Higher dimensional Witt vector

February 4, 2025

Abstract

In this paper, we generalize the theory of Witt vectors to higher dimensional case, based on the functional equation lemma by Hazwinkel, and show that the classical Dieudonne formula also holds in this case.

Introduction

0.1 Notation

We denote by $\mathbb{N} = \{0, 1, 2, \dots\}$ the set of natural numbers. Note that we assume $0 \in \mathbb{N}$. Throughout this paper, we assume that every ring is unital. For a commutative ring A, we denote by $A^\times$ the group of units in A.

Let $T = (T_1, \dots, T_r)$ be an r-tuple of indeterminates. For a commutative ring A, we denote the formal power series ring $A[[T_1, \dots, T_r]]$ by $A[[T]]$. Let $f(T) = \sum_{i \in \mathbb{N}^n} a_i T^i \in A[[T]]$ be a formal power series and let $\tau : A \to A$ be an endomorphism of A. Here $i = (i_1, \dots, i_r) \in \mathbb{N}^r$, $T^i = T_1^{i_1} \cdots T_r^{i_r}$. Then we denote the series $\sum_{i \in \mathbb{N}^n} \tau(a_i) T^i$ by $\tau_* f(T)$. For an ideal $\mathfrak{a}$ of A, $n \in \mathbb{N}$ and power series $f(T)$, $g(T) \in A[[T]]$, $f \equiv g \pmod{\deg n}$ (resp. $f \equiv g \pmod{\deg n, \mathfrak{a}}$) means $f - g \in (T_1, \dots, T_r)^n$ (resp. $f - g \in (T_1, \dots, T_r)^n + \mathfrak{a}A[[T]]$).

For a commutative ring R, we denote by $M_{m,n}(R)$ (resp. $M_n(R)$) the ring of $m \times n$ matrices (resp. $n \times n$ matrices) with coefficients in R. For $a = (a_{ij}) \in M_{m,n}(R)$ and $k \in \mathbb{N}$, we denote the matrix (a_{ij}^k) by $a^{\langle k \rangle}$. For example, if $T = {}^t(T_1, \dots, T_r) \in K[[T]]^r$, then $T^{\langle k \rangle} = {}^t(T_1^k, \dots, T_r^k)$. Here ${}^t(-)$ means the transpose.

1

1.1 Higher dimensional functional equation lemma

Let $(X_\lambda)_{\lambda \in \Lambda}$ be a family of indeterinates. Unless otherwise specified, we extend the action of σ on K to $K[X_\lambda \mid \lambda \in \Lambda]$ (resp. $K[[X_\lambda \mid \lambda \in \Lambda]]$) so that $\sigma(X_\lambda) = X_\lambda^q$. If $R = K[X_{ij} \mid 1 \le i \le m,\ 1 \le j \le n]$ is the polynomial ring with indeterminates X_{ij} over K, then $\sigma^k(X) = (X_{ij}^{q^k})$ for $X = (X_{ij}) \in M_{m,n}(R)$, Let $T = {}^t(T_1, \dots, T_r)$ be an r-tuple of indeterminates.

Theorem 1.1.1 (higher dimensional functional equation lemma, Hazewinkel [Haz78, II, 10.1])**.** *Let K be a commutative ring, A a subring of K, p a prime number, q a power of p, $\mathfrak{a}$ an ideal of A, and $\sigma : K \to K$ an endomorphism of K. We assume the following.*

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

(2) $p \in \mathfrak{a}$.

(3) *For any* $r \in \mathbb{Z}_{\geq 1}$ *and* $b \in K$, *if* $\mathfrak{a}^r b \in \mathfrak{a}$, *then* $\mathfrak{a}^r \sigma(b) \in \mathfrak{a}$.

Let $n \in \mathbb{Z}_{>0}$ *and let* $(s_k)_{k=1}^{\infty}$ *be a sequence of matrices* $s_k(i,j) \in M_m(K)$ *such that* $\mathfrak{a} s_k(i,j) \subset M_m(A)$ *for any* $k \in \mathbb{Z}_{\geq 1}$. *For* a, $b \in M_{m,n}(K)$ *and an ideal* $\mathfrak{b}$, *we write* $a \equiv b \pmod{\mathfrak{b}}$ *if* $a - b \in \mathfrak{b} M_{m,n}(\mathcal{O})$. *Let* $X_1, \dots, X_n$ *be indeterminates and* $X = {}^t(X_1, \dots, X_n)$. *Here* ${}^t(-)$ *implies the transpose. Let* $g(X) = (g_i(X_1, \dots, X_n)) \in A[[X]]^m$ *be an* m*-tuple of power series such that* $g(0, \dots, 0) = 0$. *Then there exists uniquely* $f(X) = (f_i(X_1, \dots, X_n)) \in K[[X]]^m$ *such that*

$$f(X) = g(X) + \sum_{i=1}^{\infty} s_i \sigma_*^i f(X^{\langle q^i \rangle})$$

and $f(0, \dots, 0) = 0$. *We denote the above* $f(X)$ *by* $f_g(X)$.

For $f(X) = \sum_{r=(r_1,\dots,r_n) \in \mathbb{N}^n} b_r X^r \in K[[X]]^m$, we consider the following condition:

(1.1.1) if there exist $1 \leq i < j \leq n$ such that r_i, $r_j > 0$, then $b_r = 0$.

Lemma 1.1.2. *Let the notation and the assumption be as in Theorem 1.1.1.*

(1) *If* $f(X) \in K[[X]]^m$ *satisfies* (1.1.1), *then* $f(X)$ *can be written as*

$$f(X) = \sum_{i=0}^{\infty} a_i X^{\langle i \rangle}, \quad (a_i \in M_{m,n}(K)).$$

Here we regard X *as a column vector* ${}^t(X_1, \dots, X_n) \in K[[X]]^n$.

(2) *If* $g(X) \in A[[X]]^m$ *satisfies* (1.1.1), *then so is* $f_g(X)$.

Proof. Easy. □

Theorem 1.1.3 (higher dimensional functional equation lemma, Hazewinkel [Haz78, II, 10.2])**.** *Let* K, A, $\mathfrak{a}$, σ, p, q *be as in Theorem 1.1.1. Let* $n \in \mathbb{Z}_{>0}$ *and let* $(s_k)_{k=1}^{\infty}$ *be a sequence of matrices* $s_k(i,j) \in M_n(K)$ *such that* $\mathfrak{a} s_k(i,j) \subset M_n(A)$ *for any* $k \in \mathbb{Z}_{\geq 1}$. *Let* $g(X) = (g_i(X_1, \dots, X_n)) \in A[[X_1, \dots, X_n]]^n$ *(resp.* $\overline{g}(\overline{X}) = (\overline{g}_i(\overline{X}_1, \dots, \overline{X}_m)) \in A[[\overline{X}_1, \dots, \overline{X}_m]]^n$*) be a power series in* $X = (X_1, \dots, X_n)$ *(resp. a power series in* $\overline{X} = (\overline{X}_1, \dots, \overline{X}_m)$*) with coefficients in* A. *Supposet that* $g(X) \equiv 0 \pmod{\deg 1}$, $\overline{g}(\overline{X}) \equiv 0 \pmod{\deg 1}$ *and that the Jacobian matrix* $J(g) = \left(\dfrac{\partial g_i}{\partial X_j} \right) \Big|_{X=0}$ *of* g *is invertible in* $\in M_n(A)$. *Then we have the following.*

(1) $F(X,Y) = f_g^{-1}(f_g(X) + f_g(Y))$ *has its coefficients in* A.

(2) $f_g^{-1}(f_{\overline{g}}(\overline{X}_1, \dots, \overline{X}_n))$ *has its coefficients in* A.

(3) *If* $h(\overline{X}) \in A[[\overline{X}]]^n$ *is an* n*-tuple of power series in* $\overline{X}$ *such that* $h(\overline{X}) \equiv 0 \pmod{\deg 1}$, *then there exists* $\overline{h}(\overline{X}) \in A[[\overline{X}]]^n$ *such that* $f_g(h(\overline{X})) = f_{\overline{h}}(\overline{X})$.

(4) *If* $\alpha(Z) \in A[[Z_1, \dots, Z_l]]^n$, $\beta(Z) \in K[[Z_1, \dots, Z_l]]^n$, *then for all* $r = 1, 2, 3, \dots,$

$$\alpha(Z) \equiv \beta(Z) \pmod{\mathfrak{a}^r} \Leftrightarrow f_g(\alpha(Z)) \equiv f_g(\beta(Z)) \pmod{\mathfrak{a}^r}.$$

2 Higher dimensional Witt vectors

In this section, we define Witt functor with respect to a certain function, called of Witt type. The functor is a generalization of that defined in [Mat19].

2.1 q-typical series of Witt type and ghost polynomials

Let p a prime, q a power of p, $\mathcal{O}$ a discrete valuation ring, K the field of fractions of $\mathcal{O}$, $\mathcal{P}$ the valuation ideal, $\kappa = \mathcal{O}/\mathcal{P}$, and π a uniformizer of $\mathcal{O}$. We assume that κ is of characteristic p. Let σ be a ring endomorphism of K such that $\sigma(\mathcal{O}) \subset \mathcal{O}$, $\sigma(\pi)/\pi \in \mathcal{O}^\times$, and $\sigma(a) \equiv a^q \pmod{\pi\mathcal{O}}$ for any $a \in \mathcal{O}$.

Definition 2.1.1. Let $l(T) = \sum_{i=0}^{\infty} \gamma_i T^{\langle q^i \rangle} \in K[[T]]^r$ ($\gamma_i \in M_r(K)$) be an r-tuple of power series in $T = (T_1, \dots, T_r)$. We say $l(T)$ is *of Witt type* if the following conditions hold.

(L1) γ_0 is the identity matrix I of $M_r(\mathcal{O})$.

