Tohoku Math. J.
53 (2001), 203–240

A NOTE ON EXTENSIONS OF ALGEBRAIC AND FORMAL GROUPS, IV KUMMER-ARTIN-SCHREIER-WITT THEORY OF DEGREE p^2

TSUTOMU SEKIGUCHI* AND NORIYUKI SUWA**

(Received July 12, 1999, revised March 24, 2000)

Abstract. We establish a formula for homomorphisms and extensions of group schemes and formal groups, related to deformations of the multiplicative group to the additive group. As an application, we give an explicit description of the theory unifying the Kummer and Artin-Schreier-Witt theories of degree p^2.

Introduction. Throughout this article, by p we denote a prime number. Let W_n (resp. $\hat{W}_n$) denote the group scheme (resp. the formal group scheme) over $\boldsymbol{Z}$ of Witt vectors of length n. We denote by W (resp. $\hat{W}$) the group scheme (resp. the formal group scheme) of Witt vectors over $\boldsymbol{Z}$, and by $\boldsymbol{G}_m$ (resp. $\hat{\boldsymbol{G}}_m$) the multiplicative group scheme (resp. the multiplicative formal group scheme) over $\boldsymbol{Z}$. Let F be the Frobenius endomorphism of W or of $\hat{W}$ (for the definition see Section 1.2).

In the previous papers [12, 13, 16], the authors gave an explicit description of $\mathrm{Ext}_A(W_{n,A}, \boldsymbol{G}_{m,A})$ and $\mathrm{Ext}_A(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A})$, when A is a $\boldsymbol{Z}_{(p)}$-algebra. More precisely, we constructed isomorphisms

$$\begin{aligned}
\mathrm{Ker}[F^n : \hat{W}(A) \to \hat{W}(A)] &\xrightarrow{\sim} \mathrm{Hom}(W_{n,A}, \boldsymbol{G}_{m,A}),\\
\mathrm{Coker}[F^n : \hat{W}(A) \to \hat{W}(A)] &\xrightarrow{\sim} H^2_0(W_{n,A}, \boldsymbol{G}_{m,A}),\\
\mathrm{Ker}[F^n : W(A) \to W(A)] &\xrightarrow{\sim} \mathrm{Hom}(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A}),\\
\mathrm{Coker}[F^n : W(A) \to W(A)] &\xrightarrow{\sim} H^2_0(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A}),
\end{aligned}$$

using the Artin-Hasse exponential series. In particular, in the case of $n = 1$, the result reads

$$(*)\qquad \begin{aligned}
\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)] &\xrightarrow{\sim} \mathrm{Hom}(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}),\\
\mathrm{Coker}[F : \hat{W}(A) \to \hat{W}(A)] &\xrightarrow{\sim} H^2_0(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}),\\
\mathrm{Ker}[F : W(A) \to W(A)] &\xrightarrow{\sim} \mathrm{Hom}(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A}),\\
\mathrm{Coker}[F : W(A) \to W(A)] &\xrightarrow{\sim} H^2_0(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A}).
\end{aligned}$$

2000 *Mathematics Subject Classification.* Primary 14L05; Secondary 13K05, 20G10.
* Partially supported by the Grant-in-Aid for Scientific Research No. 08640059.
** Partially supported by the Grant-in-Aid for Scientific Research No. 09640066.

Now let $\lambda \in A$. Then we have a group scheme $\mathcal{G}^{(\lambda)} = \operatorname{Spec} A[T, 1/(1+\lambda T)]$ giving a deformation of $\boldsymbol{G}_a$ to $\boldsymbol{G}_m$ for suitable λ (for the definition, see 2.1). Our aim of this article is to generalize the isomorphisms of $(*)$ to those for $\mathcal{G}^{(\lambda)}$, using the deformations of the Artin-Hasse exponential series. Namely, our result is as follows.

THEOREM. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $\lambda \in A$. Then there exist isomorphisms*:

$$\operatorname{Ker}[F - [\lambda^{p-1}] : W(A) \to W(A)] \xrightarrow{\sim} \operatorname{Hom}(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A}),$$

$$\operatorname{Coker}[F - [\lambda^{p-1}] : W(A) \to W(A)] \xrightarrow{\sim} H^2_0(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A}).$$

Moreover, if λ is nilpotent, there exist isomorphisms:

$$\operatorname{Ker}[F - [\lambda^{p-1}] : \hat{W}(A) \to \hat{W}(A)] \xrightarrow{\sim} \operatorname{Hom}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A}),$$

$$\operatorname{Coker}[F - [\lambda^{p-1}] : \hat{W}(A) \to \hat{W}(A)] \xrightarrow{\sim} H^2_0(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A}).$$

It is crucial in our argument to construct deformations of the Artin-Hasse exponential series. We owe it to the functional equation lemma due to Hazewinkel [6, Ch.1.2] to discover the required formal series.

In Section 1, we recall and establish necessary facts on Witt vectors. Section 2 is devoted to a study of deformations of the Artin-Hasse exponential series, which allows us to state the main theorem. In Section 3, we prove the main result, generalizing the argument developed in [16]. In Section 4, we present a final form of some part of the computations given in the previous papers [9, 10, 11]. Section 5 is intended for an explicit description of the Kummer-Artin-Schreier-Witt theory of degree p^2.

It should be mentioned that Green and Matignon have given a slightly different explicit formula of the theory of degree p^2 ([4]) and that there exists a theory unifying Kummer and Artin-Schreier-Witt theories of degree p^n ([14, 15]). Detailed accounts on the theory of degree p^n will appear elsewhere as a sequel to this article. We expect to find applications of the Kummer-Artin-Schreier-Witt theory, such as an investigation of lifting automorphisms of an algebraic curve over a field of positive characteristic ([17], [4]).

The authors are more grateful to M. Matignon for his valuable remarks, especially a notice on Dwork's article (Remark 2.6.3).

NOTATION. Throughout the paper, p denotes a prime integer and A a $\boldsymbol{Z}_{(p)}$-algebra.

$\boldsymbol{G}_{a,A}$:	the additive group scheme over A
$\boldsymbol{G}_{m,A}$:	the multiplicative group scheme over A
$W_{n,A}$:	the group scheme of Witt vectors of length n over A
W_A :	the group scheme of Witt vectors over A
$\hat{\boldsymbol{G}}_{a,A}$:	the additive formal group scheme over A
$\hat{\boldsymbol{G}}_{m,A}$:	the multiplicative formal group scheme over A
$\hat{W}_{n,A}$:	the formal group scheme of Witt vectors of length n over A
$\hat{W}_A$:	the formal group scheme of Witt vectors over A
F :	the Frobenius endomorphism of W_A
V :	the Verschiebung endomorphism of W_A

$[a]$: the Teichmüller lifting $(a, 0, 0, \dots) \in W(A)$ of $a \in A$
$W(A)^{F-[a]}$: $= \mathrm{Ker}[F - [a] : W(A) \to W(A)]$
$W(A)/(F - [a])$: $= \mathrm{Coker}[F - [a] : W(A) \to W(A)]$

$H_0^2(G, H)$ denotes the Hochschild cohomology group consisting of symmetric 2-cocycles of G with coefficients in H for group schemes or formal group schemes G and H.

For a commutative ring B, $B^\times$ denotes the multiplicative group $\boldsymbol{G}_m(B)$.

1. Witt vectors. We start with reviewing relevant facts on Witt vectors needed later. For details, see [2, Chap. V] or [6, Chap. III].

1.1. For each $r \geq 0$, we denote by $\Phi_r(\boldsymbol{T}) = \Phi_r(T_0, T_1, \dots, T_r)$ the so-called Witt polynomial

$$\Phi_r(\boldsymbol{T}) = T_0^{p^r} + pT_1^{p^{r-1}} + \cdots + p^r T_r$$

in $\boldsymbol{Z}[\boldsymbol{T}] = \boldsymbol{Z}[T_0, T_1, \dots]$. We define polynomials

$$S_r(\boldsymbol{X}, \boldsymbol{Y}) = S_r(X_0, \dots, X_r, Y_0, \dots, Y_r)$$

and

$$P_r(\boldsymbol{X}, \boldsymbol{Y}) = P_r(X_0, \dots, X_r, Y_0, \dots, Y_r)$$

in $\boldsymbol{Z}[\boldsymbol{X}, \boldsymbol{Y}] = \boldsymbol{Z}[X_0, X_1, \dots, Y_0, Y_1, \dots]$ inductively by

$$\Phi_r(S_0(\boldsymbol{X}, \boldsymbol{Y}), S_1(\boldsymbol{X}, \boldsymbol{Y}), \dots, S_r(\boldsymbol{X}, \boldsymbol{Y})) = \Phi_r(\boldsymbol{X}) + \Phi_r(\boldsymbol{Y})$$

and

$$\Phi_r(P_0(\boldsymbol{X}, \boldsymbol{Y}), P_1(\boldsymbol{X}, \boldsymbol{Y}), \dots, P_r(\boldsymbol{X}, \boldsymbol{Y})) = \Phi_r(\boldsymbol{X})\Phi_r(\boldsymbol{Y}).$$

Then, as is well-known, the ring structure of the scheme of Witt vectors of length n (resp. of the scheme of Witt vectors)

$$W_{n,\boldsymbol{Z}} = \mathrm{Spec}\, \boldsymbol{Z}[T_0, T_1, \dots, T_{n-1}] \quad (\text{resp. } W_{\boldsymbol{Z}} = \mathrm{Spec}\, \boldsymbol{Z}[T_0, T_1, T_2, \dots])$$

is given by the addition

$$T_0 \mapsto S_0(\boldsymbol{X}, \boldsymbol{Y}), \quad T_1 \mapsto S_1(\boldsymbol{X}, \boldsymbol{Y}), \quad T_2 \mapsto S_2(\boldsymbol{X}, \boldsymbol{Y}), \dots$$

and the multiplication

$$T_0 \mapsto P_0(\boldsymbol{X}, \boldsymbol{Y}), \quad T_1 \mapsto P_1(\boldsymbol{X}, \boldsymbol{Y}), \quad T_2 \mapsto P_2(\boldsymbol{X}, \boldsymbol{Y}), \dots.$$

We denote by $\hat{W}_{n,\boldsymbol{Z}}$ (resp. $\hat{W}_{\boldsymbol{Z}}$) the formal completion of $W_{n,\boldsymbol{Z}}$ (resp. $W_{\boldsymbol{Z}}$) along the zero section. $\hat{W}_{n,\boldsymbol{Z}}$ (resp. $\hat{W}_{\boldsymbol{Z}}$) is considered as a subfunctor of $W_{n,\boldsymbol{Z}}$ (resp. $W_{\boldsymbol{Z}}$). Indeed, if A is a ring (not necessarily a $\boldsymbol{Z}_{(p)}$-algebra), then

$$\hat{W}_n(A) = \{(a_0, a_1, \dots, a_{n-1}) \in W_n(A)\ ;\ a_i \text{ is nilpotent for all } i\}$$

and

$$\hat{W}(A) = \left\{(a_0, a_1, a_2, \dots) \in W_n(A)\ ;\ \begin{array}{l} a_i \text{ is nilpotent for all } i \text{ and} \\ a_i = 0 \text{ for all but a finite number of } i \end{array}\right\}.$$

1.2. The restriction homomorphism

$$R : W_{n+1,\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, \dots, T_n] \to W_{n,\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, \dots, T_{n-1}]$$

is defined by the canonical injection

$$T_0 \mapsto T_0\,,\ T_1 \mapsto T_1\,,\ \dots\,,\ T_{n-1} \mapsto T_{n-1} : \mathbf{Z}[T_0, T_1, \dots, T_{n-1}] \to \mathbf{Z}[T_0, T_1, \dots, T_n]\,,$$

and the Verschiebung homomorphism

$$V : W_{n,\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, \dots, T_{n-1}] \to W_{n+1,\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, \dots, T_n]$$

is defined by

$$T_0 \mapsto 0\,,\ T_1 \mapsto T_0\,,\ \dots\,,\ T_n \mapsto T_{n-1} : \mathbf{Z}[T_0, T_1, \dots, T_n] \to \mathbf{Z}[T_0, T_1, \dots, T_{n-1}]\,.$$

Define now polynomials

$$F_r(\boldsymbol{T}) = F_r(T_0, \dots, T_r, T_{r+1}) \in \boldsymbol{Q}[T_0, \dots, T_r, T_{r+1}]$$

inductively by

$$\Phi_r(F_0(\boldsymbol{T}), \dots, F_r(\boldsymbol{T})) = \Phi_{r+1}(T_0, \dots, T_r, T_{r+1})$$

for $r \geq 0$. Then

$$F_r(\boldsymbol{T}) = F_r(T_0, \dots, T_r, T_{r+1}) \in \mathbf{Z}[T_0, \dots, T_r, T_{r+1}]$$

for each $r \geq 0$. We denote by

$$F : W_{n+1,\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, \dots, T_n] \to W_{n,\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, \dots, T_{n-1}]$$

$$(\text{resp. } F : W_{\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, T_2, \dots] \to W_{\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[T_0, T_1, T_2, \dots])$$

the morphism defined by

$$T_0 \mapsto F_0(\boldsymbol{T})\,,\ T_1 \mapsto F_1(\boldsymbol{T})\,, \dots\,,\ T_{n-1} \mapsto F_{n-1}(\boldsymbol{T}) : \mathbf{Z}[T_0, T_1, \dots, T_{n-1}] \to \mathbf{Z}[T_0, T_1, \dots, T_n]$$

$$(\text{resp. } T_0 \mapsto F_0(\boldsymbol{T})\,,\ T_1 \mapsto F_1(\boldsymbol{T}),\ T_2 \mapsto F_2(\boldsymbol{T})\,, \dots : \mathbf{Z}[T_0, T_1, T_2, \dots] \to \mathbf{Z}[T_0, T_1, T_2, \dots])\,.$$

Then it is verified without difficulty that F is a homomorphism of ring schemes. It is obvious that $\hat{W}_{\mathbf{Z}}$ is stable under F. (Cf. [1, Ch.9.1.3] or [7, Ch.0.1.3]) If A is an $\boldsymbol{F}_p$-algebra, $F : W_A \to W_A$ is nothing but the usual Frobenius endomorphism. More precisely, define polynomials $G_r(\boldsymbol{T}) \in \mathbf{Z}[T_0, \dots, T_r, T_{r+1}]$ inductively by

$$G_0(\boldsymbol{T}) = T_1$$

and

$$G_r(\boldsymbol{T}) = G_r(T_0, \dots, T_r, T_{r+1}) = \begin{cases} T_{r+1} - \sum_{k=0}^{r-1} T_k^{p(p^{r-k}-1)} G_k(\boldsymbol{T}) & (p > 2), \\ T_{r+1} - \sum_{k=0}^{r-1} T_k^{2(2^{r-k}-1)} G_k(\boldsymbol{T}) - \sum_{k=0}^{r-1} T_k^{2(2^{r-k}-2)} G_k(\boldsymbol{T})^2 & (p = 2) \end{cases}$$

for $r \geq 1$.

LEMMA 1.2.1. *With the above notation,*

$$F_r(\boldsymbol{T}) \equiv T_r^p + pG_r(\boldsymbol{T}) \mod p^2.$$

PROOF. We prove the assertion by the induction on r. It is easily seen that $F_0(\boldsymbol{T}) = T_0^p + pT_1$.

Case I. $p > 2$. Assume that

$$F_k(\boldsymbol{T}) \equiv T_k^p + pG_k(\boldsymbol{T}) \mod p^2$$

for $k = 1, 2, \dots, r-1$. Then

$$F_k(\boldsymbol{T})^{p^{r-k}} \equiv T_k^{p^{r-k+1}} + p^{r-k+1} T_k^{p(p^{r-k}-1)} G_k(\boldsymbol{T}) \mod p^{r-k+2},$$

and therefore

$$p^k F_k(\boldsymbol{T})^{p^{r-k}} \equiv p^k T_k^{p^{r-k+1}} + p^{r+1} T_k^{p(p^{r-k}-1)} G_k(\boldsymbol{T}) \mod p^{r+2}.$$

It follows that

$$\sum_{k=0}^{r} p^k F_k(\boldsymbol{T})^{p^{r-k}} \equiv \sum_{k=0}^{r-1} p^k T_k^{p^{r-k+1}} + p^{r+1} \sum_{k=0}^{r-1} T_k^{p(p^{r-k}-1)} G_k(\boldsymbol{T}) + p^r F_r(\boldsymbol{T}) \mod p^{r+2}.$$

Noting

$$\sum_{k=0}^{r} p^k F_k(\boldsymbol{T})^{p^{r-k}} = \Phi_r(F_0(\boldsymbol{T}), \dots, F_r(\boldsymbol{T})) = \Phi_{r+1}(T_0, \dots, T_r, T_{r+1}) = \sum_{k=0}^{r+1} p^k T_k^{p^{r-k+1}},$$

we obtain

$$p^{r+1} \sum_{k=0}^{r-1} T_k^{p(p^{r-k}-1)} G_k(\boldsymbol{T}) + p^r F_r(\boldsymbol{T}) \equiv p^r T_r^p + p^{r+1} T_{r+1} \mod p^{r+2}$$

and

$$F_r(\boldsymbol{T}) \equiv T_r^p + pT_{r+1} - p \sum_{k=0}^{r-1} T_k^{p(p^{r-k}-1)} G_k(\boldsymbol{T}) \mod p^2.$$

Case II. $p = 2$. Assume that

$$F_k(\boldsymbol{T}) \equiv T_k^2 + 2G_k(\boldsymbol{T}) \mod 2^2$$

for $k = 1, 2, \dots, r-1$. Then

$$F_k(\boldsymbol{T})^{2^{r-k}} \equiv T_k^{2^{r-k+1}} + 2^{r-k+1}\{T_k^{2(2^{r-k}-1)}G_k(\boldsymbol{T}) + T_k^{2(2^{r-k}-2)}G_k(\boldsymbol{T})^2\} \mod 2^{r-k+2},$$

and therefore

$$2^k F_k(\boldsymbol{T})^{2^{r-k}} \equiv 2^k T_k^{2^{r-k+1}} + 2^{r+1}\{T_k^{2(2^{r-k}-1)}G_k(\boldsymbol{T}) + T_k^{2(2^{r-k}-2)}G_k(\boldsymbol{T})^2\} \mod 2^{r+2}.$$

It follows that

$$\sum_{k=0}^{r} 2^k F_k(\boldsymbol{T})^{2^{r-k}} \equiv \sum_{k=0}^{r-1} 2^k T_k^{2^{r-k+1}} + 2^{r+1}\sum_{k=0}^{r-1}\{T_k^{2(2^{r-k}-1)}G_k(\boldsymbol{T}) + T_k^{2(2^{r-k}-2)}G_k(\boldsymbol{T})^2\} + 2^r F_r(\boldsymbol{T}) \mod 2^{r+2}.$$

Noting

$$\sum_{k=0}^{r} 2^k F_k(\boldsymbol{T})^{2^{r-k}} = \Phi_r(F_0(\boldsymbol{T}), \dots, F_r(\boldsymbol{T})) = \Phi_{r+1}(T_0, \dots, T_r, T_{r+1}) = \sum_{k=0}^{r+1} 2^k T^{2^{r-k+1}},$$

we obtain

$$2^{r+1}\sum_{k=0}^{r-1}\{T_k^{2(2^{r-k}-1)}G_k(\boldsymbol{T}) + T_k^{2(2^{r-k}-2)}G_k(\boldsymbol{T})^2\} + 2^r F_r(\boldsymbol{T}) \equiv 2^r T_r^2 + 2^{r+1}T_{r+1} \mod 2^{r+2}$$

and

$$F_r(\boldsymbol{T}) \equiv T_r^2 + 2T_{r+1} - 2\sum_{k=0}^{r-1}\{T_k^{2(2^{r-k}-1)}G_k(\boldsymbol{T}) + T_k^{2(2^{r-k}-2)}G_k(\boldsymbol{T})^2\} \mod 2^2.$$

1.3. Let A be a ring and $a \in A$. We denote the Witt vector $(a, 0, 0, \dots)$ with components in A by [a]. Then we can verify without difficulty the following equalities in $\mathrm{End}_{A\text{-gr}}W$:

(1) $V[a^p] = [a]V$; (2) $F[a] = [a^p]F$; (3) $FV = p$.

