Tôhoku Math. J.
49 (1997), 241–257

A NOTE ON EXTENSIONS OF ALGEBRAIC AND FORMAL GROUPS, III

TSUTOMU SEKIGUCHI AND NORIYUKI SUWA*

(Received November 20, 1995, revised May 7, 1996)

Abstract. We will give an explicit description of extensions of the group scheme of Witt vectors of length n (resp. the formal group of Witt vectors of length n) by the multiplicative group scheme (resp. the multiplicative formal group) over an algebra for which all prime numbers except a given prime p is invertible.

Introduction. Throughout the paper, p denotes a prime number, and $\boldsymbol{Z}_{(p)}$ the localization of $\boldsymbol{Z}$ at the prime ideal (p).

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, and W (resp. $\hat{W}$) the group scheme (resp. the formal group scheme) of Witt vectors over $\boldsymbol{Z}$. Let $\boldsymbol{G}_m$ (resp. $\hat{\boldsymbol{G}}_m$) denote the multiplicative group scheme (resp. the multiplicative formal group scheme over $\boldsymbol{Z}$. In [3], we gave an explicit description of the groups $\mathrm{Ext}^1_A(W_{n,A}, \boldsymbol{G}_{m,A})$ and $\mathrm{Ext}^1_A(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A})$, when A is a ring of characteristic $p>0$. More precisely, we constructed isomorphisms

$$\hat{W}(A)/F^n \xrightarrow{\sim} H^2_0(W_{n,A}, \boldsymbol{G}_{m,A}),$$
$$W(A)/F^n \xrightarrow{\sim} H^2_0(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A}),$$

using the Artin-Hasse exponential series.

In Theorem 2.8.1 of this note, we generalize these results to $\boldsymbol{Z}_{(p)}$-algebras A as follows: (It is crucial to define an endomorphism F of $W_{\boldsymbol{Z}}$ generalizing the Frobenius endomorphism of $W_{\boldsymbol{F}_p}$. For the definition, see Section 1.)

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

$$_{F^n}\hat{W}(A) \xrightarrow{\sim} \mathrm{Hom}(W_{n,A}, \boldsymbol{G}_{m,A}),$$
$$\hat{W}(A)/F^n \xrightarrow{\sim} H^2_0(W_{n,A}, \boldsymbol{G}_{m,A}),$$
$$_{F^n}W(A) \xrightarrow{\sim} \mathrm{Hom}(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A}),$$
$$W(A)/F^n \xrightarrow{\sim} H^2_0(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A}).$$

After a short review on Witt vectors and the Artin-Hasse exponential series, we state and prove the main theorem, generalizing the argument developed in [3].

---

* Partially supported by Grant-in-Aid for Scientific Research No. 07640069.

1991 *Mathematics Subject Classification*, Primary 14L05; Secondary 13K05, 20G10.

NOTATION. Throughout the paper, p denotes a prime number, $\boldsymbol{Z}_{(p)}$ the localization of $\boldsymbol{Z}$ at the prime ideal (p), 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

$H_0^2(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A})$ and $H_0^2(W_{n,A}, \boldsymbol{G}_{m,A})$ denote the Hochschild cohomology groups consisting of symmetric 2-cocycles of $\hat{W}_{n,A}$ with coefficients in $\hat{\boldsymbol{G}}_{m,A}$ and of $W_{n,A}$ with coefficients in $\boldsymbol{G}_{m,A}$, respectively.

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

For an endomorphism l of a commutative group M, ${}_lM$ (resp. M/l) denotes $\mathrm{Ker}[l\colon M \to M]$ (resp. $\mathrm{Coker}[l\colon M \to M]$).

1. Witt vectors. We start with reviewing necessary facts on Witt vectors. For details, see [DG, Chap. V] or [HZ, Chap. III].

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

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

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

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

and

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

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

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

and

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

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

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

is given by the addition

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

and the multiplication

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

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

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

and

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

1.2. The restriction homomorphism of ring schemes $R\colon W_{n+1,\mathbf{Z}} \to W_{n,\mathbf{Z}}$ is defined by the canonical injection

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

while the Verschiebung homomorphism of group schemes $V\colon W_{n,\mathbf{Z}} \to W_{n+1,\mathbf{Z}}$ is defined by

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

Then the sequence

$$(\mathrm{E}_{m,n}) \qquad 0 \longrightarrow W_{n,\mathbf{Z}} \xrightarrow{V^m} W_{n+m,\mathbf{Z}} \xrightarrow{R^n} W_{m,\mathbf{Z}} \longrightarrow 0$$

is exact for all $n, m \geq 1$ (cf. [DG, Chap. V.1.1]).

We denote also by $R\colon \hat{W}_{n+1,\mathbf{Z}} \to \hat{W}_{n,\mathbf{Z}}$ (resp. $V\colon \hat{W}_{n,\mathbf{Z}} \to \hat{W}_{n+1,\mathbf{Z}}$) the homomorphism of formal group schemes induced by $R\colon W_{n+1,\mathbf{Z}} \to W_{n,\mathbf{Z}}$ (resp. $V\colon W_{n,\mathbf{Z}} \to W_{n+1,\mathbf{Z}}$). We also have an exact sequence of formal group schemes

$$(\mathrm{E}_{m,n}) \qquad 0 \longrightarrow \hat{W}_{n,\mathbf{Z}} \xrightarrow{V^m} \hat{W}_{n+m,\mathbf{Z}} \xrightarrow{R^n} \hat{W}_{m,\mathbf{Z}} \longrightarrow 0.$$

Let k, l be integers with $k \geq l > 0$. We define a polynomial $S_{k,l}(X, Y) = S_{k,l}(X_0, \dots, X_{l-1}, Y_0, \dots, Y_{l-1})$ in $\mathbf{Z}[X_0, \dots, X_{l-1}, Y_0, \dots, Y_{l-1}]$ by

$$S_{k,l}(X, Y) = S_k(X_0, \dots, X_{l-1}, 0, \dots, 0, Y_0, \dots, Y_{l-1}, 0, \dots, 0).$$

The extension $(\mathrm{E}_{m,n})$ is defined by the 2-cocycle

$$(S_{m,m}(X, Y), S_{m+1,m}(X, Y), \dots, S_{m+n-1,m}(X, Y))$$

of $Z^2(W_{m,\boldsymbol{Z}}, W_{n,\boldsymbol{Z}})$ or of $Z^2(\hat{W}_{m,\boldsymbol{Z}}, \hat{W}_{n,\boldsymbol{Z}})$, respectively.

1.3 (cf. [1, Ch.O.1.3]). Now we define an endomorphism of $W_{\boldsymbol{Z}}$, generalizing the Frobenius endomorphism of $W_{\boldsymbol{F}_p}$.