(L2) $\pi^n \gamma_n \in GL_r(\mathcal{O})$ for $n \in \mathbb{N}$.

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

Theorem 2.1.2. *Let s_i ($i = 1, 2, \dots$) be a sequence of matrices $s_i \in M_r(K)$ such that $\pi s_1 \in GL_r(\mathcal{O})$ and $\pi s_i \in M_r(\mathcal{O})$. Let*

$$l(T) = \sum_{i=0}^{\infty} \gamma_i T^{\langle q^i \rangle} \in K[[T]]^r, \quad (\gamma_i \in M_r(K))$$

be an r-tuple of power series in T that safisfies $\gamma_0 \in GL_r(\mathcal{O})$ and

$$l(T) - \sum_{i=1}^{\infty} s_i \sigma_*^i l(T^{\langle q^i \rangle}) \in \mathcal{O}[[T]]^r. \tag{2.1.1}$$

Then $l(T)$ satisfies the condition (L2) *and* (L3) *of Definition 2.1.1. In particular, if γ_0 is the identity matrix, then $l(T)$ is of Witt type.*

Proof. We prove (1) by induction on n. For $n = 0$, the assertion follows from the assumption. Let $n > 0$ and suppose that the assertion holds for $1, \dots, n-1$. Since $l(T)$ satisfies (2.1.1), we have

$$\gamma_n - \sum_{i=1}^{n} s_i \sigma^i(\gamma_{n-i}) \in M_r(\mathcal{O}) \tag{2.1.2}$$

and $\pi^n \gamma_n \equiv \sum_{i=1}^{n} \pi^n s_i \sigma^i(\gamma_{n-i}) \equiv \pi^n s_1 \sigma(\gamma_{n-1}) \pmod{\pi M_r(\mathcal{O})}$. By the assumption and the induction hypothesis, we have

$$\det(\pi^n s_1 \sigma(\gamma_{n-1})) = \det(\pi s_1) \det(\pi^{n-1}\sigma(\gamma_{n-1})) \in GL_r(\mathcal{O})$$

and the assertion holds for n.

Next we prove (2) by induction on n. By (2.1.2), we can write $\gamma_1 = s_1\sigma(\gamma_0) + c_1$, $\gamma_2 = s_1\sigma(\gamma_1) + s_2\sigma^2(\gamma_0) + c_2$ for some c_1, $c_2 \in M_r(\mathcal{O})$. Since $\gamma_i^{-1} \in \pi^i M_r(\mathcal{O})$ by (1), we have

$$s_1\big(\sigma(\gamma_0)\gamma_1^{-1} - \sigma(\gamma_1)\gamma_2^{-1}\big) = s_2\sigma^2(\gamma_0)\gamma_2^{-1} + c_2\gamma_2^{-1} - c_1\gamma_1^{-1} \in \pi M_r(\mathcal{O})$$

and hence $\sigma(\gamma_0)\gamma_1^{-1} - \sigma(\gamma_1)\gamma_2^{-1} \in \pi^2 M_r(\mathcal{O})$. Therefore $\sigma(\gamma_1^{-1}\gamma_0) - \gamma_2^{-1}\gamma_1 \in \pi^2 M_r(\mathcal{O})$ and the assertion for $n = 0$ holds. Let $n > 0$. By (2.1.2), we have

$$\gamma_{n+1}\sigma(\gamma_n^{-1}) \equiv \sum_{i=1}^{n+1} s_i \sigma^i(\gamma_{n+1-i})\sigma(\gamma_n^{-1}) \pmod{\pi^n}$$
$$\gamma_{n+2}\sigma(\gamma_{n+1}^{-1}) \equiv \sum_{i=1}^{n+2} s_i \sigma^i(\gamma_{n+2-i})\sigma(\gamma_{n+1}^{-1}) \pmod{\pi^{n+1}}.$$

Therefore

$$\begin{aligned}
&\gamma_{n+1}\sigma(\gamma_n^{-1}) - \gamma_{n+2}\sigma(\gamma_{n+1}^{-1}) \\
&\equiv \sum_{i=1}^{n+1} s_i \Big(\sigma^i(\gamma_{n+1-i})\sigma(\gamma_n^{-1}) - \sigma^i(\gamma_{n+2-i})\sigma(\gamma_{n+1}^{-1})\Big) \\
&\qquad - s_{n+2}\sigma^{n+2}(\gamma_0)\sigma(\gamma_{n+1}^{-1}) \pmod{\pi^n} \qquad (2.1.3) \\
&\equiv \sum_{i=2}^{n+1} s_i \Big(\sigma^i(\gamma_{n+1-i})\sigma(\gamma_n^{-1}) - \sigma^i(\gamma_{n+2-i})\sigma(\gamma_{n+1}^{-1})\Big) \pmod{\pi^n}
\end{aligned}$$

By the induction hypothesis, $\sigma(\gamma_{i+1}^{-1}\gamma_i) \equiv \gamma_{i+2}^{-1}\gamma_{i+1} \pmod{\pi^{i+2}}$ for $0 \le i \le n-1$. It follows that $\sigma^j(\gamma_{i+1}^{-1}\gamma_i) \equiv \sigma(\gamma_{i+j}^{-1}\gamma_{i+j-1}) \pmod{\pi^{i+2}}$ for i, j such that $0 \le i \le n-1$ and $1 \le j \le n+1-i$. This implies $\sigma^j(\gamma_i)\sigma(\gamma_{i+j-1}) \equiv \sigma^j(\gamma_{i+1})\sigma(\gamma_{i+j}^{-1}) \pmod{\pi^{i+j}}$. Considering the case where i is $n+1-i$ and j is i, we can see $\sigma^i(\gamma_{n+1-i})\sigma(\gamma_n^{-1}) \equiv \sigma^i(\gamma_{n+2-i})\sigma(\gamma_{n+1}^{-1}) \pmod{\pi^{n+1}}$ for $1 \le i \le n+1$. Then we have $\gamma_{n+1}\sigma(\gamma_n^{-1}) \equiv \gamma_{n+2}\sigma(\gamma_{n+1}^{-1}) \pmod{\pi^n}$ by (2.1.3) and hence, $\sigma(\gamma_{n+1}^{-1}\gamma_n) \equiv \gamma_{n+2}^{-1}\gamma_{n+1} \pmod{\pi^{n+2}}$. □

The converse also holds.

Theorem 2.1.3. *If $l(T)$ is of Witt type, then there exists a sequence $s_1, s_2, \dots$ of matrices $s_i \in M_r(K)$ such that $\pi s_1 \in GL_r(\mathcal{O})$, $\pi s_i \in M_r(\mathcal{O})$ for $i \ge 2$ and $l(T)$ satisfies*

$$l(T) - \sum_{i=1}^{\infty} s_i \sigma_*^i l(T^{\langle q^i \rangle}) \in \mathcal{O}[[T]]^r. \qquad (2.1.4)$$

Proof. It suffices to show that the existence of $s_1, s_2, \dots \in M_r(K)$ such that

$$\gamma_n - \sum_{i=1}^{n} s_i \sigma^i(\gamma_{n-i}) \in M_r(\mathcal{O}) \quad \text{for any } n \in \mathbb{N}.$$

We prove the existence of s_i by induction on i. For $i = 1$, $s_1 = \gamma_1$ satisfies the condition $\pi s_1 \in GL_r(\mathcal{O})$. Suppose that there exist $s_1, \dots, s_n \in K$ such that $\pi s_1 \in GL_r(\mathcal{O})$, $\pi s_i \in M_r(\mathcal{O})$ for $i \ge 2$ and $\gamma_n - \sum_{i=1}^{n} s_i \sigma^i(\gamma_{n-i}) \in M_r(\mathcal{O})$. We prove that there exists $s_{n+1} \in K$ such that $\pi s_{n+1} \in M_r(\mathcal{O})$ and $\gamma_{n+1} - \sum_{i=1}^{n+1} s_i \sigma^i(\gamma_{n-i}) \in M_r(\mathcal{O})$. By (L3), we have $\sigma^k(\gamma_{n+1-k}^{-1}\gamma_{n-k}) \equiv \gamma_{n+1}^{-1}\gamma_n \pmod{\pi^{n+2-k}}$ and hence

$$\gamma_n^{-1}\gamma_{n+1} \equiv \sigma^k(\gamma_{n-k}^{-1})\sigma^k(\gamma_{n+1-k}) \pmod{\pi^{n-k}}$$

for $1 \leq k \leq n$. Then we obtain

$$\gamma_{n+1} \equiv \gamma_n \sigma(\gamma_{n-1}^{-1})\sigma(\gamma_n) \pmod{\pi^{-1}}$$
$$\sigma^i(\gamma_{n+1-i}) \equiv \sigma^i(\gamma_{n-i})\sigma(\gamma_{n-1}^{-1})\sigma(\gamma_n) \pmod{\pi^0}$$

for $1 \leq i \leq n$. Therefore, by the induction hypothesis,

$$\begin{aligned}
&\gamma_{n+1} - \sum_{i=1}^{n} s_i \sigma^i(\gamma_{n+1-i}) \\
&\equiv \gamma_n \sigma(\gamma_{n-1}^{-1})\sigma(\gamma_n) - \sum_{i=1}^{n} s_i \sigma^i(\gamma_{n-i})\sigma(\gamma_{n-1}^{-1})\sigma(\gamma_n) \pmod{\pi^{-1}} \\
&\equiv \left(\gamma_n - \sum_{i=1}^{n} s_i \sigma^i(\gamma_{n-i})\right) \sigma(\gamma_{n-1}^{-1})\gamma_n \equiv 0 \pmod{\pi^{-1}}.
\end{aligned}$$

Thus, $s_{n+1} := \gamma_{n+1} - \sum_{i=1}^{n} s_i \sigma^i(\gamma_{n+1-i})$ satisfies the required condition. □

Corollary 2.1.4. *Let $X = (X_1, \dots, X_r)$, $Y = (Y_1, \dots, Y_r)$ be r-tuples of indeterminates. If $l(T) \in K[[T]]^r$ is of Witt type, then*

$$G(X, Y) := l^{-1}(l(X) + l(Y)) \in \mathcal{O}[[X, Y]]^r$$

and $G(X, Y)$ is an r-dimensional commutative formal group law over $\mathcal{O}$ [Haz78, II, 9.1].