Define a Witt vector $\tilde{p} = (\tilde{p}_0, \tilde{p}_1, \tilde{p}_2, \dots) \in W(\boldsymbol{Z})$ by $\tilde{p} = (p - V)[1]$. Then we have

$$\Phi_0(\tilde{p}_0) = p$$

and

$$\Phi_n(\tilde{p}_0, \tilde{p}_1, \dots, \tilde{p}_n) = 0 \quad \text{for } n \geq 1.$$

It follows that

$$VF = p - \tilde{p} = V[1]$$

and

$$V^n F^n = p^n - \sum_{k=1}^{n} p^{n-k} V^{k-1} \tilde{p} F^{k-1}.$$

1.4. Now we define a variant of the Verschiebung morphism. Define polynomials

$$\tilde{V}_r(\boldsymbol{T}) = \tilde{V}_r(T_0, T_1, \dots, T_{r-1}) \in \boldsymbol{Q}[T_0, T_1, \dots, T_{r-1}]$$

inductively by

$$\tilde{V}_0 = 0$$

and

$$\Phi_r(\tilde{V}_0(\boldsymbol{T}), \dots, \tilde{V}_r(\boldsymbol{T})) = p^{p^r} \Phi_{r-1}(T_0, \dots, T_{r-1}) \quad \text{for } r \geq 1 .$$

LEMMA 1.4.1. *With the above notation,* $\tilde{V}_r(\boldsymbol{T}) \in \boldsymbol{Z}[T_0, T_1, \dots, T_{r-1}]$ *and*

$$\tilde{V}_r(\boldsymbol{T}) \equiv \begin{cases} 0 \mod p^2 & (p > 2), \\ 2T_0^{2^{r-1}} \mod 2^2 & (p = 2). \end{cases}$$

PROOF. We prove the assertion by the induction on r. It is easily seen that $\tilde{V}_1(\boldsymbol{T}) = p^{p-1} T_0$.

Case I. $p > 2$. Assume that

$$\tilde{V}_k(\boldsymbol{T}) \in \boldsymbol{Z}[T_0, T_1, \dots, T_{k-1}] \quad \text{and} \quad \tilde{V}_k(\boldsymbol{T}) \equiv 0 \mod p^2$$

for $k = 1, 2, \dots, r-1$. Then

$$p^k \tilde{V}_k(\boldsymbol{T})^{p^{r-k}} \equiv 0 \mod p^{r+2},$$

since $p^{r-k} + k \geq r+2$ if $r \geq 1$ and $k \leq r-1$. It follows that

$$\Phi_r(\tilde{V}_0(\boldsymbol{T}), \dots, \tilde{V}_r(\boldsymbol{T})) = \sum_{k=0}^{r} p^k \tilde{V}_k(\boldsymbol{T})^{p^{r-k}} \equiv p^r \tilde{V}_r(\boldsymbol{T}) \mod p^{r+2} .$$

On the other hand,

$$p^{p^r} \Phi_{r-1}(T_0, \dots, T_{r-1}) \equiv 0 \mod p^{r+2}.$$

It is now verified that

$$\tilde{V}_r(\boldsymbol{T}) \in \boldsymbol{Z}[T_0, T_1, \dots, T_{r-1}]$$

and

$$\tilde{V}_r(\boldsymbol{T}) \equiv 0 \mod p^2 .$$

Case II. $p = 2$. Assume that

$$\tilde{V}_k(\boldsymbol{T}) \in \boldsymbol{Z}[T_0, T_1, \dots, T_{k-1}] \quad \text{and} \quad \tilde{V}_k(\boldsymbol{T}) \equiv 2T_0^{2^{k-1}} \mod 2^2$$

for $k = 1, 2, \dots, r-1$. Then

$$\tilde{V}_k(\boldsymbol{T})^{2^{r-k}} \equiv 2^{2^{r-k}} T_0^{2^{r-1}} \mod 2^{r-k+2},$$

and therefore

$$2^k \tilde{V}_k(\boldsymbol{T})^{2^{r-k}} \equiv 2^{2^{r-k}+k} T_0^{2^{r-1}} \mod 2^{r+2} .$$

Hence

$$\Phi_r(\tilde{V}_0(\boldsymbol{T}), \dots, \tilde{V}_r(\boldsymbol{T})) = \sum_{k=0}^{r} 2^k \tilde{V}_k(\boldsymbol{T})^{2^{r-k}} \equiv 2^{r+1} T_0^{2^{r-1}} + 2^r \tilde{V}_r(\boldsymbol{T}) \mod 2^{r+2},$$

since $2^{r-k}+k \geq r+2$ if $r \geq 2$ and $k \leq r-2$. On the other hand,

$$2^{2^r}\Phi_{r-1}(T_0, \ldots, T_{r-1}) \equiv 0 \mod 2^{r+2}$$

if $r \geq 2$. It is now verified that

$$\tilde{V}_r(\boldsymbol{T}) \in \boldsymbol{Z}[T_0, T_1, \ldots, T_{r-1}]$$

and

$$\tilde{V}_r(\boldsymbol{T}) \equiv 2T_0^{2^{r-1}} \mod 2^2 .$$

1.5. We denote by

$$\tilde{V} : W_{n,\boldsymbol{Z}} = \operatorname{Spec} \boldsymbol{Z}[T_0, T_1, \ldots, T_{n-1}] \to W_{n+1,\boldsymbol{Z}} = \operatorname{Spec} \boldsymbol{Z}[T_0, T_1, \ldots, T_n]$$

$$(\text{resp. } \tilde{V} : W_{\boldsymbol{Z}} = \operatorname{Spec} \boldsymbol{Z}[T_0, T_1, T_2, \ldots] \to W_{\boldsymbol{Z}} = \operatorname{Spec} \boldsymbol{Z}[T_0, T_1, T_2, \ldots])$$

the morphism defined by

$$T_0 \mapsto \tilde{V}_0(\boldsymbol{T}),\ T_1 \mapsto \tilde{V}_1(\boldsymbol{T}), \ldots, T_n \mapsto \tilde{V}_n(\boldsymbol{T}) :\ \boldsymbol{Z}[T_0, T_1, \ldots, T_n] \to \boldsymbol{Z}[T_0, T_1, \ldots, T_{n-1}]$$

(resp.

$$T_0 \mapsto \tilde{V}_0(\boldsymbol{T}),\ T_1 \mapsto \tilde{V}_1(\boldsymbol{T}),\ T_2 \mapsto \tilde{V}_2(\boldsymbol{T}), \ldots :\ \boldsymbol{Z}[T_0, T_1, T_2, \ldots] \to \boldsymbol{Z}[T_0, T_1, T_2, \ldots]).$$

Then $\tilde{V}$ is a homomorphism of group schemes. It is obvious that $\hat{W}_{\boldsymbol{Z}}$ is stable under $\tilde{V}$.

It is easily verified that

(1) $p\tilde{V} = [p]V$; (2) $\tilde{V}[a^p] = [a]\tilde{V}$; (3) $F\tilde{V} = [p^p]$; (4) $\tilde{V}F = [p] - \tilde{p}$.

PROPOSITION 1.6. *Let $[\Lambda]$ denote the Witt vector $(\Lambda, 0, 0, \ldots)$ with coefficients in $\boldsymbol{Z}[\Lambda]$. Then $F - [\Lambda] : W_{n+1,\boldsymbol{Z}[\Lambda]} \to W_{n,\boldsymbol{Z}[\Lambda]}$ is faithfully flat.*

PROOF. By [5, Ch.IV, Th.11.3.10], it is sufficient to prove that the morphism $(F - [\Lambda])_s : W_{n+1,s} \to W_{n,s}$ of the fibers is faithfully flat for each $s \in \operatorname{Spec} \boldsymbol{Z}[\Lambda]$, since $W_{n+1,\boldsymbol{Z}[\Lambda]}$ is flat over $\boldsymbol{Z}[\Lambda]$. Hence the assertion is a consequence of the following sublemmas.

SUBLEMMA 1.6.1. *$F - [\Lambda] : W_{n+1,\boldsymbol{Z}[1/p,\Lambda]} \to W_{n,\boldsymbol{Z}[1/p,\Lambda]}$ is smooth and surjective.*

PROOF. Note first that

$$\Phi_0 \mapsto \Phi_0(\boldsymbol{T}) = T_0,\ \Phi_1 \mapsto \Phi_1(\boldsymbol{T}) = T_0^p + pT_1, \ldots,$$

$$\Phi_n \mapsto \Phi_n(\boldsymbol{T}) = T_0^{p^n} + pT_1^{p^{n-1}} + \cdots + p^n T_n$$

gives rise to isomorphisms

$$\Phi_{n+1} : W_{n+1,\boldsymbol{Z}[1/p,\Lambda]} \xrightarrow{\sim} \boldsymbol{A}^{n+1}_{\boldsymbol{Z}[1/p,\Lambda]} = \operatorname{Spec} \boldsymbol{Z}[1/p, \Lambda][\Phi_0, \ldots, \Phi_{n-1}, \Phi_n]$$

and

$$\Phi_n : W_{n,\boldsymbol{Z}[1/p,\Lambda]} \xrightarrow{\sim} \boldsymbol{A}^{n}_{\boldsymbol{Z}[1/p,\Lambda]} = \operatorname{Spec} \boldsymbol{Z}[1/p, \Lambda][\Phi_0, \ldots, \Phi_{n-1}].$$

Now define an automorphism $\Xi^{(\Lambda)} : \boldsymbol{A}^{n+1}_{\boldsymbol{Z}[1/p,\Lambda]} \xrightarrow{\sim} \boldsymbol{A}^{n+1}_{\boldsymbol{Z}[1/p,\Lambda]}$ by

$$\Phi_0 \mapsto \Phi_0, \quad \Phi_1 \mapsto \Phi_1 - \Lambda\Phi_0, \ldots, \quad \Phi_n \mapsto \Phi_n - \Lambda^{p^{n-1}}\Phi_{n-1}.$$

Then we have a commutative diagram

$$\begin{array}{ccc} W_{n+1,\boldsymbol{Z}[1/p,\Lambda]} & \xrightarrow{\Xi^{(\Lambda)}\circ\Phi}_{\sim} & \boldsymbol{A}^{n+1}_{\boldsymbol{Z}[1/p,\Lambda]} \\ {\scriptstyle F-[\Lambda]}\downarrow & & \downarrow{\scriptstyle \mathrm{pr}} \\ W_{n,\boldsymbol{Z}[1/p,\Lambda]} & \xrightarrow[\sim]{\Phi} & \boldsymbol{A}^{n}_{\boldsymbol{Z}[1/p,\Lambda]}\,, \end{array}$$

where $\mathrm{pr} : \boldsymbol{A}^{n+1}_{\boldsymbol{Z}[1/p,\Lambda]} \to \boldsymbol{A}^{n}_{\boldsymbol{Z}[1/p,\Lambda]}$ denotes the projection defined by

$$\Phi_0 \mapsto \Phi_1\,, \quad \Phi_1 \mapsto \Phi_2\,, \ldots\,, \quad \Phi_{n-1} \mapsto \Phi_n\,.$$

It follows that $F - [\Lambda] : W_{n+1,\boldsymbol{Z}[1/p,\Lambda]} \to W_{n,\boldsymbol{Z}[1/p,\Lambda]}$ is smooth and surjective.

SUBLEMMA 1.6.2. *$F - [\Lambda] : W_{n+1,\boldsymbol{F}_p[\Lambda]} \to W_{n,\boldsymbol{F}_p[\Lambda]}$ is factorized through $R : W_{n+1,\boldsymbol{F}_p[\Lambda]} \to W_{n,\boldsymbol{F}_p[\Lambda]}$, and the homomorphism $W_{n,\boldsymbol{F}_p[\Lambda]} \to W_{n,\boldsymbol{F}_p[\Lambda]}$ induced from $F - [\Lambda]$ is finite and flat.*

PROOF. By Lemma 1.2.1, $F : W_{n+1,\boldsymbol{F}_p[\Lambda]} \to W_{n,\boldsymbol{F}_p[\Lambda]}$ is factorized to $W_{n+1,\boldsymbol{F}_p[\Lambda]} \xrightarrow{R} W_{n,\boldsymbol{F}_p[\Lambda]} \xrightarrow{F} W_{n,\boldsymbol{F}_p[\Lambda]}$, where $F : W_{n,\boldsymbol{F}_p[\Lambda]} \to W_{n,\boldsymbol{F}_p[\Lambda]}$ is the Frobenius morphism. Put now

$$(\tilde{F}_0(\boldsymbol{T}), \tilde{F}_1(\boldsymbol{T}), \tilde{F}_2(\boldsymbol{T}), \ldots) = (F - [\Lambda])\boldsymbol{T} \in W(\boldsymbol{Z}[T_0, T_1, T_2, \ldots, \Lambda])\,.$$

Then we have

$$\tilde{F}_r(\boldsymbol{T}) \equiv T_r^p - \Lambda^{p^r} T_r \mod (p, T_0, T_1, \ldots, T_{r-1}) \quad \text{for } r \geq 0\,.$$

It follows that $\boldsymbol{F}_p[\Lambda][T_0, T_1, \ldots, T_{n-1}]$ is free of finite rank as an $\boldsymbol{F}_p[\Lambda][T_0, T_1, \ldots, T_{n-1}]$-module via

$$F - [\Lambda] : W_{n,\boldsymbol{F}_p} = \operatorname{Spec} \boldsymbol{F}_p[T_0, T_1, \ldots, T_{n-1}] \to W_{n,\boldsymbol{F}_p} = \operatorname{Spec} \boldsymbol{F}_p[T_0, T_1, \ldots, T_{n-1}]\,.$$

COROLLARY 1.7. *Let A be a ring and $a \in A$. Then $F - [a] : W_{n+1,A} \to W_{n,A}$ is faithfully flat.*

COROLLARY 1.8. *Let A be a ring and $a \in A$. Then $F - [a] : W_A \to W_A$ is faithfully flat.*

2. Artin-Hasse exponential series. Statement of the theorem.

2.1. Let A be a ring and $\lambda \in A$. We define a group scheme $\mathcal{G}^{(\lambda)}$ over A by

$$\mathcal{G}^{(\lambda)} = \operatorname{Spec} A[T, 1/(1 + \lambda T)]$$

with

(1) the multiplication: $T \mapsto T \otimes 1 + 1 \otimes T + \lambda T \otimes T$,
(2) the unit: $T \mapsto 0$,
(3) the inverse: $T \mapsto -T/(1 + \lambda T)$.

Moreover, we define an A-homomorphism $\alpha^{(\lambda)} : \mathcal{G}^{(\lambda)} \to \boldsymbol{G}_{m,A}$ by

$$U \mapsto 1 + \lambda T : A[U, U^{-1}] \to A[T, 1/(1 + \lambda T)]\,.$$

If λ is invertible in A, $\alpha^{(\lambda)}$ is an A-isomorphism. On the other hand, if $\lambda = 0$, $\mathcal{G}^{(\lambda)}$ is nothing but the additive group $\boldsymbol{G}_{a,A}$.

Now we recall the definition of Hochschild cohomology. For details, see [2, Ch.II.3 and Ch.III.6].

2.2. Let A be a ring and $G(X, Y)$ a formal series in $A[[X, Y]]^\times$ (resp. a fraction in $A[X, Y, 1/(1+\lambda X), 1/(1+\lambda Y)]^\times$). Recall that $G(X, Y)$ is called a symmetric 2-cocycle of $\hat{\mathcal{G}}^{(\lambda)}$ (resp. $\mathcal{G}^{(\lambda)}$) with coefficients in $\hat{\boldsymbol{G}}_{m,A}$ (resp. $\boldsymbol{G}_{m,A}$) if $G(X, Y)$ satisfies the following functional equations:

(1) $G(X, Y)G(X + Y + \lambda XY, Z) = G(X, Y + Z + \lambda YZ)G(Y, Z)$,

(2) $G(X, Y) = G(Y, X)$.