Define 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

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

and

$$F_r(\boldsymbol{T})\equiv T_r^p \pmod p$$

for each $r\geq 0$. We denote by $F\colon W_{n+1,\boldsymbol{Z}}\to W_{n,\boldsymbol{Z}}$ the morphism defined by

$$T_0\mapsto F_0(\boldsymbol{T}),\ T_1\mapsto F_1(\boldsymbol{T}), \dots, T_{n-1}\mapsto F_{n-1}(\boldsymbol{T}):$$

$$\boldsymbol{Z}[T_0, T_1, \dots, T_{n-1}]\to \boldsymbol{Z}[T_0, T_1, \dots, T_n]\,.$$

Then we can verify without difficulty the following:

(1) F is a homomorphism of ring schemes;

(2) $FR=RF$;

(3) $FV=p$;

(4) $VF=p$ on $W_{n,A}$ if and only if A is of characteristic $p>0$.

Note that

$$W_{\boldsymbol{Z}}=\varprojlim_{R} W_{n,\boldsymbol{Z}}\,.$$

Hence (2) implies that the system $(F\colon W_{n+1,\boldsymbol{Z}}\to W_{n,\boldsymbol{Z}})_{n\geq 1}$ defines an endomorphism F of the ring scheme $W_{\boldsymbol{Z}}$. It is obvious that $\hat{W}_{\boldsymbol{Z}}$ is stable under F. If A is an $\boldsymbol{F}_p$-algebra, $F\colon W_A\to W_A$ is nothing but the usual Frobenius endomorphism.

2. Statement of the theorem. We first recall the definition of Hochschild cohomology. For details, see [DG, Ch. II.3 and Ch. III.6].

2.1. Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $G(\boldsymbol{X}, \boldsymbol{Y})=G(X_0, X_1, \dots, X_{n-1}, Y_0, Y_1, \dots, Y_{n-1})$ a formal series in $A[[X_0, X_1, \dots, X_{n-1}, Y_0, Y_1, \dots, Y_{n-1}]]^\times$ (resp. a polynomial in $A[X_0, X_1, \dots, X_{n-1}, Y_0, Y_1, \dots, Y_{n-1}]^\times$). Recall that $G(\boldsymbol{X}, \boldsymbol{Y})$ is called a symmetric 2-cocycle of $\hat{W}_{n,A}$ (resp. $W_{n,A}$) with coefficients in $\hat{\boldsymbol{G}}_{m,A}$ (resp. $\boldsymbol{G}_{m,A}$) is $G(\boldsymbol{X}, \boldsymbol{Y})$ satisfies the following functional equations:

$$G(\boldsymbol{S}(\boldsymbol{X}, \boldsymbol{Y}), \boldsymbol{Z})G(\boldsymbol{X}, \boldsymbol{Y})=G(\boldsymbol{X}, \boldsymbol{S}(\boldsymbol{Y}, \boldsymbol{Z}))G(\boldsymbol{Y}, \boldsymbol{Z}) \tag{1}$$

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

We denote by $Z^2(\hat{W}_{n,A}, \hat{G}_{n,A})$ (resp. $Z^2(W_{n,A}, G_{m,A})$) the subgroup of $A[[X_0, X_1, \ldots, X_{n-1}, Y_0, Y_1, \ldots, Y_{n-1}]]^\times$ (resp. a polynomial of $A[X_0, X_1, \ldots, X_{n-1}, Y_0, Y_1, \ldots, Y_{n-1}]^\times$) formed by the symmetric 2-cocycles of $\hat{W}_{n,A}$ (resp. $W_{n,A}$) with coefficients in $\hat{G}_{m,A}$ (resp. $G_{m,A}$).

Let $F(T)=F(T_0, T_1, \ldots, T_{n-1})$ be a formal power series in $A[[T_0, T_1, \ldots, T_{n-1}]]^\times$ (resp. a polynomial in $A[T_0, T_1, \ldots, T_{n-1}]^\times$). Then $F(X)F(Y)F(S(X, Y))^{-1}\in Z^2(\hat{W}_{n,A}, \hat{G}_{n,A})$ (resp. $Z^2(W_{n,A}, G_{m,A})$). We denote by $B^2(\hat{W}_{n,A}, \hat{G}_{n,A})$ (resp. $B^2(W_{n,A}, G_{m,A})$) the subgroup of $Z^2(\hat{W}_{n,A}, \hat{G}_{n,A})$ (resp. $Z^2(W_{n,A}, G_{m,A})$) of the symmetric 2-cocycles of the form $F(X)F(Y)F(S(X, Y))^{-1}$. Put

$$H_0^2(\hat{W}_{n,A}\hat{G}_{n,A})=Z^2(\hat{W}_{n,A}, \hat{G}_{n,A})/B^2(\hat{W}_{n,A}, \hat{G}_{n,A})$$

and

$$H_0^2(W_{n,A}, G_{m,A})=Z^2(W_{n,A}, G_{m,A})/B^2(W_{n,A}, G_{m,A}).$$

$H_0^2(\hat{W}_{n,A}, \hat{G}_{n,A})$ (resp. $H_0^2(W_{n,A}, G_{m,A})$) is isomorphic to the subgroup of $\mathrm{Ext}^1_A(\hat{W}_{n,A}, \hat{G}_{n,A})$ (resp. $\mathrm{Ext}^1_A(W_{n,A}, G_{m,A})$) formed by the classes of commutative extensions of $\hat{W}_{n,A}$ by $\hat{G}_{m,A}$ (resp. $W_{n,A}$ by $G_{m,A}$), which split as extensions of formal A-schemes (resp. A-schemes).

2.2. Recall now the definition of the Artin-Hasse exponential series

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

For $T=(T_r)_{r\geq 0}$, put

$$E_p(T; X)=\prod_{r\geq 0} E_p(T_rX^{p^r})=\exp\left(\sum_{r\geq 0}\frac{1}{p^r}\Phi_r(T)X^{p^r}\right).$$

It is readily seen that

$$E_p(T; X)E_p(U; X)=E_p(S(T, U); X).$$

For $T=(T_r)_{r\geq 0}$ and $X=(X_r)_{r\geq 0}$, we define a formal power series $E_p(T; X)\in \mathbf{Z}_{(p)}[[T, X]]$ by

$$E_p(T; X)=\exp\left(\sum_{r\geq 0}\frac{1}{p^r}\Phi_r(T)\Phi_r(X)\right)=\exp\left(\sum_{r\geq 0}\frac{1}{p^r}\Phi_r(P_r(T, X))\right).$$

It is verified without difficulty that

$$E_p(T; X)E_p(U; X)=E_p(S(T, U); X)$$

and

$$E_p(\boldsymbol{T};\boldsymbol{X})E_p(\boldsymbol{T};\boldsymbol{Y})=E_p(\boldsymbol{T};\boldsymbol{S}(\boldsymbol{X},\boldsymbol{Y}))\,.$$

LEMMA 2.3. *Let* $\boldsymbol{T}=(T_0,T_1,T_2,\dots)$, $\boldsymbol{X}=(X_0,X_1,X_2,\dots)$. *Then*

$$E_p(F\boldsymbol{T};\boldsymbol{X})=E_p(\boldsymbol{T};V\boldsymbol{X})\,.$$

Here $F\boldsymbol{T}=(F_0(\boldsymbol{T}),F_1(\boldsymbol{T}),F_2(\boldsymbol{T}),\dots)$ *and* $V\boldsymbol{X}=(0,X_0,X_1,\dots)$.

