Q}_p(\pi)[[T]]$ is overconvergent, i.e., the radius of convergence is strictly larger than 1. This series is called Dwork's exponential series or a splitting function and it is used as a fundamental tool in number theory, especially in p-adic analysis. In [Rob85], Robba showed that for any π such that its p-adic absolute value $|\pi|$ is $|p|^{1/(p-1)}$, there exists a sequence $\alpha_1, \alpha_2, \ldots$ such that, for all $m \geq 1$, the series

$$\exp\left(\pi\left(\alpha_m T + \alpha_{m-1}\frac{T^p}{p} + \cdots + \alpha_1\frac{T^{p^{m-1}}}{p^{m-1}} + \frac{T^{p^m}}{p^m}\right)\right)$$

converges in the disk $|T| < 1$. Using this series, Robba characterized the irregularity of a p-adic solvable differential equation. In [Mat95] the author introduced the series

$$E(T) = \exp\left(\pi_m T + \pi_{m-1}\frac{T^p}{p} + \cdots + \pi_1\frac{T^{p^{m-1}}}{p^{m-1}} + \pi_0\frac{T^{p^m}}{p^m}\right).$$

Here ζ is a primitive p^{m+1}-th root of unity in an extension of $\mathbb{Q}_p$ and $\pi_i = \zeta^{p^{m-i}} - 1$ for $0 \leq i \leq m$. Then he showed that $E(T)$ satisfies the condition of Robba's exponential. The key idea is to rewrite $E(T)$ algebraically with the Artin–Hasse exponential and p-powers roots of unity, using theory of Witt vectors. He also proved that

$$E(T)/E(T^p) = \exp\left(\sum_{i=0}^{m} \pi_{m-i}\frac{T^{p^i} - T^{p^{i+1}}}{p^i}\right) \tag{0.1}$$

is overconvergent for $p > 2$. As a result, he associated a character of the Galois group of a complete discrete valuation field of positive characteristic with a p-adic differential module of rank one. Then he proved that irregularity of the p-adic differential module coincide with the Swan conductor of the character. This result was generalized to any rank by N. Tsuzuki [Tsu98]. See [Cre00], [Mat02] for another proof using a canonical extension. Generalizations for higher dimensional case was also given in [CP09] (rank one) and [Xia10] (any rank). See [Ked10, 9.9, 17.1] and [Ked16, 9, 10] for an explanation on the series from another point of view.

In [Pul07], A. Pulita defined π-exponentials as a generalization of $E(T)$ above, replacing cyclotomic extension by Lubin–Tate extensions of $\mathbb{Q}_p$ [LT65]. This enables us to obtain much larger class of differential modules. As a result, he gave criterion of solvability of p-adic differential module of rank one and classified the p-adic solvable differential modules of rank one. He also proved that all of them have Frobenius structure, which was known only for perfect residue field case [CC96]. Among his comprehensive study, he gave an elegant proof of the overconvergence property including the case of $p = 2$.

In [Mor10], Y. Morofushi studied F-isocrystals on affine lines defined in [Pul07] and gave a lower bound of the Newton polygon of the L-function of such an F-isocrystal. In [Ric15], R. Richard gave beautiful account on the radius of convergence of series of the form $\exp(P(T))$ with polynomial $P(T)$, using π-exponentials. In particular, he proved the formula calculating the radius of convergence in a finite number of steps. This results generalized some estimates in [Mor10]. We remark that G. Christol also gave a finite algorithm in [Chr11] before R. Richard.

Originally Dwork's exponential was used for the analytical expression of an additive character of $\mathbb{F}_p$. In this direction, B. Benzaghou and S. Mokhfi used Pulita's π-exponential to represent a certain Gauss sum as the trace of an operator in [BM16].

In [PV11], E.J. Pickett and S. Vinatier use π-exponential to study integral structures of Galois modules. Then E. J. Pickett and L. Thomas generalized Pulita's π-exponential to the case where Lubin–Tate extensions of a finite extension of $\mathbb{Q}_p$, using formal group exponentials and ramified Witt vectors [PT16] in order to study the same problem.

In this paper, extending an idea in [PT16], we generalize π-exponentials further and prove that they have properties common with classical π-exponentials. In the first section, after reviewing Hazewinkel's functional equation integrality lemma, we generalize his theory of twisted ramified Witt vector [Haz80] and proves basic properties. In particular, we show that Frobenius for generalized Witt vectors also has good properties in §1.5. In the second section, using the generalized Witt theory developed in the previous section and twisted Lubin–Tate groups, we generalize the construction of π-exponential by E. J. Pickett and L. Thomas to those for more general formal groups. As in the original case, the radius of convergence of generalized π-exponentials are one (Theorem 2.1.8). As a consequence, we determine the radii of convergence of some formal group exponentials (Corollary 2.1.9).

We have two main results on the generalized π-exponentials. One is a generalization of a p-typical part of Richard's result (Theorem 2.2.2) that gives an algorithm in a finite number of steps to calculate the radii of convergence of certain exponential functions. Another one is the overconvergence of series generalizing (0.1) (Theorem 2.3.1). Since we admit a discrete valuation ring of positive characteristic as a base ring, we can apply the result above to determine the radius of convergence of Carlitz–Dwork exponential (Proposition 2.3.5).

Acknowledgments. The author would like to thank H. Kakuda for telling me results by A. N. Kochubei. He also would like to thank the referee for his many helpful comments.

Notation

We denote the set of natural numbers by $\mathbb{N}$ and assume that $0 \in \mathbb{N}$. Throughout this paper, we assume that every ring is unital. For a ring A, we denote by $A^\times$ the group of units in A. For a series $f(T) = \sum_{i=0}^{\infty} a_i T^i \in A[[T]]$ and a homomorphism $\tau\colon A \to A$, we denote the series $\sum_{i=0}^{\infty} \tau(a_i) T^i$ by $\tau_* f(T)$.

1. Witt rings

We generalize the theory of twisted ramified Witt rings by Hazewinkel. Basic references for his theory are [Haz78] and [Haz80]. First we review his functional equation lemma in §1.1. After proving a certain congruence property on functions satisfying a functional equation in §1.2, we generalize his theory in §1.3. We take more classical approach than original one, because it seems more suitable for our purpose.

1.1 – *Functional equation integrality lemma*

Hazewinkel's theory of Witt vectors and our generalization are based on the following functional equation integrality lemma (Theorem 1.1.2).

Lemma 1.1.1 (Hazewinkel [Haz78, Chapter I, 2.1]). *Let K be a commutative ring, $A \subset K$ a subring of K and $\sigma\colon K \to K$ a ring homomorphism. Let $I \subset A$ be an ideal of A, p a prime number, q a power of p, and s_i $(i = 1, 2, \dots)$ are elements of K. We assume that these ingredients satisfy the following conditions*:

(a) $\sigma(A) \subset A$.

(b) *For any $a \in A$, $\sigma(a) \equiv a^q \pmod{I}$.*

(c) *$p \in I$ and $s_i I = \{s_i a : a \in I\} \subset A$ for $i = 1, 2, \dots$.*

(d) *For any $r \in \mathbb{Z}_{>0}$ and $b \in K$, if $I^r b \subset I$, then $I^r \sigma(b) \subset I$.*

Let $g(T) = \sum_{i=1}^{\infty} b_i T^i \in A[[T]]$. *Then there exists uniquely a series* $f(T) = \sum_{i=1}^{\infty} a_i T^i \in K[[T]]$ *that satisfies the following functional equation*:

$$f(T) - \sum_{i=1}^{\infty} s_i \sigma_*^i f(T^{q^i}) = g(T). \tag{1.1}$$

In this case, we say that f *satisfies the functional equation* (1.1) *for* g. *We also denote the series* f *by* f_g.

THEOREM 1.1.2 (Hazewinkel [HAZ78, I, 2.2]). *Let* K, A, I, σ, p, q, s_i $(i = 1, 2, \ldots)$ *be as in Lemma* 1.1.1. *Let* $g(T) = \sum_{i=1}^{\infty} b_i T^i \in A[[T]]$ *and assume that* b_1 *is invertible in* A.

(i) $f_g^{-1}(f_g(X) + f_g(Y)) \in A[[X, Y]]$.

(ii) *Let* $\bar{g}(T) = \sum_{i=1}^{\infty} \bar{b}_i T^i \in A[[T]]$ *be any other series. Then* $f_g^{-1}(f_{\bar{g}}(T)) \in A[[T]]$.

(iii) *If* $h(T) = \sum_{i=1}^{\infty} c_i T^i \in A[[T]]$, *then there exists a power series* $\hat{h}(T) = \sum_{i=1}^{\infty} \hat{c}_i T^i \in A[[T]]$ *such that* $f_g(h(T)) = f_{\hat{h}}(T)$.

(iv) *If* $\alpha(T) \in A[[T]]$, $\beta(T) \in K[[T]]$ *and* $r \in \mathbb{Z}_{>0}$, *then the following conditions are equivalent.*

(1) $\alpha(T) \equiv \beta(T) \pmod{I^r A[[T]]}$.

(2) $f_g(\alpha(T)) \equiv f_g(\beta(T)) \pmod{I^r A[[T]]}$.

Let K, A, I, etc. be as above. Let $g(T) = \sum_{i=1}^{\infty} b_i T^i \in A[[T]]$ with $b_1 = 1$. By Lemma 1.1.1, there exists uniquely a series $l(T) = \sum_{i=1}^{\infty} a_i T^i \in K[[T]]$ such that (1.1) holds. By Theorem 1.1.2, we can see that $G(X, Y) = l^{-1}(l(X) + l(Y)) \in A[[X, Y]]$ defines a formal group law over A and $l(T)$ is the log function for G. See [HAZ78, I] for detail.

EXAMPLE 1.1.3. Let $K = \mathbb{Q}$ and let $A = \mathbb{Z}_{(p)}$ be the valuation ring with respect to the p-adic valuation on $\mathbb{Q}$. Let $q = p$, $\sigma = \mathrm{id}$, $I = (p)$, $s_1 = 1/p$ and $s_i = 0$ for $i \geq 2$. Then the assumptions of Lemma 1.1.1 are satisfied. We consider the functional equation for $g(T) \in \mathbb{Z}_{(p)}[[T]]$ and $f(T) \in \mathbb{Q}[[T]]$:

$$f(T) - \frac{f(T^p)}{p} = g(T).$$

Let $l(T)$ (resp. $l_0(T)$) be the series that satisfies the functional equation above for $g(T) = \sum_{n \in \mathbb{N},\, p \nmid n} T^n/n$ (resp. $g(T) = T$). Then we have

$$l(T) = -\log(1 - T) = \sum_{n=1}^{\infty} \frac{T^n}{n}, \quad l_0(T) = \sum_{m=0}^{\infty} \frac{T^{p^m}}{p^m}.$$

By Theorem 1.1.2 (ii), we can see that the classical Artin–Hasse exponential series

$$\exp\Big(-\sum_{m=0}^{\infty}\frac{T^{p^m}}{p^m}\Big)=1-l^{-1}(l_0(T))$$

has its coefficients in $\mathbb{Z}_{(p)}$ (cf. [Haz78, I, 2.3]).

1.2 – *Formal group logarithms*

In this section, we prove basic properties of q-typical series satisfying the functional equation (1.1). Let $p>0$ be a prime number. Let K be a discrete valuation field whose residue field is of characteristic p. Both characteristic 0 and characteristic p are allowed for K. Let $\mathcal{O}$ be the valuation ring of K. We denote the normalized discrete valuation by $v\colon K\to\mathbb{Z}\cup\{\infty\}$. We fix a uniformizer π of $\mathcal{O}$ and a power $q=p^r$ of p. We assume that K has a Frobenius endomorphism, i.e., there exists a continuous ring endomorphism $\sigma\colon K\to K$ such that $\sigma(\pi)/\pi\in\mathcal{O}^\times$ and that $\sigma(a)\equiv a^q \pmod{\pi\mathcal{O}}$ for any $a\in\mathcal{O}$. We fix a Frobenius σ of K throughout this paper. For $a\in K$, we define $\langle a\rangle_0=1$ and $\langle a\rangle_n=\prod_{i=0}^{n-1}\sigma^i(a)=a\sigma(a)\cdots\sigma^{n-1}(a)$ for $n\geq 1$. A power series $f(T)\in K[[T]]$ is called *q-typical* if it is of the form

$$f(T)=\sum_{i=0}^{\infty}a_iT^{q^i}.$$

Let $s_1,s_2,\dots$ be a sequence of elements of K such that $v(s_1)=-1$ and $v(s_i)\geq -1$ for $i\geq 2$. If we put $A=\mathcal{O}$, $I=\pi\mathcal{O}$, then the assumptions of Lemma 1.1.1 are satisfied. We consider the following functional equation:

$$f(T)-\sum_{i=1}^{\infty}s_i\sigma_*^i f(T^{q^i})=g(T). \tag{1.2}$$

Example 1.2.1. In the above setting, let $s_1=1/\pi$ and $s_i=0$ for $i\geq 2$. Then the functional equation is as follows:

$$f(T)-\frac{\sigma_* f(T^q)}{\pi}=g(T). \tag{1.3}$$

When $g(T)=T$, then the series that satisfies the functional equation (1.3) is

$$l(T)=f_T(T)=\sum_{i=0}^{\infty}\frac{T^{q^i}}{\langle\pi\rangle_i}\in K[[T]].$$

Cf. [Haz80, 3.1].

LEMMA 1.2.2. *Let* $l(T) = \sum_{i=0}^{\infty} \gamma_i T^{q^i} \in K[[T]]$ *be a* q*-typical series with* $\gamma_0 = 1$ *that satisfies* (1.2) *for some* $g(T) \in T\mathcal{O}[[T]]$*. Then*

(1) $\nu(\gamma_n) = -n$ *for* $n \in \mathbb{N}$.

(2) $\sigma(\gamma_n/\gamma_{n+1}) \equiv \gamma_{n+1}/\gamma_{n+2} \pmod{\pi^{n+2}\mathcal{O}}$ *for* $n \in \mathbb{N}$.

PROOF. Since $l(T)$ satisfies (1.2), we have a recursive condition:

$$\gamma_n - \sum_{i=1}^{n} s_i \sigma^i(\gamma_{n-i}) \in \mathcal{O} \quad \text{for } n \geq 1. \tag{1.4}$$

We prove (1) by induction on n. The assertion for $n = 0$ is trivial by the definition. Let $n > 0$. By the assumption on s_i and the induction hypothesis, $\nu(s_1\sigma(\gamma_{n-1})) = -n$ and $\nu(s_i\sigma^i(\gamma_{n-i})) \geq -(n-i) - 1 > -n$ for $i > 1$. Thus by (1.4), we obtain $\nu(\gamma_n) = -n$.