We denote by $Z^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ (resp. $Z^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$) the subgroup of $A[[X, Y]]^\times$ (resp. a fraction of $A[X, Y, 1/(1+\lambda X), 1/(1+\lambda Y)]^\times$) formed by the symmetric 2-cocycles of $\hat{\mathcal{G}}^{(\lambda)}$ (resp. $\mathcal{G}^{(\lambda)}$) with coefficients in $\hat{\boldsymbol{G}}_{m,A}$ (resp. $\boldsymbol{G}_{m,A}$).

Let $F(T)$ be a formal power series in $A[[T]]^\times$ (resp. a fraction in $A[T, 1/(1+\lambda T)]^\times$). Then $F(X)F(Y)F(X + Y + \lambda XY)^{-1} \in Z^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ (resp. $Z^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$). We denote by $B^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ (resp. $B^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$) the subgroup of $Z^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ (resp. $Z^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$) of the symmetric 2-cocycles of the form $F(X)F(Y)F(X + Y + \lambda XY)^{-1}$. Put

$$H_0^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A}) = Z^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})/B^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$$

and

$$H_0^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A}) = Z^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})/B^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})\,.$$

$H_0^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ (resp. $H_0^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$) is isomorphic to the subgroup of $\mathrm{Ext}_A(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ (resp. $\mathrm{Ext}_A(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$) formed by the classes of commutative extensions of $\hat{\mathcal{G}}^{(\lambda)}$ by $\hat{\boldsymbol{G}}_{m,A}$ (resp. $\mathcal{G}^{(\lambda)}$ by $\boldsymbol{G}_{m,A}$), which split as extensions of formal A-schemes (resp. A-schemes).

Hereafter we give an explicit description of $\mathrm{Hom}_{A\text{-gr}}(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ and $H_0^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ when A is a $\boldsymbol{Z}_{(p)}$-algebra.

2.3. We define a formal power series $E_p(U, \Lambda; T)$ in $\boldsymbol{Q}[U, \Lambda][[T]]$ by

$$E_p(U, \Lambda; T) = (1 + \Lambda T)^{U/\Lambda} \prod_{k=1}^{\infty} (1 + \Lambda^{p^k} T^{p^k})^{\{(U/\Lambda)^{p^k} - (U/\Lambda)^{p^{k-1}}\}/p^k}\,.$$

Recall now the definition of the Artin-Hasse exponential series

$$E_p(T) = \exp\left(\sum_{r \geq 0} \frac{T^{p^r}}{p^r}\right) \in \boldsymbol{Z}_{(p)}[[T]]\,.$$

THEOREM 2.4. *With the notation above we have*:

$$E_p(U, \Lambda; T) = \begin{cases} \prod_{(k,p)=1} E_p(U\Lambda^{k-1}T^k)^{(-1)^{k-1}/k} & \text{if } p > 2, \\ \prod_{(k,2)=1} E_p(U\Lambda^{k-1}T^k)^{1/k}\Big[\prod_{(k,2)=1} E_p(U\Lambda^{2k-1}T^{2k})^{1/k}\Big]^{-1} & \text{if } p = 2. \end{cases}$$

PROOF. Let $n = p^r m$ with $(m, p) = 1$. Then the coefficient of T^n in $\log E_p(U, \Lambda; T)$ is given by

$$\frac{U}{\Lambda}\frac{(-1)^{n-1}\Lambda^n}{n} + \sum_{k=1}^{r}\frac{1}{p^k}\left\{\left(\frac{U}{\Lambda}\right)^{p^k} - \left(\frac{U}{\Lambda}\right)^{p^{k-1}}\right\}\frac{(-1)^{n/p^k-1}(\Lambda^{p^k})^{n/p^k}}{n/p^k}$$

$$= \frac{U}{\Lambda}\frac{(-1)^{n-1}\Lambda^n}{n} + \sum_{k=1}^{r}\frac{(-1)^{n/p^k-1}}{n}\left\{\left(\frac{U}{\Lambda}\right)^{p^k} - \left(\frac{U}{\Lambda}\right)^{p^{k-1}}\right\}\Lambda^n,$$

since

$$\log E_p(U, \Lambda; T) = \frac{U}{\Lambda}\log(1 + \Lambda T) + \sum_{k=1}^{\infty}\frac{1}{p^k}\left\{\left(\frac{U}{\Lambda}\right)^{p^k} - \left(\frac{U}{\Lambda}\right)^{p^{k-1}}\right\}\log\left(1 + \Lambda^{p^k}T^{p^k}\right).$$

If $p > 2$,

$$\frac{U}{\Lambda}\frac{(-1)^{n-1}\Lambda^n}{n} + \sum_{k=1}^{r}\frac{(-1)^{n/p^k-1}}{n}\left\{\left(\frac{U}{\Lambda}\right)^{p^k} - \left(\frac{U}{\Lambda}\right)^{p^{k-1}}\right\}\Lambda^n = \frac{(-1)^{m-1}}{n}\left(\frac{U}{\Lambda}\right)^{p^r}\Lambda^n.$$

On the other hand, the coefficient of T^n in

$$\sum_{(k,p)=1}\frac{(-1)^{k-1}}{k}\log E_p(U\Lambda^{k-1}T^k)$$

is given by

$$\frac{(-1)^{m-1}}{m}\frac{(U\Lambda^{m-1})^{p^r}}{p^r}.$$

If $p = 2$,

$$\frac{U}{\Lambda}\frac{(-1)^{n-1}\Lambda^n}{n} + \sum_{k=1}^{r}\frac{(-1)^{n/p^k-1}}{n}\left\{\left(\frac{U}{\Lambda}\right)^{p^k} - \left(\frac{U}{\Lambda}\right)^{p^{k-1}}\right\}\Lambda^n$$

$$= \begin{cases} \frac{1}{n}\frac{U}{\Lambda}\Lambda^n & (2 \nmid n), \\ \frac{1}{n}\left(\frac{U}{\Lambda}\right)^{2^r}\Lambda^n - \frac{2}{n}\left(\frac{U}{\Lambda}\right)^{2^{r-1}}\Lambda^n & (2 \mid n). \end{cases}$$

On the other hand, the coefficient of T^n in

$$\sum_{(k,2)=1}\frac{1}{k}\log E_p(U\Lambda^{k-1}T^k) - \sum_{(k,2)=1}\frac{1}{k}\log E_p(U\Lambda^{2k-1}T^{2k})$$

is given by

$$\begin{cases} \dfrac{1}{n}U\Lambda^{n-1} & (2 \nmid n), \\ \dfrac{1}{m}\dfrac{(U\Lambda^{m-1})^{2^r}}{2^r} - \dfrac{1}{m}\dfrac{(U\Lambda^{2m-1})^{2^{r-1}}}{2^{r-1}} & (2 \mid n). \end{cases}$$

COROLLARY 2.5. *The formal power series* $E_p(U, \Lambda; T)$ *has its coefficients in* $\boldsymbol{Z}_{(p)}[U, \Lambda]$.

PROOF. As is well-known, $(1+T)^{1/k} \in \boldsymbol{Z}_{(p)}[[T]]$ if k is prime to p. Note that $E_p(T) \in \boldsymbol{Z}_{(p)}[[T]]$. It then follows that $E_p(U\Lambda^{k-1}T^k) \in \boldsymbol{Z}_{(p)}[U, \Lambda][[T]]$.

2.6. Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $a,\ \lambda \in A$. We define a formal power series $E_p(a, \lambda; T)$ in $A[[T]]$ by

$$E_p(a, \lambda; T) = \begin{cases} \displaystyle\prod_{(k,p)=1} E_p(a\lambda^{k-1}T^k)^{(-1)^{k-1}/k} & \text{if } p > 2, \\ \displaystyle\prod_{(k,2)=1} E_p(a\lambda^{k-1}T^k)^{1/k}\Big[\prod_{(k,2)=1} E_p(a\lambda^{2k-1}T^{2k})^{1/k}\Big]^{-1} & \text{if } p = 2. \end{cases}$$

EXAMPLE 2.6.1. We have an equality $E_p(1, 0; T) = E_p(T)$.

EXAMPLE 2.6.2. We have an equality $E_p(\Lambda, \Lambda; T) = 1 + \Lambda T$.

REMARK 2.6.3. The formal power series $E_p(U, 1; T)$ was introduced by Dwork [3, Sect.1] as $F(t, Y)$. Furthermore, he proved that $E_p(U, 1; T) \in \boldsymbol{Z}_{(p)}[U][[T]]$ by a different method. We can deduce that $E_p(U, \Lambda; T) \in \boldsymbol{Z}_{(p)}[U, \Lambda][[T]]$ from $E_p(U, 1; T) \in \boldsymbol{Z}_{(p)}[U][[T]]$.

2.7. Let A be a $\boldsymbol{Z}_{(p)}$-algebra, $\lambda \in A$ and $\boldsymbol{a} = (a_0, a_1, a_2, \dots) \in W(A)$. We define a formal power series $E_p(\boldsymbol{a}, \lambda; T)$ in $A[[T]]$ by

$$E_p(\boldsymbol{a}, \lambda; T) = \prod_{k=0}^{\infty} E_p(a_k, \lambda^{p^k}; T^{p^k}).$$

LEMMA 2.8. *Let* $\boldsymbol{U} = (U_0, U_1, U_2, \dots)$ *and*

$$(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \tilde{F}_2(\boldsymbol{U}), \dots) = (F - [\Lambda^{p-1}])\boldsymbol{U} \in W([U_0, U_1, U_2, \dots, \Lambda]).$$

Then we have

$$\begin{aligned} E_p(\boldsymbol{U}, \Lambda; T) &= (1 + \Lambda T)^{\Phi_0(\boldsymbol{U})/\Lambda} \prod_{k=1}^{\infty} (1 + \Lambda^{p^k} T^{p^k})^{\{\Phi_k(\boldsymbol{U}) - \Lambda^{p^{k-1}(p-1)}\Phi_{k-1}(\boldsymbol{U})\}/p^k\Lambda^{p^k}} \\ &= (1 + \Lambda T)^{U_0/\Lambda} \prod_{k=1}^{\infty} (1 + \Lambda^{p^k} T^{p^k})^{\Phi_{k-1}(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \dots, \tilde{F}_{k-1}(\boldsymbol{U}))/p^k\Lambda^{p^k}} \end{aligned}$$

in $\boldsymbol{Z}_{(p)}[U_0, U_1, U_2, \dots, \Lambda][[T]]$.

COROLLARY 2.9. *Let* $\boldsymbol{U} = (U_0, U_1, U_2, \dots)$, $\boldsymbol{V} = (V_0, V_1, V_2, \dots)$ *and* $\boldsymbol{S}(\boldsymbol{U}, \boldsymbol{V}) = (S_0(\boldsymbol{U}, \boldsymbol{V}), S_1(\boldsymbol{U}, \boldsymbol{V}), S_2(\boldsymbol{U}, \boldsymbol{V}), \dots)$. *Then we have*

$$E_p(\boldsymbol{U}, \Lambda; T)E_p(\boldsymbol{V}, \Lambda; T) = E_p(\boldsymbol{S}(\boldsymbol{U}, \boldsymbol{V}), \Lambda; T)$$

in $\boldsymbol{Z}_{(p)}[U_0, U_1, U_2, \dots, V_0, V_1, V_2, \dots, \Lambda][[T]]$.

COROLLARY 2.9.1. *Let* A *be a* $\boldsymbol{Z}_{(p)}$*-algebra,* $\lambda \in A$ *and* $\boldsymbol{a}, \boldsymbol{b} \in W(A)$. *Then we have*

$$E_p(\boldsymbol{a}, \lambda; T)E_p(\boldsymbol{b}, \lambda; T) = E_p(\boldsymbol{a} + \boldsymbol{b}, \lambda; T)\,.$$

REMARK 2.10. Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $F(T) \in A[[T]]$ with $F(0) = 1$. Then $F(T)$ is written uniquely in the form $\prod_{(k,p)=1} E_p(\boldsymbol{a}_k, \lambda; T^k)$ $(\boldsymbol{a}_k \in W(A))$.

PROPOSITION 2.11. *Let* A *be a* $\boldsymbol{Z}_{(p)}$*-algebra and* $\boldsymbol{a} = (a_0, a_1, a_2, \dots) \in \hat{W}(A)$. *Assume that* λ *is nilpotent in* A. *Then* $E_p(\boldsymbol{a}, \lambda; T) \in A[T]$ *if and only if* $\boldsymbol{a} \in \hat{W}(A)$.

PROOF. Put

$$E_p(\boldsymbol{U}, \Lambda; T) = \sum_{k=0}^{\infty} c_k(\boldsymbol{U}, \Lambda)T^k\,.$$

If we assign to U_k the weight p^k and to Λ the weight 1, respectively, then $c_k(\boldsymbol{U}, \Lambda)$ is isobaric of wieght k. Moreover,

$$c_{p^r}(\boldsymbol{U}, \Lambda) \equiv U_r \mod (U_0, U_1, \dots, U_{r-1}, \Lambda)\,.$$

Now assume that $F(T) = E_p(\boldsymbol{a}, \lambda; T) \in A[T]$. Let $d = \deg F(T)$ and $\mathfrak{a}$ the ideal of A generated by λ and the coefficients of $F(T)$ except the constant. Then $\mathfrak{a}$ is nilpotent, since $F(T)$ is invertible in $A[T]$. Put $s = [\log_p d]$; the greatest integer not greater than $\log_p d$. Then we can verify that

1) $a_r \in \mathfrak{a}$ if $r \leq s$; 2) $a_{s+j} \in \mathfrak{a}^{p^j}$ for all $j > 0$.

Conversely, if $\boldsymbol{a} \in \hat{W}(A)$, then $c_k(\boldsymbol{a}, \lambda)$ is nilpotent for all $k > 0$, and $c_k(\boldsymbol{a}, \lambda) = 0$ for all but a finite number of k.

LEMMA 2.12. *Let* $\boldsymbol{U} = (U_0, U_1, U_2, \dots)$. *Then we have*

$$\frac{E_p(\boldsymbol{U}, \Lambda; X)E_p(\boldsymbol{U}, \Lambda; Y)}{E_p(\boldsymbol{U}, \Lambda; X + Y + \Lambda XY)} = \prod_{k=1}^{\infty}\left[\frac{(1 + \Lambda^{p^k}X^{p^k})(1 + \Lambda^{p^k}Y^{p^k})}{1 + \Lambda^{p^k}(X + Y + \Lambda XY)^{p^k}}\right]^{\{\Phi_k(\boldsymbol{U}) - \Lambda^{p^{k-1}(p-1)}\Phi_{k-1}(\boldsymbol{U})\}/p^k\Lambda^{p^k}}\,.$$

COROLLARY 2.13. *Let*

$$(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \tilde{F}_2(\boldsymbol{U}), \dots) = (F - [\Lambda^{p-1}])\boldsymbol{U} \in W(\boldsymbol{Z}[U_0, U_1, U_2, \dots, \Lambda])$$

and

$$A = \boldsymbol{Z}_{(p)}[U_0, U_1, U_2, \dots, \Lambda]/(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \tilde{F}_2(\boldsymbol{U}), \dots)\,.$$

Then we have

$$E_p(\boldsymbol{U}, \Lambda; X)E_p(\boldsymbol{U}, \Lambda; Y) = E_p(\boldsymbol{U}, \Lambda; X + Y + \Lambda XY)$$

in $A[[X, Y]]$.

PROOF. Put $B = \boldsymbol{Q}[U_0, U_1, U_2, \dots, \Lambda, 1/\Lambda]/((\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \tilde{F}_2(\boldsymbol{U}), \dots)$. Then we have

$$\frac{1}{p^k \Lambda^{p^k}}\{\Phi_k(\boldsymbol{U}) - \Lambda^{p^{k-1}(p-1)}\Phi_{k-1}(\boldsymbol{U})\} = \frac{1}{p^k \Lambda^{p^k}}\Phi_{k-1}(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \dots, \tilde{F}_{k-1}(\boldsymbol{U})) = 0$$

in B. It follows from Lemma 2.12 that

$$\frac{E_p(\boldsymbol{U}, \Lambda; X)E_p(\boldsymbol{U}, \Lambda; Y)}{E_p(\boldsymbol{U}, \Lambda; X + Y + \Lambda XY)} = 1$$

in $B[[X, Y]]$. By Corollary 1.8, A is flat over $\boldsymbol{Z}[\Lambda]$, and therefore the canonical map $A[[X, Y]] \to B[[X, Y]]$ is injective. Hence we obtain the equality

$$E_p(\boldsymbol{U}, \Lambda; X)E_p(\boldsymbol{U}, \Lambda; Y) = E_p(\boldsymbol{U}, \Lambda; X + Y + \Lambda XY)$$

in $A[[X, Y]]$.