PROOF. Indeed, we have

$$\begin{aligned}E_p(F\boldsymbol{T};\boldsymbol{X})&=E_p\left(\sum_{r\geq 0}\frac{1}{p^r}\Phi_r(F\boldsymbol{T})\Phi_r(\boldsymbol{X})\right)\\&=E_p\left(\sum_{r\geq 0}\frac{1}{p^r}\Phi_{r+1}(\boldsymbol{T})\frac{1}{p}\Phi_{r+1}(V\boldsymbol{X})\right)=E_p(\boldsymbol{T};V\boldsymbol{X})\,.\end{aligned}$$

2.4. Let n be a positive integer. We define a polynomial $\Phi_{r,n}(\boldsymbol{X})=\Phi_{r,n}(X_0,X_1,\dots,X_{n-1})$ in $\boldsymbol{Z}[X_0,X_1,\dots,X_{n-1}]$ by

$$\Phi_{r,n}(\boldsymbol{X})=\begin{cases}\Phi_r(X_0,X_1,\dots,X_r) & \text{if } r\leq n-1\,,\\ \Phi_r(X_0,X_1,\dots,X_{n-1},0,0,\dots) & \text{if } r\geq n\,.\end{cases}$$

For $\boldsymbol{X}=(X_r)_{r\geq 0}$, we put

$$E_{p,n}(\boldsymbol{T};\boldsymbol{X})=E_p(\boldsymbol{T};X_0,\dots,X_{n-1},0,0,\dots)=\exp\left(\sum_{r\geq 0}\frac{1}{p^r}\Phi_r(\boldsymbol{T})\Phi_{r,n}(\boldsymbol{X})\right).$$

For example, we have

$$E_{p,1}(\boldsymbol{T};\boldsymbol{X})=E_p(\boldsymbol{T};X_0)\,.$$

REMARK 2.5. This definition of the formal power series $E_{p,n}(\boldsymbol{T};\boldsymbol{X})$ is a modification of that of $E_{p,n}(\boldsymbol{a};\boldsymbol{T})$ in [3,II.1.4]. As long as we treat the case of characteristic $p>0$, there is no difference between the two definitions.

LEMMA 2.6. *Let* $\boldsymbol{X}=(X_0,X_1,\dots,X_{n-1})$, $\boldsymbol{Y}=(Y_0,Y_1,\dots,Y_{n-1})$ *and* $\boldsymbol{S}=(S_0(\boldsymbol{X},\boldsymbol{Y}),S_1(\boldsymbol{X},\boldsymbol{Y}),\dots,S_{n-1}(\boldsymbol{X},\boldsymbol{Y}))$. *Then*

$$E_{p,n}(\boldsymbol{T};\boldsymbol{X})E_{p,n}(\boldsymbol{T};\boldsymbol{Y})E_{p,n}(\boldsymbol{T};\boldsymbol{S})^{-1}=E_p(F^n\boldsymbol{T};\tilde{\boldsymbol{S}}_n)\,,$$

where $\tilde{\boldsymbol{S}}_n=(S_{n,n}(\boldsymbol{X},\boldsymbol{Y}),S_{n+1,n}(\boldsymbol{X},\boldsymbol{Y}),\dots)$.

PROOF. Indeed,

$$\begin{aligned}E_{p,n}(\boldsymbol{T};\boldsymbol{X})E_{p,n}(\boldsymbol{T};\boldsymbol{Y})E_{p,n}(\boldsymbol{T};\boldsymbol{S})^{-1}&=\exp\left(\sum_{r\geq 0}\frac{1}{p^r}\Phi_r(\boldsymbol{T})(\Phi_{r,n}(\boldsymbol{X})+\Phi_{r,n}(\boldsymbol{Y})-\Phi_{r,n}(\boldsymbol{S}))\right)\\&=\exp\left(\sum_{r\geq n}\frac{1}{p^r}\Phi_r(\boldsymbol{T})(p^nS_{n,n}^{p^{r-n}}+p^{n+1}S_{n+1,n}^{p^{r-n-1}}+\cdots+p^rS_{r,n})\right)\end{aligned}$$

$$
\begin{aligned}
&=\exp\left(\sum_{i\geq 0}\frac{1}{p^i}\Phi_{n+i}(T)(S_{n,n}^{p^i}+pS_{n+1,n}^{p^{i-1}}+\cdots+p^iS_{n+i,n})\right)\\
&=\exp\left(\sum_{i\geq 0}\frac{1}{p^i}\Phi_{n+i}(T)\Phi_i(S_{n,n},S_{n+1,n},\ldots,S_{n+i,n})\right)\\
&=\exp\left(\sum_{i\geq 0}\frac{1}{p^i}\Phi_i(F^nT)\Phi_i(S_{n,n},S_{n+1,n},\ldots,S_{n+i,n})\right)\\
&=E_p(F^n\boldsymbol{T};\tilde{\boldsymbol{S}}_n)\,.
\end{aligned}
$$

2.7. Now we define a formal power series $F_{p,n}(\boldsymbol{U};\boldsymbol{X},\boldsymbol{Y})$ in $\boldsymbol{U}=(U_0,U_1,\ldots)$, $\boldsymbol{X}=(X_0,X_1,\ldots,X_{n-1})$ and $\boldsymbol{Y}=(Y_0,Y_1,\ldots,Y_{n-1})$ by

$$F_{p,n}(\boldsymbol{U};\boldsymbol{X},\boldsymbol{Y})=E_p(\boldsymbol{U};\tilde{\boldsymbol{S}}_n)=E_p(\boldsymbol{U};S_{n,n},S_{n+1,n},\ldots)\,.$$