Next we prove (2). We use induction on n. By (1.4), there exist $c_1, c_2 \in \mathcal{O}$ such that $\gamma_1 = s_1\sigma(\gamma_0) + c_1$ and $\gamma_2 = s_1\sigma(\gamma_1) + s_2\sigma^2(\gamma_0) + c_2$. Then we have

$$s_1\Big(\frac{\sigma(\gamma_0)}{\gamma_1} - \frac{\sigma(\gamma_1)}{\gamma_2}\Big) = \frac{s_2(\sigma^2(\gamma_0))}{\gamma_2} + \frac{c_2}{\gamma_2} - \frac{c_1}{\gamma_1} \in \pi\mathcal{O}.$$

Therefore $\sigma(\gamma_0/\gamma_1) - \gamma_1/\gamma_2 \in \pi^2\mathcal{O}$ and the assertion for $n = 0$ holds. Suppose that $n \geq 1$. By the induction hypothesis, we have

$$\sigma\Big(\frac{\gamma_i}{\gamma_{i+1}}\Big) \equiv \frac{\gamma_{i+1}}{\gamma_{i+2}} \pmod{\pi^{i+2}}$$

for $0 \leq i < n$. Then we can see that $\sigma^j(\gamma_i/\gamma_{i+1}) \equiv \sigma(\gamma_{i+j-1}/\gamma_{i+j}) \pmod{\pi^{i+2}}$ for $1 \leq j \leq n+1-i$, inductively. Taking $i = n+1-j$, we have $\sigma^j(\gamma_{n+1-j}/\gamma_{n+2-j}) \equiv \sigma(\gamma_n/\gamma_{n+1}) \pmod{\pi^{n+3-j}}$. Thus, for $1 \leq j \leq n+1$,

$$\frac{\sigma^j(\gamma_{n+1-j})}{\sigma(\gamma_n)} \equiv \frac{\sigma^j(\gamma_{n+2-j})}{\sigma(\gamma_{n+1})} \pmod{\pi^{n+1}}. \tag{1.5}$$

On the other hand, by (1.4), we have

$$\frac{\gamma_{n+1}}{\sigma(\gamma_n)} - \sum_{i=1}^{n+1} s_i \frac{\sigma^i(\gamma_{n+1-i})}{\sigma(\gamma_n)} \in \pi^n\mathcal{O},$$

$$\frac{\gamma_{n+2}}{\sigma(\gamma_{n+1})} - \sum_{i=1}^{n+2} s_i \frac{\sigma^i(\gamma_{n+2-i})}{\sigma(\gamma_{n+1})} \in \pi^{n+1}\mathcal{O}.$$

Then, since $s_{n+2}\sigma^{n+2}(\gamma_0)/\sigma(\gamma_{n+1}) \in \pi^n\mathcal{O}$,

$$\Big(\frac{\gamma_{n+1}}{\sigma(\gamma_n)} - \frac{\gamma_{n+2}}{\sigma(\gamma_{n+1})}\Big) - \sum_{i=2}^{n+1} s_i\Big(\frac{\sigma^i(\gamma_{n+1-i})}{\sigma(\gamma_n)} - \frac{\sigma^i(\gamma_{n+2-i})}{\sigma(\gamma_{n+1})}\Big) \in \pi^n\mathcal{O}.$$

By (1.5), we have $s_i(\sigma^i(\gamma_{n+1-i})/\sigma(\gamma_n) - \sigma^i(\gamma_{n+2-i})/\sigma(\gamma_{n+1})) \in \pi^n\mathcal{O}$ for $2 \le i \le n+1$. Therefore $\gamma_{n+1}/\sigma(\gamma_n) - \gamma_{n+2}/\sigma(\gamma_{n+1}) \in \pi^n\mathcal{O}$ and hence

$$\frac{\gamma_{n+1}}{\gamma_{n+2}} - \frac{\sigma(\gamma_n)}{\sigma(\gamma_{n+1})} \in \pi^{n+2}\mathcal{O}.$$

Thus the assertion for n holds. □

1.3 – *Generalized Witt rings*

In this section, we generalize Hazewinkel's theory of ramified Witt rings [Haz80]. In [Haz80], Hazewinkel defines Witt rings for "logarithmic" function which satisfies the functional equation of the form (1.3). We generalize his theory starting from a function which satisfies more general functional equations. In [Haz80], Hazewinkel mainly considers the case of $l(T) = \sum_{i=0}^{\infty} T^{q^i}/\langle\pi\rangle_i$ as in Example 1.2.1, because a strictly isomorphism class of formal groups depends only on π [Haz80, Rem.3.8]. We consider general case here, because we are interested in properties involving Verschiebung (Definition 1.3.17) and it depends on the choice of $l(T)$, as we will see in §1.4. See Theorem 2.3.1 for example.

Let K, $\mathcal{O}$, p, q, $\nu\colon K \to \mathbb{Z} \cup \{\infty\}$ and $\sigma\colon \mathcal{O} \to \mathcal{O}$ be as in the previous section. Let $\underline{X} = (X_0, X_1, \dots)$ be an infinite sequence of indeterminates. We denote by $\mathcal{O}[\underline{X}]$ the polynomial ring $\mathcal{O}[X_i : i \in \mathbb{N}]$.

Definition 1.3.1. Let $l(T) = \sum_{i=0}^{\infty} \gamma_i T^{q^i} \in K[[T]]$ be a series that satisfies the following conditions:

(L1) $\gamma_0 = 1$;

(L2) $\nu(\gamma_n) = -n$ for $n \in \mathbb{N}$;

(L3) $\sigma(\gamma_n/\gamma_{n+1}) \equiv \gamma_{n+1}/\gamma_{n+2} \pmod{\pi^{n+2}\mathcal{O}}$ for $n \in \mathbb{N}$.

Then, for $n \in \mathbb{N}$, we define

$$\phi_n(\underline{X}) = \sum_{i=0}^{n} (\gamma_{n-i}/\gamma_n) X_i^{q^{n-i}} \in \mathcal{O}[\underline{X}]$$

and call it the n-th ghost polynomial for $l(T)$. Since $\phi_n(\underline{X}) \in \mathcal{O}[X_0, \dots, X_n]$, we sometimes write $\phi_n(\underline{X})$ as $\phi_n(X_0, \dots, X_n)$. We denote the series of polynomials $(\phi_n(\underline{X}))_n \in \mathcal{O}[\underline{X}]^{\mathbb{N}}$ by $\phi(\underline{X})$. Let A be a commutative $\mathcal{O}$-algebra. Then we define $\phi_A\colon A^{\mathbb{N}} \to A^{\mathbb{N}}$ so that for $\underline{a} = (a_i)_i \in A^N$, $\phi_A(\underline{a}) = (\phi_n(\underline{a}))_n$. We call ϕ_A the ghost map for $l(T)$ on A. When $A = \mathcal{O}$, we denote $\phi_{\mathcal{O}}$ by ϕ for simplicity.

REMARK 1.3.2. If $l(T) = \sum_{i=0}^{\infty} \gamma_i T^{q^i} \in TK[[T]]$ satisfies the functional equation (1.2) for some $g(T) \in T\mathcal{O}[[T]]$ and $\gamma_0 = 1$, then the above conditions hold by Lemma 1.2.2.

EXAMPLE 1.3.3. If $l(T) = \sum_{i=0}^{\infty} T^{p^i}/p^i$, then $\phi_n(\underline{X}) = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}$ and we obtain the usual n-th ghost polynomial for p-typical Witt rings.

In the rest of this section, we fix a series $l(T) = \sum_{i=0}^{\infty} \gamma_i T^{q^i}$ satisfying the assumption of Definition 1.3.1. Unless otherwise specified, $\phi_n(\underline{X})$ and ϕ_A mean the n-th ghost polynomial and the ghost map for $l(T)$.

The above definition of ghost polynomials is based on the following observation by Hazewinkel.

LEMMA 1.3.4 (cf. [HAZ80, 6.7]). *In the ring $\mathcal{O}[\underline{X}][[T]]$, we have*

$$\sum_{i=0}^{\infty} l(X_i T^{q^i}) = \sum_{n=0}^{\infty} \phi_n(\underline{X}) \gamma_n T^{q^n}.$$

PROOF. The statement follows from the next calculation:

$$\begin{aligned}
&\sum_{i=0}^{\infty} l(X_i T^{q^i}) \\
&= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \gamma_j (X_i T^{q^i})^{q^j} \\
&= \sum_{n=0}^{\infty} \sum_{i=0}^{n} \gamma_{n-i} X_i^{q^{n-i}} T^{q^n} \\
&= \sum_{n=0}^{\infty} \Big(\sum_{i=0}^{n} (\gamma_{n-i}/\gamma_n) X_i^{q^{n-i}} \Big) \gamma_n T^{q^n} \\
&= \sum_{n=0}^{\infty} \phi_n(\underline{X}) \gamma_n T^{q^n}.
\end{aligned}$$

□

LEMMA 1.3.5. *We denote $(X_i^q)_i$ by $\underline{X}^q$. Then for $n \in \mathbb{N}$, $\phi_n(\underline{X}) \in \mathcal{O}[\underline{X}]$ and*

(1) $\phi_{n+1}(\underline{X}) = X_0^{q^{n+1}} + (\gamma_n/\gamma_{n+1})\phi_n(X_1, \ldots, X_{n+1})$.

(2) $\phi_{n+1}(\underline{X}) \equiv \sigma_* \phi_n(\underline{X}^q) \pmod{\pi^{n+1}\mathcal{O}[\underline{X}]}$.

Proof. Since $\nu(\gamma_{n-i}/\gamma_n) = i \geq 0$ by (L2), we have $\phi_n(\underline{X}) \in \mathcal{O}[\underline{X}]$. (1) is evident by the definition. We prove (2). By (L3), $\sigma(\gamma_i)/\gamma_{i+1} \equiv \sigma(\gamma_{i+1})/\gamma_{i+2} \pmod{\pi^{i+2}\mathcal{O}}$ for $i \in \mathbb{N}$. Then we get $\sigma(\gamma_i)/\gamma_{i+1} \equiv \sigma(\gamma_n)/\gamma_{n+1} \pmod{\pi^{i+2}\mathcal{O}}$ for $n \geq i$ by induction. Therefore $\sigma(\gamma_i)/\sigma(\gamma_n) \equiv \gamma_{i+1}/\gamma_{n+1} \pmod{\pi^{n+1}\mathcal{O}}$. Since $\gamma_0/\gamma_{n+1} \in \pi^{n+1}\mathcal{O}$ by (L2),

$$\begin{aligned}&\phi_{n+1}(\underline{X}) - \sigma_*\phi_n(\underline{X}^q)\\ &= \sum_{i=1}^{n}\left(\frac{\gamma_{n+1-i}}{\gamma_{n+1}} - \sigma\left(\frac{\gamma_{n-i}}{\gamma_n}\right)\right)X_i^{q^{n+1-i}} + \frac{\gamma_0}{\gamma_{n+1}}X_{n+1} \in \pi^{n+1}\mathcal{O}[\underline{X}].\end{aligned}$$ □

Proposition 1.3.6. *Let A be a commutative $\mathcal{O}$-algebra.*

(1) *If π is a non zero-divisor in A, then ϕ_A is injective.*

(2) *If π is invertible in A, then ϕ_A is bijective.*

(3) *Assume that there exists a σ-semilinear ring homomorphism $\sigma_A\colon A \to A$ such that $\sigma_A(a) \equiv a^q \pmod{\pi A}$ for any $a \in A$. Then, for $(u_n)_n \in A^{\mathbb{N}}$,*

$$(u_n)_n \in \phi_A(A^{\mathbb{N}}) \iff \sigma_A(u_n) \equiv u_{n+1} \pmod{\pi^{n+1}A}.$$

Proof. We can prove the assertions in the same way as in the classical case by Lemma 1.3.5 (cf. [Bou83, IX, §1, no.2, Proposition 2]). Note that the image of $1/\gamma_n \in \mathcal{O}$ in A is a non zero-divisor if so is π, because $1/\gamma_n$ can be written as $\pi^n u$ with $u \in \mathcal{O}^\times$. □

Example 1.3.7. Let $A = \mathcal{O}[\underline{X}]$ and let $\sigma_A\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be the σ-linear endomorphism such that $\sigma_A(X_i) = X_i^q$. Then σ_A satisfies the assumption of (3) in Proposition 1.3.6. We often denote this σ_A by σ for simplicity.

Theorem 1.3.8. *Let $\underline{X} = (X_n)_{n\in\mathbb{N}}$ and $\underline{Y} = (Y_n)_{n\in\mathbb{N}}$ be infinite sequences of indeterminates. Then there exist uniquely families of polynomials $\underline{S} = (S_n(\underline{X},\underline{Y}))_n$, $\underline{P} = (P_n(\underline{X},\underline{Y}))_n$, and $\underline{I}(\underline{X}) = (I_n(\underline{X}))$ with coefficients in $\mathcal{O}$ such that the following equations hold:*

(1) $\phi(\underline{S}) = \phi(\underline{X}) + \phi(\underline{Y})$,

(2) $\phi(\underline{P}) = \phi(\underline{X})\phi(\underline{Y})$,

(3) $\phi(\underline{I}) = -\phi(\underline{X})$.

Moreover, we have $S_n(\underline{X},\underline{Y})$, $P_n(\underline{X},\underline{Y}) \in \mathcal{O}[X_0,\dots,X_n,Y_0,\dots,Y_n]$, and $I_n(\underline{X}) \in \mathcal{O}[X_0,\dots,X_n]$.

There also exists uniquely a family of polynomials $\underline{C}_x = (C_{x,n}(\underline{X}))_n$ for each $x \in \mathcal{O}$ such that

(4) $\phi(\underline{C}_x) = \big(\sigma^n(x)\phi_n(\underline{X})\big)_n$,

and we have $C_{x,n}(\underline{X}) \in \mathcal{O}[X_0,\dots,X_n]$.

PROOF. All the statements are easily obtained from Proposition 1.3.6 (cf. [Bou83, IX, §1, 3]). □

DEFINITION 1.3.9. Let A be a commutative $\mathcal{O}$-algebra and let $W(A)$ be $A^{\mathbb{N}}$ as a set. We define addition and multiplication of $W(A)$ by $\underline{a} + \underline{b} = \underline{S}(\underline{a}, \underline{b})$ and $\underline{a}\underline{b} = \underline{P}(\underline{a}, \underline{b})$ for $\underline{a}, \underline{b} \in W(A)$. Then $\underline{I}(\underline{a}) + \underline{a} = 0$. $W(A)$ is a commutative ring with these operations and $\phi_A \colon W(A) \to A^{\mathbb{N}}$ is a ring homomorphism. Here we regard $A^{\mathbb{N}}$ as a ring product. For $x \in \mathcal{O}$ and $\underline{a} \in W(A)$, we define $x\underline{a}$ by $\underline{C}_x(\underline{a})$. This operation gives $W(A)$ a structure of an $\mathcal{O}$-algebra. For $\underline{a} \in W(A)$, we call the components of $\phi_A(\underline{a})$ the *ghost components* of $\underline{a}$.