COROLLARY 2.14. *Let* A *be a* $\boldsymbol{Z}_{(p)}$*-algebra,* $\boldsymbol{a} \in W(A)$ *and* $\lambda \in A$. *If* $F(\boldsymbol{a}) = [\lambda^{p-1}]\boldsymbol{a}$, *then we have*

$$E_p(\boldsymbol{a}, \lambda; X)E_p(\boldsymbol{a}, \lambda; Y) = E_p(\boldsymbol{a}, \lambda; X + Y + \lambda XY).$$

2.15. Let $\boldsymbol{U} = (U_0, U_1, U_2, \dots)$. We define a formal power series

$$F_p(\boldsymbol{U}, \Lambda; X, Y) \in \boldsymbol{Q}[U_0, U_1, U_2, \dots, \Lambda][[X, Y]]$$

by

$$F_p(\boldsymbol{U}, \Lambda; X, Y) = \prod_{k=1}^{\infty}\left[\frac{(1 + \Lambda^{p^k}X^{p^k})(1 + \Lambda^{p^k}Y^{p^k})}{1 + \Lambda^{p^k}(X + Y + \Lambda XY)^{p^k}}\right]^{\Phi_{k-1}(\boldsymbol{U})/p^k\Lambda^{p^k}}.$$

It is readily seen that

$$F_p(\boldsymbol{U}, \Lambda; X, Y)F_p(\boldsymbol{U}, \Lambda; X + Y + \Lambda XY, Z) = F_p(\boldsymbol{U}, \Lambda; X, Y + Z + \Lambda YZ)F_p(\boldsymbol{U}, \Lambda; Y, Z)$$

and

$$F_p(\boldsymbol{U}, \Lambda; X, Y) = F_p(\boldsymbol{U}, \Lambda; Y, X).$$

LEMMA 2.16. *Let* $\boldsymbol{U} = (U_0, U_1, U_2, \dots)$. *Then* $F_p(\boldsymbol{U}, \Lambda; X, Y) \in \boldsymbol{Z}_{(p)}[U_0, U_1, U_2, \dots, \Lambda][[X, Y]]$.

PROOF. Put

$$(\tilde{F}_0(\boldsymbol{V}), \tilde{F}_1(\boldsymbol{V}), \tilde{F}_2(\boldsymbol{V}), \dots) = (F - [\Lambda^{p-1}])\boldsymbol{V} \in W(\boldsymbol{Z}[V_0, V_1, V_2, \dots, \Lambda])$$

and

$$B = \boldsymbol{Z}_{(p)}[U_0, U_1, U_2, \dots, V_0, V_1, V_2, \dots, \Lambda]/(\tilde{F}_0(\boldsymbol{V}) - U_0, \tilde{F}_1(\boldsymbol{V}) - U_1, \tilde{F}_2(\boldsymbol{V}) - U_2, \dots).$$

Then B is flat over $\boldsymbol{Z}_{(p)}[U_0, U_1, U_2, \ldots, \Lambda]$ by Corollary 1.8, and

$$F_p(\boldsymbol{U}, \Lambda; X, Y) = F_p((F - [\Lambda^{p-1}])\boldsymbol{V}, \Lambda; X, Y) = \frac{E_p(\boldsymbol{V}, \Lambda; X)E_p(\boldsymbol{V}, \Lambda; Y)}{E_p(\boldsymbol{V}, \Lambda; X + Y + \Lambda XY)} \in B[[X, Y]].$$

Note now that

$$\boldsymbol{Q}[U_0, U_1, U_2, \ldots, \Lambda] \cap B = \boldsymbol{Z}_{(p)}[U_0, U_1, U_2, \ldots, \Lambda].$$

COROLLARY 2.17. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $\boldsymbol{a} \in W(A)$. Then*

$$F_p(\boldsymbol{a}, \lambda; X, Y) \in Z^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A}).$$

If λ is nilpotent and $\boldsymbol{a} \in \hat{W}(A)$, then

$$F_p(\boldsymbol{a}, \lambda; X, Y) \in Z^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A}).$$

PROOF. The first asseertion follows directly from Lemma 2.16. For the second assertion, we have only to verify the following lemma.

LEMMA 2.18. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $\boldsymbol{a} \in W(A)$. Assume that λ is nilpotent. Then $F_p(\boldsymbol{a}, \lambda; X, Y) \in A[X, Y]$ if and only if $\boldsymbol{a} \in \hat{W}(A)$.*

PROOF. Put

$$F_p(\boldsymbol{U}, \Lambda; X, Y) = \sum_{i,j} c_{ij}(\boldsymbol{U}, \Lambda)X^iY^j.$$

If we assign to U_k the weight p^{k+1} and to Λ the weight 1, respectively, then $c_{ij}(\boldsymbol{U}, \Lambda)$ is isobaric of weight $i + j$. Moreover,

$$\sum_{i+j=p^r} c_{ij}(\boldsymbol{U}, \Lambda)X^iY^j \equiv U_r \frac{X^{p^{r+1}} + Y^{p^{r+1}} - (X + Y)^{p^{r+1}}}{p} \mod (U_0, U_1, \ldots, U_{r-1}, \Lambda).$$

Now assume that $F(X, Y) = E_p(\boldsymbol{a}, \lambda; X, Y) \in A[X, Y]$. Let $d = \deg F(X, Y)$ and $\mathfrak{a}$ the ideal of A generated by λ and the coefficients of $F(X, Y)$ except the constant. Then $\mathfrak{a}$ is nilpotent, since $F(X, Y)$ is invertible in $A[X, Y]$. Put $s = [\log_p d]$. Then we can verify that

(1) $a_r \in \mathfrak{a}$ if $r \leq s - 1$; (2) $a_{s+j} \in \mathfrak{a}^{p^{j+1}}$ for all $j \geq 0$.

Conversely, if $\boldsymbol{a} \in \hat{W}(A)$, then $c_{ij}(\boldsymbol{a}, \lambda)$ is nilpotent for all $(i, j) \neq (0, 0)$, and $c_{ij}(\boldsymbol{a}, \lambda) = 0$ for all but a finite number of (i, j).

2.19. Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $\lambda \in A$. Let $\boldsymbol{a} \in W(A)$. By 2.14 and 2.11, we can define homomorphisms

$$\xi_A^0 : W(A)^{F-[\lambda^{p-1}]} \to \mathrm{Hom}_{A\text{-gr}}(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A}); \ \boldsymbol{a} \mapsto E_p(\boldsymbol{a}, \lambda; T)$$

and, when λ is nilpotent,

$$\xi_A^0 : \hat{W}(A)^{F-[\lambda^{p-1}]} \to \mathrm{Hom}_{A\text{-gr}}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A}); \ \boldsymbol{a} \mapsto E_p(\boldsymbol{a}, \lambda; T).$$

Moreover,

$$F_p((F - [\lambda^{p-1}])\boldsymbol{a}, \lambda; X, Y) \in B^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$$

and, if λ is nilpotent and $\boldsymbol{a} \in \hat{W}(A)$,

$$F_p((F - [\lambda^{p-1}])\boldsymbol{a}, \lambda; X, Y) \in B^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A}) .$$

By 2.17 and 2.18, we can define homomorphisms

$$\xi_A^1 : W(A)/(F - [\lambda^{p-1}]) \to H_0^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A}); \ \boldsymbol{a} \mapsto F_p(\boldsymbol{a}, \lambda; X, Y)$$

and, when λ is nilpotent,

$$\xi_A^1 : \hat{W}(A)/(F - [\lambda^{p-1}]) \to H_0^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A}); \ \boldsymbol{a} \mapsto F_p(\boldsymbol{a}, \lambda; X, Y) .$$

With these notations, we can state our main theorem as follows.

THEOREM 2.19.1. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $\lambda \in A$. Then the homomorphisms*

$$\xi_A^0 : W(A)^{F-[\lambda^{p-1}]} \to Hom_{A\text{-gr}}(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A}) ,$$
$$\xi_A^1 : W(A)/(F - [\lambda^{p-1}]) \to H_0^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$$

are bijective. Moreover, if λ is nilpotent, then the homomorphisms

$$\xi_A^0 : \hat{W}(A)^{F-[\lambda^{p-1}]} \to Hom_{A\text{-gr}}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A}) ,$$
$$\xi_A^1 : \hat{W}(A)/(F - [\lambda^{p-1}]) \to H_0^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$$

are bijective.

3. Proof of the theorem. Hereafter, we denote by P the set $P = \{p^l \mid l \geq 0\} \subset \boldsymbol{N}$.

LEMMA 3.1. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra, $\lambda \in A$, and $F(T) \in A[[T]]^{\times}$. If $F(T)$ satisfies the functional equation $F(X + Y + \lambda XY) = F(X)F(Y)$, then there exists $\boldsymbol{a} \in W(A)^{F-[\lambda^{p-1}]}$ such that $F(T) = E_p(\boldsymbol{a}, \lambda; T)$.*

PROOF. As is remarked in 2.10, $F(T)$ is written uniquely in the form

$$F(T) = \prod_{(k,p)=1} E_p(\boldsymbol{a}_k, \lambda; T^k), \ \boldsymbol{a}_k \in W(A) .$$

Now we put

$$\boldsymbol{a} = \boldsymbol{a}_1 \quad \text{and} \quad G(T) = \prod_{\substack{(k,p)=1 \\ k>1}} E_p(\boldsymbol{a}_k, \lambda; T^k) .$$

Then we have that

$$(G(X)G(Y)G(X + Y + \lambda XY)^{-1})^{-1}$$
$$= E_p(\boldsymbol{a}, \lambda; X)E_p(\boldsymbol{a}, \lambda; Y)E_p(\boldsymbol{a}, \lambda; X + Y + \lambda XY)^{-1} = F_p((F - [\lambda^{p-1}])\boldsymbol{a}, \lambda; X, Y) .$$

Note that if $F_p((F - [\lambda^{p-1}])\boldsymbol{a}, \lambda; X, Y) \neq 1$, then

$$F_p((F - [\lambda^{p-1}])\boldsymbol{a}, \lambda; X, Y) = 1 + H_k + H_{k+1} + \cdots ,$$

where H_j is a homogeneous polynomial of degree j and k is a power of p. On the other hand, if $G(T) \neq 1$, then

$$G(T) \equiv 1 + cT^k \mod \text{degree } k+1$$

with $c \neq 0$ for some $k \notin P$. Hence

$$\begin{aligned} &G(X)G(Y)G(X+Y+\lambda XY)^{-1} \\ &\quad \equiv 1 + c\{X^k + Y^k - (X+Y+\lambda XY)^k\} \mod \text{degree } k+1 \\ &\quad \equiv 1 + c\{X^k + Y^k - (X+Y)^k\} \mod \text{degree } k+1, \end{aligned}$$

and we come to a contradiction. It follows that $G(T) = 1$ and $F_p((F - [\lambda^{p-1}])\boldsymbol{a}, \lambda; X, Y) = 1$, and therefore $(F - [\lambda^{p-1}])\boldsymbol{a} = 0$.

COROLLARY 3.2. *Let A be a $\mathbf{Z}_{(p)}$-algebra, $\lambda \in A$ and $F(T) \in A[T]^\times$. Suppose that λ is nilpotent. If $F(T)$ satisfies the functional equation $F(X+Y+\lambda XY) = F(X)F(Y)$, then there exists $\boldsymbol{a} \in \hat{W}(A)^{F-[\lambda^{p-1}]}$ such that $F(T) = E_p(\boldsymbol{a}, \lambda; T)$.*

PROOF. Combine Lemma 3.1 and Proposition 2.11.

3.3. We conclude immediately the bijectivity of $\xi_A^0 : W(A)^{F-[\lambda^{p-1}]} \to \mathrm{Hom}_{A\text{-gr}}(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ and $\xi_A^0 : \hat{W}(A)^{F-[\lambda^{p-1}]} \to \mathrm{Hom}_{A\text{-gr}}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$ from of Lemma 3.1 and Corollary 3.2, respectively.

LEMMA 3.4. *Let A be a $\mathbf{Z}_{(p)}$-algebra, and $\lambda \in A$. Then for $F(X,Y) \in Z^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A}) \subset A[[X,Y]]^\times$, there exist $\boldsymbol{a} \in W(A)$ and $G(T) = \prod_{k \notin P}(1 + c_k T^k) \in A[[T]]^\times$ such that*

$$F(X,Y) = F_p(\boldsymbol{a}, \lambda; X, Y)G(X)G(Y)G(X+Y+\lambda XY)^{-1}.$$

PROOF. Dividing $F(X,Y)$ by its constant term, we may assume that $F(X,Y) \equiv 1$ mod degree 1. Assume now that there exist $\boldsymbol{a}_k \in W(A)$ and $G_k(T) \in A[T]$ such that

$$F_p(\boldsymbol{a}_k, \lambda; X, Y)G_k(X)G_k(Y)G_k(X+Y+\lambda XY)^{-1} \equiv F(X,Y) \mod \text{degree } k.$$

Let $H(X,Y)$ be the homogeneous component of degree k of

$$F(X,Y)\{F_p(\boldsymbol{a}_k, \lambda; X, Y)G_k(X)G_k(Y)G_k(X+Y+\lambda XY)^{-1}\}^{-1}.$$

Since

$$F(X,Y)\{F_p(\boldsymbol{a}_k, \lambda; X, Y)G_k(X)G_k(Y)G_k(X+Y+\lambda XY)^{-1}\}^{-1} \in Z^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A}),$$

$H(X,Y)$ satisfies

$$H(X+Y) + H(X,Y) = H(X,Y+Z) + H(Y,Z) \quad \text{and} \quad H(X,Y) = H(Y,X).$$

By Lazard's comparison lemma [8, Lemme 3], there exists an element $a \in A$ such that

$$H(X,Y) = \begin{cases} a\{X^k + Y^k - (X+Y)^k\} & \text{if } k \text{ is not a power of } p, \\ a\dfrac{X^k + Y^k - (X+Y)^k}{p} & \text{if } k \text{ is a power of } p. \end{cases}$$

(1) When k is not a power of p, put $E(T) = 1 + aT^k$ and $G_{k+1}(T) = G_k(T)E(T)$. Then we have

$$F_p(\boldsymbol{a}_k, \lambda; X, Y)G_{k+1}(X)G_{k+1}(Y)G_{k+1}(X + Y + \lambda XY)^{-1} \equiv F(X, Y) \mod \text{degree } k+1,$$

noting that

$$\begin{aligned} &E(X)E(Y)E(X + Y + \lambda XY)^{-1} \\ &\quad \equiv 1 + a\{X^k + Y^k - (X + Y + \lambda XY)^k\} \mod \text{degree } k+1 \\ &\quad \equiv 1 + a\{X^k + Y^k - (X + Y)^k\} \mod \text{degree } k+1. \end{aligned}$$

(2) When $k = p^r$, put $\boldsymbol{a}_{k+1} = \boldsymbol{a}_k + \boldsymbol{b}$. Here $\boldsymbol{b} = (b_i)_{i\geq 0}$ with $b_{r-1} = a$ and $b_i = 0$ for $i \neq r-1$. Then we have

$$F_p(\boldsymbol{a}_{k+1}, \lambda; X, Y)G_k(X)G_k(Y)G_k(X + Y + \lambda XY)^{-1} \equiv F(X, Y) \mod \text{degree } k+1.$$

Continuing this process, we find $\boldsymbol{a} \in W(A)$ and $G(T) \in A[[T]]$ such that

$$F(X, Y) = F_p(\boldsymbol{a}, \lambda; X, Y)G(X)G(Y)G(X + Y + \lambda XY)^{-1}.$$

LEMMA 3.5. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $\lambda \in A$. Assume that λ is nilpotent. Let $F(X, Y) \in Z^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A}) \subset A[X, Y]^\times$. Then there exist $\boldsymbol{a} \in \hat{W}(A)$ and $G(T) = \prod_{k\notin P}(1 + c_kT^k) \in A[T]^\times$ such that*

$$F(X, Y) = F_p(\boldsymbol{a}, \lambda; X, Y)G(X)G(Y)G(X + Y + \lambda XY)^{-1}.$$

PROOF. As above, dividing $F(X, Y)$ by its constant term, we may assume that $F(X, Y) \equiv 1$ mod degree 1. By Lemma 3.4, there exist $\boldsymbol{a} = (a_i)_{i\geq 0} \in W(A)$ and $G(T) = \prod_{k\notin P}(1 + c_kT^k) \in A[[T]]^\times$ such that $F(X, Y) = F_p(\boldsymbol{a}; X, Y)G(X)G(Y)G(X + Y + \lambda XY)^{-1}$. We prove that $\boldsymbol{a} \in \hat{W}(A)$ and $G(T) \in A[T]^\times$.

Let d be the degree of $F(X, Y)$ and let $\mathfrak{a}$ denote the ideal of A generated by λ and the coefficients of $F(X, Y)$ except the constant. Since the polynomial $F(X, Y)$ is invertible, $\mathfrak{a}$ is nilpotent.

Now observe the following:

1) For $j \notin P$, put

$$(1 + c_jX^j)(1 + c_jY^j)\{1 + c_j(X + Y + \lambda XY)^j\}^{-1} = 1 + \sum_{k=1}^{\infty} H_k(X, Y),$$

where $H_k(X, Y)$ is homogeneous of degree jk. Then the ideal generated by the coefficients of $H_1(X, Y)$ coincides with (c_j), and the ideal generated by the coefficients of $H_k(X, Y)$ is contained in $(c_j, \lambda)^k$ for $k > 1$;

2) Put

$$F_p(\underbrace{0, \ldots, 0}_{i}, a_i, 0, \ldots, \lambda; X, Y) = 1 + \sum_{k=1}^{\infty} H_k(X, Y),$$

where $H_k(X, Y)$ is homogeneous of degree $p^{i+1}k$. Then the ideal generated by the coefficients of $H_1(X, Y)$ coincides with (a_i), and the ideal generated by the coefficients of $H_k(X, Y)$ is contained in $(a_i, \lambda)^k$ for $k > 1$.

These imply the following:

1) If j is not a power of p and $(s-1)d < j \leq sd$, then $c_j \in \mathfrak{a}^s$;

2) If $(s-1)d < p^{i+1} \leq sd$, then $a_i \in \mathfrak{a}^s$.

Hence, a_i and c_j are nilpotent for all i and j, and are zero for all but a finite number of i and j.

3.6. Now we prove the bijectivity of $\xi_A^1 : W(A)/(F - [\lambda^{p-1}]) \to H_0^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ and $\xi_A^1 : \hat{W}(A)/(F - [\lambda^{p-1}]) \to H_0^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$.

Lemma 3.4 and Lemma 3.5 imply the surjectivity of $\xi_A^1 : W(A)/(F - [\lambda^{p-1}]) \to H_0^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ and $\xi_A^1 : \hat{W}(A)/(F - [\lambda^{p-1}]) \to H_0^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$, respectively.