Next, We define ghost polynomials for $l(T)$ of Witt type.

Definition 2.1.5. Let $(X_n)_{n\in\mathbb{N}}$ be a series of r-tuples of indeterminates $X_n = (X_{n,i})_{1\leq i\leq r}$. We also denote $(X_0, X_1, \dots)$ by $\underline{X}$. For a commutative ring R, we denote $R[X_{k,i} \mid 1 \leq k \leq n,\ 1 \leq i \leq r]$ by $R[X_1, \dots, X_n]$ and $R[X_{n,i} \mid n \in \mathbb{N},\ 1 \leq i \leq r]$ by $R[\underline{X}]$. For $n \in \mathbb{N}$, we define the *n-th ghost polynomial vector* $\phi_n(\underline{X}) = (\phi_{n,i}(\underline{X})) \in \mathcal{O}[\underline{X}]^r$ for $l(T)$ by

$$\phi_n(\underline{X}) = \sum_{i=0}^{n} \gamma_n^{-1}\gamma_{n-i} {X_i}^{q^{n-i}} = \sum_{i=0}^{n} \gamma_n^{-1}\gamma_{n-i} \begin{pmatrix} X_{i,1}^{q^{n-i}} \\ \vdots \\ X_{i,r}^{q^{n-i}} \end{pmatrix}.$$

We denote $(\phi_0(\underline{X}), \phi_1(\underline{X}), \dots)$ by $\underline{\phi}(\underline{X})$ or $\underline{\phi}$. Since $\phi_n(\underline{X}) \in \mathcal{O}[X_0, \dots, X_n]^r$, we often write $\phi_n(\underline{X})$ as $\phi_n(X_0, \dots, X_n)$.

We also define a matrix variant. Let R be a commutative ring. For $C = (c_{ij}) \in M_r(A)$ and $m \in \mathbb{Z}_{\geq 0}$, we denote (c_{ij}^m) by $C^{\langle m \rangle}$. For a sequence $\underline{c} = (c_{n,ij}) \in \prod_{n\in\mathbb{N}} M_r(A)$, we denote by $\underline{c}^{\langle q^i \rangle}$ the sequence $(c_1^{\langle q^i \rangle}, c_2^{\langle q^i \rangle}, \dots)$.

Definition 2.1.6. Let $\underline{X} = (X_n)_{n\in\mathbb{N}}$ be a series of r^2-tuple of indeterminates $X_n = (X_{n,i,j})$ $(1 \leq i, j \leq r)$. We regard X_n as an element of $M_r(\mathcal{O}[\underline{X}])$. For $l(T) \in K[[\underline{T}]]$ of Witt type, we define the *n-th ghost polynomial matrix* $\widetilde{\phi}_n(\underline{X}) = (\widetilde{\phi}_{n,i,j}(\underline{X})) \in M_r(\mathcal{O}[\underline{X}])$ for $l(T)$ by

$$\widetilde{\phi}_n(\underline{X}) = \sum_{k=0}^{n} \gamma_n^{-1}\gamma_{n-k} X_k^{\langle q^{n-k} \rangle} = \sum_{k=0}^{n} \gamma_n^{-1}\gamma_{n-k} \begin{pmatrix} X_{k,11}^{q^{n-k}} & \cdots & X_{k,1r}^{q^{n-k}} \\ \vdots & \ddots & \vdots \\ X_{k,r1}^{q^{n-k}} & \cdots & X_{k,rr}^{q^{n-k}} \end{pmatrix}.$$

As in Definition 2.1.5, we denote $(\widetilde{\phi}_0(\underline{X}), \widetilde{\phi}_1(\underline{X}), \dots)$ by $\underline{\widetilde{\phi}}(\underline{X})$ or $\underline{\widetilde{\phi}}$. Since $\widetilde{\phi}_n(\underline{X}) \in M_r(\mathcal{O}[X_0, \dots, X_n])$, we often write $\widetilde{\phi}_n(\underline{X})$ as $\widetilde{\phi}_n(X_0, \dots, X_n)$.

In the rest of this section, we fix a series $l(T) = \sum_{i=0}^{\infty} \gamma_i T^{q^i} \in \mathcal{O}[[T]]^r$ of Witt type (Definition 2.1.1) and denote the ghost polynomial vectors and matrices for $l(T)$ by ϕ, $\widetilde{\phi}$.

Lemma 2.1.7. *Let $X_n = {}^t(X_{n,1}, \dots, X_{n,r})$ (resp. $X_n = ((X_{n,ij})_{ij})_{n\in\mathbb{N}}$) and $\underline{X} = (X_n)_{n\in\mathbb{N}}$. Then, for $n \in \mathbb{N}$, $\phi_n(\underline{X}) \in \mathcal{O}[\underline{X}]^r$ (resp. $\widetilde{\phi}_n(\underline{X}) \in M_r(\mathcal{O}[\underline{X}])$) and the following hold.*

(1) $\phi_{n+1}(\underline{X}) = X_0^{q^{n+1}} + \gamma_{n+1}^{-1}\gamma_n \phi_n(X_1, \dots, X_{n+1})$
(resp. $\widetilde{\phi}_{n+1}(\underline{X}) = X_0^{\langle q^{n+1}\rangle} + \gamma_{n+1}^{-1}\gamma_n \phi_n(X_1, \dots, X_{n+1})$).

(2) $\phi_{n+1}(\underline{X}) \equiv \sigma_* \phi_n(\underline{X}^q) \pmod{\pi^{n+1}}$
(resp. $\widetilde{\phi}_{n+1}(\underline{X}) \equiv \sigma_* \widetilde{\phi}_n(\underline{X}^{\langle q\rangle}) \pmod{\pi^{n+1}}$).

Proof. We prove the vector version. The assertion for matrices can be proven in the same way. Since $\gamma_n^{-1}\gamma_{n-i} \in \pi^i M_r(\mathcal{O})$ by (L2), we have $\phi_n(\underline{X}) \in \mathcal{O}[\underline{X}]^r$. (1) is evident by the definition. We prove (2). By (L3), $\gamma_{i+1}^{-1}\sigma(\gamma_i) \equiv \gamma_{i+2}^{-1}\sigma(\gamma_{i+1}) \pmod{\pi^{i+2}\mathcal{O}}$ for $i \in \mathbb{N}$. Then we get $\gamma_{i+1}^{-1}\sigma(\gamma_i) \equiv \gamma_{n+1}^{-1}\sigma(\gamma_n) \pmod{\pi^{i+2}\mathcal{O}}$ for $i \le n$ by induction. Therefore $\sigma(\gamma_n^{-1})\sigma(\gamma_i) \equiv \gamma_{n+1}^{-1}\gamma_{i+1} \pmod{\pi^{n+1}\mathcal{O}}$. Since $\gamma_{n+1}^{-1}\gamma_0 \in \pi^{n+1} M_r(\mathcal{O})$ by (L2),

$$\begin{aligned}&\phi_{n+1}(\underline{X}) - \sigma_*\phi_n(\underline{X}^q)\\ &= \sum_{i=1}^{n} \left(\gamma_{n+1}^{-1}\gamma_{n+1-i} - \sigma\left(\gamma_n^{-1}\gamma_{n-i}\right)\right) X_i^{q^{n+1-i}} + \gamma_{n+1}^{-1}\gamma_0 X_{n+1} \equiv 0 \pmod{\pi^{n+1}}.\end{aligned}$$

□

Definition 2.1.8. Let A be a commutative $\mathcal{O}$-algebra. Then we define $\phi_A : \prod_{n\in\mathbb{N}} A^r \to \prod_{n\in\mathbb{N}} A^r$ so that, for $\underline{a} = (a_n)_n \in \prod_{n\in\mathbb{N}} A^r$, $\phi_A(\underline{a}) = (\phi_n(\underline{a}))_n$. We also define $\widetilde{\phi}_A : \prod_{n\in\mathbb{N}} M_r(A) \to \prod_{n\in\mathbb{N}} M_r(A)$ so that, for $\underline{a} = (a_n)_n \in \prod_{n\in\mathbb{N}} M_r(A)$, $\widetilde{\phi}_A(\underline{a}) = (\widetilde{\phi}_n(\underline{a}))_n$. We call ϕ_A and $\widetilde{\phi}_A$ the ghost maps for $l(T)$ on A. We often denote ϕ_A (resp. $\widetilde{\phi}_A$) by ϕ (resp. $\widetilde{\phi}$) for simplicity.

Lemma 2.1.9. *Let A be a commutative $\mathcal{O}$-algebra and $\sigma_A : A \to A$ a σ-semilinear ring endomorphism such that $\sigma_A(a) \equiv a^q \pmod{\pi}$ for any $a \in A$. Let $b = (b_i) \in A^r$ and $c = (c_{ij}) \in M_r(A)$.*

(1) *If $\sigma_A(b) \equiv b^q \pmod{\pi}$, then $\sigma_A(b^{q^k}) \equiv b^{q^{k+1}} \pmod{\pi^{k+1}}$ for $k \in \mathbb{N}$.*

(2) *If $\sigma_A(c) \equiv c^{\langle q\rangle} \pmod{\pi}$, then $\sigma_A(c^{\langle q^k\rangle}) \equiv c^{\langle q^{k+1}\rangle} \pmod{\pi^{k+1}}$ for $k \in \mathbb{N}$.*

(3) $\sigma_A(\phi_n(\underline{b})) \equiv \sigma_*\phi_n(\underline{b}^q) \pmod{\pi^{n+1}}$

(4) $\sigma_A(\widetilde{\phi}_n(\underline{c})) \equiv \sigma_*\widetilde{\phi}_n(\underline{c}^{\langle q\rangle}) \pmod{\pi^{n+1}}$.