LEMMA 1.3.10. *Let $P(T) \in \mathcal{O}[T]$ be a polynomial. Since $W(A)$ is a commutative $\mathcal{O}$-algebra, we can regard $P(T)$ as the map $P \colon W(A) \to W(A)$ that sends $\underline{a} \in W(A)$ to $P(\underline{a}) \in W(A)$. Let $(\sigma_*^n P)_n \colon A^{\mathbb{N}} \to A^{\mathbb{N}}$ be the map which sends $(x_n)_n$ to $(\sigma_*^n P(x_n))_n$. Then the following diagram is commutative.*

$$\begin{array}{ccc} W(A) & \xrightarrow{\phi} & A^{\mathbb{N}} \\ {\scriptstyle P}\downarrow & & \downarrow{\scriptstyle (\sigma_*^n P)_n} \\ W(A) & \xrightarrow{\phi} & A^{\mathbb{N}} \end{array}$$

PROOF. It is evident by the definition. □

DEFINITION 1.3.11. Let A be a commutative $\mathcal{O}$-algebra and $\sigma_A \colon A \to A$ a σ-semilinear ring homomorphism such that $\sigma_A(a) \equiv a^q \pmod{\pi A}$ for any $a \in A$. We call such a pair (A, σ_A) an $(\mathcal{O}, \sigma)$-algebra. Let (A, σ_A) and (B, σ_B) be $(\mathcal{O}, \sigma)$-algebras. We call a ring homomorphism $f \colon A \to B$ a σ-homomorphism if $f \circ \sigma_A = \sigma_B \circ f$. We denote by $((\mathcal{O}, \sigma)\text{-Alg})$ the category whose objects are the $(\mathcal{O}, \sigma)$-algebras and whose morphisms are the σ-homomorphisms. We denote by $(\mathcal{O}\text{-Alg})$ the category of commutative $\mathcal{O}$-algebras. We extend the Frobenius endomorphism $\sigma \colon \mathcal{O} \to \mathcal{O}$ to $\mathcal{O}[\underline{X}]$, $\mathcal{O}[\underline{X}, \underline{Y}], \dots$ so that $\sigma(X_i) = X_i^q$ and $\sigma(Y_i) = Y_i^q, \dots$ unless otherwise specified. We also denote these endomorphisms by σ for simplicity (cf. Example 1.3.7).

We can regard W as a functor from $(\mathcal{O}\text{-Alg})$ to $(\mathcal{O}\text{-Alg})$. Then W is representable by $\mathcal{O}[\underline{X}]$. The structure of addition $W \times W \to W$ as a functor is given by the $\mathcal{O}$-homomorphisms $S^* \colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}, \underline{Y}]$ such that $S^*(X_n) = S_n(\underline{X}, \underline{Y})$. We omit the detail for the structure of multiplication etc. We denote by $\phi^* \colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ the $\mathcal{O}$-endomorphism such that $\phi^*(X_n) = \phi_n(\underline{X})$. Then ϕ^* induces a morphism of functors $\phi_A \colon W(A) \to A^{\mathbb{N}}$ on A.

Definition 1.3.12. We call the functor $W\colon (\mathcal{O}\text{-Alg}) \to (\mathcal{O}\text{-Alg})$ defined above the Witt functor for $l(T)$.

Remark 1.3.13. (1) The functor W depends on $\mathcal{O}$, q, σ and $l(T)$.

(2) Hazewinkel defined the operations on $W(A)$ in terms of q-typical curves, but they coincide with ours in the case that $l(T)$ satisfies the functional equation is (1.3) in Example 1.2.1 (cf. [Haz80, 6.7]).

Lemma 1.3.14. *Let $f^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be an $\mathcal{O}$-endomorphism defined by $f^*(X_i) = X_{i+1}$. Then there exists a unique $\mathcal{O}$-homomorphism $F^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ such that $F^* \circ \phi^* = \phi^* \circ f^*$, i.e., the following diagram is commutative.*

$$\begin{array}{ccc} \mathcal{O}[\underline{X}] & \xleftarrow{\ \phi^*\ } & \mathcal{O}[\underline{X}] \\ {\scriptstyle F^*}\uparrow & & \uparrow{\scriptstyle f^*} \\ \mathcal{O}[\underline{X}] & \xleftarrow[\ \phi^*\ ]{} & \mathcal{O}[\underline{X}] \end{array}$$

Proof. The map F^* is determined by the images $F_n(\underline{X})$ of X_n $(n \in \mathbb{N})$, so it suffices to show that there exists a series of polynomials $F_n(\underline{X}) \in \mathcal{O}[\underline{X}]$ such that $\phi_n((F_n(\underline{X}))_n)$ is equal to $\phi^*(f^*(X_n)) = \phi_{n+1}(\underline{X})$. Let $\sigma\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be as in Example 1.3.7. By Lemma 1.3.5, $\sigma(\phi_{n+1}(\underline{X})) = \sigma_*\phi_{n+1}(\underline{X}^q) \equiv \phi_{n+2}(\underline{X})$ $(\mathrm{mod}\ \pi^{n+2}\mathcal{O}[\underline{X}])$ and hence the assertion follows from Lemma 1.3.6. □

Definition 1.3.15. From F^* in Lemma 1.3.14, we obtain a morphism of functors $F\colon W \to W$ such that, for any object A in $(\mathcal{O}\text{-Alg})$, the following diagram is commutative.

$$\begin{array}{ccc} W(A) & \xrightarrow{\ \phi_A\ } & A^{\mathbb{N}} \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle f} \\ W(A) & \xrightarrow{\ \phi_A\ } & A^{\mathbb{N}} \end{array}$$

Here $f\colon A^{\mathbb{N}} \to A^{\mathbb{N}}$ is the map which sends $(a_i)_i$ to $(a_{i+1})_i$. $F\colon W(A) \to W(A)$ is a ring homomorphism because so is f. We call F a *Frobenius*. Moreover, F is σ-semilinear because the following diagram is commutative for any $x \in \mathcal{O}$.

$$\begin{array}{ccc} \mathcal{O}[\underline{X}] & \xleftarrow{\ C_x^*\ } & \mathcal{O}[\underline{X}] \\ {\scriptstyle f^*}\uparrow & & \uparrow{\scriptstyle f^*} \\ \mathcal{O}[\underline{X}] & \xleftarrow{\ C_{\sigma(x)}^*\ } & \mathcal{O}[\underline{X}] \end{array}$$

Here $C_a^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ is a homomorphism of $\mathcal{O}$-algebras such that $C_a^*(X_n) = \sigma^n(a)X_n$. Let $F_n(\underline{X}) \in \mathcal{O}[\underline{X}]$ $(n \in \mathbb{N})$ be a sequence of polynomials as in the proof of Lemma 1.3.14, i.e., $\phi_n((F_m(\underline{X}))_m) = \phi_{n+1}(\underline{X})$ for any $n \in \mathbb{N}$. Then for $\underline{a} \in W(A)$, $F(\underline{a}) = (F_n(\underline{a}))_n$. It is easy to see that $F_n(\underline{X}) \in \mathcal{O}[X_0, \dots, X_{n+1}]$.

Lemma 1.3.16. *Let $v_n(\underline{X}) = (\gamma_{n-1}/\gamma_n)X_{n-1} \in \mathcal{O}[\underline{X}]$ and $v^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be a homomorphism of $\mathcal{O}$-algebras such that $v^*(X_n) = v_n(\underline{X})$. Let $V^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be an $\mathcal{O}$-homomorphism such that $V^*(X_n) = X_{n-1}$ for $n \geq 1$ and $V^*(X_0) = 0$. Then the following diagram is commutative.*

$$\begin{array}{ccc} \mathcal{O}[\underline{X}] & \xleftarrow{\phi^*} & \mathcal{O}[\underline{X}] \\ {\scriptstyle V^*}\uparrow & & \uparrow{\scriptstyle v^*} \\ \mathcal{O}[\underline{X}] & \xleftarrow[\phi^*]{} & \mathcal{O}[\underline{X}] \end{array}$$

Proof. The assertion follows from direct calculation. □

Definition 1.3.17. From V^* in Lemma 1.3.16, we obtain a morphism of functors $V\colon W \to W$ such that for any object A in ($\mathcal{O}$-Alg), the following diagram is commutative.

$$\begin{array}{ccc} W(A) & \xrightarrow{\phi_A} & A^{\mathbb{N}} \\ {\scriptstyle V}\downarrow & & \downarrow{\scriptstyle v} \\ W(A) & \xrightarrow{\phi_A} & A^{\mathbb{N}} \end{array}$$

Here $v((a_n)_n) = ((\gamma_{n-1}/\gamma_n)a_{n-1})_n$ (we define $a_{-1} = 0$). We call V a *Verschiebung*. For any object A in ($\mathcal{O}$-Alg), $V\colon W(A) \to W(A)$ is a homomorphism of modules, but it is not necessarily $\mathcal{O}$-linear. In fact, we have $V(\sigma(x)\underline{a}) = xV(\underline{a})$ for any $x \in \mathcal{O}$ and $\underline{a} \in W(A)$.

Example 1.3.18. If $l(T) = \sum_{i=0}^{\infty} T^{q^i}/\langle\pi\rangle_i$, then $v_n(\underline{X}) = \sigma^{n-1}(\pi)X_{n-1}$.

Definition 1.3.19. We define $\underline{\mu} = (0, 1, 0, \dots) = V(1) \in W(\mathcal{O})$. We also define $\delta_n = \gamma_n/\gamma_{n+1}$ for $n \in \mathbb{N}$ and $\delta_{-1} = 0$. Then if we denote $\underline{\delta} = (\delta_{n-1})_n = (0, \gamma_0/\gamma_1, \gamma_1/\gamma_2, \dots)$, $\phi(\underline{\mu}) = \underline{\delta}$.

Lemma 1.3.20. *We have*

(1) $VF = \underline{\mu}$,

(2) $FV = F(\underline{\mu})$.

Here we regard $\underline{\mu}$ and $F(\underline{\mu})$ as multiplication endomorphisms.

Proof. It suffices to show the corresponding equalities for ghost components. For any $\mathcal{O}$-algebra A and $\underline{u} = (u_0, u_1, \dots) \in A^{\mathbb{N}}$, $vf(\underline{u}) = (0, \delta_0 u_1, \delta_1 u_2, \dots) = \underline{\delta u}$. Then it is easy to see that $\phi(\underline{\mu})$ coincides with $(0, \delta_0, \delta_1, \dots)$ by the definition of ghost map. Thus we obtain (1). We can prove (2) in a similar way. $\square$

Remark 1.3.21. (1) In the case where $l(T) = \sum_{i=0}^{\infty} T^{q^i}/\langle\pi\rangle_i$, we have $\phi(\underline{\mu}) = (0, \pi, \sigma(\pi), \dots) \in \mathcal{O}^{\mathbb{N}}$ and $\phi(F(\underline{\mu})) = (\sigma^n(\pi))_n \in \mathcal{O}^{\mathbb{N}}$. Hence $F(\underline{\mu}) = \pi$ in $W(\mathcal{O})$.

(2) If $l(T) = \sum_{i=0}^{\infty} T^{q^i}/\langle\pi\rangle_i$ and $\sigma = \mathrm{id}$, then $\phi(F(\underline{\mu}) - \underline{\mu}) = (\pi, 0, \dots)$ and hence $F(\underline{\mu}) - \underline{\mu} \in \operatorname{Ker} F$.

1.4 – *Compatibility*

In this section, we study the compatibility of Frobenius functors and Verschiebung functors for different "logarithmic" functions satisfying a common functional equation.

Let $\mathcal{O}$, K, σ, π, p, q be as in §1.2. Let $l(T) = \sum_{i=0}^{\infty} \gamma_i T^{q^i}$ and $l'(T) = \sum_{i=0}^{\infty} \gamma'_i T^{q^i}$ be q-typical series in $K[[T]]$ that satisfy the assumption of Definition 1.3.1. Let $\phi'_n(\underline{X}) = \sum_{i=0}^{\infty} (\gamma'_{n-i}/\gamma'_n) X_i^{q^{n-i}} \in \mathcal{O}[X_0, \dots, X_n] \subset \mathcal{O}[\underline{X}]$ be the n-th ghost polynomial for $l'(T)$ and $\phi'(\underline{X}) = (\phi'_n(\underline{X}))_n$. We denote by $\phi'^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ the homomorphism of $\mathcal{O}$-algebras which maps X_n to $\phi'_n(\underline{X})$.

Lemma 1.4.1. *There exists a unique homomorphism $u^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ of $\mathcal{O}$-algebras such that the following diagram is commutative*:

$$\begin{array}{ccc} \mathcal{O}[\underline{X}] & \xleftarrow{\ \phi^*\ } & \mathcal{O}[\underline{X}] \\ {\scriptstyle u^*}\uparrow & \swarrow{\scriptstyle \phi'^*} & \\ \mathcal{O}[\underline{X}] & & \end{array}$$

Proof. It suffices to show that there exists a sequence of polynomials $\underline{u}(\underline{X}) = (u_n(\underline{X}))_n \in \mathcal{O}[\underline{X}]^{\mathbb{N}}$ such that $\phi'_n(\underline{u}(\underline{X})) = \phi_n(\underline{X})$. Let $\sigma\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be as in Example 1.3.7. By Proposition 1.3.6, it suffices to show $\sigma(\phi_n(\underline{X})) \equiv \phi_{n+1}(\underline{X})$ (mod $\pi^{n+1}\mathcal{O}[\underline{X}]$) and it is nothing but Lemma 1.3.5. $\square$

Definition 1.4.2. Let W (resp. W') be the Witt functor for l (resp. l') (Definition 1.3.12). For any object A in ($\mathcal{O}$-Alg), we denote by ϕ_A (resp. ϕ'_A) the ghost map for l (resp. l') (Definition 1.3.1). Then the homomorphism u^* in Lemma 1.4.1 induces a morphism of functors $u\colon W \to W'$ such that, for any object A in ($\mathcal{O}$-Alg), the following diagram is commutative.

$$\begin{array}{ccc} W(A) & \xrightarrow{\phi_A} & A^{\mathbb{N}} \\ {\scriptstyle u_A}\downarrow & \nearrow {\scriptstyle \phi'_A} & \\ W'(A) & & \end{array}$$

It is evident that u_A is a ring homomorphism. It is also $\mathcal{O}$-linear. Indeed if we denote by C_x (resp. C'_x) the functor defined by $\underline{C}_x$ for $x \in \mathcal{O}$ in Definition 1.3.9 with respect to $l(T)$ (resp. $l'(T)$), then $u \circ C_x = C'_x \circ u$ because both correspond to the map $A^{\mathbb{N}} \to A^{\mathbb{N}}; (a_i)_i \mapsto (\sigma^i(x)a_i)_i$.