Now assume that $F_p(\boldsymbol{a}, \lambda; X, Y) \in B^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ for $\boldsymbol{a} \in W(A)$. Then there exsits $F(T) \in A[[T]]^\times$ such that

$$F(X)F(Y)F(X + Y + \lambda XY)^{-1} = F_p(\boldsymbol{a}, \lambda; X, Y).$$

Put $F(T) = \prod_{k \geq 1} E_p(c_k, \lambda; T^k)$. Then

$$F_p(\boldsymbol{a}, \lambda; X, Y)F_p((F - [\lambda^{p-1}])\boldsymbol{b}, \lambda; X, Y)^{-1} = \prod_{k \notin P} E_p(c_k, \lambda; X^k)E_p(c_k, \lambda; Y^k)E_p(c_k, \lambda; (X + Y + \lambda XY)^k)^{-1},$$

where $\boldsymbol{b} = (c_{p^r})_{r \geq 0}$. As in the proof of Lemma 3.1, we see that $c_k = 0$ if k is not a power of p, and hence $F_p(\boldsymbol{a}, \lambda; X, Y) = F_p((F - [\lambda^{p-1}])\boldsymbol{b}, \lambda; X, Y)$. It follows that $\xi_A^1 : W(A)/(F - [\lambda^{p-1}]) \to H_0^2(\hat{\mathcal{G}}^{(\lambda)}, \hat{\boldsymbol{G}}_{m,A})$ is injective. Similarly, it is seen that $\xi_A^1 : \hat{W}(A)/(F - [\lambda^{p-1}]) \to H_0^2(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A})$ is injective.

EXAMPLE 3.7. If $\lambda = 1$, $\mathcal{G}^{(\lambda)}$ is isomorphic to the multiplicative formal group $\hat{\boldsymbol{G}}_{m,A}$. Then $\mathrm{End}_{A\text{-gr}}\hat{\boldsymbol{G}}_{m,A}$ is isomorphic to $\mathrm{Ker}[F - 1 : W(A) \to W(A)]$.

If A is of characteristic p and $\mathrm{Spec}\, A$ is connected, $\mathrm{Ker}[F - 1 : W(A) \to W(A)]$ is isomorphic to $\boldsymbol{Z}_p = W(\boldsymbol{F}_p)$. Hence all the endomophisms of $\hat{\boldsymbol{G}}_{m,A} = \mathrm{Spf}\, A[[T]]$ are given by $T \mapsto E_p(\boldsymbol{a}, 1; T) - 1$ ($\boldsymbol{a} \in W(\boldsymbol{F}_p)$) when the formal group law of $\hat{\boldsymbol{G}}_{m,A}$ is given by $F(X, Y) = X + Y + XY$.

We conclude this section by giving a formula concerning a functorial isomorphism ξ^0.

REMARK 3.8. Put

$$A = \boldsymbol{Z}_{(p)}\left[\Lambda, M, \frac{p^n\Lambda}{M}, \frac{p^{n-1}\Lambda^p}{M}, \frac{p^{n-2}\Lambda^{p^2}}{M}, \ldots, \frac{p\Lambda^{p^{n-1}}}{M}, \frac{\Lambda^{p^n}}{M}\right].$$

We define a A-homomorphism of formal groups $\Psi_{p^n} : \hat{\mathcal{G}}^{(\Lambda)} \to \hat{\mathcal{G}}^{(M)}$ by

$$T \mapsto \frac{(1 + \Lambda T)^{p^n} - 1}{M} : A[[T]] \to A[[T]].$$

Let B be an A-algebra. Under the identifications

$$\mathrm{Hom}_{B\text{-gr}}(\hat{\mathcal{G}}^{(\Lambda)}, \hat{\boldsymbol{G}}_{m,B}) = W(B)^{F-[\Lambda^{p-1}]}$$

and

$$\mathrm{Hom}_{B\text{-gr}}(\hat{\mathcal{G}}^{(M)}, \hat{\boldsymbol{G}}_{m,B}) = W(B)^{F-[M^{p-1}]},$$

$\Psi_{p^n}^* : \mathrm{Hom}_{B\text{-gr}}(\hat{\mathcal{G}}^{(M)}, \hat{\boldsymbol{G}}_{m,B}) \to \mathrm{Hom}_{B\text{-gr}}(\hat{\mathcal{G}}^{(\Lambda)}, \hat{\boldsymbol{G}}_{m,B})$ is given by

$$\boldsymbol{a} \mapsto \sum_{k=1}^{n} \left\{ V^{k-1}\left[\frac{p^{n-k+1}\Lambda^{p^{k-1}}}{M}\right]\boldsymbol{a} - V^{k-1}\tilde{V}\left[\frac{p^{(n-k)p}\Lambda^{p^k}}{M}\right]\boldsymbol{a} \right\} + V^n\left[\frac{\Lambda^{p^n}}{M}\right]\boldsymbol{a}.$$

Indeed, let $\boldsymbol{a} \in W(B)^{F-[M^{p-1}]}$. By Corollary 1.8, $\mathrm{Ker}[F - [M^{p-1}] : W_A \to W_A]$ is flat over A. Therefore there exist a flat A-algebra $\tilde{B}$, a surjevtive homomorphism of A-algebras $\varphi : \tilde{B} \to B$ and $\tilde{\boldsymbol{a}} \in W(\tilde{B})^{F-[M^{p-1}]}$ such that $\varphi(\tilde{\boldsymbol{a}}) = \boldsymbol{a}$. Hence we may assume that B is flat over A.

Put now $A' = \boldsymbol{Z}_{(p)}[\Lambda, M, \Lambda/M, M/\Lambda]$ and $B' = B \otimes_A A'$. Then B is a subring of B'. Define an A'-homomorphism of formal groups $[M/\Lambda] : \hat{\mathcal{G}}^{(M)} \to \hat{\mathcal{G}}^{(\Lambda)}$ by

$$T \mapsto \frac{M}{\Lambda}T : A'[[T]] \to A'[[T]].$$

Then $[M/\Lambda]$ is an A'-isomorphism and $[M/\Lambda] \circ \Psi_{p^n} = p^n$. We have obtained a commutative diagram

$$\begin{array}{ccccc} W(B')^{F-[M^{p-1}]} & \xrightarrow{\Psi_{p^n}^*} & W(B')^{F-[\Lambda^{p-1}]} & \xrightarrow{[M/\Lambda]^*} & W(B')^{F-[M^{p-1}]} \\ \uparrow & & \uparrow & & \\ W(B)^{F-[M^{p-1}]} & \xrightarrow[\Psi_{p^n}^*]{} & W(B)^{F-[\Lambda^{p-1}]}. & & \end{array}$$

Note that

(1) $(p^n)^* = p^n : W(B')^{F-[M^{p-1}]} \to W(B')^{F-[M^{p-1}]}$, since

$$E_p\left(\boldsymbol{a}, M; \frac{(1+MT)^{p^n}-1}{M}\right) = E_p(\boldsymbol{a}, M; T)^{p^n} = E_p(p^n\boldsymbol{a}, M; T);$$

(2) $[M/\Lambda]^* = [M/\Lambda] : W(B')^{F-[\Lambda^{p-1}]} \to W(B')^{F-[M^{p-1}]}$, since

$$[M/\Lambda]^* E_p(\boldsymbol{a}, \Lambda; T) = E_p\left(\boldsymbol{a}, \Lambda; \frac{M}{\Lambda}T\right) = E_p([M/\Lambda]\boldsymbol{a}, M; T).$$

We have $F^k\boldsymbol{a} = [M^{p^k-1}]\boldsymbol{a}$ since $F\boldsymbol{a} = [M^{p-1}]\boldsymbol{a}$. Hence we obtain

$$
\begin{aligned}
&[M/\Lambda]\Bigg(\sum_{k=1}^{n}\left\{V^{k-1}\left[\frac{p^{n-k+1}\Lambda^{p^{k-1}}}{M}\right]\boldsymbol{a}-V^{k-1}\tilde{V}\left[\frac{p^{(n-k)p}\Lambda^{p^k}}{M}\right]\boldsymbol{a}\right\}+V^n\left[\frac{\Lambda^{p^n}}{M}\right]\boldsymbol{a}\Bigg)\\
&\quad=\sum_{k=1}^{n}\{V^{k-1}[p^{n-k+1}M^{p^{k-1}-1}]\boldsymbol{a}-V^{k-1}\tilde{V}[p^{(n-k)p}M^{p^k-1}]\boldsymbol{a}\}+V^n[M^{p^n-1}]\boldsymbol{a}\\
&\quad=\sum_{k=1}^{n}\{V^{k-1}[p^{n-k+1}]F^{k-1}\boldsymbol{a}-V^{k-1}[p^{n-k}]\tilde{V}F^k\boldsymbol{a}\}+V^nF^n\boldsymbol{a}\\
&\quad=\sum_{k=1}^{n}\{V^{k-1}[p^{n-k+1}]F^{k-1}\boldsymbol{a}-V^{k-1}[p^{n-k}]([p]-\tilde{p})F^{k-1}\boldsymbol{a}\}+V^nF^n\boldsymbol{a}\\
&\quad=\sum_{k=1}^{n}p^{n-k}V^{k-1}\tilde{p}F^{k-1}\boldsymbol{a}+V^nF^n\boldsymbol{a}=p^n\boldsymbol{a}\,.
\end{aligned}
$$

4. Application: A case of extensions of group schemes over a discrete valuation ring. In this section, we complete a study on extensions of group schemes over a discrete valuation ring, treated in the previous articles [9], [10] and [11]. In particular, we describe some functorial maps in terms of Witt vectors.

Throughout the section, A denotes a discrete valuation ring and $\mathfrak{m}$ (resp. k) the maximal ideal (resp. the residue field) of A. We denote by π a uniformizing parameter of A and by v the valuation of A normalized by $v(\pi)=1$, if there are no restrictions. We refer to relevant results of [9, 10, 11].

4.1. Let $\lambda, \mu \in \mathfrak{m}-\{0\}$. Put $n=v(\mu)$ and $A_0=A/\mathfrak{m}^n$. Let $F(T)\in A[T]$, satisfying

1) $F(0)\equiv 1 \mod \mu$; 2) $F(X)F(Y)\equiv F(X+Y+\lambda XY) \mod \mu$.

We define a smooth affine group scheme $\mathcal{E}^{(\lambda,\mu;F)}$ over A as follows:

$$
\mathcal{E}^{(\lambda,\mu;F)}=\operatorname{Spec} A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right]
$$

with

1) multiplication:

$$
\begin{aligned}
&T_0\mapsto \lambda T_0\otimes T_0+T_0\otimes 1+1\otimes T_0\,,\\
&T_1\mapsto \mu T_1\otimes T_1+T_1\otimes F(T_0)+F(T_0)\otimes T_1\\
&\qquad+\frac{1}{\mu}[F(T_0)\otimes F(T_0)-F(\lambda T_0\otimes T_0+T_0\otimes 1+1\otimes T_0)]\,;
\end{aligned}
$$

2) unit:

$$
T_0\mapsto 0\,,\quad T_1\mapsto \frac{1}{\mu}[1-F(0)]\,;
$$

3) inverse:

$$T_0 \mapsto -\frac{T_0}{\lambda T_0 + 1}, \quad T_1 \mapsto \frac{1}{\mu}\left[\frac{1}{\mu T_1 + F(T_0)} - F\left(-\frac{T_0}{\lambda T_0 + 1}\right)\right].$$

A homomorphism of group A-schemes

$$\alpha^{(\lambda,\mu;F)} : \mathcal{E}^{(\lambda,\mu;F)} = \operatorname{Spec} A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right]$$
$$\to (\boldsymbol{G}_{m,A})^2 = \operatorname{Spec} A[U_0, U_0^{-1}, U_1, U_1^{-1}]$$

is defined by

$$(U_0, U_1) \mapsto (1+\lambda T_0, F(T_0)+\mu T_1) :$$
$$A\left[U_0, \frac{1}{U_0}, U_1, \frac{1}{U_1}\right] \to A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right].$$

The generic fiber $\alpha_K^{(\lambda,\mu;F)}$ is an isomorphism.

Moreover, we define a homomorphism of group schemes

$$\mathcal{G}^{(\mu)} = \operatorname{Spec} A\left[T, \frac{1}{1+\mu T}\right] \to \mathcal{E}^{(\lambda,\mu;F)} = \operatorname{Spec} A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right]$$

by

$$T_0 \mapsto 0, \ T_1 \mapsto T + \frac{1}{\mu}[1 - F(0)] : A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right] \to A\left[T, \frac{1}{1+\mu T}\right]$$

and a homomorphism

$$\mathcal{E}^{(\lambda,\mu;F)} = \operatorname{Spec} A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right] \to \mathcal{G}^{(\lambda)} = \operatorname{Spec} A\left[T, \frac{1}{1+\lambda T}\right]$$

by

$$T \mapsto T_0 : A\left[T, \frac{1}{1+\lambda T}\right] \to A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right].$$

Then the sequence of group schemes

$$0 \to \mathcal{G}^{(\mu)} \to \mathcal{E}^{(\lambda,\mu;F)} \to \mathcal{G}^{(\lambda)} \to 0$$

is exact.

$F \mapsto [\mathcal{E}^{(\lambda,\mu;F)}]$ gives rise to a surjective homomorphism

$$\partial : \operatorname{Hom}_{A_0\text{-gr}}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A_0}) \to \operatorname{Ext}^1_A(\mathcal{G}^{(\lambda)}, \mathcal{G}^{(\mu)}),$$

and $\operatorname{Ker}\partial$ is generated by the class of $1 + \lambda T$. (Cf. [9, Sect.3], [11, II.1.2])

4.2. We purchase the homomorphism

$$\partial : {}_{F(\lambda)}\hat{W}(A_0) \xrightarrow{\sim} \operatorname{Hom}_{A_0\text{-gr}}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A_0}) \to \operatorname{Ext}^1_A(\mathcal{G}^{(\lambda)}, \mathcal{G}^{(\mu)}).$$

Let $\boldsymbol{a} \in \hat{W}(A_0)^{F-[\lambda^{p-1}]}$. Then $E_p(\boldsymbol{a}, \lambda; T) \in A_0[T]$ and we have

$$E_p(\boldsymbol{a}, \lambda; 0) = 1 \quad \text{and} \quad E_p(\boldsymbol{a}, \lambda; X)E_p(\boldsymbol{a}, \lambda; Y) = E_p(\boldsymbol{a}, \lambda; X + Y + \lambda XY).$$

Then, if we take a lifting $F(T) \in A[T]$ of $E_p(\boldsymbol{a}, \lambda; T)$, we have

$$F(0) \equiv 1 \mod \mu$$

and

$$F(X)F(Y) \equiv F(X + Y + \lambda XY) \mod \mu .$$

The class $[\mathcal{E}^{(\lambda,\mu;F)}] \in \mathrm{Ext}^1_A(\mathcal{G}^{(\lambda)}, \mathcal{G}^{(\mu)})$ depends only on $\boldsymbol{a}$. Moreover, let $\tilde{\boldsymbol{a}} \in W(A)$ be a lifting of $\boldsymbol{a} \in W(A_0)$. Then

$$F(T) \equiv E_p(\tilde{\boldsymbol{a}}, \lambda; T) \mod \mu .$$

4.3. Let m be an integer with $1 \leq m \leq \min(v(\lambda), v(\mu))$, and let A_1 denote the residue ring $A/\mathfrak{m}^m$. Let $F(T) \in A[T]$, satisfying $F(0) \equiv 1 \mod \mu$ and $F(X)F(Y) \equiv F(X + Y + \lambda XY) \mod \mu$. We denote also by $F(T)$ the reduction of $F(T)$ modulo $\mathfrak{m}^m$. Then $F(T) \in (A_1[T])^\times$, and $T \mapsto F(T)$ defines a character of $\boldsymbol{G}_{a,A_1}$. Moreover, the fiber $\mathcal{E}^{(\lambda,\mu;F)}_{A_1}$ is a commutative extension of $\boldsymbol{G}_{a,A_1}$ by $\boldsymbol{G}_{a,A_1}$. The multiplication of $\mathcal{E}^{(\lambda,\mu;F)}_{A_1} = \mathrm{Spec}\, A_1[T_0, T_1]$ is given by

$$T_0 \mapsto T_0 \otimes 1 + 1 \otimes T_0 , \quad T_1 \mapsto T_1 \otimes F(T_0) + F(T_0) \otimes T_1 + G(T_0 \otimes 1, 1 \otimes T_0) ,$$

where $G(X, Y)$ denotes the reduction of $[F(X)F(Y) - F(\lambda XY + X + Y)]/\mu$ modulo $\mathfrak{m}^m$.

Put

$$C(X, Y) = \frac{G(X, Y)}{F(X)F(Y)} \in A_1[X, Y] .$$

Then $C(X, Y)$ is a symmetric 2-cocycle in $Z^2(\boldsymbol{G}_{a,A_1}, \boldsymbol{G}_{a,A_1})$. Define a group scheme $\mathcal{E} = \mathrm{Spec}\, A_1[T_0, T_1]$ with the multiplication

$$T_0 \mapsto T_0 \otimes 1 + 1 \otimes T_0 , \quad T_1 \mapsto T_1 \otimes 1 + 1 \otimes T_1 + C(T_0 \otimes 1, 1 \otimes T_0) .$$

It is easily verified that $(T_0, T_1) \mapsto (T_0, F(T_0)^{-1}T_1) : A_1[T_0, T_1] \to A_1[T_0, T_1]$ defines an isomorphism $\mathcal{E}^{(\lambda,\mu;F)}_{A_1} \xrightarrow{\sim} \mathcal{E}$ of extensions of $\boldsymbol{G}_{a,A_1}$ by $\boldsymbol{G}_{a,A_1}$.