Proof. It is easy to see that, if $\sigma_A(a) \equiv a^q \pmod{\pi}$ for $a \in A$, then $\sigma_A(a^{q^k}) \equiv a^{q^{k+1}} \pmod{\pi^{k+1}}$ for $k \in \mathbb{N}$. (1) and (2) follows immediately. Since we can prove (3) and (4) in the same way, we only show (4). By (2), we have $\sigma_A(c_i)^{\langle q^{n-i}\rangle} \equiv c_i^{\langle q^{n+1-i}\rangle} \pmod{\pi^{n+1-i}}$. Since $\sigma_A(\gamma_n^{-1}\gamma_{n-i}) \in \pi^i M_r(\mathcal{O})$,

$$\sigma_A(\phi_n(\underline{c})) = \sum_{i=0}^{n} \sigma_A(\gamma_n^{-1}\gamma_{n-i})\sigma_A(c_i)^{\langle q^{n-i}\rangle} \equiv \sum_{i=0}^{n} \sigma_A(\gamma_n^{-1}\gamma_{n-i})c_i^{\langle q^{n+1-i}\rangle}$$
$$\equiv \sum_{i=0}^{n} \sigma_A(\gamma_n^{-1}\gamma_{n-i})(c_i^{\langle q\rangle})^{\langle q^{n-i}\rangle} \equiv \sigma_* \phi_n(\underline{c}^{\langle q\rangle}) \pmod{\pi^{n+1}}.$$

□

2.2 Witt functors

Proposition 2.2.1. *Let A be a commutative $\mathcal{O}$-algebra.*

(1) *If π is a non zero-divisor in A, then ϕ_A and $\widetilde{\phi}_A$ are injective.*

(2) *If π is invertible in A, then ϕ_A and $\widetilde{\phi}_A$ are bijective.*

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

$$(u_n)_n \in \phi_A\left(\prod_{n\in\mathbb{N}} A^r\right) \Leftrightarrow \sigma_A(u_n) \equiv u_{n+1} \pmod{\pi^{n+1}}$$
$$\left(\text{resp. } (u_n)_n \in \widetilde{\phi}_A\left(\prod_{n\in\mathbb{N}} M_r(A)\right) \Leftrightarrow \sigma_A(u_n) \equiv u_{n+1} \pmod{\pi^{n+1}}\right)$$

Proof. (1) Since $\pi^n\gamma_n \in GL_r(\mathcal{O})$ by (L2) of Definition 2.1.1, if π is a non zero-divisor in A, then, for $a \in A^r$, $\gamma_n^{-1}a = (\pi^n\gamma_n)^{-1}\pi^n a = 0$ implies $a = 0$. Hence the injectivity of ϕ_A is evident. We can prove (2) in a similar way. We prove (3) for the case of matrices. The case of vectors can be proven in the same way. Assume that $\underline{u} = (u_n)_n = \phi_A(\underline{a})$ for $\underline{a} = (a_n)_n \in \prod_{n\in\mathbb{N}} M_r(A)$. By Lemma 2.1.7 and Lemma 2.1.9, $\phi_{n+1}(\underline{a}) \equiv \sigma_*\phi_n(\underline{a}^{\langle q\rangle}) \equiv \sigma_A(\phi_n(\underline{a})) \pmod{\pi^{n+1}}$. Therefore, $\sigma_A(u_n) - u_{n+1} = \sigma_A(\phi_n(\underline{a})) - \phi_{n+1}(\underline{a}) \equiv 0 \pmod{\pi^{n+1}}$.

We show the converse by induction on n. Assume that $\sigma_A(u_n) \equiv u_{n+1} \pmod{\pi^{n+1}}$ for any $n \in \mathbb{N}$. It is evident that there exists $a_0 \in M_r(A)$ such that $\phi_0(a_0) = u_0$. Suppose that there exist $a_0, \ldots, a_n \in M_r(A)$ such that $u_i = \phi_i(a_0, \ldots, a_i)$ for $0 \le i \le n$. It suffices to show that there exists $a_{n+1} \in M_r(A)$ such that $\gamma_{n+1}^{-1}a_{n+1} = u_{n+1} - \sum_{i=0}^{n} \gamma_{n+1}^{-1}\gamma_{n+1-i}a_i^{\langle q^{n+1-i}\rangle}$. By the same argument as in the proof of Lemma 2.1.9, we obtain

$$\sum_{i=0}^{n} \gamma_{n+1}^{-1}\gamma_{n+1-i}a_i^{\langle q^{n+1-i}\rangle} \equiv \sigma(\widetilde{\phi}_n(a_0, \ldots, a_n)) \pmod{\pi^{n+1}}$$

and hence

$$u_{n+1} - \sum_{i=0}^{n} \gamma_{n+1}^{-1}\gamma_{n+1-i}a_i^{\langle n+1-i\rangle} \equiv u_{n+1} - \sigma(\widetilde{\phi}_n(a_0,\dots,a_n))$$
$$\equiv u_{n+1} - \sigma(u_n) \equiv 0 \pmod{\pi^{n+1}}.$$

Therefore $\gamma_{n+1}(u_{n+1} - \sum_{i=0}^{n} \gamma_{n+1}^{-1}\gamma_{n+1-i}a_i^{\langle n+1-i\rangle}) \in M_r(A)$ and it satisfies the condition for a_{n+1}. □

Theorem 2.2.2. *Let $X_{n,i}$, $Y_{n,i}$ ($n \in \mathbb{N}$, $1 \leq i \leq r$) be families of indeterminates. We write $X_n = {}^t(X_1,\dots,X_r)$, $Y_n = {}^t(Y_1,\dots,Y_r)$, $\underline{X} = (X_n)_{n\in\mathbb{N}}$ and $\underline{Y} = (Y_n)_{n\in\mathbb{N}}$. Then there exist sequences of r-tuples $\underline{S} = (S_n(\underline{X},\underline{Y}))_n$, $\underline{P} = (P_n(\underline{X},\underline{Y}))_n$ and $\underline{I}(\underline{X}) = (I_n(\underline{X}))$ whose components are polynomials 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 $S_n(\underline{X},\underline{Y})$, $P_n(\underline{X},\underline{Y}) \in \mathcal{O}[X_0,\dots,X_n,Y_0,\dots,Y_n]^r$, and $I_n(\underline{X}) \in \mathcal{O}[X_0,\dots,X_n]^r$. There also exists uniquely a sequence of vectors $\underline{C}(x) = (C_n(x))_n$ for each $x \in \mathcal{O}$ such that

(4) $\phi(\underline{C}(x)) = \left({}^t(\sigma^n(x),\dots,\sigma^n(x))\right)_n \in \prod_{n\in\mathbb{N}} \mathcal{O}^r$.

Proof. Let $A = \mathcal{O}[\underline{X},\underline{Y}]$ and define the σ-semilinear endomorphism σ_A of $\mathcal{O}$-algebra A so that $\sigma_A(X_{n,i}) = X_{n,i}^q$, $\sigma_A(Y_{n,i}) = Y_{n,i}^q$. Let $u_n = \phi_n(\underline{X}) + \phi_n(\underline{Y}) \in \prod_{n\in\mathbb{N}} A^r$ for $n \in \mathbb{N}$. Then they clearly satisfy $\sigma_A(u_n) \equiv u_{n+1} \pmod{\pi^{n+1}}$. Hence the exisitence and uniqueness of $\underline{S}$ follows from Proposition 2.2.1. We can show the existence and uniqueness of $\underline{P}$, $\underline{I}$ and $\underline{C}$ in the same way. □

Definition 2.2.3. Let A be a commutative $\mathcal{O}$-algebra and let $W(A)$ be $\prod_{n\in\mathbb{N}} A^r$ 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 ring with these operations and $\phi_A : W(A) \to \prod_{n\in\mathbb{N}} A^r$ is a ring homomorphism. Here we regard $\prod_{n\in\mathbb{N}} A^r$ as a ring product of A^r. For $x \in \mathcal{O}$, we define $C(x) \in W(\mathcal{O})$ by $\underline{C}(x)$. Since σ is a ring homomorphism, C defines a ring homomorphism $\mathcal{O} \to W(\mathcal{O})$ and we can regard $W(\mathcal{O})$ as an $\mathcal{O}$-algebra. For a commutative $\mathcal{O}$-algebra A, we often identify $C(x)$ with the image by the natural homomorphism $W(\mathcal{O}) \to W(A)$. Then C defines a ring homomorphism $\mathcal{O} \to W(A)$ and we can regard $W(A)$ as an $\mathcal{O}$-algebra. For $\underline{a} \in W(A)$, we call the components of $\phi_A(\underline{a})$ the *ghost components* of $\underline{a}$.

Let ($\mathsf{com}\mathcal{O}$-Alg) be the category of commutative $\mathcal{O}$-algebras. We can regard W as a functor from ($\mathsf{com}\mathcal{O}$-Alg) to ($\mathsf{com}\mathcal{O}$-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 $S^* : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X},\underline{Y}]$ such that $S^*(X_n) = S_n(\underline{X},\underline{Y})$. We omit the detail for the structure of multiplication etc. We denote by $\phi^* : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ the $\mathcal{O}$-endomorphism such that $\phi^*(X_n) = \phi_n(\underline{X})$. Then ϕ^* induces a morphism of functors $\phi_A : W(A) \to \prod_{n\in\mathbb{N}} A^r$ on A.