Let $u^*: \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ and $u: W \to W'$ be as in Lemma 1.4.1 and Definition 1.4.2.

Proposition 1.4.3. *Let f^* and F^* be as in Lemma 1.3.14. Let us define F'^* in the same way as F^* for ϕ'. Then the following diagram is commutative.*

$$\begin{array}{ccc} \mathcal{O}[\underline{X}] & \xleftarrow{F^*} & \mathcal{O}[\underline{X}] \\ \uparrow {\scriptstyle u^*} & & \uparrow {\scriptstyle u^*} \\ \mathcal{O}[\underline{X}] & \xleftarrow{F'^*} & \mathcal{O}[\underline{X}] \end{array}$$

Consequently we have the following commutative diagram of morphisms of functors.

$$\begin{array}{ccc} W & \xrightarrow{F} & W \\ \downarrow {\scriptstyle u} & & \downarrow {\scriptstyle u} \\ W' & \xrightarrow{F'} & W' \end{array}$$

Proof. It is obvious from the definition. □

Remark 1.4.4. Proposition 1.4.3 above implies that the Frobenius functor is independent of the choice of $l(T)$, but depends only on $\mathcal{O}$, q, σ.

Lemma 1.4.5. *Let $d^*: \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be an $\mathcal{O}$-homomorphism such that $d^*(X_n) = (\delta_n/\delta'_n)X_n$. Then there exists uniquely an $\mathcal{O}$-homomorphism Δ^* such that the following diagram is commutative.*

$$\begin{array}{ccc} \mathcal{O}[\underline{X}] & \xleftarrow{\phi^*} & \mathcal{O}[\underline{X}] \\ {\scriptstyle \Delta^*} \uparrow & & \uparrow {\scriptstyle d^*} \\ \mathcal{O}[\underline{X}] & \xleftarrow{\phi^*} & \mathcal{O}[\underline{X}] \end{array}$$

Proof. The homomorphism Δ^* is determined by the images $\Delta_n^*(\underline{X}) \in \mathcal{O}[\underline{X}]$ of X_n for $n \in \mathbb{N}$. Since $\phi^* \circ d^*(X_n) = \phi^*((\delta_n/\delta'_n)X_n) = (\delta_n/\delta'_n)\phi_n(\underline{X})$, by Proposition 1.3.6, it suffices to show that

$$\sigma\big((\delta_n/\delta'_n)\phi_n(\underline{X})\big) \equiv (\delta_{n+1}/\delta'_{n+1})\phi_{n+1}(\underline{X}) \pmod{\pi^{n+1}\mathcal{O}[\underline{X}]}.$$

Then it is enough to show that for $0 \le i \le n$,

$$\sigma\Big(\frac{\gamma_n}{\gamma_{n+1}}\frac{\gamma'_{n+1}}{\gamma'_n}\frac{\gamma_{n-i}}{\gamma_n}\Big) \equiv \frac{\gamma_{n+1}}{\gamma_{n+2}}\frac{\gamma'_{n+2}}{\gamma'_{n+1}}\frac{\gamma_{n+1-i}}{\gamma_{n+1}} \pmod{\pi^{n+1}}.$$

By Definition 1.3.1 (L3) we have

$$\frac{\sigma(\gamma'_n)}{\pi\sigma(\gamma'_{n+1})} \equiv \frac{\gamma'_{n+1}}{\pi\gamma'_{n+2}} \pmod{\pi^{n+1}}.$$

Since they are invertible in $\mathcal{O}$,

$$\frac{\pi\sigma(\gamma'_{n+1})}{\sigma(\gamma'_n)} \equiv \frac{\pi\gamma'_{n+2}}{\gamma'_{n+1}} \pmod{\pi^{n+1}}.$$

On the other hand, we have

$$\frac{\sigma(\gamma_n)}{\pi\sigma(\gamma_{n+1})} \equiv \frac{\gamma_{n+1}}{\pi\gamma_{n+2}}, \qquad \frac{\sigma(\gamma_{n-i})}{\sigma(\gamma_n)} \equiv \frac{\gamma_{n+1-i}}{\gamma_{n+1}} \pmod{\pi^{n+1}}.$$

The assertion follows from these relations. □

Let v^* and $v'^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be homomorphisms as in Lemma 1.3.16 for l and l' respectively.

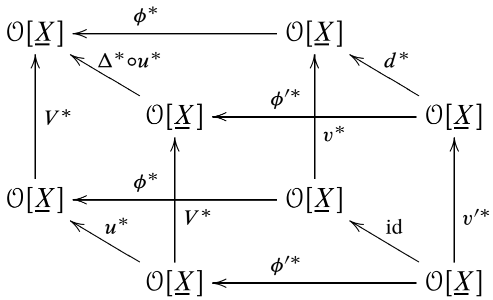
Proposition 1.4.6. *Let $u\colon W \to W'$ and $v^*, v'^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be as above. By definition, $v^*(X_n) = \delta_{n-1}X_{n-1} = (\gamma_{n-1}/\gamma_n)X_{n-1}$, $v'^*(X_n) = \delta'_{n-1}X_{n-1} = (\gamma'_{n-1}/\gamma'_n)X_{n-1}$ (we define $X_{-1} = 0$). Let $V^*\colon \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be as in Lemma 1.3.16. Then the following diagram is commutative.*

$$\begin{array}{ccc} \mathcal{O}[\underline{X}] & \xleftarrow{V^*} & \mathcal{O}[\underline{X}] \\ {\scriptstyle \Delta^*\circ u^*}\uparrow & & \uparrow{\scriptstyle u^*} \\ \mathcal{O}[\underline{X}] & \xleftarrow{V^*} & \mathcal{O}[\underline{X}] \end{array}$$

Proof. Since $d^* \circ v'^*(X_n) = d^*(\delta'_{n-1}X_{n-1}) = (\delta_{n-1}/\delta'_{n-1})\delta'_{n-1}X_{n-1} = \delta_{n-1}X_{n-1} = v^*(X_n)$, the following diagram is commutative:

$$\begin{array}{ccc} \mathcal{O}[\underline{X}] & \xleftarrow{d^*} & \mathcal{O}[\underline{X}] \\ {\scriptstyle v^*}\uparrow & & \uparrow{\scriptstyle v'^*} \\ \mathcal{O}[\underline{X}] & \xleftarrow[\mathrm{id}]{} & \mathcal{O}[\underline{X}]. \end{array}$$

Then the assertion follows from elementary diagram chasing in the following diagram:



□

Remark 1.4.7. Proposition 1.4.6 implies that the Verschiebung functor depends on the choice of $l(T)$, in contrast with the Frobenius functor.

1.5 – *More on Frobenius*

In this section, we prove some lemmas on Frobenius. In the classical case, if we denote by $F_n(\underline{X})$ the polynomial for the n-th component of Frobenius map (Definition 1.3.15), we have

$$F_n(\underline{X}) \equiv X_n^p \pmod{p}.$$

Consequently, $F_n(\underline{X}) \mod p$ is independent of X_{n+1}. This is not always the case in general (see Example 1.5.3), but we will see that a similar formula holds with a weakened congruence condition (Lemma 1.5.4).

The following lemma and its corollary are not used in the rest of this paper, but it seems that they have its own interest.

Lemma 1.5.1. *Let $l(T) = \sum_{i=0}^{\infty} \gamma_i T^{q^i}$ be a series satisfying the assumption in Definition 1.3.1. We denote $\delta_i = \gamma_i / \gamma_{i+1}$ for $i \in \mathbb{N}$ as in Definition 1.3.19. Let $F_n(\underline{X})$ $(n \in \mathbb{N})$ be the series of polynomials defining Frobenius functor (cf. Definition 1.3.15). If*

$$\left(\frac{\delta_i}{\delta_{i+1}}\right)^{q^j} \equiv \left(\frac{\delta_{i+j}}{\delta_{i+j+1}}\right) \pmod{\pi^{j+1}}$$

for any $i, j \in \mathbb{Z}$ such that $i \geq 0$, $j \geq 0$, then

$$F_n(\underline{X}) \equiv \frac{\delta_n}{\delta_0} X_n^q \pmod{\pi} \textit{ for any } n \in \mathbb{N}.$$

Proof. By the assumption, we can show inductively

$$\left(\frac{\delta_i}{\delta_0}\right)^{q^j} \equiv \left(\frac{\delta_{i+j}}{\delta_j}\right) \pmod{\pi^{j+1}}. \tag{1.6}$$

If we put $n = i + j$, then $(\delta_i/\delta_0)^{q^{n-i}} \equiv \delta_n/\delta_{n-i} \pmod{\pi^{n+1-i}}$. We prove the assertion by induction on n. It is obvious for $n = 0$. Suppose that the assertion holds for $i = 1, 2, \ldots, n-1$. Since $F_i(\underline{X}) \equiv (\delta_i/\delta_0)X_i^q$ for $0 \leq i \leq n-1$, $(\gamma_{n-i}/\gamma_n)F_i(\underline{X})^{q^{n-i}} \equiv (\gamma_{n-i}/\gamma_n)(\delta_i/\delta_0)^{q^{n-i}} X_i^{q^{n+1-i}} \pmod{\pi^{n+1}}$. Then by (1.6), we have

$$\begin{aligned}(\gamma_{n-i}/\gamma_n)F_i(\underline{X})^{q^{n-i}} &\equiv (\gamma_{n-i}/\gamma_n)(\delta_n/\delta_{n-i})X_i^{q^{n+1-i}} \\ &\equiv (\gamma_{n+1-i}/\gamma_{n+1})X_i^{q^{n+1-i}} \pmod{\pi^{n+1}}.\end{aligned}$$

On the other hand, by the definition of $(F_n(\underline{X}))_n$, we have

$$\sum_{i=0}^{n-1} \frac{\gamma_{n-i}}{\gamma_n} F_i(\underline{X})^{q^{n-i}} + \frac{\gamma_0}{\gamma_n} F_n(\underline{X}) = \sum_{i=0}^{n+1} \frac{\gamma_{n+1-i}}{\gamma_{n+1}} X_i^{q^{n+1-i}}.$$

Therefore we have $(\gamma_0/\gamma_n)F_n(\underline{X})^{q^n} \equiv (\gamma_n/\gamma_{n+1})X_n^q \pmod{\pi^{n+1}}$, which implies the assertion holds for n. □

Corollary 1.5.2. *Suppose that* $l(T) = \sum_{i=0}^{\infty} T^{q^i}/\langle\pi\rangle_i$. *Then*

$$\delta_i = \langle\pi\rangle_{i+1}/\langle\pi\rangle_i = \sigma^i(\pi),$$

and hence $\delta_i/\delta_{i+1} = \sigma^i(\pi/\sigma(\pi))$. *In this case, the assumption in Lemma 1.5.1 is equivalent to the condition that,*

$$\textit{for any } j \in \mathbb{N}, \quad \sigma^j\left(\frac{\pi}{\sigma(\pi)}\right) \equiv \left(\frac{\pi}{\sigma(\pi)}\right)^{q^j} \pmod{\pi^{j+1}}.$$

If this holds, we have $F_n(\underline{X}) \equiv (\sigma^n(\pi)/\pi)X_n^q \pmod{\pi}$.

Example 1.5.3. The assumption in Lemma 1.5.1 does not necessarily hold. Consider the case where $\mathcal{O}$ is the p-adic completion of $\mathbb{Z}_{(p)}[[t]][1/t]$. Then $\mathcal{O}$ is a complete discrete valuation ring. The residue field of $\mathcal{O}$ is isomorphic to $\mathbb{F}_p((T))$, where $\mathbb{F}_p$ is a finite field of order p. As a uniformizer of $\mathcal{O}$, we take $\pi = tp \in \mathcal{O}$. Let $P(T) = (1+T)^p - 1$ and define $\sigma\colon \mathcal{O} \to \mathcal{O}$ to be the continuous homomorphism such that $\sigma(t) = P(t)$. Let $l(T) = \sum_{i=0}^{\infty} T^{q^i}/\langle\pi\rangle_i$ as in Corollary 1.5.2. Then $\sigma(\pi)/\pi \in \mathcal{O}^\times$ and $\sigma(a) \equiv a^p \pmod{\pi}$. In this case,

$(\sigma(\pi)/\pi)^p = (P(t)/t)^p \equiv t^{p(p-1)} \pmod{\pi}$. On the other hand, $\sigma(\sigma(\pi)/\pi) = \sigma(P(t)/t) = P(P(t))/P(t)$, which is not congruent to $t^{p(p-1)}$ modulo π^2. For example, if $p = 3$, then we have $P(P(t))/P(t) = P(t)^2 + 3P(t) + 3 = t^6 + 6t^5 + 15t^4 + 21t^3 + 18t^2 + 9t + 3 \not\equiv t^6 \pmod{9}$. In this case, we have

$$\begin{aligned} F_2(\underline{X}) &\equiv \frac{\delta_2}{\delta_0} X_2^3 + \frac{1}{\delta_0}\Big(\frac{\delta_2}{\delta_1} - \Big(\frac{\delta_1}{\delta_0}\Big)^3\Big) X_1^9 \pmod{3} \\ &\equiv \frac{\delta_2}{\delta_0} X_2^3 + \frac{1}{3t}\Big(\sigma\Big(\frac{\sigma(t)}{t}\Big) - \Big(\frac{\sigma(t)}{t}\Big)^3\Big) X_1^9 \pmod{3} \\ &\equiv \frac{\delta_2}{\delta_0} X_2^3 - t^2\Big(t^2 + t - 1 + \frac{1}{t^3}\Big) X_1^9 \not\equiv \frac{\delta_2}{\delta_0} X_2^3 \pmod{3}. \end{aligned}$$

Still we have the following lemma in general.