Assume now that the residue field of A is of characteristic $p > 0$. As is well-known, $\mathrm{Ext}^1_k(\boldsymbol{G}_{a,A_1}, \boldsymbol{G}_{a,A_1}) = H^2_0(\boldsymbol{G}_{a,A_1}, \boldsymbol{G}_{a,A_1})$ is generated by 2-cocycles

$$C_k(X, Y) = \frac{X^{p^k} + Y^{p^k} - (X + Y)^{p^k}}{p} \quad (k \geq 1)$$

as an A_1-module. (Cf. [2, Ch.II,Th.4.6])

Let $\boldsymbol{a} \in W(A_0)^{F-[\lambda^{p-1}]}$. Let $F(T) \in A[T]$ be a lifting of $E_p(\boldsymbol{a}, \lambda; T) \in A_0[T]$, and $\tilde{\boldsymbol{a}} \in W(A)$ a lifting of $\boldsymbol{a}$. Put

$$(\tilde{F}_0(\boldsymbol{a}), \tilde{F}_1(\boldsymbol{a}), \tilde{F}_2(\boldsymbol{a}), \dots) = (F - [\Lambda^{p-1}])\boldsymbol{a} \in W(A_0) .$$

Then, by the assumption,

$$\tilde{F}_k(\tilde{\boldsymbol{a}}) \equiv 0 \mod \mathfrak{m}^n$$

for each $k \geq 0$. With these notations, we have:

PROPOSITION 4.3.1. $[\mathcal{E}_{A_1}^{(\lambda,\mu;F)}] \in H_0^2(\boldsymbol{G}_{a,A_1}, \boldsymbol{G}_{a,A_1})$ *coincides with the class of*

$$\sum_{k=1}^{\infty} \frac{\tilde{F}_{k-1}(\tilde{\boldsymbol{a}})}{\mu} C_k(X, Y) .$$

The assertion follows immediately from the following lemma.

LEMMA 4.4. *Let* $B = \boldsymbol{Z}_{(p)}[\Pi]$, $\Lambda \in B$ *and* $\boldsymbol{U} = (U_0, U_1, U_2, \dots) \in W(B)$. *Put*

$$(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \tilde{F}_2(\boldsymbol{U}), \dots) = (F - [\Lambda^{p-1}])\boldsymbol{U} \in W(\boldsymbol{Z}[U_0, U_1, U_2, \dots, \Lambda]) .$$

Let m, n *be integers with* $1 \leq m \leq n$. *Assume that*

(1) $\Lambda \equiv 0 \mod \Pi^m$; (2) $\tilde{F}_k(\boldsymbol{U}) \equiv 0 \mod \Pi^n$ *for all* $k \geq 0$.

Then

$$1 - \frac{E_p(\boldsymbol{U}, \Lambda; X + Y + \Lambda XY)}{E_p(\boldsymbol{U}, \Lambda; X) E_p(\boldsymbol{U}, \Lambda; Y)} \equiv \sum_{k=1}^{\infty} \tilde{F}_{k-1}(\boldsymbol{U}) \frac{X^{p^k} + Y^{p^k} - (X + Y)^{p^k}}{p} \mod \Pi^{n+m} .$$

PROOF. By the assumption (2), we have

$$\begin{aligned} &\Phi_{k-1}(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \dots, \tilde{F}_{k-1}(\boldsymbol{U})) \\ &\quad = \tilde{F}_0(\boldsymbol{U})^{p^{k-1}} + p\tilde{F}_1(\boldsymbol{U})^{p^{k-2}} + \cdots + p^{k-1}\tilde{F}_{k-1}(\boldsymbol{U}) \\ &\quad \equiv p^{k-1}\tilde{F}_{k-1}(\boldsymbol{U}) \mod \Pi^{n+m} . \end{aligned}$$

Hence, by the assumption (1), we obtain

$$\begin{aligned} &(1+\Lambda^{p^k} T^{p^k})^{\Phi_{k-1}(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \dots, \tilde{F}_{k-1}(\boldsymbol{U}))/p^k \Lambda^{p^k}} \\ &\quad \equiv 1 + \frac{1}{p^k} \Phi_{k-1}(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \dots, \tilde{F}_{k-1}(\boldsymbol{U})) T^{p^k} \\ &\quad \equiv 1 + \tilde{F}_{k-1}(\boldsymbol{U}) \frac{T^{p^k}}{p} \mod \Pi^{n+m} . \end{aligned}$$

Therefore we have

$$\begin{aligned} &E_p(\boldsymbol{U}, \Lambda; T) \\ &\quad = (1 + \Lambda T)^{U_0/\Lambda} \prod_{k=1}^{\infty} (1 + \Lambda^{p^k} T^{p^k})^{\Phi_{k-1}(\tilde{F}_0(\boldsymbol{U}), \tilde{F}_1(\boldsymbol{U}), \dots, \tilde{F}_{k-1}(\boldsymbol{U}))/p^k \Lambda^{p^k}} \\ &\quad \equiv (1 + \Lambda T)^{U_0/\Lambda} \prod_{k=1}^{\infty} \left(1 + \tilde{F}_{k-1}(\boldsymbol{U}) \frac{T^{p^k}}{p}\right) \\ &\quad \equiv (1 + \Lambda T)^{U_0/\Lambda} \left(1 + \sum_{k=1}^{\infty} \tilde{F}_{k-1}(\boldsymbol{U}) \frac{T^{p^k}}{p}\right) \mod \Pi^{n+m} , \end{aligned}$$

and hence, again by the assumtions (1) and (2),

$$1-\frac{E_p(\boldsymbol{U}, \Lambda; X+Y+\Lambda XY)}{E_p(\boldsymbol{U}, \Lambda; X)E_p(\boldsymbol{U}, \Lambda; Y)}$$

$$\equiv 1-\frac{1+\sum_{k=1}^{\infty}\tilde{F}_{k-1}(\boldsymbol{U})\dfrac{(X+Y+\Lambda XY)^{p^k}}{p}}{\left(1+\sum_{k=1}^{\infty}\tilde{F}_{k-1}(\boldsymbol{U})\dfrac{X^{p^k}}{p}\right)\left(1+\sum_{k=1}^{\infty}\tilde{F}_{k-1}(\boldsymbol{U})\dfrac{Y^{p^k}}{p}\right)}$$

$$\equiv \sum_{k=1}^{\infty}\tilde{F}_{k-1}(\boldsymbol{U})\frac{X^{p^k}+Y^{p^k}-(X+Y+\Lambda XY)^{p^k}}{p}$$

$$\equiv \sum_{k=1}^{\infty}\tilde{F}_{k-1}(\boldsymbol{U})\frac{X^{p^k}+Y^{p^k}-(X+Y)^{p^k}}{p}=\sum_{k=1}^{\infty}\tilde{F}_{k-1}(\boldsymbol{U})C_k(X,Y) \mod \Pi^{n+m}.$$

4.5. Let $\lambda, \lambda', \mu \in \mathfrak{m}-\{0\}$. Assume that $p^{n-k}\lambda'^{p^k}$ $(0 \le k \le n)$ are divisible by λ. Then

$$T \mapsto \frac{(\lambda' T+1)^{p^n}-1}{\lambda} : A\left[T, \frac{1}{1+\lambda T}\right] \to A\left[T, \frac{1}{1+\lambda' T}\right]$$

defines an A-homomorphism

$$\Psi_{p^n} : \mathcal{G}^{(\lambda')} = \operatorname{Spec} A\left[T, \frac{1}{1+\lambda' T}\right] \to \mathcal{G}^{(\lambda)} = \operatorname{Spec} A\left[T, \frac{1}{1+\lambda T}\right].$$

Let $F(T) \in A[T]$ and

$$F'(T) = F\left(\frac{(\lambda' T+1)^{p^n}-1}{\lambda}\right).$$

If $F(T)$ satisfies

(1) $F(0) \equiv 1 \mod \mu$; (2) $F(X)F(Y) \equiv F(X+Y+\lambda XY) \mod \mu$,

then $F'(T)$ satisfies

(1) $F'(0) \equiv 1 \mod \mu$; (2) $F'(X)F'(Y) \equiv F'(X+Y+\lambda' XY) \mod \mu$.

Define an A-homomorphism

$$\widetilde{\Psi_{p^n}} : \mathcal{E}^{(\lambda', \mu; F')} = \operatorname{Spec} A\left[T_0, T_1, \frac{1}{1+\lambda' T_0}, \frac{1}{F'(T_0)+\mu T_1}\right]$$

$$\to \mathcal{E}^{(\lambda, \mu; F)} = \operatorname{Spec} A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right]$$

by

$$T_0 \mapsto \frac{(\lambda' T_0+1)^{p^n}-1}{\lambda}, \quad T_1 \mapsto T_1 :$$

$$A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right] \to A\left[T_0, T_1, \frac{1}{1+\lambda' T_0}, \frac{1}{F'(T_0)+\mu T_1}\right].$$

Then we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{G}^{(\mu)} & \longrightarrow & \mathcal{E}^{(\lambda',\mu;F')} & \longrightarrow & \mathcal{G}^{(\lambda')} & \longrightarrow & 0 \\ & & \| & & \downarrow \widetilde{\Psi_{p^n}} & & \downarrow \Psi_{p^n} & & \\ 0 & \longrightarrow & \mathcal{G}^{(\mu)} & \longrightarrow & \mathcal{E}^{(\lambda,\mu;F)} & \longrightarrow & \mathcal{G}^{(\lambda)} & \longrightarrow & 0. \end{array}$$

We have $\Psi_{p^n}^*[\mathcal{E}^{(\lambda,\mu;F)}] = [\mathcal{E}^{(\lambda',\mu;F')}]$ in $\mathrm{Ext}_A^1(\mathcal{G}^{(\lambda')}, \mathcal{G}^{(\mu)})$. Since $F' = F \circ \Psi_{p^n} : \mathcal{G}^{(\lambda')} \to \mathcal{G}^{(\lambda')} \to \boldsymbol{G}_{m,A_0}$, we have a commutative diagram

$$\begin{array}{ccccc} W(A_0)^{F-[\lambda^{p-1}]} & \xrightarrow{\sim} & \mathrm{Hom}_{A_0}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A_0}) & \xrightarrow{\partial} & \mathrm{Ext}_A^1(\mathcal{G}^{(\lambda)}, \mathcal{G}^{(\mu)}) \\ \downarrow \Psi_{p^n}^* & & \downarrow \Psi_{p^n}^* & & \downarrow \Psi_{p^n}^* \\ W(A_0)^{F-[\lambda'^{p-1}]} & \xrightarrow{\sim} & \mathrm{Hom}_{A_0}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A_0}) & \xrightarrow{\partial} & \mathrm{Ext}_A^1(\mathcal{G}^{(\lambda')}, \mathcal{G}^{(\mu)}). \end{array}$$

Here by 3.8,

$$\Psi_{p^n}^*(\boldsymbol{a}) = \sum_{k=1}^{n} \left\{ V^{k-1}\left[\frac{p^{n-k+1}\lambda'^{p^{k-1}}}{\lambda}\right]\boldsymbol{a} - V^{k-1}\tilde{V}\left[\frac{p^{(n-k)p}\lambda'^{p^k}}{\lambda}\right]\boldsymbol{a} \right\} + V^n\left[\frac{\lambda'^{p^n}}{\lambda}\right]\boldsymbol{a}.$$

4.6. Let $\lambda, \mu, \mu' \in \mathfrak{m} - \{0\}$. Assume that $p^{n-k}\mu^{p^k}$ $(0 \le k \le n)$ are divisible by μ'. Then

$$T \mapsto \frac{(\mu T + 1)^{p^n} - 1}{\lambda} : A\left[T, \frac{1}{1+\mu' T}\right] \to A\left[T, \frac{1}{1+\mu T}\right]$$

defines an A-homomorphism

$$\Psi_{p^n} : \mathcal{G}^{(\mu)} = \mathrm{Spec}\, A\left[T, \frac{1}{1+\mu T}\right] \to \mathcal{G}^{(\mu')} = \mathrm{Spec}\, A\left[T, \frac{1}{1+\mu' T}\right].$$

Let $F(T) \in A[T]$ and $F'(T) = F(T)^{p^n}$. If $F(T)$ satisfies

(1) $F(0) \equiv 1 \mod \mu$; (2) $F(X)F(Y) \equiv F(X + Y + \lambda XY) \mod \mu$,

then $F'(T)$ satisfies

(1) $F'(0) \equiv 1 \mod \mu'$; (2) $F'(X)F'(Y) \equiv F'(X + Y + \lambda' XY) \mod \mu'$.

Define an A-homomorphism

$$\widetilde{\Psi_{p^n}} : \mathcal{E}^{(\lambda,\mu;F)} = \mathrm{Spec}\, A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right]$$
$$\to \mathcal{E}^{(\lambda,\mu';F')} = \mathrm{Spec}\, A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F'(T_0)+\mu' T_1}\right]$$

by

$$T_0 \mapsto T_0, \quad T_1 \mapsto \frac{(\mu T_1 + F(T_0))^{p^n} - F(T_0)^{p^n}}{\mu'} :$$
$$A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F'(T_0)+\mu' T_1}\right] \to A\left[T_0, T_1, \frac{1}{1+\lambda T_0}, \frac{1}{F(T_0)+\mu T_1}\right].$$

Then we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{G}^{(\mu)} & \longrightarrow & \mathcal{E}^{(\lambda,\mu;F)} & \longrightarrow & \mathcal{G}^{(\lambda)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \Psi_{p^n}} & & \downarrow{\scriptstyle \widetilde{\Psi_{p^n}}} & & \| & & \\ 0 & \longrightarrow & \mathcal{G}^{(\mu')} & \longrightarrow & \mathcal{E}^{(\lambda,\mu';F')} & \longrightarrow & \mathcal{G}^{(\lambda)} & \longrightarrow & 0. \end{array}$$

We have $\Psi_{p^n *}[\mathcal{E}^{(\lambda,\mu;F)}] = [\mathcal{E}^{(\lambda,\mu';F')}]$ in $\mathrm{Ext}^1_A(\mathcal{G}^{(\lambda)}, \mathcal{G}^{(\mu')})$.

Put $A_0 = A/(\mu)$ and $A_1 = A/(\mu')$. Let $\boldsymbol{a} \in W(A_0)$ and $\tilde{\boldsymbol{a}} \in W(A)$ a lifting of $\boldsymbol{a}$. Then the image of $p^n\tilde{\boldsymbol{a}}$ in $W(A_1)$ depends only on $\boldsymbol{a}$. Hence $\boldsymbol{a} \mapsto p^n\tilde{\boldsymbol{a}} \mod \mu'$ gives rise to a homomorphism $p^n : W(A_0) \to W(A_1)$. Since $E_p(\tilde{\boldsymbol{a}}, \lambda; T)^{p^n} = E_p(p^n\tilde{\boldsymbol{a}}, \lambda; T)$, we have a commutative diagram

$$\begin{array}{ccccc} W(A_0)^{F-[\lambda^{p-1}]} & \xrightarrow{\sim} & \mathrm{Hom}_{A_0}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A_0}) & \xrightarrow{\partial} & \mathrm{Ext}^1_A(\mathcal{G}^{(\lambda)}, \mathcal{G}^{(\mu)}) \\ \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle \Psi_{p^n *}} \\ W(A_1)^{F-[\lambda^{p-1}]} & \xrightarrow{\sim} & \mathrm{Hom}_{A_1}(\mathcal{G}^{(\lambda)}, \boldsymbol{G}_{m,A_1}) & \xrightarrow{\partial} & \mathrm{Ext}^1_A(\mathcal{G}^{(\lambda)}, \mathcal{G}^{(\mu')}). \end{array}$$

5. Kummer-Artin-Schreier-Witt theory of degree p^2. We conclude this article by giving an explicit description of the Kummer-Artin-Schreier-Witt theory of degree p^2.

5.1. Let ζ_2 be a primitive p^2-th root of unity, and put $\zeta = \zeta_2^p$, $\lambda = \zeta - 1$, $\lambda_2 = \zeta_2 - 1$ and $A = \boldsymbol{Z}_{(p)}[\zeta_2]$. Then A is a disctrete valuation ring and λ_2 is a uniformizing parameter of A. Let v denote the valuation of A normalized by $v(\lambda_2) = 1$. Then we have $v(\lambda) = p$ and $v(p) = p(p-1)$. We put $A_0 = A/(\lambda)$ and $A_1 = A/(\lambda^p)$. Put

$$\eta = \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k}\lambda_2^k \quad \text{and} \quad \tilde{\eta} = \frac{\lambda^{p-1}}{p}(p\eta - \lambda).$$

Then we have $v(\eta) = v(\lambda_2)$ and $v(\tilde{\eta}) = v(\lambda)$.

Put

$$F(T) = \sum_{k=0}^{p-1} \frac{(\eta T)^k}{k!}, \quad G(T) = \sum_{k=0}^{p-1} \frac{(\tilde{\eta} T)^k}{k!},$$

$$\Lambda_0^F(X_0, Y_0) = \lambda X_0 Y_0 + X_0 + Y_0, \quad \Lambda_0^G(X_0, Y_0) = \lambda^p X_0 Y_0 + X_0 + Y_0,$$

$$\begin{aligned} \Lambda_1^F(X_0, X_1, Y_0, Y_1) &= \lambda X_1 Y_1 + X_1 F(Y_0) + F(X_0) Y_0 \\ &\quad + \frac{1}{\lambda}[F(X_0)F(Y_0) - F(\lambda X_0 Y_0 + X_0 + Y_0)], \\ \Lambda_1^G(X_0, X_1, Y_0, Y_1) &= \lambda^p X_1 Y_1 + X_1 G(Y_0) + G(X_0) Y_0 \\ &\quad + \frac{1}{\lambda^p}[G(X_0)G(Y_0) - G(\lambda^p X_0 Y_0 + X_0 + Y_0)], \end{aligned}$$

$$\Psi_0(T_0) = \frac{(\lambda T_0 + 1)^p - 1}{\lambda^p},$$

$$\Psi_1(T_0, T_1) = \frac{1}{\lambda^p}\left[\frac{\{\lambda T_1 + F(T_0)\}^p}{\lambda T_0 + 1} - G\left(\frac{(\lambda T_0 + 1)^p - 1}{\lambda^p}\right)\right],$$

$$\mathcal{W}_2 = \operatorname{Spec} A\left[T_0, T_1, \frac{1}{\lambda T_0 + 1}, \frac{1}{\lambda T_1 + F(T_0)}\right],$$

$$\mathcal{V}_2 = \operatorname{Spec} A\left[T_0, T_1, \frac{1}{\lambda^p T_0 + 1}, \frac{1}{\lambda^p T_1 + G(T_0)}\right].$$

THEOREM 5.2. *With the above notation*:

(1) *The polynomials* $\Lambda_1^F(X_0, X_1, Y_0, Y_1)$, $\Lambda_1^G(X_0, X_1, Y_0, Y_1)$ *have their coefficients in A. Moreover,*

$$(T_0, T_1) \mapsto (\Lambda_0^F(T_0 \otimes 1, 1 \otimes T_0), \Lambda_1^F(T_0 \otimes 1, T_1 \otimes 1, 1 \otimes T_0, 1 \otimes T_1))$$

defines a structure of group on $\mathcal{W}_2$, *and*

$$(T_0, T_1) \mapsto (\Lambda_0^G(T_0 \otimes 1, 1 \otimes T_0), \Lambda_1^G(T_0 \otimes 1, T_1 \otimes 1, 1 \otimes T_0, 1 \otimes T_1))$$

defines a structure of group on $\mathcal{V}_2$.