Definition 2.2.4. We call the functor $W : (\mathsf{com}\mathcal{O}\text{-}\mathsf{Alg}) \to (\mathsf{com}\mathcal{O}\text{-}\mathsf{Alg})$ defined above the *Witt functor for* $l(T)$.

Let A be a commutative $\mathcal{O}$-algebra. For $n \in \mathbb{N}$, we denote by $A^{(\sigma^n)}$ the $\mathcal{O}$-algebra A with the structure map $\mathcal{O} \xrightarrow{\sigma^n} \mathcal{O} \to A$. Then $\phi_A : W(A) \to \prod_{n\in\mathbb{N}} A^{(\sigma^n)^r}; \underline{a} \mapsto \phi_A(\underline{a})$ is $\mathcal{O}$-linear. Let $P(T) \in \mathcal{O}[T]$ be a polynomial. Since $W(A)$ is an $\mathcal{O}$-algebra, we can regard $P(T)$ as the map $P : W(A) \to W(A)$ that sends $\underline{a} \in W(A)$ to $P(\underline{a}) \in W(A)$. Then by Theorem 2.2.2 the following diagram is commutative

$$\begin{array}{ccc} W(A) & \xrightarrow{\phi_A} & \prod_{n\in\mathbb{N}} A^{(\sigma^n)^r} \\ {\scriptstyle P}\downarrow & & \downarrow{\scriptstyle P} \\ W(A) & \xrightarrow{\phi_A} & \prod_{n\in\mathbb{N}} A^{(\sigma^n)^r}. \end{array}$$

Remark 2.2.5. Let $(\sigma^n_* P)_n : \prod_{n\in\mathbb{N}} A^r \to \prod_{n\in\mathbb{N}} A^r$ be the map which sends $(x_n)_n$ to $(\sigma^n_* P(x_n))_n$. Then the commutativity of the above diagram means that the following diagram is commutative

$$\begin{array}{ccc} W(A) & \xrightarrow{\phi} & \prod_{n\in\mathbb{N}} A^r \\ {\scriptstyle P}\downarrow & & \downarrow{\scriptstyle (\sigma^n_* P)_n} \\ W(A) & \xrightarrow{\phi} & \prod_{n\in\mathbb{N}} A^r. \end{array}$$

We also have matrix variants of a Witt functor. Let $X_{n,i,j}, Y_{n,i,j}$ $(n \in \mathbb{N}, 1 \leq i, j \leq r)$ be families of indeterminates. We write $X_n = \begin{pmatrix} X_{n,1,1} & \cdots & X_{n,1,r} \\ \vdots & \ddots & \vdots \\ X_{n,r,1} & \cdots & Y_{n,r,r} \end{pmatrix}$ and $Y_n = \begin{pmatrix} Y_{n,1,1} & \cdots & Y_{n,1,r} \\ \vdots & \ddots & \vdots \\ Y_{n,r,1} & \cdots & Y_{n,r,r} \end{pmatrix}$, $\underline{X} = (X_n)_n$, $\underline{Y} = (Y_n)$. Replacing ϕ by $\widetilde{\phi}$ in Theorem 2.2.2, we obtain series of matrices of polynomials $\underline{\widetilde{S}} = (\widetilde{S}_n(\underline{X}, \underline{Y}))$, $\underline{\widetilde{P}} = (\widetilde{P}_n(\underline{X}, \underline{Y})) \in \mathcal{O}[\underline{X}, \underline{Y}]$ and $\underline{\widetilde{I}} = (\widetilde{I}_n(\underline{X})) \in \mathcal{O}[\underline{X}]$ such that

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

(2) $\widetilde{\phi}_n(\underline{\widetilde{P}}) = \widetilde{\phi}_n(\underline{X})\widetilde{\phi}_n(\underline{Y})$ (matrix multiplication),

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

for $n \in \mathbb{N}$. For a commutative $\mathcal{O}$-algebra A, we define $\widetilde{W}(A) = \prod_{n\in\mathbb{N}} M_r(A)$ as a set. Using the polynomials above, we can equip $\widetilde{W}(A)$ with a ring structure so that the map

$$\begin{array}{ccc} \widetilde{W}(A) & \xrightarrow{\widetilde{\phi}_A} & \prod_{n\in\mathbb{N}} M_r(A) \\ \cup & & \cup \\ \underline{a} = (a_n) & \longmapsto & (\widetilde{\phi}_n(\underline{a})) \end{array}$$

is a ring homomorphism. Let $(\mathcal{O}\text{-}\mathsf{Alg})$ be the category of the $\mathcal{O}$-algebras. From the construction above, we obtain the functor $\widetilde{W} : (\mathsf{com}\mathcal{O}\text{-}\mathsf{Alg}) \to (\mathcal{O}\text{-}\mathsf{Alg})$.

Moreover, for each $x \in \mathcal{O}$, there exists uniquely a sequence of square matrices $\underline{C}(x) = (C_n(x))_n$ such that

(4) $\widetilde{\phi}(\underline{C}(x)) = (\sigma^n(x)I_r)_n$.

Then C defines a ring homomorphism $\mathcal{O} \to \widetilde{W}(A)$ and we can regard $\widetilde{W}(A)$ as an $\mathcal{O}$-algebra in a similar way as in the case of $W(A)$.

Lemma 2.2.6. *Let $Y_{n,i,j}$, $X_{n,i}$ $(n \in \mathbb{N},\ 1 \le i, j \le r)$ be families of indeterminates. We write $Y_n = \begin{pmatrix} Y_{n,1,1} & \cdots & Y_{n,1,r} \\ \vdots & \ddots & \vdots \\ Y_{n,r,1} & \cdots & Y_{n,r,r} \end{pmatrix}$, $X_n = \begin{pmatrix} X_{n,1} \\ \vdots \\ X_{n,r} \end{pmatrix}$, $\underline{Y} = (Y_n)_{n\in\mathbb{N}}$ and $\underline{X} = (X_n)_{n\in\mathbb{N}}$. Then there exists uniquely a seqence of r-tuples $\underline{Q}(\underline{Y}, \underline{X}) = (Q_n(\underline{Y}, \underline{X}))_n = ((Q_{n,i}(\underline{Y}, \underline{X}))_i)_n$ whose components $Q_{n,i}$ $(n \in \mathbb{N},\ 1 \le i \le r)$ are polynomials with coefficients in $\mathcal{O}$ such that $\phi(\underline{Q}) = \widetilde{\phi}(\underline{Y})\phi(\underline{X})$ in $M_r(\mathcal{O}[\underline{Y}, \underline{X}])$.*

Proof. Let $A = \mathcal{O}[\underline{Y}, \underline{X}]$ and define the σ-semilinear endomorphism σ_A of $\mathcal{O}$-algebra A so that $\sigma_A(Y_{n,i,j}) = Y^q_{n,i,j}$, $\sigma_A(X_{n,i}) = X^q_{n,i}$. Let $u_n = \widetilde{\phi}_n(\underline{Y})\phi_n(\underline{X}) \in \prod_{n\in\mathbb{N}} A^r$ for $n \in \mathbb{N}$. By Lemma 2.1.9, $\sigma_A(\phi_n(\underline{Y})) \equiv \phi_{n+1}(\underline{Y}) \pmod{\pi^{n+1}}$ in $M_r(A)$ and $\sigma_A(\phi_n(\underline{X})) \equiv \phi_{n+1}(\underline{X}) \pmod{\pi^{n+1}}$ in A^r and hence $\sigma_A(u_n) \equiv u_{n+1} \pmod{\pi^{n+1}}$ for $n \in \mathbb{N}$. Therefore the exisitence and uniqueness of $\underline{Q}$ follows from Proposition 2.2.1. □

Definition 2.2.7. Let $\underline{Y}$ and $\underline{X}$ be as in Lemma 2.2.6. We define $\mathcal{O}$-endomorphisms $\widetilde{\phi}^* : \mathcal{O}[\underline{Y}] \to \mathcal{O}[\underline{Y}]$ and $\phi^* : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ so that $\widetilde{\phi}^*(Y_{n,i,j}) = \widetilde{\phi}_{n,i,j}(\underline{Y})$ and $\widetilde{\phi}^*(X_n) = \phi_{n,i}(\underline{X})$. Let $Q_n(\underline{Y}, \underline{X})$ $(n \in \mathbb{N})$ be as in Lemma 2.2.6. We identify $\mathcal{O}[\underline{Y}] \otimes_{\mathcal{O}} \mathcal{O}[\underline{X}]$ with $\mathcal{O}[\underline{Y}, \underline{X}]$ and define an $\mathcal{O}$-algebra homomorphism $G^* : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{Y}, \underline{X}]$ so that $G^*(X_n) = Q_n(\underline{Y}, \underline{X})$. Let $g^* : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{Y}, \underline{X}]$ be an $\mathcal{O}$-endomorphism defined by $g^*(X_n) = \sum_{k=1}^r Y_{n,i,k}X_{n,k}$. By the defintion of Q_n, the following diagram is commutative

$$\begin{array}{ccc} \mathcal{O}[\underline{Y}] \otimes_{\mathcal{O}} \mathcal{O}[\underline{X}] & \xleftarrow{\widetilde{\phi}^* \otimes \phi^*} & \mathcal{O}[\underline{Y}] \otimes_{\mathcal{O}} \mathcal{O}[\underline{X}] \\ {\scriptstyle G^*}\uparrow & & \uparrow{\scriptstyle g^*} \\ \mathcal{O}[\underline{X}] & \xleftarrow[\phi^*]{} & \mathcal{O}[\underline{X}]. \end{array}$$

Then, for a commutative $\mathcal{O}$-algebra A, the above diagram induces the following commutative diagram.

$$\begin{array}{ccc} \widetilde{W}(A) \times W(A) & \xrightarrow{\widetilde{\phi}_A \times \phi_A} & \prod_{n\in\mathbb{N}} M_r(A) \times \prod_{n\in\mathbb{N}} A^r \\ {\scriptstyle G_A}\downarrow & & \downarrow{\scriptstyle g_A} \\ W(A) & \xrightarrow{\phi_A} & \prod_{n\in\mathbb{N}} A^r. \end{array}$$

Thus we have an action G_A of $\widetilde{W}(A)$ on $W(A)$, which is functorial on A.