Lemma 1.5.4. *Let I_n be the ideal of $\mathcal{O}[\underline{X}]$ generated by $X_0, \ldots, X_n$ for $n \in \mathbb{N}$ and $I_{-1} = 0$. Then*

$$F_n(\underline{X}) \equiv \frac{\delta_n}{\delta_0} X_n^q \pmod{I_{n-1}^{q+1} + \pi\mathcal{O}[\underline{X}]} \text{ for any } n \in \mathbb{N}.$$

Proof. The statement for $n = 0$ is evident, because $F_0(\underline{X}) = X_0^q + (\gamma_0/\gamma_1)X_1$. We proceed by induction on n. Suppose $n > 0$. By the definition of $F_i(\underline{X})$, we have

$$\text{(1.7)} \quad \frac{\gamma_1}{\gamma_n} F_{n-1}(\underline{X})^q + \frac{\gamma_0}{\gamma_n} F_n(\underline{X}) \equiv \frac{\gamma_1}{\gamma_{n+1}} X_n^q + \frac{\gamma_0}{\gamma_{n+1}} X_{n+1} \pmod{I_{n-1}^{q+1} K[\underline{X}]}$$

in $K[\underline{X}]$. By the induction hypothesis,

$$F_{n-1}(\underline{X}) \equiv (\delta_{n-1}/\delta_0) X_{n-1}^q \pmod{I_{n-2}^{q+1} + \pi\mathcal{O}[\underline{X}]}$$

and hence we can write $F_{n-1}(\underline{X}) = (\delta_{n-1}/\delta_0)X_{n-1}^q + g(\underline{X}) + \pi h(\underline{X})$ with $g(\underline{X}) \in I_{n-2}^{q+1}$ and $h(\underline{X}) \in \mathcal{O}[\underline{X}]$. Therefore

$$\begin{aligned} F_{n-1}(\underline{X})^q &\equiv ((\delta_{n-1}/\delta_0)X_{n-1}^q + g(\underline{X}))^q \pmod{\pi^2\mathcal{O}[\underline{X}]} \\ &\equiv 0 \pmod{I_{n-1}^{q+1} + \pi^2\mathcal{O}[\underline{X}]}. \end{aligned}$$

Hence $(1/\delta_0)F_{n-1}(\underline{X})^q \in I_{n-1}^{q+1}K[\underline{X}] + \pi\mathcal{O}[\underline{X}]$. Thus, by (1.7),

$$F_n(\underline{X}) \equiv \frac{\delta_n}{\delta_0} X_n^q + \delta_n X_{n+1} - \frac{1}{\delta_0} F_{n-1}(\underline{X})^q \equiv \frac{\delta_n}{\delta_0} X_n^q \pmod{I_{n-1}^{q+1} K[\underline{X}] + \pi\mathcal{O}[\underline{X}]}.$$

Since $F_n(\underline{X})$ and $(\delta_n/\delta_0)X_n^q$ belong to $\mathcal{O}[\underline{X}]$ and $I_{n-1}^{q+1}K[\underline{X}] \cap \mathcal{O}[\underline{X}] = I_{n-1}^{q+1}$, the statement for n follows. □

LEMMA 1.5.5 (cf. [Bou83, IX, §1, ex. 14) a)]). *Let* (A, σ_A) *be an* $(\mathcal{O}, \sigma)$*-algebra* (*Definition* 1.3.11) *and assume that* π *is a non zero-divisor in* A. *Let* $F\colon W(A) \to W(A)$ *be the Frobenius. Then there exists uniquely a ring homomorphism* $s\colon A \to W(A)$ *such that* $\phi_0 \circ s = \mathrm{id}$ *and the following diagram is commutative.*

$$\begin{array}{ccc} A & \xrightarrow{s} & W(A) \\ {\scriptstyle \sigma_A}\downarrow & & \downarrow{\scriptstyle F} \\ A & \xrightarrow{s} & W(A) \end{array}$$

PROOF. By (1) of Proposition 1.3.6, the commutativity of the diagram is equivalent to $f \circ \phi \circ s = \phi \circ s \circ \sigma_A$.

$$\begin{array}{ccccc} A & \xrightarrow{s} & W(A) & \xrightarrow{\phi} & W(A) \\ {\scriptstyle \sigma_A}\downarrow & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle f} \\ A & \xrightarrow{s} & W(A) & \xrightarrow{\phi} & W(A) \end{array}$$

This means that for any $a \in A$ and $n \in \mathbb{N}$, we have $\phi_{n+1}(s(a)) = \phi_n(s(\sigma_A(a)))$. Then we obtain $\phi_n(s(a)) = \sigma_A^n(a)$ by induction. Thus for the existence of s, it is enough to show there exists $\underline{b} \in W(A)$ such that $\phi_n(\underline{b}) = \sigma_A^n(a)$ for any $n \in \mathbb{N}$, which is evident from Proposition 1.3.6. Finally s is a ring homomorphism because so is σ_A. □

In Definition 1.5.6 and Definition 1.5.8 below, we do not need to assume that P is Lubin–Tate polynomial, but only have to assume that P induces Frobenius endomorphism modulo π.

DEFINITION 1.5.6. Let $P \in \mathcal{O}[T]$ be a polynomial that satisfies the following:

(i) $P(T) \equiv T^q \pmod{\pi}$,

(ii) $P(0) = 0$.

Let $\sigma_P\colon \mathcal{O}[T] \to \mathcal{O}[T]$ be a σ-semilinear homomorphism such that $\sigma_P(T) = P(T)$. We define $P^{[n]}(T)$ to be $\sigma_P^n(T)$. Then we have $P^{[0]}(T) = T$ and $P^{[n+1]}(T) = \sigma_* P^{[n]}(P(T))$ for any $n \in \mathbb{N}$. If we write the composition of polynomials f and g by $f \circ g$, then $P^{[n]} = \sigma_*^{n-1} P \circ \sigma_*^{n-2} P \circ \cdots \circ \sigma_* P \circ P$. By Lemma 1.5.5, there exists a map $s_P\colon \mathcal{O}[T] \to W(\mathcal{O}[T])$ such that $F \circ s_P = s_P \circ \sigma_P$ and $\phi_0 \circ s_P = \mathrm{id}$.

$$\begin{array}{ccc} \mathcal{O}[T] & \xrightarrow{s_P} & W(\mathcal{O}[T]) \\ {\scriptstyle \sigma_P}\downarrow & & \downarrow{\scriptstyle F} \\ \mathcal{O}[T] & \xrightarrow{s_P} & W(\mathcal{O}[T]) \end{array}$$

Then $\phi_n(s_P(T)) = P^{[n]}(T)$.

Lemma 1.5.7. *Let A be an $\mathcal{O}$-algebra. For any $a \in A$ and $n \in \mathbb{N}$, $\phi_n(s_P(a)) = P^{[n]}(a)$. In particular, if $\pi_n, \pi_{n-1}, \ldots, \pi_0$ is a sequence of elements of A such that $\sigma_*^n P(\pi_0) = 0$ and $\sigma_*^{n-i} P(\pi_i) = \pi_{i-1}$ for $1 \leq i \leq n$, then $\phi_A(s_P(\pi_n)) = (P^{[i]}(\pi_n))_i = (\pi_n, \pi_{n-1}, \ldots, \pi_0, 0, \ldots)$.*

Proof. It is clear by the definition. □

Definition 1.5.8. We call a sequence $(\pi_d, \pi_{d-1}, \ldots, \pi_0, 0, \ldots) \in A^{\mathbb{N}}$ that satisfies $\sigma_*^{d-i} P(\pi_i) = \pi_{i-1}$ for $0 \leq i \leq d-1$ and $\sigma_*^d P(\pi_0) = 0$, $\pi_0 \neq 0$, $\nu(\pi_0) > 0$ a *P-sequence of length d*.

Now we consider the case where P is a Lubin–Tate polynomial. Let K^{a} be an algebraic closure of K. We know that the normalized discrete valuation $\nu\colon K \to \mathbb{Z} \cup \{\infty\}$ can be extended to $K^{\mathrm{a}} \to \mathbb{Q} \cup \{\infty\}$ ([Rib98, 4.1, Theorem 1 and **B**]). We fix one of them and also denote by ν. Let π' be a uniformizer of $\mathcal{O}$. Let $P \in \mathcal{O}[T]$ be a polynomial that satisfies

(1) $P(T) \equiv T^q \pmod{\pi}$,

(2) $P(T) \equiv \pi' T \pmod{T^2}$

and let $P^{[n]}(T) \in \mathcal{O}[T]$ ($n \in \mathbb{N}$) be as above. Let $\pi_0, \pi_1, \ldots, \pi_d \in K^{\mathrm{a}}$ be a sequence as in Lemma 1.5.7. Let $\underline{e} = (e_n)_n = s_P(\pi_d)$, then we have $\phi(\underline{e}) = (\pi_d, \ldots, \pi_1, \pi_0, 0, \ldots)$ by Lemma 1.5.7.

Lemma 1.5.9. *Let d and $\underline{e} = (e_n)$ be as above. Then $\nu(e_n) = 1/q^d(q-1)$ for any $n \in \mathbb{N}$.*

Proof. First we prove the statement when $d = 0$. Since $P(\pi_0) = 0$, $\pi_0 \neq 0$ and $\nu(\pi_0) > 0$, $\nu(e_0) = \nu(\pi_0) = \nu(\pi)/(q-1) = 1/(q-1)$. For $n > 0$, we can assume $\nu(e_i) = 1/(q-1)$ for $i < n$ by induction. By definition, we have $\sum_{i=0}^n (\gamma_{n-i}/\gamma_n) e_i^{q^{n-i}} = 0$. Since $\nu((\gamma_{n-i}/\gamma_n) e_i^{q^{n-i}}) = i + q^{n-i}/(q-1)$, we obtain

$$\begin{aligned} \nu((\gamma_{n-i+1}/\gamma_n) e_{i-1}^{q^{n-i+1}}) - \nu((\gamma_{n-i}/\gamma_n) e_i^{q^{n-i}}) &= i - 1 + \frac{q^{n+1-i}}{q-1} - i - \frac{q^{n-i}}{q-1} \\ &= q^{n-i} - 1 > 0 \end{aligned}$$

for $0 < i < n$. Therefore, $\nu((\gamma_0/\gamma_n) e_n) = \nu((\gamma_1/\gamma_n) e_{n-1}^q)$ and hence $\nu(e_n) = q/(q-1) - 1 = 1/(q-1)$. For $d > 0$, we use induction on d. Suppose that the statement holds for $d-1$. Since $\phi(F(\underline{e})) = (\pi_{d-1}, \ldots, \pi_1, \pi_0, 0, \ldots)$ is a $\sigma_* P$-sequence of length $d-1$ and $\sigma_* P$ also satisfies the assumption (1), (2) above for a uniformizer $\sigma(\pi')$, we have $\nu(F_n(\underline{e})) = 1/q^{d-1}(q-1)$ for any $n \in \mathbb{N}$.

We show $\nu(e_n) = 1/q^d(q-1)$ by induction on n. It is evident that $\nu(e_0) = \nu(\pi_d) = 1/q^d(q-1)$. Suppose that $n > 0$. Let $I_n = (X_0, \dots, X_n) \subset \mathcal{O}[\underline{X}]$. By Lemma 1.5.4, there exists a polynomial $g(X_0, \dots, X_{n+1}) \in I_{n-1}^{q+1} + \pi\mathcal{O}[\underline{X}]$ such that

$$F_n(\underline{X}) \equiv (\delta_n/\delta_0)X_n^q + g(X_0, \dots, X_{n+1}) \pmod{\pi}.$$

By the induction hypothesis, $\nu(e_i) = 1/q^d(q-1)$ for $0 \le i \le n-1$. Since $\nu(e_n)$, $\nu(e_{n+1}) \ge 0$, we have $\nu(g(e_0, \dots, e_{n+1})) \ge (q+1)/q^d(q-1) > 1/q^{d-1}(q-1) = \nu(F_n(\underline{e}))$. Therefore $\nu(e_n^q) = \nu((\delta_n/\delta_0)e_n^q) = \nu(F_n(\underline{e})) = 1/q^{d-1}(q-1)$ and the assertion for n follows. □

2. π-Exponentials

In this section, we generalize Pulita's π-exponentials and investigate properties of them.

2.1 – *Generalized π-exponentials*

In [PT16], Pickett and Thomas generalized Pulita's π-exponential to the case of Lubin–Tate module over any finite extension of $\mathbb{Q}_p$, using ramified Witt vectors. Using generalized Witt vectors studied in the previous section, we extend their construction to the case of a more general formal group whose "logarithmic" function satisfies a certain type of functional equation. These formal groups include twisted Lubin–Tate groups, i.e., those with Frobenius action. We also admit a discrete valuation ring in positive characteristic as the base ring of the formal group.

We use the same notation as in §1.2. We fix a q-typical series $l_0(T) = \sum_{i=0}^{\infty} \gamma_i T^{q^i} \in K[[T]]$ with $\gamma_0 = 1$ that satisfies the functional equation (1.2):

$$l_0(T) - \sum_{i=1}^{\infty} s_i \sigma_*^i l_0(T^{q^i}) = g(T)$$

for some $g(T) \in T\mathcal{O}[[T]]$. Remember that we assumed $\nu(s_1) = -1$ and $\nu(s_i) \ge -1$ for $i \ge 2$. Let $G_0(X,Y) = l_0^{-1}(l_0(X) + l_0(Y)) \in \mathcal{O}[[X,Y]]$ be a formal group law whose logarithm is $l_0(T)$. By Lemma 1.2.2, we can define a Witt functor $W\colon (\mathcal{O}\text{-Alg}) \to (\mathcal{O}\text{-Alg})$ for $l_0(T)$ (Definition 1.3.12). For $n \in \mathbb{N}$, let $\phi_n(\underline{X})$ be the n-th ghost polynomial for $l_0(T)$ (Definition 1.3.1).

Let $l(T) = \sum_{i=1}^{\infty} c_i T^i \in K[[T]]$ be another series with $c_1 = 1$ that satisfies the same functional equation as that for $l_0(T)$ for possibly different $g(T)$. Note that we do not assume that $l(T)$ is q-typical. Let $G(X,Y) = l^{-1}(l(X) + l(Y)) \in \mathcal{O}[[X,Y]]$

be the formal group law corresponding to $l(T)$. Let A be a commutative $\mathcal{O}$-algebra. Then G defines a group law on $TA[[T]]$. We denote by $(TA[[T]], +_G)$ when we regard $TA[[T]]$ as the group with the operation $+_G$. We equip a group $A[[T]]$ with the usual addition with the topology such that $\{T^n A[[T]] : n \in \mathbb{N}\}$ is a fundamental system of neighborhood of 0. Then $A[[T]]$ is complete with respect to this topology.