(2) *The fraction* $\Psi_1(T_0, T_1)$ *belongs to* $A\left[T_0, T_1, 1/(\lambda T_0 + 1), 1/(\lambda T_1 + F(T_0))\right]$. *Moreover,*

$$(T_0, T_1) \mapsto (\Psi_0(T_0), \Psi_1(T_0, T_1))$$

defines an A-homomorphism $\Psi : \mathcal{W}_2 \to \mathcal{V}_2$, *and* $Ker[\Psi : \mathcal{W}_2 \to \mathcal{V}_2]$ *is isomorphic to the constant group scheme* $\mathbf{Z}/p^2\mathbf{Z}$.

(3) $(U_0, U_1) \mapsto (\lambda T_0 + 1, \lambda T_1 + F(T_0))$ *defines a homomorphism* $\alpha^{(F)} : \mathcal{W}_2 \to (\boldsymbol{G}_{m,A})^2$ *of group schemes over A, and* $(U_0, U_1) \mapsto (\lambda^p T_0 + 1, \lambda^p T_1 + G(T_0))$ *defines a homomorphism* $\alpha^{(G)} : \mathcal{V}_2 \to (\boldsymbol{G}_{m,A})^2$ *of group schemes over A. Moreover,* $\alpha_K^{(F)} : \mathcal{W}_{2,K} \to (\boldsymbol{G}_{m,K})^2$ *and* $\alpha_K^{(G)} : \mathcal{V}_{2,K} \to (\boldsymbol{G}_{m,K})^2$ *are isomorphisms.*

(4) *The diagram of group schemes over A*

$$\begin{array}{ccc} \mathcal{W}_2 & \xrightarrow{\Psi} & \mathcal{V}_2 \\ {\scriptstyle \alpha^{(F)}}\downarrow & & \downarrow{\scriptstyle \alpha^{(G)}} \\ (\boldsymbol{G}_{m,A})^2 & \xrightarrow{\Theta} & (\boldsymbol{G}_{m,A})^2 \end{array}$$

is commutative. Here Θ *is defined by*

$$(U_0, U_1) \mapsto (U_0^p, U_0^{-1}U_1^p).$$

(5) *The closed fiber of the exact sequence of group schemes over A*

$$0 \longrightarrow \mathbf{Z}/p^2\mathbf{Z} \longrightarrow \mathcal{W}_2 \xrightarrow{\Psi} \mathcal{V}_2 \longrightarrow 0$$

is isomorphic to the Artin-Schreier-Witt sequence

$$0 \longrightarrow \mathbf{Z}/p^2\mathbf{Z} \longrightarrow W_2 \xrightarrow{F-1} W_2 \longrightarrow 0.$$

EXAMPLE 5.3. We can verify the assertions directly in the case of $p = 2$. Indeed, we have

$$\zeta = -1\,, \quad \zeta_2 = i\,, \quad \lambda = -2\,, \quad \eta = \lambda_2 = i - 1\,, \quad \tilde{\eta} = -2i$$

and

$$\begin{aligned}
\Lambda_0^F(X_0, Y_0) &= -2X_0Y_0 + X_0 + Y_0\,, \quad \Lambda_0^G(X_0, Y_0) = 4X_0Y_0 + X_0 + Y_0\,,\\
\Lambda_1^F(X_0, Y_0, X_1, Y_1) &= -2X_1Y_1 + X_1\{1 + (i-1)Y_0\} + \{1 + (i-1)X_0\}Y_1 + X_0Y_0\,,\\
\Lambda_1^G(X_0, Y_0, X_1, Y_1) &= 4X_1Y_1 + X_1(1 - 2iY_0) + (1 - 2iX_0)Y_1 + (-1 + 2i)X_0Y_0\,,\\
\Psi_0(T_0) &= T_0^2 - T_0\,,\\
\Psi_1(T_0, T_1) &= \frac{T_1^2 - T_1 + iT_0^2 - iT_0^3 - (i-1)T_0T_1}{-2T_0 + 1}\,.
\end{aligned}$$

Taking the reductions modulo λ_2, we obtain

$$\begin{aligned}
\Lambda_0^F(X_0, Y_0) &= X_0 + Y_0\,, \quad \Lambda_1^F(X_0, Y_0, X_1, Y_1) = X_1 + Y_1 + X_0Y_0\,,\\
\Lambda_0^G(X_0, Y_0) &= X_0 + Y_0\,, \quad \Lambda_1^G(X_0, Y_0, X_1, Y_1) = X_1 + Y_1 + X_0Y_0\,,\\
\Psi_0(T_0) &= T_0^2 - T_0\,, \quad \Psi_1(T_0, T_1) = T_1^2 + T_1 + T_0^2 + T_0^3\,.
\end{aligned}$$

Then it is seen without difficulty that $\Phi : \mathcal{W}_2 \to \mathcal{V}_2$ is well defined and the closed fiber of

$$0 \to \mathbf{Z}/p^2\mathbf{Z} \to \mathcal{W}_2 \to \mathcal{V}_2 \to 0$$

is isomorphic to the Artin-Schreier-Witt sequence

$$0 \to \mathbf{Z}/p^2\mathbf{Z} \to W_{2,\mathbf{F}_p} \to W_{2,\mathbf{F}_p} \to 0\,.$$

5.4. Hereafter we will prove the thoerem in the case of $p > 2$. Now *we assume that* $p > 2$. The assertion (1) is a consequence of the congruence relations

$$F(X)F(Y) \equiv F(X + Y + \lambda XY) \mod \lambda$$

and

$$G(X)G(Y) \equiv G(X + Y + \lambda^p XY) \mod \lambda^p\,,$$

which follow from the divisibilities $\lambda \mid \eta^p$ and $\lambda^p \mid \tilde{\eta}^p$. $\mathcal{W}_2$ or $\mathcal{V}_2$ is nothing but $\mathcal{E}^{(\lambda,\lambda;F)}$ or $\mathcal{E}^{(\lambda^p,\lambda^p;G)}$ respectively in the notation of Section 4. The assertrions (3) and (4) are easily verified.

First we establish some congruence relations among λ, λ_2, η and $\tilde{\eta}$ to prove the assertions (2) and (5).

LEMMA 5.5. *Let A be a $\mathbf{Z}_{(p)}$-algebra and $a \in A$. Then*

$$\sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} a^k \equiv \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} a^k \mod pa^2\,.$$

PROOF. By the following sublemma,

$$\frac{1}{p}\binom{p}{k}a^k \equiv \frac{(-1)^{k-1}}{k}a^k \mod pa^2$$

for $2 \leq k \leq p-1$. Hence we obtain

$$\sum_{k=1}^{p-1}\frac{1}{p}\binom{p}{k}a^k = a + \sum_{k=2}^{p-1}\frac{1}{p}\binom{p}{k}a^k \equiv a + \sum_{k=2}^{p-1}\frac{(-1)^{k-1}}{k}a^k$$
$$= \sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}a^k \mod pa^2.$$

SUBLEMMA 5.5.1. *For* $2 \leq k \leq p-1$,

$$\frac{1}{p}\binom{p}{k} \equiv \frac{(-1)^{k-1}}{k} \mod p.$$

PROOF. In fact,

$$\frac{1}{p}\binom{p}{k} = \frac{1}{p}\frac{p(p-1)\cdots(p-k+1)}{k!} \equiv (-1)^{k-1}\frac{(k-1)!}{k!} \mod p.$$

LEMMA 5.6. *With the above notation,*

(1) $\eta \equiv \dfrac{\lambda - \lambda_2^p}{p} \mod p$,

(2) $\lambda \equiv \lambda_2^p + p\eta \mod \lambda^p$,

(3) $\lambda^k \equiv \lambda_2^{pk} \mod \lambda^p$ *for* $k \geq 2$.

PROOF. By Lemma 5.5,

$$\eta = \sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\lambda_2^k \equiv \frac{(\lambda_2+1)^p - \lambda_2^p - 1}{p} \mod p\lambda_2^2.$$

We obtain the assertions, noting that $(\lambda_2+1)^p - 1 = \lambda$ and that $\lambda^{p-1} \mid p$, $\lambda \mid \lambda_2^p$.

LEMMA 5.7. *We have a congruence*

$$\eta^p \equiv \sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\lambda_2^{pk} \equiv \sum_{k=1}^{p-1}\frac{1}{p}\binom{p}{k}\lambda_2^{pk} \mod \lambda^p.$$

PROOF. By the definition,

$$\eta = \sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\lambda_2^k.$$

Then we obtain

$$\eta^p \equiv \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \lambda_2^{pk} \mod \lambda^p,$$

noting that $\lambda^p \mid p\lambda_2^p$ and that $\{(-1)^{k-1}/k\}^p \equiv (-1)^{k-1}/k \mod p$. Moreover, it follows from Lemma 5.5 that

$$\sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \lambda_2^{pk} \equiv \sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} \lambda_2^{pk} \mod p\lambda_2^{2p}.$$

Hence we obtain the result.

LEMMA 5.8. *We have an equality*

$$\frac{\lambda^{p-1}}{p} = -\sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} \lambda^{k-1}.$$

PROOF. Develop and divide by $p\lambda$ the right hand side of $\lambda^p = \lambda^p + 1 - (\lambda + 1)^p$.

PROPOSITION 5.9. *We have a congruence*

$$\eta^p \equiv \tilde{\eta} \mod \lambda^p.$$

PROOF. By Lemma 5.8,

$$\tilde{\eta} = \frac{\lambda^{p-1}}{p}(p\eta - \lambda) = -\left\{\sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} \lambda^{k-1}\right\} (p\eta - \lambda)$$

$$= -\sum_{k=1}^{p-1} \binom{p}{k} \lambda^{k-1}\eta + \sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} \lambda^k.$$

Now we have

$$-\sum_{k=1}^{p-1} \binom{p}{k} \lambda^{k-1}\eta + \sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} \lambda^k \equiv -p\eta + \sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} \lambda^k \mod \lambda^p,$$

since $\lambda^p \mid p\lambda$. Hence we obtain

$$\tilde{\eta} \equiv -p\eta + \sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} \lambda^k \mod \lambda^p.$$

On the other hand, by Lemma 5.7, we have

$$\eta^p \equiv \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \lambda_2^{pk} \equiv \sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} \lambda_2^{pk} \mod \lambda^p.$$

Hence the assertion follows from Lemma 5.6.

LEMMA 5.10. *Let A be a $\mathbf{Z}_{(p)}$-algebra and $a \in A$. Then we have*

$$p[a] \equiv (pa, a^p, 0, 0, \dots) \mod p^2 .$$

PROOF. It is sufficient to prove the assertion in the case where $A = \mathbf{Z}_{(p)}[U]$ and $a = U$. Put $\boldsymbol{V} = (V_0, V_1, V_2, \dots) = p[U] \in W(A)$. By the definition,

$$\Phi_r(\boldsymbol{V}) = V_0^{p^r} + pV_1^{p^{r-1}} + \cdots + p^{r-1}V_{r-1}^p + p^r V_r = pU^{p^r} .$$

In particular, we have

$$V_0 = pU , \quad V_1 = (1 - p^{p-1})U^p ,$$

and therefore

$$V_1 \equiv U^p \mod p^2 .$$

Hence we obtain

$$V_0^{p^r} \equiv 0 \mod p^{r+2} ,$$

since $p^r \geq r + 2$ if $r \geq 2$, and

$$pV_1^{p^{r-1}} \equiv pU^{p^r} \mod p^{r+2} ,$$

since $2p^{r-1} + 1 \geq r + 2$.

Assume now that $V_k \equiv 0 \mod p^2$ for $2 \leq k \leq r - 1$. Then we obtain $p^k V_k^{p^{r-k}} \equiv 0 \mod p^{r+2}$, since $2p^{r-k} + k \geq r + 2$ for $2 \leq k \leq r - 1$. It follows that

$$pU^{p^r} = V_0^{p^r} + pV_1^{p^{r-1}} + \cdots + p^{r-1}V_{r-1}^p + p^r V_r \equiv pU^{p^r} + p^r V_r \mod p^{r+2}$$

and that

$$V_r \equiv 0 \mod p^2 \text{ for } r \geq 2 .$$

REMARK 5.10.1. If $p = 2$, then we have

$$p[a] \equiv (2a, -a^2, 0, 0, \dots) \mod 2^2 .$$

LEMMA 5.11. *We have a congruence*

$$p[\eta] - [\lambda] \equiv (p\eta - \lambda, \eta^p, 0, 0, \dots) \mod p^2 .$$

PROOF. By Lemma 5.10,

$$p[\eta] \equiv (p\eta, \eta^p, 0, 0, \dots) \mod p^2 .$$

Put $\boldsymbol{a} = (a_0, a_1, a_2, \dots) = (p\eta, \eta^p, 0, \dots) - (\lambda, 0, 0, \dots) \in W(A)$. By the definition,

$$\Phi_r(\boldsymbol{a}) = a_0^{p^r} + pa_1^{p^{r-1}} + \cdots + p^{r-1}a_{r-1}^p + p^r a_r = (p\eta)^{p^r} + p(\eta^p)^{p^{r-1}} - \lambda^{p^r} .$$

In particular, we have

$$a_0 = p\eta - \lambda , \quad a_1 = \eta^p - \sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} (p\eta)^k (-\lambda)^{p-k} ,$$

and therefore

$$a_1 \equiv \eta^p \mod p^2,$$

since $p^2 \mid (p\eta)^k(-\lambda)^{p-k}$ for $1 \leq k \leq p-1$. Moreover, we have

$$\lambda^{p^r} \equiv 0 \mod p^{r+2}$$

for $r \geq 2$, since $v(p) = (p-1)v(\lambda)$ and $p^r \geq (p-1)(r+2)$ if $r \geq 2$. Hence we obtain

$$(p\eta)^{p^r} + p(\eta^p)^{p^{r-1}} - \lambda^{p^r} \equiv p(\eta^p)^{p^{r-1}} \mod p^{r+2}$$

for $r \geq 2$, since $\lambda \mid p\eta$.

Assume now that $a_k \equiv 0 \mod p^2$ for $2 \leq k \leq r-1$. Then we obtain $p^k a_k^{p^{r-k}} \equiv 0 \mod p^{r+2}$ for $2 \leq k \leq r-1$. On the other hand, $a_0^{p^r} \equiv 0 \mod p^{r+2}$, since $\lambda \mid a_0$. It follows that

$$a_0^{p^r} + pa_1^{p^{r-1}} + \cdots + p^{r-1}a_{r-1}^p + p^r a_r \equiv p(\eta^p)^{p^{r-1}} + p^r a_r \mod p^{r+2}$$

and that

$$p(\eta^p)^{p^{r-1}} + p^r a_r \equiv p(\eta^p)^{p^{r-1}} \mod p^{r+2}.$$

Hence we obtain the result.

PROPOSITION 5.12. *We have a congruence*

$$\frac{F(T)^p}{\lambda T + 1} \equiv E_p(p\eta - \lambda, \lambda; T)E_p(\eta^p, \lambda^p; T^p) \mod \lambda^p.$$

PROOF. First note that

$$F(T) \equiv E_p(\eta, \lambda; T) = E_p([\eta], \lambda; T) \mod \lambda$$

and that

$$F(T)^p \equiv E_p([\eta], \lambda; T)^p = E_p(p[\eta], \lambda; T) \mod \lambda^p.$$

Hence we obtain

$$\frac{F(T)^p}{\lambda T + 1} \equiv E_p(p[\eta] - [\lambda], \lambda; T) \mod \lambda^p,$$

since $\lambda T + 1 = E_p([\lambda], \lambda; T)$. By the Lemma 5.11,

$$E_p(p[\eta] - [\lambda], \lambda; T) \equiv E_p(p\eta - \lambda, \lambda; T)E_p(\eta^p, \lambda^p; T^p) \mod p^2.$$

Hence the result follows.