Then obviously

$$F_{p,n}(\boldsymbol{U};\boldsymbol{X},\boldsymbol{Y})\in Z^2(\hat{\boldsymbol{W}}_{n\boldsymbol{Z}_{(p)}[\boldsymbol{U}]},\hat{\boldsymbol{G}}_{m,\boldsymbol{Z}_{(p)}[\boldsymbol{U}]})\,.$$

COROLLARY 2.7.1. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $\boldsymbol{a}\in W(A)$. Then*:

(1) $E_{p,n}(\boldsymbol{a};\boldsymbol{T})\in \mathrm{Hom}_{A-\mathrm{gr}}(\hat{\boldsymbol{W}}_{n,A},\hat{\boldsymbol{G}}_{m,A})$ *if* $\boldsymbol{a}\in {}_{F^n}W(A)$;
(2) $E_{p,n}(\boldsymbol{a};\boldsymbol{T})\in \mathrm{Hom}_{A-\mathrm{gr}}(\boldsymbol{W}_{n,A},\boldsymbol{G}_{m,A})$ *if* $\boldsymbol{a}\in {}_{F^n}\hat{W}(A)$;
(3) $F_{p,n}(\boldsymbol{a};\boldsymbol{X},\boldsymbol{Y})\in Z^2(\hat{\boldsymbol{W}}_{n,A},\hat{\boldsymbol{G}}_{m,A})$ *and* $F_{p,n}(F^n\boldsymbol{a};\boldsymbol{X},\boldsymbol{Y})\in B^2(\hat{\boldsymbol{W}}_{n,A},\hat{\boldsymbol{G}}_{m,A})$;
(4) $F_{p,n}(\boldsymbol{a};\boldsymbol{X},\boldsymbol{Y})\in Z^2(\boldsymbol{W}_{n,A},\boldsymbol{G}_{m,A})$ *and* $F_{p,n}(F^n\boldsymbol{a};\boldsymbol{X},\boldsymbol{Y})\in B^2(\hat{\boldsymbol{W}}_{n,A},\boldsymbol{G}_{m,A})$ *if* $\boldsymbol{a}\in\hat{W}(A)$.

2.8. Let A be a $\boldsymbol{Z}_{(p)}$-algebra. We now define homomorphisms

$$
\begin{aligned}
&\xi^0_{n,A}: {}_{F^n}\hat{W}(A)\to \mathrm{Hom}_{A-\mathrm{gr}}(\boldsymbol{W}_{n,A},\boldsymbol{G}_{m,A})\,;\quad \boldsymbol{a}\mapsto E_{p,n}(\boldsymbol{a};\boldsymbol{X})\,,\\
&\xi^1_{n,A}: \hat{W}(A)/F^n\to H^2_0(\boldsymbol{W}_{n,A},\boldsymbol{G}_{m,A})\,;\quad \boldsymbol{a}\mapsto F_{p,n}(\boldsymbol{a};\boldsymbol{X},\boldsymbol{Y})\,,\\
&\xi^0_{n,A}: {}_{F^n}W(A)\to \mathrm{Hom}_{A-\mathrm{gr}}(\hat{\boldsymbol{W}}_{n,A},\hat{\boldsymbol{G}}_{m,A})\,;\quad \boldsymbol{a}\mapsto E_{p,n}(\boldsymbol{a};\boldsymbol{X})\,,\\
&\xi^1_{n,A}: W(A)/F^n\to H^2_0(\hat{\boldsymbol{W}}_{n,A},\hat{\boldsymbol{G}}_{m,A})\,;\quad \boldsymbol{a}\mapsto F_{p,n}(\boldsymbol{a};\boldsymbol{X},\boldsymbol{Y})\,.
\end{aligned}
$$

In this notation, our main result is given as follows:

THEOREM 2.8.1. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra. Then the homomorphisms*

$$
\begin{aligned}
&\xi^0_{n,A}: {}_{F^n}\hat{W}(A)\to \mathrm{Hom}_{A-\mathrm{gr}}(\boldsymbol{W}_{n,A},\boldsymbol{G}_{m,A})\,,\\
&\xi^0_{n,A}: {}_{F^n}W(A)\to \mathrm{Hom}_{A-\mathrm{gr}}(\hat{\boldsymbol{W}}_{n,A},\hat{\boldsymbol{G}}_{m,A})\,,\\
&\xi^1_{n,A}: \hat{W}(A)/F^n\to H^2_0(\boldsymbol{W}_{n,A},\boldsymbol{G}_{m,A})\,,\\
&\xi^1_{n,A}: W(A)/F^n\to H^2_0(\hat{\boldsymbol{W}}_{n,A},\hat{\boldsymbol{G}}_{m,A})\,,
\end{aligned}
$$

are isomorphisms.

We verify some compatibilites for ξ_n^0 and ξ_n^1, which are needed to prove the theorem.

LEMMA 2.9. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra. Then*:

(1) *The diagrams*

$$\begin{tikzcd} {}_{F^n}W(A) \arrow[r] \arrow[d, "\xi_n^0"] & {}_{F^{n+1}}W(A) \arrow[d, "\xi_{n+1}^0"] \\ \mathrm{Hom}_{A-\mathrm{gr}}(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A}) \arrow[r, "R^*"] & \mathrm{Hom}_{A-\mathrm{gr}}(\hat{W}_{n+1,A}, \hat{\boldsymbol{G}}_{m,A}) \end{tikzcd}$$

and

$$\begin{tikzcd} {}_{F^n}\hat{W}(A) \arrow[r] \arrow[d, "\xi_n^0"] & {}_{F^{n+1}}\hat{W}(A) \arrow[d, "\xi_{n+1}^0"] \\ \mathrm{Hom}_{A-\mathrm{gr}}(W_{n,A}, \boldsymbol{G}_{m,A}) \arrow[r, "R^*"] & \mathrm{Hom}_{A-\mathrm{gr}}(W_{n+1,A}, \boldsymbol{G}_{m,A}) \end{tikzcd}$$

are commutative. Here the horizontal arrows denote the canonical injections.

(2) *The diagrams*

$$\begin{tikzcd} {}_{F^{n+1}}W(A) \arrow[r, "F"] \arrow[d, "\xi_{n+1}^0"] & {}_{F^n}W(A) \arrow[d, "\xi_n^0"] \\ \mathrm{Hom}_{A-\mathrm{gr}}(\hat{W}_{n+1,A}, \hat{\boldsymbol{G}}_{m,A}) \arrow[r, "V^*"] & \mathrm{Hom}_{A-\mathrm{gr}}(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A}) \end{tikzcd}$$

and

$$\begin{tikzcd} {}_{F^{n+1}}\hat{W}(A) \arrow[r, "F"] \arrow[d, "\xi_{n+1}^0"] & {}_{F^n}\hat{W}(A) \arrow[d, "\xi_n^0"] \\ \mathrm{Hom}_{A-\mathrm{gr}}(W_{n+1,A}, \boldsymbol{G}_{m,A}) \arrow[r, "V^*"] & \mathrm{Hom}_{A-\mathrm{gr}}(W_{n,A}, \boldsymbol{G}_{m,A}) \end{tikzcd}$$

are commutative.