Lemma 2.1.1. *Let R be a commutative ring and $I \subset R$ an ideal. Assume that R is I-adically complete. Let $\alpha \in I$. Then for any series $f(X) \in R[[X]]$, there exist $g(X) \in R[[X]]$ and $\beta \in R$ such that $f(X) = (X - \alpha)g(X) + \beta$.*

Proof. In fact, if $f(X) = \sum_{n=0}^{\infty} a_n X^n \in R[[X]]$, then

$$g(X) = \sum_{n=0}^{\infty}\Big(\sum_{i=n+1}^{\infty} a_i \alpha^{i-n-1}\Big)T^n \quad \text{and} \quad \beta = f(\alpha) = \sum_{n=0}^{\infty} a_i \alpha^i$$

satisfy the condition. □

Lemma 2.1.2. *Let $f, g \in TA[[T]]$. We denote by $f -_G g$ the subtraction with respect to G. Then $f -_G g \in T^n A[[T]]$ is equivalent to $f - g \in T^n A[[T]]$.*

Proof. Let $\varphi(X) \in A[[T]]$ be a series such that $G(X, \varphi(X)) = 0$ and $\varphi(X) \equiv X \pmod{\deg 2}$. By definition $f -_G g = G(f, \varphi(g))$. Put $H(X, Y) = G(X, \varphi(Y))$ and regard it as an element of $A[[Y]][[X]]$. Since $H(X, X) = 0$, there exist $Q(X, Y) \in (X, Y)A[[Y]][[X]]$ such that $H(X, Y) = (X - Y)Q(X, Y)$ by Lemma 2.1.1. Since $G(X, Y) \equiv X - Y \pmod{\deg 2}$, $Q(X, Y) \equiv 1 \pmod{\deg 1}$ and the assertion follows. □

Lemma 2.1.3. *If $f_i \in TA[[T]]$ $(i = 0, 1, 2, \dots)$ is a sequence in $TA[[T]]$ that converges to* 0, *then the sum of f_i $(i = 0, 1, 2 \dots)$ with respect to G also converges.*

Proof. By Lemma 2.1.2, the sequence of finite sums $g_n = {}^G\sum_{i=0}^{n} f_i$ with respect to G is a Cauchy sequence. Hence it converges. □

In the following, we denote the infinite sum of $f_i \in TA[[T]]$ $(i = 0, 1, 2, \dots)$ by ${}^G\sum_{i=0}^{\infty} f_i$.

Now we define generalized Artin–Hasse exponentials. By Theorem 1.1.2 (ii), $l^{-1}(l_0(T)) \in \mathcal{O}[[T]]$. In the rest of this section, we denote $l^{-1}(l_0(T))$ by $E(T)$ and call it the Artin–Hasse exponential for (l_0, l). As we saw in Example 1.1.3,

$E(T)$ is a generalization of classical Artin–Hasse exponentials. Let A be a commutative $\mathcal{O}$-algebra. For $\underline{a} = (a_n)_n \in W(A)$, we define

$$E(\underline{a}, T) = {}^G\sum_{i=0}^{\infty} E(a_i T^{q^i}).$$

Note that the sum in the right hand side converges by Lemma 2.1.3 because $E(a_i T^{q^i}) \in T^{q^i} A[[T]]$. We often denote $l^{-1}(T)$ by $\exp_G(T)$, because it is the exponential function associated to the formal group law G when K is of characteristic zero.

Lemma 2.1.4. *We have*

$$E(\underline{a}, T) = \exp_G\Big(\sum_{m=0}^{\infty} \phi_m(\underline{a})\gamma_m T^{q^m}\Big).$$

Proof. It is easily obtained from the next calculation by Lemma 1.3.4.

$$\begin{aligned} E(\underline{a}, T) &= {}^G\sum_{i=0}^{\infty} l^{-1} l_0(a_i T^{q^i}) \\ &= l^{-1}\Big(\sum_{i=0}^{\infty} l_0(a_i T^{q^i})\Big) \\ &= l^{-1}\Big(\sum_{m=0}^{\infty} \phi_m(\underline{a})\gamma_m T^{q^m}\Big). \end{aligned}$$ □

Corollary 2.1.5. *The map $E(-, T)\colon W(A) \to (TA[[T]], +_G)$; $\underline{a} \mapsto E(\underline{a}, T)$ is a homomorphism of groups, i.e.,*

$$E(\underline{a} + \underline{b}, T) = E(\underline{a}, T) +_G E(\underline{b}, T).$$

Proof. The assertion follows immediately from Lemma 2.1.4. □

In order to clarify the background of the definition of $E(\underline{a}, T)$, we explain Corollary 2.1.5 in more detail. Since W is the Witt functor for l_0, if we denote the ghost maps by ϕ_m,

$$\sum_{i=0}^{\infty} l_0(a_i T^{q^i}) = \sum_{m=0}^{\infty} \phi_m(\underline{a})\gamma_m T^{q^m}$$

by Lemma 1.3.4. Therefore the map $L\colon W(A) \to TK[[T]]$ defined by

$$L((a_i)) = \sum_{i=0}^{\infty} l_0(a_i T^{q^i})$$

is a homomorphism of groups. Here we regard $TK[[T]]$ as a group with the usual addition. Since $G(X,Y) = l^{-1}(l(X) + l(Y))$,

$$l^{-1}\colon TK[[T]] \to (TK[[T]], +_G)\,;$$

is also a homomorphism of groups. Since the composite of $E(-,T)\colon W(A) \to TA[[T]]$ and the inclusion map $(TA[[T]], +_G) \to (TK[[T]], +_G)$ is the composite of the two homomorphisms above, the additivity of $E(-,T)$ follows.

$$\begin{array}{ccc} W(A) & \xrightarrow{E(-,T)} & (TA[[T]], +_G) \\ {\scriptstyle L}\downarrow & & \downarrow \\ TK[[T]] & \xrightarrow{l^{-1}} & (TK[[T]], +_G) \end{array}$$

Lemma 2.1.6. *For* $\underline{a}$, $\underline{b} = (b_i)_i \in W(A)$,

$$E(\underline{a}\underline{b}, T) = {}^{G}\sum_{i=0}^{\infty} E(F^i(\underline{a}), b_i T^{q^i}).$$

Proof. By Lemma 2.1.4, we have

$$\begin{aligned} l(E(F^i(\underline{a}), b_i T^{q^i})) &= \sum_{k=0}^{\infty} \phi_{k+i}(\underline{a})\gamma_k (b_i T^{q^i})^{q^k} \\ &= \sum_{k=0}^{\infty} \phi_{k+i}(\underline{a})\gamma_k b_i^{q^k} T^{q^{k+i}} \\ &= \sum_{m=i}^{\infty} \phi_m(\underline{a}) \frac{\gamma_{m-i}}{\gamma_m} b_i^{q^{m-i}} \gamma_m T^{q^m}. \end{aligned}$$

Therefore

$$\begin{aligned} l\Big({}^{G}\sum_{i=0}^{\infty} E(F^i(\underline{a}), b_i T^{q^i})\Big) &= \sum_{i=0}^{\infty}\sum_{m=i}^{\infty} \phi_m(\underline{a}) \frac{\gamma_{m-i}}{\gamma_m} b_i^{q^{m-i}} \gamma_m T^{q^m} \\ &= \sum_{m=0}^{\infty} \phi_m(\underline{a}) \Big(\sum_{i=0}^{m} \frac{\gamma_{m-i}}{\gamma_m} b_i^{q^{m-i}}\Big) \gamma_m T^{q^m} \\ &= \sum_{m=0}^{\infty} \phi_m(\underline{a})\phi_m(\underline{b})\gamma_m T^{q^m} \\ &= l(E(\underline{a}\underline{b}), T) \end{aligned}$$

and the assertion follows. □

As in the previous section, we fix an algebraic closure K^{a} of K and a valuation $v\colon K^{\mathrm{a}} \to \mathbb{Q} \cup \{\infty\}$ extending the normalized discrete valuation of K.

Definition 2.1.7 (generalized π-exponential). Let π' be a uniformizer of $\mathcal{O}$. Let $P(T) \in \mathcal{O}[T]$ be a polynomial such that

(1) $P(T) \equiv T^q \pmod{\pi}$, and

(2) $P(T) \equiv \pi' T \pmod{\deg 2}$.

Let $\underline{\pi} = (\pi_d, \dots, \pi_1, \pi_0, 0, \dots)$ be a P-sequence (Definition 1.5.8) in K^{a}, $L = K(\pi_d) \subset K^{\mathrm{a}}$ and $\mathcal{O}_L$ the valuation ring of L. We define the π-exponential for $\underline{\pi}$ to be

$$\epsilon(\underline{\pi}, T) := \exp_G\left(\sum_{i=0}^{d} \pi_{d-i}\gamma_i T^{q^i}\right) \in L[[T]].$$

The following theorem is a generalization of [Ric15, B.2, Proposition 5] to the case of our π-exponential.

Theorem 2.1.8. *Let the notation and the assumption be as in Definition 2.1.7. Then* $\epsilon(\underline{\pi}, T) = \sum_{i=1}^{\infty} a_i T^i \in \mathcal{O}_L[[T]]$. *Moreover,* $v(a_i) \geq 1/q^d(q-1)$ *for any* $i \in \mathbb{N}$ *and the equality holds if and only if* $i = q^m$ *for some* $m \in \mathbb{N}$. *Consequently, the radius of convergence of* $\epsilon(\underline{\pi}, T)$ *is 1.*

Proof. Let $L = K(\pi_d) \subset K^{\mathrm{a}}$ and $\mathcal{O}_L = \{x \in L\colon v(x) \geq 0\}$. Let $s_P\colon \mathcal{O}_L \to W(\mathcal{O}_L)$ be as in Definition 1.5.6. If we put $\underline{e} = s_P(\pi_d)$, then $\phi(\underline{e}) = \underline{\pi}$ by Lemma 1.5.7. Since

$$\epsilon(\underline{\pi}, T) = E(\underline{e}, T) = {}^{G}\sum_{i=0}^{\infty} E(e_i T^{q^i}),$$

the assertion follows from Lemma 1.5.9. □

The following corollary generalizes and refines [PT16, Proposition 3.7].

Corollary 2.1.9. *Let* $l(T) = \sum_{i=1}^{\infty} c_i T^i \in K[[T]]$ *be a series with* $c_1 = 1$ *that satisfies the functional equation* (1.2) *and let* $|\ |\colon K^{\mathrm{a}} \to \mathbb{R}_{\geq 0}$ *be an absolute value corresponding to* v. *Then the radius of convergence of* $\exp_G(T) = l^{-1}(T)$ *is* $|\pi|^{1/(q-1)}$.

Proof. Let $l_0(T)$ be the series that satisfying the same functional equation (1.2) for $g(T) = T$. Then $l_0(T)$ is q-typical and the coefficient of T is 1. Applying Theorem 2.1.8 to $l_0(T)$ and $l(T)$ with $d = 0$, we see that the radius of convergence of $\epsilon(\underline{\pi}, T) = \exp_G(\pi_0 T)$ is 1. Since $v(\pi_0) = 1/(q-1)$, the assertion follows. □

REMARK 2.1.10. When K is of characteristic zero, then $l(T)$ is recovered from the formal group law $G(X, Y) = l^{-1}(l(X) + l(Y))$ by the formula

$$l(T) = \int_0^T \frac{\mathrm{d}Y}{\frac{\partial G}{\partial X}(0, Y)},$$

so we may call $\exp_G(T) = l^{-1}(T)$ the exponential series of G. On the other hand, when K is of characteristic $p > 0$, $l(T)$ is not uniquely determined from $G(X, Y)$. For example, Carlitz logarithm $l_C(T)$ (2.2) gives the additive formal group law, because $l_C^{-1}(l_C(X) + l_C(Y)) = X + Y$.

2.2 – *Radii of convergence of exponential type functions*

In this section, we generalize results of Richard on the radii of convergence of functions of the form $\exp(Q(T))$ with a polynomial $Q[T]$ ([Ric15]). First we generalize a theorem on Witt rings [Ric15, 1.2, Theorem 1].

THEOREM 2.2.1. *Let π' and $P(T) \in \mathcal{O}[T]$ be as in Theorem 2.1.8 and $\underline{\pi}^{(d)} = (\pi_d, \dots, \pi_0, 0, \dots)$ be a P-sequence. Let $L \subset K^{\mathrm{a}}$ be an extension field of K such that $\pi_d \in L$ and $\mathcal{O}_L$ the valuation ring of L. Then* $\mathrm{Ker}(F^{d+1}\colon W(\mathcal{O}_L) \to W(\mathcal{O}_L))$ *is a free $W(\mathcal{O}_L)/V^{d+1}W(\mathcal{O}_L)$-module of rank one that has $\underline{e}^{(d)}$ as a basis.*