LEMMA 5.13. *We have a congruence*

$$\left[\frac{p}{\lambda^{p-1}}\right][\tilde{\eta}] - \tilde{V}[\tilde{\eta}] + V[\tilde{\eta}] \equiv \left(\frac{p}{\lambda^{p-1}}\tilde{\eta}, \tilde{\eta}, 0, 0, \ldots\right) \mod p^2.$$

PROOF. By Lemma 1.4.1,

$$\tilde{V}[\tilde{\eta}] \equiv 0 \mod p^2.$$

Hence

$$\left[\frac{p}{\lambda^{p-1}}\right][\tilde{\eta}] - \tilde{V}[\tilde{\eta}] + V[\tilde{\eta}] \equiv \left[\frac{p}{\lambda^{p-1}}\right][\tilde{\eta}] + V[\tilde{\eta}]$$

$$= \left(\frac{p}{\lambda^{p-1}}\tilde{\eta}, 0, 0, 0, \dots\right) + (0, \tilde{\eta}, 0, 0, \dots) = \left(\frac{p}{\lambda^{p-1}}\tilde{\eta}, \tilde{\eta}, 0, 0, \dots\right) \mod p^2.$$

PROPOSITION 5.14. *We have a congruence*

$$G\left(\frac{(\lambda T+1)^p - 1}{\lambda^p}\right) \equiv E_p\left(\frac{p\tilde{\eta}}{\lambda^{p-1}}, \lambda; T\right) E_p(\tilde{\eta}, \lambda^p; T^p) \mod \lambda^p.$$

PROOF. By Remark 3.8,

$$G\left(\frac{(\lambda T+1)^p - 1}{\lambda^p}\right) \equiv E_p\left(\left[\frac{p}{\lambda^{p-1}}\right][\tilde{\eta}] - \tilde{V}[\tilde{\eta}] + V[\tilde{\eta}], \lambda; T\right) \mod \lambda^p,$$

and by Lemma 5.13,

$$E_p\left(\left[\frac{p}{\lambda^{p-1}}\right][\tilde{\eta}] - \tilde{V}[\tilde{\eta}] + V[\tilde{\eta}], \lambda; T\right) \equiv E_p\left(\frac{p\tilde{\eta}}{\lambda^{p-1}}\lambda; T\right) E_p(\tilde{\eta}, \lambda^p; T^p) \mod p^2.$$

Hence the result follows.

5.15. Proof of (2). Combining 5.12, 5.14 and 5.9, we obtain a congruence

$$\frac{F(T)^p}{\lambda T+1} \equiv G\left(\frac{(\lambda T+1)^p - 1}{\lambda^p}\right) \mod \lambda^p.$$

This implies that the fraction

$$\Psi_1(T_0, T_1) = \frac{1}{\lambda^p}\left[\frac{\{\lambda T_1 + F(T_0)\}^p}{\lambda T_0 + 1} - G\left(\frac{(\lambda T_0+1)^p - 1}{\lambda^p}\right)\right]$$

belongs to $A[T_0, T_1, 1/(\lambda T_0+1), 1/(\lambda T_1 + F(T_0))]$.

Now we prove that $\mathrm{Ker}[\Psi : \mathcal{W}_2 \to \mathcal{V}_2]$ is isomorphic to $\mathbf{Z}/p^2\mathbf{Z}$. First note that a diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{G}^{(\lambda)} & \longrightarrow & \mathcal{W}_2 & \longrightarrow & \mathcal{G}^{(\lambda)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \Psi} & & \\ 0 & \longrightarrow & \mathcal{G}^{(\lambda^p)} & \longrightarrow & \mathcal{V}_2 & \longrightarrow & \mathcal{G}^{(\lambda^p)} & \longrightarrow & 0 \end{array}$$

is commutative. Here

$$\Psi : \mathcal{G}^{(\lambda)} = \mathrm{Spec}\, A\left[T, \frac{1}{1+\lambda T}\right] \to \mathcal{G}^{(\lambda^p)} = \mathrm{Spec}\, A\left[T, \frac{1}{1+\lambda^p T}\right]$$

is defined by

$$T \mapsto \Psi_0(T) = \frac{(1+\lambda T)^p - 1}{\lambda^p} : A\left[T, \frac{1}{1+\lambda^p T}\right] \to A\left[T, \frac{1}{1+\lambda T}\right],$$

and the horizontal arrows are defined as in 4.1. Then $\mathrm{Ker}[\Psi : \mathcal{W}_2 \to \mathcal{V}_2]$ is an extension of $\mathbf{Z}/p\mathbf{Z}$ by $\mathbf{Z}/p\mathbf{Z}$, since $\mathrm{Ker}[\Psi : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}]$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ and $\Psi : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}$ is faithfully flat (cf. [17, Ch.II]).

Put now

$$(a_0, a_1) = \left(1, \frac{\zeta_2 - F(1)}{\lambda}\right).$$

Then $\Psi_0(a_0) = 0$, $\Psi_1(a_0, a_1) = 0$, that is, (a_0, a_1) is a K-rational point of

$$\mathrm{Ker}[\Psi : \mathcal{W}_2 \to \mathcal{V}_2] = \mathrm{Spec}\, A\left[T_0, T_1, \frac{1}{\lambda T_0 + 1}, \frac{1}{\lambda T_1 + F(T_0)}\right] \Big/ (\Psi_0(T_0), \Psi(T_0, T_1)).$$

We can verify that (a_0, a_1) is an A-valued point of $\mathrm{Ker}\,\Psi$, noting that $\mathrm{Ker}\,\Psi$ is finite and étale over A. Furthermore, (a_0, a_1) is of order p^2, since $\alpha^{(F)}(a_0, a_1) = (\zeta, \zeta_2) \in (K^\times)^2$. It then follows that $\mathrm{Ker}[\Psi : \mathcal{W}_2 \to \mathcal{V}_2]$ is isomorphic to $\mathbf{Z}/p^2\mathbf{Z}$.

REMARK 5.15.1. It is deduced from 5.12 and 5.14 that

$$(1) \quad F(T)^p \equiv p\eta T + \sum_{k=0}^{p-1} \frac{\eta^{pk}}{k!} T^{pk} \mod \lambda^p;$$

$$(2) \quad (\lambda T + 1) G\left(\frac{(\lambda T + 1)^p - 1}{\lambda^p}\right) \equiv p\eta T + \sum_{k=0}^{p-1} \frac{\tilde{\eta}^k}{k!} T^{pk} \mod \lambda^p.$$

LEMMA 5.16. *With the above notation,*

(1) $F[\eta] - [\lambda^{p-1}][\eta] \equiv (\eta^p - \lambda^{p-1}\eta, 0, 0, \dots) \mod \lambda^p$,

(2) $F[\tilde{\eta}] - [\lambda^{p(p-1)}][\tilde{\eta}] \equiv (\tilde{\eta}^p - \lambda^{p(p-1)}\tilde{\eta}, 0, 0, \dots) \mod \lambda^{2p}$.

PROOF. Put $\boldsymbol{a} = (a_0, a_1, a_2, \dots) = F[\eta] - [\lambda^{p-1}][\eta]$. By the definition,

$$\Phi_r(\boldsymbol{a}) = a_0^{p^r} + p a_1^{p^{r-1}} + \cdots + p^{r-1} a_{r-1}^p + p^r a_r = \eta^{p^{r+1}} - \lambda^{p^r(p-1)} \eta^{p^r}.$$

In particular, we obtain

$$a_0 = \eta^p - \lambda^{p-1}\eta \quad \text{and} \quad a_1 = -\sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} \eta^{pk} (-\lambda^{p-1}\eta)^{p-k}.$$

Hence we obtain $a_1 \equiv 0 \mod \lambda^p$, noting that $\lambda^p \mid (\eta)^{pk}(-\lambda^{p-1}\eta)^{p-k}$ for $1 \le k \le p-1$. Assume now that $a_k \equiv 0 \mod \lambda^p$ for $1 \le k \le r-1$. Then we have $p^k a_k^{p^{r-k}} \equiv 0 \mod p^r\lambda^p$ for $1 \le k \le r-1$, since $v(p) = (p-1)v(\lambda)$ and $k(p-1) + p^{r-k+1} \ge r(p-1) + p$ if $1 \le k \le r-1$. On the other hand, $a_0 \equiv 0 \mod \lambda$, and therefore, $a_0^{p^r} \equiv 0 \mod p^r\lambda^p$. It follows that

$$a_0^{p^r} + p a_1^{p^{r-1}} + \cdots + p^{r-1} a_{r-1}^p + p^r a_r \equiv 0 \mod p^r\lambda^p$$

and $a_r \equiv 0 \mod \lambda^p$.

Put now $\boldsymbol{b} = (b_0, b_1, b_2, \dots) = F[\tilde{\eta}] - [\lambda^{p(p-1)}][\tilde{\eta}]$. By the definition,

$$\Phi_r(\boldsymbol{b}) = b_0^{p^r} + p b_1^{p^{r-1}} + \cdots + p^{r-1} b_{r-1}^p + p^r b_r = \tilde{\eta}^{p^{r+1}} - \lambda^{p^{r+1}(p-1)} \tilde{\eta}^{p^r}.$$

In particular, we obtain

$$b_0 = \tilde{\eta}^p - \lambda^{p(p-1)}\tilde{\eta} \quad \text{and} \quad b_1 = -\sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} \tilde{\eta}^{pk}\{-\lambda^{p(p-1)}\tilde{\eta}\}^{p-k}.$$

Hence we obtain $b_1 \equiv 0 \mod \lambda^{2p}$, noting that $\lambda^{2p} \mid (\tilde{\eta})^{pk}\{-\lambda^{p(p-1)}\tilde{\eta}\}^{p-k}$ for $1 \leq k \leq p-1$. Assume now that $b_k \equiv 0 \mod \lambda^{2p}$ for $1 \leq k \leq r-1$. Then we have $p^k b_k^{p^{r-k}} \equiv 0 \mod p^r\lambda^{2p}$ for $1 \leq k \leq r-1$, since $v(p) = (p-1)v(\lambda)$ and $k(p-1) + 2p^{r-k+1} \geq r(p-1) + 2p$ if $1 \leq k \leq r-1$. On the other hand, $b_0 \equiv 0 \mod \lambda^p$, and therefore, $b_0^{p^r} \equiv 0 \mod p^r\lambda^{2p}$, since $v(p) = (p-1)v(\lambda)$ and $p^{r+1} \geq r(p-1) + 2p$. It follows that

$$b_0^{p^r} + pb_1^{p^{r-1}} + \cdots + p^{r-1}b_{r-1}^p + p^r b_r \equiv 0 \mod p^r\lambda^{2p}$$

and $b_r \equiv 0 \mod \lambda^{2p}$.

5.17. Proof of (5). Put

$$(\tilde{F}_0([\eta]), \tilde{F}_1([\eta]), \tilde{F}_2([\eta]), \dots) = (F - [\lambda^{p-1}])[\eta].$$

Then, by Proposition 4.3.1, the class of $\mathcal{W}_{2,A_0}$ in $\mathrm{Ext}_{A_0}(\boldsymbol{G}_{a,A_0}, \boldsymbol{G}_{a,A_0}) = H_0^2(\boldsymbol{G}_{a,A_0}, \boldsymbol{G}_{a,A_0})$ is given by the class of

$$\sum_{k=1}^{\infty} \frac{\tilde{F}_{k-1}([\eta])}{\lambda} C_k.$$

By Lemma 5.16,

$$\tilde{F}_0([\eta]) \equiv \eta^p - \lambda^{p-1}\eta \mod \lambda^p$$

and

$$\tilde{F}_k([\eta]) \equiv 0 \mod \lambda^p$$

for $k \geq 1$. Moreover, by Proposition 5.9,

$$\eta^p \equiv \tilde{\eta} = \frac{\lambda^{p-1}}{p}(p\eta - \lambda) \mod \lambda^p.$$

Hence we obtain

$$\eta^p - \lambda^{p-1}\eta \equiv \lambda \mod \lambda^2,$$

noting that $\lambda \mid p\eta$, $\lambda \mid \lambda^{p-1}\eta$ and that $\lambda^{p-1}/p \equiv -1 \mod \lambda$. Therefore, we see that $\mathcal{W}_{2,A_0}$ is isomorphic to W_{2,A_0}, since the class of W_{2,A_0} in $H_0^2(\boldsymbol{G}_{a,A_0}, \boldsymbol{G}_{a,A_0})$ is represented by the 2-cocycle

$$C_1(X, Y) = \frac{X^p + Y^p - (X+Y)^p}{p}.$$

Similarly, we can verify that $\mathcal{V}_{2,A_1}$ is isomorphic to W_{2,A_1}. These imply the assertion (5) of the theorem.

REMARK 5.18. Green and Matignon [4] have given independently an explicit form of the Kummer-Artin-Schreier-Witt theory of degree p^2. They empoly (η, η^p) instead of

$(\eta, \tilde{\eta})$ to define an isogeny of degree p^2. It follows from Proposition 5.9 that their isogeny is isomorphic to ours.

Indeed, put

$$G'(T) = \sum_{k=0}^{p-1} \frac{(\eta^p T)^k}{k!},$$

$$\Lambda_0^{G'}(X_0, Y_0) = \lambda^p X_0 Y_0 + X_0 + Y_0,$$

$$\Lambda_1^{G'}(X_0, X_1, Y_0, Y_1) = \lambda^p X_1 Y_1 + X_1 G'(Y_0) + G'(X_0) Y_0 + \frac{1}{\lambda^p}[G'(X_0)G'(Y_0) - G'(\lambda^p X_0 Y_0 + X_0 + Y_0)],$$

$$\Psi_0'(T_0) = \frac{(\lambda T_0 + 1)^p - 1}{\lambda^p},$$

$$\Psi_1'(T_0, T_1) = \frac{1}{\lambda^p}\left[\frac{\{\lambda T_1 + F(T_0)\}^p}{\lambda T_0 + 1} - G'\left(\frac{(\lambda T_0 + 1)^p - 1}{\lambda^p}\right)\right],$$

$$\mathcal{V}_2' = \operatorname{Spec} A\left[T_0, T_1, \frac{1}{\lambda^p T_0 + 1}, \frac{1}{\lambda^p T_1 + G(T_0)}\right].$$

The multiplication of $\mathcal{V}_2'$ is given by

$$(T_0, T_1) \mapsto (\Lambda_0^{G'}(T_0 \otimes 1, 1 \otimes T_0), \Lambda_1^{G'}(T_0 \otimes 1, T_1 \otimes 1, 1 \otimes T_0, 1 \otimes T_1)).$$

As was shown by Green and Matignon,

$$(T_0, T_1) \mapsto (\Psi_0'(T_0), \Psi_1'(T_0, T_1))$$

defines an A-homomorphism $\Psi' : \mathcal{W}_2 \to \mathcal{V}_2'$, which is an isogeny with kernel isomorphic to $\mathbf{Z}/p^2\mathbf{Z}$.

Now we can verify $(T_0, T_1) \mapsto (T_0, T_1 + (G(T_0) - G'(T_0))/\lambda^p)$ defines an A-isomorphism $\mathcal{V}_2 \xrightarrow{\sim} \mathcal{V}_2'$ and that the diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{Z}/p^2\mathbf{Z} & \longrightarrow & \mathcal{W}_2 & \xrightarrow{\Psi} & \mathcal{V}_2 & \longrightarrow & 0 \\ & & \| & & \| & & \downarrow & & \\ 0 & \longrightarrow & \mathbf{Z}/p^2\mathbf{Z} & \longrightarrow & \mathcal{W}_2 & \xrightarrow[\Psi']{} & \mathcal{V}_2' & \longrightarrow & 0 \end{array}$$

is commutative.

It is crucial to prove the congruence relation mentioned in the proposition for an explicit description of the Kummer-Artin-Schreier-Witt thoery of degree p^2. The congruence relation was proved independently by Green and Matignon [4, Sect.5, Sublemma].

REFERENCES

[1] N. BOURBAKI, Algèbre commutative, Chapitres 8 et 9, Masson, Paris, 1983.

[2] M. DEMAZURE and P. GABRIEL, Groupes algébriques, Tome 1, Masson-North-Holland, Paris-Amsterdam, 1970.

[3] B. DWORK, On the rationality of the zeta function of an algebraic variety, Amer. J. Math. 82 (1960), 631–648.
[4] B. GREEN and M. MATIGNON, Liftings of Galois covers of smooth curves, Compositio Math. 113 (1998), 237–272.
[5] A. GROTHENDIECK with J. DIEUDONNÉ, Eléments de géométrie algébrique, IV, Inst. Hautes Études Sci. Publ. Math. No. 28, 1966, 255 pp.
[6] M. HAZEWINKEL, Formal groups and applications, Academic Press, New York, 1978.
[7] L. ILLUSIE, Complexe de de Rham-Witt et cohomologie cristalline, Ann. Sci. École Norm. Sup. (4) 12 (1979), 501–661.
[8] M. LAZARD, Sur les groupes de Lie formels à un paramétre, Bull. Soc. Math. France 83 (1955), 251–274.
[9] T. SEKIGUCHI, On the deformations of Witt groups to tori II, J. Algebra 138 (1991), 273–297.
[10] T. SEKIGUCHI and N. SUWA, A case of extensions of group schemes over a discrete valuation ring, Tsukuba J. Math. 14 (1990), 459–487.
[11] T. SEKIGUCHI and N. SUWA, Some cases of extensions of group schemes over a discrete valuation ring I, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 38 (1991), 1–45.
[12] T. SEKIGUCHI and N. SUWA, A note on extensions of algebraic and formal groups I, Math. Z. 206 (1991), 567–575.
[13] T. SEKIGUCHI and N. SUWA, A note on extensions of algebraic and formal groups II, Math. Z. 217 (1994), 447–457.
[14] T. SEKIGUCHI and N. SUWA, On the unified Kummer-Artin-Schreier-Witt theory, Preprint series, CHUO MATH No. 41, 1994.
[15] T. SEKIGUCHI and N. SUWA, Théories de Kummer-Artin-Schreier-Witt, C. R. Acad. Sci. Paris Sér. I Math. 319 (1994), 105–110.
[16] T. SEKIGUCHI and N. SUWA, A note on extensions of algebraic and formal groups III, Tôhoku Math. J. (1997), 241–257.
[17] T. SEKIGUCHI, F. OORT and N. SUWA, On the deformation of Artin-Schreier to Kummer, Ann. Sci. École Norm. Sup. (4) 22 (1989), 345–375.

DEPARTMENT OF MATHEMATICS
CHUO UNIVERSITY
1–13–27 KASUGA, BUNKYO-KU
TOKYO 112
JAPAN

E-mail address: sekiguti@math.chuo-u.ac.jp

DEPARTMENT OF MATHEMATICS
CHUO UNIVERSITY
1–13–27 KASUGA, BUNKYO-KU
TOKYO 112
JAPAN

E-mail address: suwa@math.chuo-u.ac.jp