(3) *The diagrams*

$$\begin{tikzcd} W(A)/F^n \arrow[r, "F"] \arrow[d, "\xi_n^1"] & W(A)/F^{n+1} \arrow[d, "\xi_{n+1}^1"] \\ H_0^2(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A}) \arrow[r, "R^*"] & H_0^2(\hat{W}_{n+1,A}, \hat{\boldsymbol{G}}_{m,A}) \end{tikzcd}$$

and

$$\begin{tikzcd} \hat{W}(A)/F^n \arrow[r, "F"] \arrow[d, "\xi_n^1"] & \hat{W}(A)/F^{n+1} \arrow[d, "\xi_{n+1}^1"] \\ H_0^2(W_{n,A}, G_{m,A}) \arrow[r, "R^*"] & H_0^2(W_{n+1,A}, G_{m,A}) \end{tikzcd}$$

are commutative.

(4) *The diagrams*

$$\begin{tikzcd} W(A)/F^{n+1} \arrow[r] \arrow[d, "\xi_n^1"] & W(A)/F^n \arrow[d, "\xi_{n+1}^1"] \\ H_0^2(\hat{W}_{n+1,A}, \hat{G}_{m,A}) \arrow[r, "V^*"] & H_0^2(\hat{W}_{n,A}, \hat{G}_{m,A}) \end{tikzcd}$$

and

$$\begin{tikzcd} \hat{W}(A)/F^{n+1} \arrow[r] \arrow[d, "\xi_n^1"] & \hat{W}(A)/F^n \arrow[d, "\xi_{n+1}^1"] \\ H_0^2(W_{n+1,A}, G_{m,A}) \arrow[r, "V^*"] & H_0^2(W_{n,A}, G_{m,A}) \end{tikzcd}$$

are commutative. Here the horizontal arrows denote the canonical surjections.

PROOF. By Lemma 2.3, we have the equalities

$$E_{p,n+1}(\boldsymbol{U}; X_0, \dots, X_{n-1}) = E_{p,n}(\boldsymbol{U}; X_0, \dots, X_{n-1}),$$

and

$$E_{p,n+1}(\boldsymbol{U}; 0, X_0, \dots, X_{n-1}) = E_{p,n}(F\boldsymbol{U}; X_0, \dots, X_{n-1}),$$

which imply (1) and (2).

Now we prove (3). Noting that

$$\Phi_{r,n+1}(\boldsymbol{T}) - \Phi_{r,n}(\boldsymbol{T}) = \begin{cases} 0 & (r \le n-1) \\ p^n T_n^{p^{r-n}} & (r \ge n), \end{cases}$$

we obtain

$$E_{p,n+1}(\boldsymbol{V}, \boldsymbol{T}) E_{p,n}(\boldsymbol{V}, \boldsymbol{T})^{-1} = \exp\left(\sum_{r=0}^{\infty} \frac{1}{p^r} \Phi_{r+n}(\boldsymbol{V}) T_n^{p^r} \right) = E_p(F^n \boldsymbol{V}; T_n).$$

Putting $\boldsymbol{U} = F^n \boldsymbol{V}$, we get

$$F_{p,n+1}(F\boldsymbol{U}; \boldsymbol{X}, \boldsymbol{Y}) F_{p,n}(\boldsymbol{U}; \boldsymbol{X}, \boldsymbol{Y})^{-1} = E_p(\boldsymbol{U}; X_n) E_p(\boldsymbol{U}; Y_n) E_p(\boldsymbol{U}; S_n(\boldsymbol{X}, \boldsymbol{Y}))^{-1},$$

which implies that

$$[F_{p,n+1}(FU;X,Y)]=[F_{p,n}(U;X,Y)] \quad \text{in} \quad H_0^2(\hat{W}_{n+1,\boldsymbol{Z}_{(p)}[\boldsymbol{U}]}, \hat{G}_{m,\boldsymbol{Z}_{(p)}[\boldsymbol{U}]}) .$$

To verify (4), it is enough to note that

$$\begin{aligned} F_{p,n+1}(U;VX,VY) &= E_p(U;S_{n+1,n+1}(VX,VY),S_{n+2,n+1}(VX,VY),\dots) \\ &= E_p(U;S_{n,n}(X,Y),S_{n+1,n}(X,Y),\dots) \\ &= F_p(U;X,Y) . \end{aligned}$$

LEMMA 2.10. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra. Then the diagrams*

$$\begin{array}{ccc} {}_{F^n}W(A) & \longrightarrow & W(A)/F^m \\ \Big\downarrow \xi_n^0 & & \Big\downarrow \xi_m^1 \\ \mathrm{Hom}_{A\text{-gr}}(\hat{W}_{n,A},\hat{G}_{m,A}) & \xrightarrow{\partial} & H_0^2(\hat{W}_{m,A},\hat{G}_{m,A}) \end{array}$$

and

$$\begin{array}{ccc} {}_{F^n}\hat{W}(A) & \longrightarrow & \hat{W}(A)/F^m \\ \Big\downarrow \xi_n^0 & & \Big\downarrow \xi_m^1 \\ \mathrm{Hom}_{A\text{-gr}}(W_{n,A},G_{m,A}) & \xrightarrow{\partial} & H_0^2(W_{m,A},G_{m,A}) \end{array}$$

are commutative. Here the horizontal arrows above denote the maps induced by $\boldsymbol{a}\mapsto\boldsymbol{a}$, and ∂'s denote the boundary maps defined by the exact sequences of formal group schemes

$$0 \longrightarrow \hat{W}_{n,A} \xrightarrow{V^m} \hat{W}_{n+m,A} \xrightarrow{R^n} \hat{W}_{m,A} \longrightarrow 0$$

or of group schemes

$$0 \longrightarrow W_{n,A} \xrightarrow{V^m} W_{n+m,A} \xrightarrow{R^n} W_{m,A} \longrightarrow 0 .$$

PROOF. The extension of formal group schemes

$$0 \longrightarrow \hat{W}_{n,A} \xrightarrow{V^m} \hat{W}_{n+m,A} \xrightarrow{R^n} \hat{W}_{m,A} \longrightarrow 0$$

is defined by the 2-cocycle

$$(S_{m,m}(X,Y),S_{m+1,m}(X,Y),\dots,S_{m+n-1,m}(X,Y))\in Z^2(\hat{W}_{m,A},\hat{W}_{n,A}) .$$