PROOF. We denote $\mathrm{Ker}(F^n\colon W(A) \to W(A))$ (resp. $W(A)/V^n W(A)$) by ${}_nW(A)$ (resp. $W_n(A)$) for an $\mathcal{O}$-algebra A. It is obvious from the definition that if $F^{d+1}\underline{a} = 0$ and $\underline{b} \in V^{d+1}W(A) = 0$, then $\underline{b}\underline{a} = 0$. Therefore we can regard ${}_{d+1}W(\mathcal{O}_L)$ as a $W_{d+1}(\mathcal{O}_L)$-module. Thus it is sufficient to show that the map $h\colon W_{d+1}(\mathcal{O}_L) \to {}_{d+1}W(\mathcal{O}_L)$ which sends $\underline{b} \pmod{V^{d+1}W(\mathcal{O}_L)}$ to $\underline{b}\underline{e}^{(d)}$ is an isomorphism. It is easy to see that h is injective, because $\pi_i \neq 0$ for $i = 0, 1, \dots, d$. We show the surjectivity by induction on d. Let $\underline{a} \in {}_{d+1}W(\mathcal{O}_L)$, then $\phi_n(\underline{a}) = 0$ for $n > d$. Since $\underline{\pi}^{(d)} = \phi(\underline{e}^{(d)}) = (\pi_d, \dots, \pi_0, 0, \dots)$ and $W_{d+1}(L) \simeq L^{d+1}$, there exists an element $\underline{b} = (b_i)_i \in W(L)$ such that $\underline{a} = \underline{b}\underline{e}^{(d)}$. It is enough to show $b_0, \dots, b_d \in \mathcal{O}_L$. When $d = 0$, $E(\underline{a}, T) = E(\underline{e}^{(0)}, b_0 T) = \epsilon(\underline{\pi}^{(0)}, b_0 T)$ by Lemma 2.1.4 and Lemma 2.1.6. Since $E(\underline{a}, T) \in T\mathcal{O}_L[[T]]$, $v(b_0^{q^i}) + 1/(q-1) \geq 0$ for any i by Theorem 2.1.8. Hence $v(b_0) \geq 0$. Suppose that $d > 0$. Since $F^i(\underline{e}^{(d)}) = \underline{e}^{(d-i)}$, we have

$$E(\underline{a}, T) = {}^G\!\sum_{i=0}^{d} E(F^i(\underline{e}), b_i T^{q^i}) = {}^G\!\sum_{i=0}^{d} \epsilon(\underline{\pi}^{(d-i)}, b_i T^{q^i})$$

by Lemma 2.1.4 and Lemma 2.1.6. Since $E(\underline{a}, T) \in T\mathcal{O}_L[[T]]$, comparing the coefficient of T, we have $\nu(b_0) + 1/q^d(q-1) \geq 0$. Then the coefficient of T^q of ${}^G\sum_{i=1}^d \epsilon(\underline{\pi}^{(d-i)}, b_i T^{q^i})$ is also in $\mathcal{O}_L$ and hence $\nu(b_1) + 1/q^{d-1}(q-1) \geq 0$. By induction, we can see that $\nu(b_i) \geq -1/q^{d-i}(q-1)$ for $0 \leq i \leq d$. Since $F(\underline{a}) \in {}_dW(\mathcal{O}_L)$ and $F(\underline{a}) = F(\underline{b})F(\underline{e}^{(d)}) = F(\underline{b})\underline{e}^{(d-1)}$, $F(\underline{b}) \in W(\mathcal{O}_L)$ by the induction hypothesis. We prove $b_i \in \mathcal{O}_L$ by induction on i. Recall that we defined $\delta_i = \gamma_i/\gamma_{i+1}$. Since $F_0(\underline{b}) = b_0^q + \delta_0 b_1 \in \mathcal{O}_L$ and $\nu(\delta_0 b_1) \geq 1 - 1/q^{d-1}(q-1) > 0$, we see $\nu(b_0^q) \geq 0$ and hence $b_0 \in \mathcal{O}_L$. Let $i > 0$. We can choose $\underline{b}$ so that $b_{d+1} = 0$. Then $\nu(b_{i+1}) \geq -1/q^{d-i-1}(q-1)$ for $0 \leq i \leq d$. Since $b_0, \ldots, b_{i-1} \in \mathcal{O}_L$ by the induction hypothesis, we have $(\delta_i/\delta_0)b_i^q \in \mathcal{O}_L$ by Lemma 1.5.4. Thus we obtain $b_i \in \mathcal{O}_L$. □

The following theorem generalizes p-typical part of §2.5, Theorem 2 and §2.12, Proposition 2 in [Ric15].

Theorem 2.2.2. *Let K' be an extension field of K equipped with a valuation extending that of K and $\mathcal{O}_{K'}$ the valuation ring of K'. Let $Q(T) = w_0 T + w_1 T^q + \cdots + w_d T^{q^d} \in K'[T]$ be a q-typical polynomial of degree q^d. Let π' and $P(T) \in \mathcal{O}[T]$ be as in Theorem 2.1.8 and $\underline{\pi}^{(d)} = (\pi_d, \ldots, \pi_0, 0, \ldots)$ be a P-sequence of length d. Set $L = K'(\pi_d)$ and we equip L with a valuation extending the valuation of K'. Let $\mathcal{O}_L$ be the valuation ring of L. We put $\widetilde{Q}(T) = (w_0/\pi_d)T + (w_1/\pi_{d-1})T^q + \cdots + (w_d/\pi_0)T^{q^d}$. Then the following conditions are equivalent*:

(1) *The radius of convergence of* $\exp_G(Q(T)) \in TK'[[T]]$ *is at least 1.*
(2) $\exp_G(Q(T)) \in T\mathcal{O}_{K'}[[T]]$.
(3) *The coefficient of degree j in* $\exp_G(\widetilde{Q}(T))$ *is in $\mathcal{O}_L$ for $1 \leq j \leq q^d$.*
(4) *The coefficient of degree q^i in* $\exp_G(\widetilde{Q}(T))$ *is in $\mathcal{O}_L$ for $0 \leq i \leq d$.*

Proof. We first show that the conditions (2), (3) and (4) are equivalent. Let $u_i = w_i/\gamma_i$ for $0 \leq i \leq d$ and $u_i = 0$ for $i > d$. Since $\phi \colon W(L) \to L^{\mathbb{N}}$ is a bijection, there exists uniquely an element $\underline{a} = (a_i) \in W(L)$ such that $\phi(\underline{a}) = \underline{u} = (u_i)$. Then by Lemma 2.1.4, we have

$$\exp_G(Q(T)) = \exp_G\Bigl(\sum_{i=0}^{d} u_i \gamma_i T^{q^i}\Bigr) = E(\underline{a}, T) = {}^G\sum_{i=0}^{\infty} E(a_i T^{q^i})$$

and hence $\exp_G(Q(T)) \in T\mathcal{O}[[T]]$ if and only if $\underline{a} \in W(\mathcal{O})$. Let $\underline{\pi}^{(d)} = (\pi_d, \ldots, \pi_0, 0, \ldots)$ and let $\underline{e}^{(d)} \in W(\mathcal{O}_L)$ be an element such that $\phi(\underline{e}^{(d)}) = \underline{\pi}^{(d)}$.

Then there exists an element $\underset{\sim}{b} \in W(L)$ such that $\underset{\sim}{a} = \underset{\sim}{b}\underset{\sim}{e}^{(d)}$, because $F^{d+1}(\underset{\sim}{a}) = 0$. By Theorem 2.2.1, $\underset{\sim}{a} \in {}_{d+1}W(\mathcal{O})$ if and only if $\underset{\sim}{b} + V^{d+1}W(L) \in W_{d+1}(\mathcal{O}_L)$. Since

$$\exp_G(\tilde{Q}(T)) = \exp_G\Big(\sum_{i=0}^{d} \frac{u_i}{\pi_{d-i}} \gamma_i T^{q^i}\Big) = E(\underset{\sim}{b}, T) = {}^G\sum_{i=0}^{\infty} E(b_i T^{q^i}),$$

the condition (2) is equivalent to the condition (3) or (4). Next we show the equivalence of (1) and (2). It is evident that (2) implies (1). Conversely, suppose that $\exp_G(Q(T)) \notin T\mathcal{O}[[T]]$. We write $\exp_G(Q(T)) = {}^G\sum_{i=0}^{\infty} E(a_i T^{q^i}) = \sum_{j=1}^{\infty} c_j T^j$. Let $n \in \mathbb{N}$. If

$$\text{(2.1)} \qquad \frac{\nu(a_n)}{q^n} < 0 \quad \text{and} \quad \frac{\nu(a_n)}{q^n} < \frac{\nu(a_i)}{q^i} \quad \text{for any } i \text{ such that } 0 \le i < n,$$

then $\nu(c_{q^n})/q^n = \nu(a_n)/q^n$. By the assumption, there exists $n \in \mathbb{N}$ such that $\nu(a_n) < 0$. Therefore, by Lemma 2.2.3 below, there exists an infinite sequence of positive integers $n_0 < n_1 < n_2 < \cdots$ such that each n_k satisfies the condition (2.1). This shows $\liminf_j \nu(c_j)/j < 0$ and hence the radius of convergence of $\exp_G(Q(T))$ is less than 1. Thus (1) implies (2) and the proof is completed. □

Lemma 2.2.3. *Let L be as in Theorem 2.2.2. Let $\underset{\sim}{a} = (a_i)_i \in \operatorname{Ker}(F^{d+1}\colon W(L) \to W(L))$ for some $d \in \mathbb{N}$ and $\underset{\sim}{a} \notin W(\mathcal{O}_L)$. Then $\{\nu(a_i)/q^i : i \in \mathbb{N}\} \subset \mathbb{R}$ does not have the minimum value.*

Proof. Suppose that $\{\nu(a_i)/q^i : i \in \mathbb{N}\}$ has the minimum value. Let $M = \min\{\nu(a_i)/q^i : i \in \mathbb{N}\}$ and $i_0 = \min\{i \in \mathbb{N} : \nu(a_i)/q^i = M\}$. By the assumption, we have $M < 0$. Let j and n be integers such that $0 \le j$ and $d < n$. Since $\underset{\sim}{a} \in \operatorname{Ker} F^{d+1}$, we have

$$a_0^{q^n} + \frac{\gamma_{n-1}}{\gamma_n} a_1^{q^{n-1}} + \cdots + \frac{\gamma_0}{\gamma_n} a_n = 0.$$

If $0 \le j < i_0$, then $\nu(a_j)/q^j > \nu(a_{i_0})/q^{i_0}$. Therefore, if n is sufficiently large so that $i_0/q^n < \nu(a_j)/q^j - \nu(a_{i_0})/q^{i_0}$, we have $\nu(a_j)/q^j + j/q^n > \nu(a_{i_0})/q^{i_0} + i_0/q^n$. If $i_0 < j$, then $\nu(a_{i_0})/q^{i^0} \le \nu(a_j)/q^j$ and hence $\nu(a_j)/q^j + j/q^n > \nu(a_{i_0})/q^{i^0} + i_0/q^n$. Thus there exists an integer $N \ge i_0$ such that for any integer j and $n > N$ satisfying $j \ne i_0$ and $0 \le j < n$, $\nu((\gamma_{n-j}/\gamma_n) a_j^{q^{n-j}}) > \nu((\gamma_{n-i_0}/\gamma_n) a_{i_0}^{q^{n-i_0}})$. For such an n, we have $\nu(a_n) = \frac{q^n}{q^{i_0}} \nu(a_{i_0}) + i_0 - n$. Then

$$\frac{\nu(a_n)}{q^n} = M + \frac{i_0 - n}{q^n} < M$$

and we have a contradiction. □

The following corollary is a generalization of p-typical case of [Ric15, 3, Cor.3].

Corollary 2.2.4. *Let* $\underline{\pi}^{(d)} = (\pi_d, \ldots, \pi_0, 0, \ldots)$, K', L, $\mathcal{O}_L$ *and* $Q(T) = \sum_{i=0}^{d} w_0 T^{q^i} \in K[T]$ *be as in Theorem* 2.2.2. *Let* $\widetilde{Q}(T) = \widetilde{Q}(T) = (w_0/\pi_d)T + (w_1/\pi_{d-1}) + \cdots + (w_d/\pi_0)T^{q^d}$ *and* $\exp_G(\widetilde{Q}(T)) = \sum_{j=1}^{\infty} \tilde{c}_j T^j$. *We denote by* $|\ |\colon K^{\mathrm{a}} \to \mathbb{R}_{\geq 0}$ *an absolute value corresponding to* ν. *If we put*

$$\alpha = \min_{1 \leq j \leq q^d} \frac{\nu(\tilde{c}_j)}{j},$$

then the radius of convergence of $\exp_G(Q(T))$ *is* $|\pi|^{-\alpha}$.

Proof. Replacing K' by its some extension, we can assume that there exists an element $y \in K'$ such that $\nu(y) = \alpha$. Then by homothety, we can reduce to the case of $\alpha = 0$. Thus it suffices to show that the radius of convergence of $\exp_G(Q(T))$ is at least 1 if and only if $\nu(\tilde{c}_j)/j \geq 0$ for any j such that $1 \leq j \leq q^d$ and the assertion follows from Theorem 2.2.2. □

2.3 – *Overconvergence*

In this section, we prove that the overconvergence property also holds for generalized π-exponentials.

Theorem 2.3.1. *Assume that there exists a uniformizer* $\pi' \in \mathcal{O}$ *such that* $\sigma^n(\pi') \equiv \delta_{n-1} \pmod{\pi^{n+1}}$ *for* $0 \leq n \leq d+1$ (*note that we defined* $\delta_{-1} = 0$). *Let* $P(T) \in \mathcal{O}[T]$ *be a polynomial such that*

(1) $P(T) \equiv T^q \pmod{\pi}$,

(2) $P(T) \equiv \pi' T \pmod{\deg 2}$

and let $\underline{\pi} = (\pi_d, \ldots, \pi_0, 0, \ldots)$ *be a* $\sigma_* P$*-sequence of length* d. *Then the series*

$$\exp_G\Big(\sum_{i=0}^{d} \pi_{d-i}\gamma_i\big(T^{q^i} - T^{q^{i+1}}\big)\Big)$$

is overconvergent, i.e., the radius of convergence is strictly larger than 1.

Proof. Let $\pi_{d+1} \in K^{\mathrm{a}}$ be an element such that $P(\pi_{d+1}) = \pi_d$, $L = K(\pi_{d+1}) \subset K^{\mathrm{a}}$ and $\mathcal{O}_L$ the valuation ring of L. We put $\underline{\pi}^{(d+1)} = (\pi_{d+1}, \pi_d, \ldots, \pi_0, 0, \ldots) \in L^{\mathbb{N}}$. Let $\underline{e}^{(d+1)} = s_P(\pi_{d+1})$ and put $\underline{e}^{(d+1-i)} = F^i(\underline{e}^{(d+1)})$ for

$1 \le i \le d+1$. Then $\phi(\underline{e}^{(i)}) = \underline{\pi}^{(i)}$ for $0 \le i \le d+1$ by Lemma 1.5.7. Since $\phi(V(\underline{e}^{(d)})) = (0, (\gamma_0/\gamma_1)\pi_d, (\gamma_1/\gamma_2)\pi_{d-1}, \dots)$, we have

$$\begin{aligned} E((F - VF)(\underline{e}^{(d+1)}), T) &= E(\underline{e}^{(d)} - V(\underline{e}^{(d)}), T) \\ &= \exp_G\Big(\sum_{i=0}^{d} \pi_{d-i}\gamma_i T^{q^i} - \sum_{i=1}^{d+1} \frac{\gamma_{i-1}}{\gamma_i}\pi_{d-i+1}\gamma_i T^{q^i}\Big) \\ &= \exp_G\Big(\sum_{i=0}^{d} \pi_{d-i}\gamma_i (T^{q^i} - T^{q^{i+1}})\Big). \end{aligned}$$

Since $F(\underline{e}^{(d+1)}) = P(\underline{e}^{(d+1)})$ by Lemma 1.3.10 and $VF(\underline{e}^{(d+1)}) = \underline{\mu}\underline{e}^{(d+1)}$ by Lemma 1.3.20, if we put $H(T) = (P(T) - \pi' T)/T$, then we have

$$(F - VF)(\underline{e}^{(d+1)}) = H(\underline{e}^{(d+1)})\underline{e}^{(d+1)} + (\pi' - \underline{\mu})\underline{e}^{(d+1)}.$$