Example 2.2.8. Let $K = \mathbb{F}_q(\theta)$ be a rational function field over a finite field $\mathbb{F}_q$ of order q, $\nu : K \to \mathbb{Z} \cup \{\infty\}$ be the normalized θ-adic discrete valuation, $\mathcal{O} = \mathbb{F}_q[\theta]_{(\theta)}$ the valuation ring. We denote $[i] = \theta^{q^i} - \theta$ for $i \in \mathbb{N}$

and define $L_0 = 1$, $L_i = [i][i-1]\cdots[1]$ for $i \geq 1$. Let $T = \begin{pmatrix} T_1 \\ T_2 \end{pmatrix}$ and $l(T) = \sum_{i=0}^{\infty} \frac{(-1)^i}{L_i} \begin{pmatrix} 1 & -i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} T_1 \\ T_2 \end{pmatrix}$. Then $l(T)$ satisfies the following functional equation.

$$l\begin{pmatrix} T_1 \\ T_2 \end{pmatrix} - \begin{pmatrix} \theta & \theta \\ 0 & \theta \end{pmatrix}^{-1} l\begin{pmatrix} T_1^q \\ T_2^2 \end{pmatrix} = \begin{pmatrix} \theta & \theta \\ 0 & \theta \end{pmatrix}^{-1} l\left(\begin{pmatrix} \theta & \theta \\ 0 & \theta \end{pmatrix}\begin{pmatrix} T_1 \\ T_2 \end{pmatrix}\right) \in \mathcal{O}[[T]].$$

The n-th ghost polynomial of $l(T)$ is $\phi_n(\underline{X}) = \sum_{i=0}^{n} \frac{(-1)^i L_n}{L_{n-i}} \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} X_i^{q^n}$.

2.3 Frobenius, Verschiebung and Teichmüller lift

Lemma 2.3.1. *Let $X_{n,i}$ $(n \in \mathbb{N},\ 1 \leq i \leq r)$ be a family of indeterminates. We denote $X_n = {}^t(X_{n,1}, \ldots, X_{n,r})$ and $\underline{X} = (X_n)_{n\in\mathbb{N}}$. Let $f^* : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be an $\mathcal{O}$-endomorphism defined by $f^*(X_n) = X_{n+1}$, i.e., $f^*(X_{n,i}) = X_{n+1,i}$ for $n \in \mathbb{N}$, $1 \leq i \leq r$. Then there exists a unique $\mathcal{O}$-homomorphism $F^* : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ such that $F^* \circ \phi^* = \phi^* \circ f^*$.*

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

Proof. The map F^* is determined by the images $F_n(\underline{X}) \in \mathcal{O}[\underline{X}]^r$ of X_n $(n \in \mathbb{N})$, so it suffices to show that there exists a series of r-tuples $(F_n(\underline{X}))_n$ such that $\phi_n((F_n(\underline{X}))_n)$ is equal to $\phi^*(f^*(X_n)) = \phi_{n+1}(\underline{X})$. Let $\sigma : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be an $\mathcal{O}$-endomorphism such that $\sigma(X_n(j)) = X_n(j)^q$. By Lemma 2.1.7, $\sigma(\phi_{n+1}(\underline{X})) = \sigma_*\phi_{n+1}(\underline{X}^{\langle q \rangle}) \equiv \phi_{n+2}(\underline{X}) \pmod{\pi^{n+2}}$ and hence the assertion follows from Proposition 2.2.1. □

Lemma 2.3.2. *Let $Y_{n,i,j}$ $(n \in \mathbb{N},\ 1 \leq i,j \leq r)$ be a family of indeterminates. We denote $Y_n = \begin{pmatrix} Y_{n,1,1} & \cdots & Y_{n,1,r} \\ \vdots & \ddots & \vdots \\ Y_{n,r,1} & \cdots & Y_{n,r,r} \end{pmatrix}$ and $\underline{Y} = (Y_n)_{n\in\mathbb{N}}$. Let $f^* : \mathcal{O}[\underline{Y}] \to \mathcal{O}[\underline{Y}]$ be an $\mathcal{O}$-endomorphism defined by $f^*(Y_n) = Y_{n+1}$, i.e., $f^*(Y_{n,i,j}) = Y_{n+1,i,j}$ for $n \in \mathbb{N}$, $1 \leq i,j \leq r$. Then there exists a unique $\mathcal{O}$-homomorphism $F^* : \mathcal{O}[\underline{Y}] \to \mathcal{O}[\underline{Y}]$ such that $F^* \circ \widetilde{\phi}^* = \widetilde{\phi}^* \circ f^*$.*

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

Proof. We can prove the lemma in the same way as Lemma 2.3.1 □

Definition 2.3.3. From F^* in Lemma 2.3.1 (resp. Lemma 2.3.2), we obtain a morphism of functors $F : W \to W$ (resp. $F : \widetilde{W} \to \widetilde{W}$) such that, for any object A in ($\mathcal{O}$-Alg), the following diagrams are commutative.

$$\begin{array}{ccc} W(A) & \xrightarrow{\phi_A} & \prod_{n\in\mathbb{N}} A^r \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle f} \\ W(A) & \xrightarrow{\phi_A} & \prod_{n\in\mathbb{N}} A^r \end{array} \qquad \left(\text{resp.} \quad \begin{array}{ccc} \widetilde{W}(A) & \xrightarrow{\widetilde{\phi}_A} & \prod_{n\in\mathbb{N}} M_r(A) \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle f} \\ \widetilde{W}(A) & \xrightarrow{\widetilde{\phi}_A} & \prod_{n\in\mathbb{N}} M_r(A) \end{array} \right)$$

Here $f : \prod_{n\in\mathbb{N}} A^r \to \prod_{n\in\mathbb{N}} A^r$ or $f : \prod_{n\in\mathbb{N}} M_r(A) \to \prod_{n\in\mathbb{N}} M_r(A)$ is the map which sends $(a_i)_i$ to $(a_{i+1})_i$. $F : W(A) \to W(A)$ is a ring homomorphism because so is f. We call F a *Frobenius* of W or $\widetilde{W}$. 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 2.3.1, 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 $F_n(\underline{X}) \in \mathcal{O}[X_0, \dots, X_{n+1}]^r$. Moreover, F is σ-semilinear, i.e., for any $x \in \mathcal{O}$ and $\underline{a} \in W(A)$, $F(x\underline{a}) = \sigma(x)F(\underline{a})$. For the proof, we can reduce to the case that $A = \mathcal{O}[\underline{X}]$ and $\underline{a} = \underline{X}$. Since $\phi(\sigma(x)F(\underline{X})) = (\sigma^n(\sigma(x))f^*(\phi(\underline{X})))_n = (\sigma^{n+1}(x)\phi_{n+1}(\underline{X}))_n = f^*((\sigma^n(x)\phi_n(\underline{X})_n) = \phi(F(x\underline{X}))$, the assertion follows.

Lemma 2.3.4. *Let $\underline{X}$ be as in Lemma 2.3.1. Let $v_n(\underline{X}) = \gamma_n^{-1}\gamma_{n-1}X_{n-1} \in \mathcal{O}[\underline{X}]^r$ and let $v^* : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be an endomorphism of $\mathcal{O}$-algebras such that $v^*(X_n) = v_n(\underline{X})$. Let $V^* : \mathcal{O}[\underline{X}] \to \mathcal{O}[\underline{X}]$ be an $\mathcal{O}$-endomorphism 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. We have $V^*\phi^* = \phi^*v^*$ from the calculation below.

$$\begin{aligned} V^*(\phi^*(X_n)) &= V^*(\phi_n(\underline{X})) = \phi_n(0, X_0, X_1, \dots) = \sum_{i=1}^{n} \gamma_n^{-1}\gamma_{n-i}X_{i-1}^{\langle q^{n-i}\rangle} \\ &= \sum_{i=0}^{n-1} \gamma_n^{-1}\gamma_{n-1-i}X_{i-1}^{\langle q^{n-1-i}\rangle} = \gamma_n^{-1}\gamma_{n-1}\sum_{i=0}^{n-1} \gamma_{n-1}^{-1}\gamma_{n-1-i}X_{i-1}^{\langle q^{n-1-i}\rangle} \\ &= \gamma_n^{-1}\gamma_{n-1}\phi_{n-1}(\underline{X}) = \phi^*(\gamma_n^{-1}\gamma_{n-1}X_{n-1}) = \phi^*(v^*(X_n)), \end{aligned}$$

□

Definition 2.3.5. From V^* in Lemma 2.3.4, we obtain a morphism of functors $V : W \to W$ such that for any object A in ($\mathcal{O}$-Alg), the following diagram is commutative.

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

Here $v((a_n)_n) = ((\gamma_n^{-1}\gamma_{n-1})a_{n-1})_n$ (we define $a_{-1} = 0$). We call V a *Verschiebung*. For any object A in $(\mathcal{O}\text{-}\mathsf{Alg})$, $V : W(A) \to W(A)$ is an endomomorphism 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 $\underline{a} \in W(A)$.