Hence the boundary map $\partial\colon \mathrm{Hom}_{A\text{-gr}}(\hat{W}_{n,A},\hat{G}_{m,A})\to H_0^2(\hat{W}_{m,A},\hat{G}_{m,A})$ is defined by

$$E_{p,n}(\boldsymbol{a};\, T) \mapsto E_{p,n}(\boldsymbol{a};\, S_{m,m}(X, Y), S_{m+1,m}(X, Y), \dots, S_{m+n-1,m}(X, Y)).$$

Noting that

$$F_{p,m}(\boldsymbol{a};\, X, Y) = E_p(\boldsymbol{a};\, S_{m,m}(X, Y), S_{m+1,m}(X, Y), \dots, S_{m+n-1,m}(X, Y), S_{n+m,m}(X, Y), \dots),$$

we obtain

$$\begin{aligned} F_{p,m}(\boldsymbol{a};\, X, Y)&E_{p,n}(\boldsymbol{a};\, S_{m,m}(X, Y), S_{m+1,m}(X, Y), \dots, S_{m+n-1,m}(X, Y))^{-1} \\ &= E_p(\boldsymbol{a};\, 0, \dots, 0, S_{m+n,m}(X, Y), S_{m+n+1,m}(X, Y), \dots) \\ &= E_p(F^n\boldsymbol{a};\, S_{m+n,m}(X, Y), S_{m+n+1,m}(X, Y), \dots), \end{aligned}$$

which implies the asserted commutativity of the diagram. The case of group schemes is verified similarly.

3. Proof of the theorem.

3.1. It remains to prove the case $n=1$, in view of the commutative diagrams with exact rows:

$$\begin{array}{ccccc} 0 \longrightarrow & {}_{F^n}W(A) & \longrightarrow & {}_{F^{n+1}}W(A) & \\ & \downarrow \xi_n^0 & & \downarrow \xi_{n+1}^0 & \\ 0 \longrightarrow & \mathrm{Hom}_{A-\mathrm{gr}}(\hat{W}_{n,A}, \hat{G}_{m,A}) & \xrightarrow{R^*} & \mathrm{Hom}_{A-\mathrm{gr}}(\hat{W}_{n+1,A}, \hat{G}_{m,A}) & \end{array}$$

$$\begin{array}{ccccc} \xrightarrow{F^n} & {}_{F}W(A) & \longrightarrow & W(A)/F^n & \\ & \downarrow \xi_1^0 & & \downarrow \xi_n^1 & \\ \xrightarrow{(V^n)^*} & \mathrm{Hom}_{A-\mathrm{gr}}(\hat{G}_{a,A}, \hat{G}_{m,A}) & \xrightarrow{\partial} & H_0^2(\hat{W}_{n,A}, \hat{G}_{m,A}) & \end{array}$$

$$\begin{array}{cccccc} \xrightarrow{F} & W(A)/F^{n+1} & \longrightarrow & W(A)/F & \longrightarrow 0 \\ & \downarrow \xi_{n+1}^1 & & \downarrow \xi_1^1 & \\ \xrightarrow{R^*} & H_0^2(\hat{W}_{n+1,A}, \hat{G}_{m,A}) & \xrightarrow{(V^n)^*} & H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A}), & \end{array}$$

induced by the exact sequence of formal group schemes

$$0 \longrightarrow \hat{G}_{a,A} \xrightarrow{V^n} \hat{W}_{n+1,A} \xrightarrow{R} \hat{W}_{n,A} \longrightarrow 0,$$

and

$$\begin{array}{ccccc}
0 \longrightarrow & {}_{F^n}\hat{W}(A) & \longrightarrow & {}_{F^{n+1}}\hat{W}(A) & \\
& \Big\downarrow \xi_n^0 & & \Big\downarrow \xi_{n+1}^0 & \\
0 \longrightarrow & \mathrm{Hom}_{A-\mathrm{gr}}(W_{n,A}, \boldsymbol{G}_{m,A}) & \xrightarrow{R^*} & \mathrm{Hom}_{A-\mathrm{gr}}(W_{n+1,A}, \boldsymbol{G}_{m,A}) &
\end{array}$$

$$\begin{array}{ccccc}
\xrightarrow{F^n} & {}_F W(A) & \longrightarrow & \hat{W}(A)/F^n & \\
& \Big\downarrow \xi_1^0 & & \Big\downarrow \xi_n^1 & \\
\xrightarrow{(V^n)^*} & \mathrm{Hom}_{A-\mathrm{gr}}(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) & \xrightarrow{\partial} & H_0^2(W_{n,A}, \boldsymbol{G}_{m,A}) &
\end{array}$$

$$\begin{array}{cccccc}
\xrightarrow{F} & \hat{W}(A)/F^{n+1} & \longrightarrow & \hat{W}(A)/F & \longrightarrow 0 \\
& \Big\downarrow \xi_{n+1}^1 & & \Big\downarrow \xi_1^1 & \\
\xrightarrow{R^*} & H_0^2(W_{n+1,A}, \boldsymbol{G}_{m,A}) & \xrightarrow{(V^n)^*} & H_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) \,, &
\end{array}$$

induced by the exact sequence of formal group schemes

$$0 \longrightarrow \boldsymbol{G}_{a,A} \xrightarrow{V^n} W_{n+1,A} \xrightarrow{R} W_{n,A} \longrightarrow 0 \,.$$

The following lemma implies the bijectivity of

$$\xi_{1,A}^0 : {}_F W(A) \to \mathrm{Hom}_{A-\mathrm{gr}}(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$$

and

$$\xi_{1,A}^0 : {}_F \hat{W}(A) \to \mathrm{Hom}_{A-\mathrm{gr}}(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) \,.$$

LEMMA 3.2. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $F(T) \in A[[T]]^\times$. If $F(X+Y) = F(X)F(Y)$, then there exists $\boldsymbol{a} \in {}_F W(A)$ such that $F(T) = E_p(\boldsymbol{a}; T)$. Moreover, if $F(T) \in A[T]^\times$, then $\boldsymbol{a} \in {}_F \hat{W}(A)$.*

PROOF. Put

$$F(T) = \prod_{k=1}^{\infty} E_p(c_k T^k) \,, \qquad c_k \in A \,,$$

and set $\boldsymbol{a} = (c_{p^r})_{r \geq 0}$ and $G(T) = \prod_{k \notin P} E_p(c_k T)$, where $P = \{p^j; j \geq 0\}$. Then

$$F(T) = E_p(\boldsymbol{a}; T) G(T) \,,$$

hence

$$\begin{aligned}
(G(X)G(Y)G(X+Y)^{-1})^{-1} &= E_p(\boldsymbol{a}; X) E_p(\boldsymbol{a}; Y) E_p(\boldsymbol{a}; X+Y)^{-1} \\
&= F_{p,1}(F\boldsymbol{a}; X, Y) \,.
\end{aligned}$$