Let $\underline{a} = (a_i) = H(\underline{e}^{(d+1)})$ and $\underline{b} = (b_i) = \pi' - \underline{\mu}$. Let us denote the i-th component of $\underline{e}^{(d+1)}$ by $e_i^{(d+1)}$. Since $H(0) = 0$ and $\nu(e_i^{(d+1)}) > 0$ by Lemma 1.5.9, it is evident that $\nu(a_i) > 0$ for any $i \in \mathbb{N}$. If we define $\delta_{-1} = 0$, then $\phi(\underline{b}) = \phi(\pi' - \underline{\mu}) = (\sigma^i(\pi') - \delta_{i-1}) \in \mathcal{O}_L^{\mathbb{N}}$. By the assumption, $\nu(\phi_n(\underline{b})) = \nu(\sigma^n(\pi') - \delta_{n-1}) \ge n + 1$ for $0 \le n \le d+1$. Then we can show that $\nu(b_i) \ge 1$ for $0 \le i \le d+1$ by induction on i. Let $\underline{c} = (c_i) = \underline{a} + \underline{b}$. Then $\nu(c_i) > 0$ for $0 \le i \le d+1$, because each c_i is a polynomial in a_j and b_j ($j \in \mathbb{N}$) without constant term. By Lemma 2.1.6, we have

$$\begin{aligned} E((F - VF)(\underline{e}^{(d+1)}), T) &= E(\underline{e}^{(d+1)}\underline{c}, T) \\ &= {}^G\sum_{i=0}^{d+1} E(F^i(\underline{e}^{(d+1)}), c_i T^{q^i}) \\ &= {}^G\sum_{i=0}^{d+1} \epsilon(\underline{\pi}^{(d+1-i)}, c_i T^{q^i}). \end{aligned}$$

Let

$$\epsilon(\underline{\pi}^{(d+1-i)}, c_i T^{q^i}) = \sum_{j=1}^{\infty} u_{ij} T^j \quad \text{and} \quad {}^G\sum_{i=0}^{d+1} \epsilon(\underline{\pi}^{(d+1-i)}, c_i T^{q^i}) = \sum_{j=1}^{\infty} u_j T^j.$$

Since $\epsilon(\underline{\pi}^{(d+1-i)}, T) \in \mathcal{O}_L[[T]]$ and $\nu(c_i) > 0$ for $0 \le i \le d+1$, there exists a positive number $\eta > 0$ such that $\nu(u_{ij}) \ge j\eta$ for any $j \in \mathbb{N}$ and $0 \le i \le d+1$. Therefore $\nu(u_j) \ge j\eta$ and the proof is completed. □

Proposition 2.3.2. *Let the notation and the assumption be as in Theorem 2.3.1. Suppose that either one of the following conditions holds.*

(1) *$l_0(T)$ satisfies the functional equation (1.3) for some $g(T) \in T\mathcal{O}[[T]]$, $\sigma = \mathrm{id}$ and $\pi' = \pi$.*

(2) *$l_0(T) = \sum_{i=0}^{\infty} T^{q^i}/\langle\pi\rangle_i$ and $\sigma(\pi') = \pi$.*

Then $\sigma^n(\pi') \equiv \delta_{n-1} \pmod{\pi^{n+1}}$ for any $n \in \mathbb{N}$ (note that we defined $\delta_{-1} = 0$). Consequently,

$$\exp_G\Big(\sum_{i=0}^{d} \pi_{d-i}\gamma_i(T^{q^i} - T^{q^{i+1}})\Big)$$

is overconvergent.

Proof. Suppose that the assumption (1) holds. Then there exists $c_n \in \mathcal{O}$ such that $\gamma_{n+1} - \gamma_n/\pi = c_n \in \mathcal{O}$ for any $n \in \mathbb{N}$. Then $\delta_n - \pi = c_n\pi/\gamma_{n+1} \equiv 0 \pmod{\pi^{n+2}}$. Next suppose that the assumption (2) holds. Then $\gamma_n = 1/\langle\pi\rangle_n$ and hence $\delta_n = \gamma_n/\gamma_{n+1} = \sigma^n(\pi)$. Therefore $\sigma^n(\pi') - \delta_{n-1} = 0$. □

Remark 2.3.3. Theorem 2.3.1 is a generalization of [Mat95, Propoposition 1.10], [Pul07, Theorem 2.28] and [PT16, Theorem 1]. The above proof basically follows Pulita's proof except that we do not decompose $(F - VF)(\underline{e}^{(d+1)})$ to $(F - FV)(\underline{e}^{(d+1)}) + (FV - VF)(\underline{e}^{(d+1)})$. The reason is that, in general, valuations of components of $FV - VF = F(\underline{\mu}) - \underline{\mu}$ are not always positive, contrary to the classical case (cf. Remark 1.3.21). For example, let $\mathcal{O}$ and $\sigma\colon \mathcal{O} \to \mathcal{O}$ be as in Example 1.5.3. Assume that $l_0(T) = \sum_{i=0}^{\infty} T^{q^i}/\langle\pi\rangle_i$ and $p = 3$. Then $\delta_1 - \delta_0 = \sigma(\pi) - \pi = (t+1)(t+2)\pi \notin (\pi^2)$. Let $F(\underline{\mu}) - \underline{\mu} = (a_i)$. Since $\phi(F(\underline{\mu}) - \underline{\mu}) = (\delta_0, \delta_1 - \delta_0, \dots)$, $a_0 = \delta_0 = \pi$ and $a_0^q + (\gamma_0/\gamma_1)a_1 = \sigma(\pi) - \pi$. Therefore $a_1 = \gamma_1(\sigma(\pi) - \pi - \pi^q) \notin (\pi)$. Note that the assumption (2) of Proposition 2.3.2 still holds for π' such that $\sigma(\pi') = \pi$.

Finally we give an example where the base ring is in positive characteristic. Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements. Let $A = \mathbb{F}_q[\theta]$ be a polynomial ring in θ over $\mathbb{F}_q$, K the field of fractions of A and $\mathcal{O}$ the localization of A at θA. We set $[i] = \theta^{q^i} - \theta$, $L_0 = 1$ $D_0 = 1$ and $L_i = \prod_{j=1}^{i}[j] = [i][i-1]\cdots[1]$, $D_i = \prod_{j=1}^{i}[j]^{q^{j-i}} = [i][i-1]^q\cdots[1]^{q^{i-1}}$ for $i \in \mathbb{Z}_{>0}$. Then the Carlitz exponential $e_C(T)$ and the Carlitz logarithm $l_C(T)$ are defined to be

$$e_C(T) = \sum_{i=1}^{\infty}\frac{T^{q^i}}{D_i}, \quad l_C(T) = \sum_{i=1}^{\infty}\frac{(-1)^i T^{q^i}}{L_i}. \tag{2.2}$$

See e.g., [Gos96]. Note that, if we denote by $[\ ]_C\colon A \to \mathrm{End}(C)$ the A-module structure of the Carlitz module, then $l_C(T)$ is recovered by

$$l_C(T) = \lim_{n\to\infty} \frac{[\theta^n]_C(T)}{\theta^n}.$$

Let $\sigma = \mathrm{id}$, $\pi = \theta$. Then $l_C(T)$ satisfies a functional equation

$$l_C(T) - \frac{l_C(T^q)}{\theta} = \frac{l_C(\theta T)}{\theta}.$$

Since $(1/\theta)l_C(\theta T) \in \mathcal{O}[[T]]$, the assumptions of Theorem 1.1.1 are satisfied. We take $l_C(T)$ as $l_0(T)$ and $l(T)$. In this case, the formal group law is $l_C^{-1}(l_C(X) + l_C(Y)) = X + Y$ and the Artin–Hasse exponential $E(T)$ is $l_C^{-1}(l_C(T)) = T$. The n-th ghost polynomial for the Witt functor is as follows:

$$\phi_n(\underline{X}) = \sum_{i=0}^{n} \frac{(-1)^i L_n}{L_{n-i}} X_i^{q^{n-i}}.$$

Set $P(T) = T^q + \theta T$ and $\underline{\pi} = (\pi_d, \ldots, \pi_0, 0, \ldots)$ be a P-sequence of length d. Then, by Proposition 2.3.2 (1), we have the following proposition.

Proposition 2.3.4. *The series*

$$e_C\Big(\sum_{i=0}^{d} \pi_{d-i} \frac{(-1)^i\big(T^{q^i} - T^{q^{i+1}}\big)}{L_i}\Big)$$

is overconvergent.

Proposition 2.3.4 generalizes the theorem by A. N. Kochubei [Koc08, Proposition 2]. He proved that the radius of convergence of $e_C(\pi_0(T - T^q))$ (the case where $d = 0$) is greater than or equal to $|\pi|^{-(q-1)/q^2}$. Using Corollary 2.2.4, we can prove that the equality holds.

Proposition 2.3.5. *The radius of convergence of $e_C(\pi_0(T - T^q))$ is equal to $|\pi|^{-(q-1)/q^2}$.*

Proof. It is easy to see that

$$e_C\Big(\pi_0\Big(\frac{T}{\pi_1} - \frac{T^q}{\pi_0}\Big)\Big) = \frac{\pi_0 T}{\pi_1} + \Big(\frac{\pi_0^q}{D_1\pi_1^q} - 1\Big)T^q + \text{higher degree terms}.$$

Let $\tilde{c}_1 = \pi_0/\pi_1$ and $\tilde{c}_q = \pi_0^q/D_1\pi_1^q - 1$ be the coefficients of degree 1 and degree q respectively. Then

$$\tilde{c}_q = \frac{\pi_0^q - (\theta^q - \theta)\pi_1^q}{D_1\pi_1^q} = \frac{\theta^q\pi_1^q - \theta^2\pi_1}{(\theta^q - \theta)\pi_1^q}$$

and we have $\nu(\tilde{c}_1) = 1/(q-1) - 1/q(q-1) = 1/q$ and $\nu(\tilde{c}_q) = 2 + 1/q(q-1) - 1 - 1/(q-1) = (q-1)/q$. Thus $\min\{\nu(\tilde{c}_1), \nu(\tilde{c}_q)/q\} = \min\{1/q, (q-1)/q^2\} = (q-1)/q^2$. By Corollary 2.2.4, the radius of convergence of $e_C(\pi_0(T - T^q))$ is $|\pi|^{-(q-1)/q^2}$. □

References

[BM16] B. Benzaghou and S. Mokhfi, *Formule de Trace pour les anneaux de Witt*, preprint, 2016. arXiv:1605.07676

[Bou83] N. Bourbaki, *Éléments de Mathématique,* Algèbre commutative, Chapitre 8. Dimension. Chapitre 9, Anneaux locaux noethériens complets, Masson, Paris, 1983.

[CC96] B. Chiarellotto – G. Christol, *On overconvergent isocrystals and F-isocrystals of rank one*, Compositio Math. 100 (1996), no. 1, pp. 77–99.

[CP09] B. Chiarellotto – A. Pulita, *Arithmetic and differential Swan conductors of rank one representations with finite local monodromy*, Amer. J. Math. 131 (2009), no. 6, pp. 1743–1794.

[Chr11] G. Christol, *The radius of convergence function for first order differential equations*, In *Advances in non-Archimedean analysis* (Clermont-Ferrand, 2010), edited by J. Araujo-Gomez, B. Diarra, and A. Escassut, Contemporary Mathematics, 551, American Mathematical Society, Providence, R.I., 2011, pp. 71–89.

[Cre00] R. Crew, *Canonical extensions, irregularities, and the Swan conductor,* Math. Ann. 316 (2000), no. 1, pp. 19–37.

[Gos96] D. Goss, *Basic structures of function field arithmetic,* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 35. Springer-Verlag, Berlin, 1996.

[Haz78] M. Hazewinkel, *Formal groups and applications,* Pure and Applied Mathematics, 78. Academic Press, New York and London, 1978.

[Haz80] M. Hazewinkel, *Twisted Lubin–Tate formal group laws, ramified Witt vectors and (ramified) Artin–Hasse exponentials,* Trans. Amer. Math. Soc. 259 (1980), no. 1, pp. 47–63.

[Ked10] K. S. Kedlaya, *p-adic differential equations,* Cambridge Studies in Advanced Mathematics, 125. Cambridge University Press, Cambridge, 2010.

[Ked16] K. S. Kedlaya, *Convergence polygons for connections on nonarchimedean curves,* In *Nonarchimedean and tropical geometry* (St. John, 2013, and Puerto Rico, 2015), edited by M. Baker and S. Payne, Simons Symposia, Springer, Cham, 2016. pp. 51–97.

[Koc08] A. N. Kochubei, *Dwork–Carlitz exponential and overconvergence for additive functions in positive characteristic,* Int. J. Number Theory 4 (2008), no. 3, pp. 453–460.

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

[Mat95] S. Matsuda, *Local indices of p-adic differential operators corresponding to Artin–Schreier–Witt coverings,* Duke Math. J. 77 (1995), no. 3, pp. 607–625.

[Mat02] S. Matsuda, *Katz correspondence for quasi-unipotent overconvergent isocrystals,* Compositio Math. 134 (2002), no. 1, pp. 1–34.

[Mor10] Y. Morofushi, *p-adic theory of exponential sums on the affine line,* dissertation, University of Florida, 2010. http://ufdcimages.uflib.ufl.edu/uf/e0/04/14/24/00001/morofushi_y.pdf

[PT16] E. J. Pickett – L. Thomas, *Formal group exponentials and Galois modules in Lubin–Tate extension,* Int. Math. Res. Not. IMRN 2016, no. 11, pp. 3205–3236.

[PV11] E. J. Pickett – S. Vinatier, *Exponential power series, Galois module structure and differential modules,* Preprint, 2011. arXiv:1107.1120

[Pul07] A. Pulita, *Rank one solvable p-adic differential equations and finite abelian characters via Lubin–Tate groups,* Math. Ann. 337 (2007), no. 3, pp. 489–555.

[Rib98] P. Ribenboim, *The theory of classical valuations*, Springer Monographs in Mathematics, (1998), Springer.

[Ric15] R. Richard, *Sur les π-exponentielles* I, Rend. Sem. Mat. Univ. Padova 133 (2015), pp. 125–158.

[Rob85] P. Robba, *Indice d'un opérateur différentiel p-adique,* IV. *Cas des systèmes. Measure de l'irrégularité dans un disque*, Ann. Inst. Fourier (Grenoble) 35 (1985), no. 2, pp. 13–55.

[Tsu98] N. Tsuzuki, *The local index and the Swan conductor*, Compositio Math. 111 (1998), no. 3, pp. 245–288.

[Xia10] L. Xiao, *On ramification filtrations and p-adic differential modules,* I: *the equal characteristic case,* Algebra Number Theory 4 (2010), no. 8, pp. 969–1027.

Manoscritto pervenuto in redazione il 24 ottobre 2017.