Definition 2.3.6. We define a Verschiebung $V : \widetilde{W} \to \widetilde{W}$ in the same way as in Definition 2.3.5. Then for a commutative $\mathcal{O}$-algebra A and $\underline{a} = (a_0, a_1, \dots) \in \widetilde{W}(A)$, $V(a_0, a_1, \dots) = (0, a_0, a_1, \dots)$. If we define $v : \prod_{n\in\mathbb{N}} M_r(A) \to \prod_{n\in\mathbb{N}} M_r(A)$ so that $v(u_0, u_1, \dots) = v(\gamma_1^{-1}u_0, \gamma_2^{-1}\gamma_1 u_1, \gamma_3^{-1}\gamma_2 u_2, \dots)$, then the following diagram is commutative.

$$\begin{array}{ccc} \widetilde{W}(A) & \xrightarrow{\widetilde{\phi}_A} & \prod_{n\in\mathbb{N}} M_r(A) \\ {\scriptstyle V}\downarrow & & \downarrow{\scriptstyle v} \\ \widetilde{W}(A) & \xrightarrow{\widetilde{\phi}_A} & \prod_{n\in\mathbb{N}} M_r(A) \end{array}$$

Definition 2.3.7. Let A be a commutative $\mathcal{O}$-algebra. We define a *Teichmüller lift* $\tau : A^r \to W(A)$ (resp. $\tau : M_r(A) \to \widetilde{W}(A)$) by $\tau(a) = (a, 0, \dots)$. It is evidently a morphism of functors from $(\mathsf{com}\mathcal{O}\text{-}\mathsf{Alg})$ to $(\mathsf{com}\mathcal{O}\text{-}\mathsf{Alg})$ (resp. $(\mathsf{com}\mathcal{O}\text{-}\mathsf{Alg})$ to $(\mathcal{O}\text{-}\mathsf{Alg})$).

Remark 2.3.8. When $r = 1$, for $\underline{a} = (a_n)_n$ and $\underline{b} = (b_0, 0, 0, \dots) \in W(A)$, $\underline{ab} = (a_n b_0^{q^n})_n$, but it is not for $r > 1$. For example, consider the case of Example 2.2.8. Let $\underline{a} = \left(\begin{pmatrix} a_{01} \\ a_{02} \end{pmatrix}, \begin{pmatrix} a_{11} \\ a_{12} \end{pmatrix}, \dots\right)$ and $\underline{b} = \left(\begin{pmatrix} b_{01} \\ b_{02} \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \dots\right)$. Then $\underline{ab} = \left(\begin{pmatrix} a_{01}b_{01} \\ a_{02}b_{02} \end{pmatrix}, \begin{pmatrix} a_{11}b_{01}^q + a_{12}b_{01}^q - a_{12}b_{02}^q \\ a_{12}b_{02}^q \end{pmatrix}, \dots\right)$.

Definition 2.3.9. We define $\underline{\mu} = (0, I_r, 0, \dots) \in \widetilde{W}(\mathcal{O})$, where I_r is the identity matrix of degree r. Then it is easy to see that $\widetilde{\phi}(\underline{\mu}) = (0, \gamma_1^{-1}\gamma_0, \gamma_2^{-1}\gamma_1, \dots) \in \prod_{n\in\mathbb{N}} M_r(\mathcal{O})$.

For a commutative $\mathcal{O}$-algebra, we regard $\underline{\mu}$ as an element of $W(A)$ or $\widetilde{W}(A)$ via $W(\mathcal{O}) \to W(A)$ or $\widetilde{W}(\mathcal{O}) \to \widetilde{W}(A)$.

Lemma 2.3.10. *Let A be a commutative $\mathcal{O}$-algebra. As a map from $W(A)$ to $W(A)$ or $\widetilde{W}(A) \to \widetilde{W}(A)$, we have the following.*

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

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

Here we regard $\underline{\mu}$ and $F(\underline{\mu})$ as left multiplication endomorphisms via G (Definition 2.2.7).

Proof. We prove the statements for $W(A)$. It suffices to show the corresponding equalities for ghost components. For any commutative $\mathcal{O}$-algebra A and $\underline{a} \in \prod_{n\in\mathbb{N}} A^r$, we have $\phi(VF(\underline{a})) = vf(\phi(\underline{a})) = (0, \gamma_1^{-1}\phi_1(\underline{a}), \gamma_2^{-1}\gamma_1\phi_2(\underline{a}), \dots) = \widetilde{\phi}(\underline{\mu})\phi(\underline{a})$. Thus we obtain (1). Similarly $fv(\phi(\underline{a})) = (\gamma_1^{-1}\phi_0(\underline{a})), \gamma_2^{-1}\gamma_1\phi_1(\underline{a}, \dots) = f(\widetilde{\phi}(\underline{\mu}))\phi(\underline{a}) = \widetilde{\phi}(F(\underline{\mu}))\phi(\underline{a})$ proves (2). We can show the statements for $\widetilde{W}(A)$ in the same way. □

3 Artin-Hasse exponentials

3.1 Series in formal groups

Let R be a commutative ring. Let $X = (X_1, \dots, X_r)$ and $Y = (Y_1, \dots, Y_r)$ be r-tuples of indeterminates and $G(X, Y) = (G_i(X, Y)) \in R[[X, Y]]$ a r-dimensional formal group law over R ([Haz78, 9.1]). If A is a commutative R-algebra, $I \subset A$ an ideal and A is I-adically complete, then G defines a group law on $\prod^r I := I \times \cdots \times I$. We denote the addition and the subtraction of $\prod^r I$ with respect to G by $+_G$ and $-_G$.

Lemma 3.1.1. *Let R, $G = G(X, Y)$, A and I be as above. If $f = (f_i), g = (g_i) \in \prod^r I$, then $f -_G g \in \prod^r I^n$ is equivalent to $f - g \in \prod^r I^n$.*

Proof. By the formal implicit function theorem [Haz78, A.4.7], there exists $\varphi(X) = (\varphi_i(X))_i \in \prod^r R[[X]]$ such that $G(X, \varphi(X)) = 0$. Then

$$G(X, \varphi(Y)) = G(X, \varphi(Y)) - G(X, \varphi(X)) = (X_1 - Y_1, \dots, X_r - Y_r)R[[X, Y]]^r$$

and there exist a square matrix of degree r $Q(X, Y) \in M_r(R[[X, Y]])$ such that

$$\begin{pmatrix} G_1(X, \varphi(Y)) \\ \vdots \\ G_r(X, \varphi(Y)) \end{pmatrix} = Q(X, Y) \begin{pmatrix} X_1 - Y_1 \\ \vdots \\ X_r - Y_r \end{pmatrix}.$$

Since $\varphi_i(X) \equiv -X_i \pmod{\deg 2}$, $Q(X, Y) \equiv I_r \pmod{\deg 1}$ and $Q(X, Y)$ is invertible in $M_r(R[[X, Y]])$. Since $f -_G g = G(f, \varphi(g)) = Q(f, g)(f - g)$, the assertion holds. □

In the following, we denote a sum with respect to G by ${}^G\sum_{i=0}^n$, ${}^G\sum_{i=0}^\infty$ etc.

Lemma 3.1.2. *Let A be a commutative R-algebra, I and ideal of A and assume that A is I-adically complete. Let $r \in \mathbb{Z}_{>0}$ and let $\underline{a} = (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} A^r$. ($a_n = (a_{n,i})_{1\le i\le r} \in A^r$). If $\lim_{n\to\infty} a_n = 0$, then ${}^G\sum_{n\to 0} a_i$ converges.*

Proof. By Lemma 3.1.1, the sequence of finite sums $b_n = {}^G\sum_{i=0}^n a_i$ with respect to G is a Cauchy sequence. □

3.2 Artin-Hasse exponentials

We use the same notation as in §2.1. Let $T = (T_1, \dots, T_r)$ be an r-tuple of indeterminates. We often regard T as a column vector ${}^t(T_1, \dots, T_r)$. When $r = 1$, we identify T with T_1. We fix a series $l(T) \in K[[T]]^r$ of functional equation type, i.e., $l(T)$ satisfies

$$l(T) - \sum_{i=1}^{\infty} s_i \sigma_*^i l(T^{\langle q^i \rangle}) \in \mathcal{O}[[T]]^r. \tag{3.2.1}$$

for a sequence of $s_i \in M_r(K)$ such that $\pi s_1 \in GL_r(\mathcal{O})$ and $\pi s_i \in M_r(\mathcal{O})$ for $i \ge 2$. By Hazewinkel's higher dimensional functional equation lemma (Theorem 1.1.3), $l^{-1}(l(X) + l(Y)) \in \mathcal{O}[[X, Y]]$ ($X = (X_1, \dots, X_r)$, $Y = (Y_1, \dots, Y_r)$)

and defines r-dimensional formal group law (Corollary 2.1.4). We denote it by $G = G(X, Y)$. We often denote $l^{-1}(T)$ by $\exp_G(T)$. We also fix another series

$$l_0(T) = \sum_{i=0}^{\infty} \gamma_i T^{\langle q^i \rangle} \in K[[T]]^r, \quad (\gamma_i \in M_r(K))$$

of Witt type that satisfies the same functional equation (3.2.1). Then $l_0(T)$ is of Witt type by Theorem 2.1.2. We denote by W the Witt functor for $l_0(T)$. We denote by $\phi_n(\underline{X})$ and $\widetilde{\phi}_n(\underline{Y})$ the n-th ghost polynomials for W.

Definition 3.2.1. We define the *Artin-Hasse exponential* for l and l_0 to be $E(T) = l^{-1}(l_0(T))$. By Theorem 1.1.3 (2), $E(T) \in \prod^r T\mathcal{O}[[T]]$. Here $T\mathcal{O}[[T]]$ is the ideal of $\mathcal{O}[[T]]$ generated by $T_1, \dots, T_r$.