Note that

$$F_{p,1}(F\boldsymbol{a};\, X,\, Y) \equiv 1 + \text{the term of degree } p^r \quad (\text{mod degree } p^r+1)$$

for some r. If $G(T) \neq 1$, then $G(T) \equiv 1 + cT^k$ (mod degree $k+1$) with $c \neq 0$ for some $k>0$. Then k is not a power of p, and

$$G(X)G(Y)G(X+Y)^{-1} \equiv 1 + c\{X^k + Y^k - (X+Y)^k\} \quad (\text{mod degree } k+1)\,.$$

It follows that $G(T)=1$ and $F_{p,1}(F\boldsymbol{a};\, X,\, Y)=1$, and therefore $F\boldsymbol{a}=0$.

To prove the bijectivity of $\xi^1_{1,A}\colon W(A)/F \to H^2_0(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ and $\xi^1_{1,A}\colon \hat{W}(A)/F \to H^2_0(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$, we need several lemmas. We put $P=\{p^j;\, j\geq 0\}$ as above.

SUBLEMMA 3.3. *Let $\boldsymbol{U}=(U_0, U_1, \ldots)$. Then we have*

$$F_{p,1}(\boldsymbol{U};\, X,\, Y) = \exp\left(\sum_{r\geq 0} \frac{1}{p^r}\, \Phi_r(U_0, U_1, \ldots, U_r)\, \frac{X^{p^{r+1}} + Y^{p^{r+1}} - (X+Y)^{p^{r+1}}}{p}\right).$$

PROOF. By definition,

$$\begin{aligned} &F_{p,1}(\boldsymbol{U};\, X,\, Y)\\ &= \exp\left(\sum_{r\geq 0} \frac{1}{p^r}\, \Phi_r(U_0, U_1, \ldots, U_r)\Phi_r(S_{1,1}(X, Y), S_{2,1}(X, Y), \ldots, S_{r+1,1}(X, Y))\right), \end{aligned}$$

where

$$S_{r+1,1}(X,\, Y) = S_{r+1}(X, 0, \ldots, 0, Y, 0, \ldots, 0)\,.$$

Hence we obtain the assertion, noting that

$$\begin{aligned} &(X+Y)^{p^{r+1}} + p\Phi_r(S_{1,1}(X, Y), S_{2,1}(X, Y), \ldots, S_{r+1,1}(X, Y))\\ &\quad = \Phi_{r+1}(S_0(X, Y), S_{1,1}(X, Y), S_{2,1}(X, Y), \ldots, S_{r+1,1}(X, Y))\\ &\quad = \Phi_{r+1}(X, 0, \ldots, 0) + \Phi_{r+1}(Y, 0, \ldots, 0) = X^{p^{r+1}} + Y^{p^{r+1}} \end{aligned}$$

and that

$$\Phi_r(S_{1,1}(X, Y), S_{2,1}(X, Y), \ldots, S_{r+1,1}(X, Y)) = \frac{X^{p^{r+1}} + Y^{p^{r+1}} - (X+Y)^{p^{r+1}}}{p}\,.$$

COROLLARY 3.3.1. *Let A be a $\boldsymbol{Z}_{(p)}$-algebra and $\boldsymbol{a}=(a_i)_{i\geq 0} \in W(A)$. Then*

$$F_{p,1}(\boldsymbol{a};\, X,\, Y) \equiv 1 + a_0\, \frac{X^p + Y^p - (X+Y)^p}{p} \quad (\text{mod degree } p+1)\,.$$

Moreover, if $a_i=0$ for $i<r$, then

$$F_{p,1}(\boldsymbol{a};\, X,\, Y) \equiv 1 + a_r\, \frac{X^{p^{r+1}} + Y^{p^{r+1}} - (X+Y)^{p^{r+1}}}{p} \quad (\text{mod degree } p^{r+1}+1)\,.$$

PROOF. By Lemma 3.3,

$$F_{p,1}(U; X, Y)=\exp\left(U_0\frac{X^p+Y^p-(X+Y)^p}{p}+\text{terms of degree } >p\right).$$

Hence we obtain

$$F_{p,1}(U; X, Y)\equiv 1+U_0\frac{X^p+Y^p-(X+Y)^p}{p} \quad (\mathrm{mod}\ (X, Y)^{p+1}).$$

Moreover,

$$\begin{aligned}&F_{p,1}(0, \ldots, 0, U_r, U_{r+1}, \ldots; X, Y)\\ &\quad=\exp\left(U_r\frac{X^{p^{r+1}}+Y^{p^{r+1}}-(X+Y)^{p^{r+1}}}{p}+\text{terms of degree}>p^{r+1}\right),\end{aligned}$$

since $\Phi_i(0, \ldots, 0)=0$ for $i<r$ and $\Phi_r(0, \ldots, 0, U_r)=p^rU_r$. Hence we have

$$\begin{aligned}&F_{p,1}(0, \ldots, 0, U_r, U_{r+1}, \ldots; X, Y)\\ &\quad\equiv 1+U_r\frac{X^{p^{r+1}}+Y^{p^{r+1}}-(X+Y)^{p^{r+1}}}{p} \quad (\mathrm{mod}\ (X, Y)^{p^{r+1}+1}).\end{aligned}$$

These imply the assertion.

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

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 a_i, $c_j\in A$ $(0\leq i<r-1$ and $1<j<k$, $j\notin P)$ such that

$$F_{p,1}(a_0, a_1, \ldots, a_{r-2}, 0, \ldots; X, Y)G_k(X)G_k(Y)G_k(X+Y)^{-1}\equiv F(X, Y) \quad (\text{mod degree } k),$$

where $r=[\log_p k]$, the greatest integer not greater than $\log_p k$, and $G_k(T)=\prod_{j<k}(1+c_jT^j)$. Let $H(X, Y)$ denote the homogeneous component of degree k of $F(X, Y)[F_{p,1}(a_0, a_1, \ldots, a_{r-2}, 0, \ldots; X, Y)G_k(X)G_k(Y)G_k(X+Y)^{-1}]^{-1}$. Since $F(X, Y)[F_{p,1}(a_0, a_1, \ldots, a_{r-2}, 0, \ldots; X, Y)G_k(X)G_k(Y)G_k(X+Y)^{-1}]^{-1}\in Z^2(\hat{\boldsymbol{G}}_{a,B}, \hat{\boldsymbol{G}}_{m,B})$, we see that $H(X, Y)$ satisfies the functional equations:

1) $H(X+Y, Z)+H(X, Y)=H(X, Y+Z)+H(Y, Z)$;
2) $H(X, Y)=H(Y, X)$.

By Lazard's comparison lemma [2, Lemma 3], there exists $a\in A$ 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 $c_k = a$ and $G_{k+1}(T) = G_k(T)(1 + c_k T^k)$. Then we have

$$F_{p,1}(\boldsymbol{a}_k; X, Y)G_{k+1}(X)G_{k+1}(Y)G_{k+1}(X+Y)^{-1} \equiv F(X, Y) \pmod{\text{degree } k+1}$$

since

$$(1 + c_k X^k)(1 + c_k Y^k)\{1 + c_k(X+Y)^k\}^{-1} \equiv 1 + c_k\{X^k + Y^k - (X+Y)^k\} \pmod{\text{degree } k+1}.$$

(2) When $k = p^r$, put $a_{r-1} = a$. By Corollary 3.3.1, we have

$$F_{p,1}(\underbrace{0, \ldots, 0}_{r-1}, a_{r-1}, 0, \ldots; X, Y) \equiv 1 + a_{r-1}\frac{X^{p^r} + Y^{p^r} - (X+Y)^{p^r}}{p} \pmod{\text{degree } p^r + 1}.$$

Hence we obtain

$$F_{p,1}(a_0, \ldots, a_{r-2}, a_{r-1}, 0, \ldots; X, Y)G_k(X)G_k(Y)G_k(X+Y)^{-1} \equiv F(X, Y) \pmod{\text{degree } p^r + 1},$$

noting that

$$\begin{aligned} F_{p,1}(a_0, \ldots, a_{r-2}, 0, \ldots; X, Y)F_{p,1}(0, \ldots, 0, a_{r-1}, 0, \ldots; X, Y) \\ = F_{p,1}(a_0, \ldots, a_{r-2}, a_{r-1}, 0, \ldots; X, Y). \end{aligned}$$

Continuing this process, we find $\boldsymbol{a} \in W(A)$ and $G(T) = \prod_{k \notin P}(1 + c_k T^k) \in A[[T]]$ such that $F(X, Y) = F_{p,1}(\boldsymbol{a}; X, Y)G(X)G(Y)G(X+Y)^{-1}$.

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

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 $G(T) = \prod_{k \notin P}(1 + c_k T^k) \in A[[T]]^\times$ such that $F(X, Y) = F_{p,1}(\boldsymbol{a}; X, Y)G(X)G(Y)G(X+Y)^{-1}$. 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 the coefficients of the terms of degree ≥ 1 in $F(X, Y)$. Since the polynomial $F(X, Y)$ is invertible, $\mathfrak{a}$ is nilpotent.

Now observe the following:

1) For $j \notin P$, put

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

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 $(c_j)^k$ for $k > 1$;

2) Put

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

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 $(a_i)^k$ 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 $\xi^1_{1,A}: W(A)/F \to H^2_0(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ and $\xi^1_{1,A}: \hat{W}(A)/F \to H^2_0(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$.

Lemma 3.4 and Lemma 3.5 imply the surjectivity of $\xi^1_{1,A}: W(A)/F \to H^2_0(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ and $\xi^1_{1,A}: \hat{W}(A)/F \to H^2_0(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$, respectively.

Now assume that $F_{p,1}(\boldsymbol{a}; X, Y) \in B^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ for $\boldsymbol{a} \in W(A)$. Then there exists $F(T) \in A[[T]]^\times$ such that $F(X)F(Y)F(X+Y)^{-1} = F_{p,1}(\boldsymbol{a}; X, Y)$. Put $F(T) = \prod_{k \geq 1} E_p(c_k T^k)$. Then

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

where $\boldsymbol{b} = (c_{p^r})_{r \geq 0}$. As in the proof of Lemma 3.2, we see that $c_k = 0$ if k is not a power of p, hence $F_{p,1}(\boldsymbol{a}; X, Y) = F_{p,1}(F\boldsymbol{b}; X, Y)$. It follows that $\xi^1_{1,A}: W(A)/F \to H^2_0(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ is injective. It is similarly seen that $\xi^1_{1,A}: \hat{W}(A)/F \to H^2_0(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$ is injective.

REMARK 3.7. $\mathrm{End}_{A-\mathrm{gr}}(\hat{W}_{n,A})$ (resp. $\mathrm{End}_{A-\mathrm{gr}}(W_{n,A})$) acts on $H^2_0(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A})$ (resp. $H^2_0(W_{n,A}, \boldsymbol{G}_{m,A})$) by the pull-back. We can describe the action under the identifications $H^2_0(\hat{W}_{n,A}, \hat{\boldsymbol{G}}_{m,A}) = W(A)/F^n$ and $H^2_0(W_{n,A}, \boldsymbol{G}_{m,A}) = \hat{W}(A)/F^n$ as follows:

Let $[\boldsymbol{b}]$ denote the endomorphism of $\hat{W}_{n,A}$ or $W_{n,A}$, defined by $\boldsymbol{b} = (b_r)_{0 \leq r \leq n-1} \in W_n(A)$. Then $\boldsymbol{a}[\boldsymbol{b}] = (F^n \boldsymbol{b}) \cdot \boldsymbol{a}$.

REMARK 3.8. It is more or less known that $H^2_0(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A}) = 0$ and $H^2_0(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) = 0$ if A is of characteristic 0. We can also verify these facts, noting that the homomorphism F is surjective on $W(A)$ and on $\hat{W}(A)$.

REFERENCES

[1] L. ILLUSE, Complexe de de Rham-Witt et cohomologie cristalline, Ann. Sci. École Norm. Sup. (4) 12 (1979), 501–661.
[2] M. LAZARD, Sur les groupes de Lie formels à un paramétre, Bull. Soc. Math. France 83 (1955), 251–274.
[3] T. SEKIGUCHI AND N. SUWA, A note on extensions of algebraic and formal groups I, II, Math. Z. 206 (1991), 567–575; 217 (1994), 447–457.
[DG] M. DEMAZURE AND P. GABRIEL, Groupes algébriques, Tome 1, Masson-North-Holland, Paris-

Amsterdam, 1970.
[HZ] M. HAZEWINKEL, Formal groups and applications, Academic Press, New York, 1978.

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

DEPARTMENT OF MATHEMATICS
TOKYO DENKI UNIVERSITY
KANDA-NISHIKI-CHO, CHIYODA-KU
TOKYO 101
JAPAN