Example 3.2.2. Consider the case where $K = \mathbb{Q}$, p a prime, $\mathcal{O} = \mathbb{Z}_{(p)}$, $\sigma = \mathrm{id}$, $r = 1$, $l(T) = \sum_{n=0}^{\infty} \frac{T^n}{n}$ and $l_0(T) = \sum_{i=0}^{\infty} \frac{T^{p^i}}{p^i}$. In this case, $G(X, Y) = X + Y - XY$ is the formal multiplicative group, $\phi_n(\underline{X}) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n$ is the classical n-th ghost polynomial and

$$l^{-1}(l_0(T)) = 1 - \exp\left(-\sum_{i=0}^{\infty} \frac{T^{p^i}}{p^i}\right) \in T\mathbb{Z}_{(p)}[[T]].$$

Lemma 3.2.3. *Let R be a commutative $\mathcal{O}$-algebra and I an ideal of R. Assume that R is I-adically complete. Let $\underline{x} = (x_n)_{n\in\mathbb{N}} \in W(R)$ $(x_n = (x_{n,i})_{1\le i\le r})$ and suppose that $x_n \in \prod^r I$ for any $n \in \mathbb{N}$ and that $\lim_{n\to\infty} x_n = 0$. Then ${}^G\sum_{n=0}^{\infty} E(x_i)$ converges in $\prod^r I$.*

Proof. By the assumption that $x_n \in \prod^r I$, each $E(x_n)$ converges in $\prod^r I$, because $E(T) \in T\mathcal{O}[[T]]^r$. Since $\lim_{n\to\infty} E(x_n) = 0$, ${}^G\sum_{n=0}^{\infty} E(x_n)$ converges by Lemma 3.1.2. □

Let A be a commutative $\mathcal{O}$-algebra and $T = (T_1, \dots, T_r)$ an r-tuple of indeterminates. We denote by $TA[[T]]$ the ideal of $A[[T]]$ generated by $T_1, \dots, T_r$ and we equip $\prod^r TA[[T]]$ with $(T_1, \dots, T_r)$-adic topology. Then $\prod^r TA[[T]]$ is complete with respect to this topology and we can define a group structure on it by G. We denote this group by $(\prod^r TA[[T]], +_G)$.

Let $\underline{a} = (a_n)_{n\in\mathbb{N}} \in W(A)$ and $[T] = (T, 0, 0, \dots)$. Let $b = (b_n)_{n\in\mathbb{N}} = \underline{a}[T]$. then we can easily see by induction that $b_n \in \prod^r (TA[[T]])^{q^n}$. Thus $E(\underline{a}[T]) = {}^G\sum_{n=0}^{\infty} E(b_i)$ converges.

Definition 3.2.4. Let A be a commutative $\mathcal{O}$-algebra and $T = {}^t(T_1, \dots, T_r)$. For $\underline{a} = (a_i)_i \in W(A)$ (resp. $\widetilde{W}(A)$), we define

$$E(\underline{a}, T) := E(\underline{a}[T]) \in TA[[T]]^r,$$

where $[T] = (T, 0, \dots) \in W(A[[T]])$ is a Teichmüller lift (Definition 2.3.7) of T.

Remark 3.2.5. When $r = 1$, then $\underline{a}[T] = (a_i T^{q^i})$ and hence $E(\underline{a}, T) = {}^G\sum_{i=0}^{\infty} E(a_i T^{q^i})$. In particular, when $l(T) = -\log(1-T)$ and $l_0(T) = \sum_{m=0}^{\infty} T^{p^m}/p^m$ as in Example 3.2.2,

$$E(\underline{a}, T) = 1 - \prod_{i=0}^{\infty} \exp\left(-\sum_{m=0}^{\infty} \frac{(a_i T^{p^i})^{p^m}}{p^m}\right).$$

On the other hand, when $r > 2$, $\underline{a}[T]$ is not necessarily equal to $(a_i T^{q^i})$. See Remark 2.3.9.

Lemma 3.2.6. *Let A be a commutative $\mathcal{O}$-algebra. Let $\underline{a} = (a_n)_{n\in\mathbb{N}} \in W(A)$ or $\widetilde{W}(A)$, $T = {}^r(T_1, \dots, T_r)$ and $\underline{b} = (b_i)_i = \underline{a}[T]$. Then we have*

$$\sum_{i=0}^{\infty} l_0(b_i) = \sum_{n=0}^{\infty} \gamma_n \left(\phi_n(\underline{a}) T^{\langle q^n \rangle}\right)$$
$$\left(\textit{resp. } \sum_{i=0}^{\infty} l_0(b_i) = \sum_{n=0}^{\infty} \gamma_n \left(\widetilde{\phi}_n(\underline{a}) T^{\langle q^n \rangle}\right)\right).$$

Proof. We show the case of ϕ. The assertion follows from the calculation below.

$$\begin{aligned}
&\sum_{i=0}^{\infty} l_0(b_i) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} \gamma_j b_i^{\langle q^j \rangle} = \sum_{n=0}^{\infty}\sum_{i=0}^{n} \gamma_{n-i} b_i^{\langle q^{n-i} \rangle} \\
&= \sum_{n=0}^{\infty} \gamma_n \left(\sum_{i=0}^{n} \gamma_n^{-1}\gamma_{n-i} b_i^{\langle q^{n-i} \rangle}\right) = \sum_{n=0}^{\infty} \gamma_n \phi_n(\underline{b}) \\
&= \sum_{n=0}^{\infty} \gamma_n \left(\phi_n(\underline{a})\phi_n(\underline{T})\right) = \sum_{n=0}^{\infty} \gamma_n \left(\phi_n(\underline{a}) T^{\langle q^n \rangle}\right)
\end{aligned}$$

We can show the case of $\widetilde{\phi}$ in the same way. □

Remark 3.2.7. Note that $\gamma_n \left(\phi_n(\underline{a}) T^{q^n}\right)$ does not necessarily equal $\left(\gamma_n \phi_n(\underline{a})\right) T^{q^n}$ in the above calculation.

Proposition 3.2.8. *Let $\underline{a} = (a_n)_n \in W(A)$ (resp. $\widetilde{W}(A)$). In $(A \otimes_{\mathcal{O}} K[[T]])^r$,*

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

Proof. We use the same notation as in Lemma 3.2.6. By Lemma 3.2.6, we have

$$E(\underline{a}, T) = {}^G\sum_{i=0}^{\infty} l^{-1} l_0(b_i) = l^{-1}\left(\sum_{i=0}^{\infty} l_0(b_i)\right) = l^{-1}\left(\sum_{m=0}^{\infty} \gamma_m \left(\phi_m(\underline{a}) T^{\langle q^m \rangle}\right)\right).$$

□

By $E(\underline{a}, T)$, we can define a map

$$E(-, T) : W(A) \to \prod^r TA[[T]] \quad (\text{resp. } \widetilde{W}(A) \to \prod^r TA[[T]])$$

Proposition 3.2.9. *If π is a non zero-divisor in A, then $E(-, T) : W(A) \to \prod^r TA[[T]]$ (resp. $\widetilde{W}(A) \to \prod^r TA[[T]]$) is injective.*

Proof. By the assumption, $TA[[T]] \to T(A \otimes_{\mathcal{O}} K)[[T]]$ is injective. Since $\phi_A : W(A) \to \prod_{n\in\mathbb{N}} A^r$ (resp. $\widetilde{\phi}_A : \widetilde{W}(A) \to \prod_{n\in\mathbb{N}} M_r(A)$) is injective by Proposition 2.2.1 (1) and $\phi_n(\underline{a})$ (resp. $\widetilde{\phi}_n(\underline{a})$) are determined by $\sum_{n=0}^{\infty} \gamma_n \left(\phi_n(\underline{a}) T^{\langle q^n \rangle}\right)$ (resp. $\sum_{n=0}^{\infty} \gamma_n \left(\widetilde{\phi}_n(\underline{a}) T^{\langle q^n \rangle}\right)$) for all $n \in \mathbb{N}$, the assertion holds. □

Corollary 3.2.10. *Under the assumption of Lemma 3.2.6, the map* $E(-,T): W(A) \to (TA[[T]]^r, +_G)$ *(resp.* $\widetilde{W}(A) \to (TA[[T]]^r, +_G)$*) which sends* $\underline{a}$ *to* $E(\underline{a},T)$ *is a homomorphism of groups, i.e.,*

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

Proof. We prove the assertion for $\underline{a} \in W(A)$. We can reduce to the case where $A = \mathcal{O}[\underline{X}]$. Then it is enough to show the additivity in $\prod(A \otimes_{\mathcal{O}} K[[T]])^r$. By Proposition 3.2.8,

$$\begin{aligned}
E(\underline{a}+\underline{b},T) &= \exp_G\left(\sum_{m=0}^{\infty} \gamma_m\left(\phi_m(\underline{a}+\underline{b})T^{\langle q^m\rangle}\right)\right) \\
&= \exp_G\left(\sum_{m=0}^{\infty} \gamma_m\left((\phi_m(\underline{a})+\phi_m(\underline{b}))T^{\langle q^m\rangle}\right)\right) \\
&= \exp_G\left(\sum_{m=0}^{\infty} \gamma_m\left(\phi_m(\underline{a})T^{\langle q^m\rangle}\right) + \sum_{m=0}^{\infty} \gamma_m\left(\phi_m(\underline{b})T^{\langle q^m\rangle}\right)\right) \\
&= \exp_G\left(\sum_{m=0}^{\infty} \gamma_m\left(\phi_m(\underline{a})T^{\langle q^m\rangle}\right)\right) +_G \exp_G\left(\sum_{m=0}^{\infty} \gamma_m\left(\phi_m(\underline{b})T^{\langle q^m\rangle}\right)\right) \\
&= E(\underline{a},T) +_G E(\underline{b},T)
\end{aligned}$$

The case of $\underline{a} \in \widetilde{W}(A)$ can be proven in a similar way. □

References

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

[Mat19] S. Matsuda, *π-exponentials for generalized twisted ramified Witt vectors*, Rend. Semin. Mat. Univ. Padova **142** (2019), 145–179.