TSUKUBA J. MATH.
Vol. 29 No. 2 (2005), 405–435

ON NON-COMMUTATIVE EXTENSIONS OF G_a BY G_m OVER AN F_p-ALGEBRA

By

Yuki HARAGUCHI*)

Abstract. We will give an explicit description of non-commutative extensions of the additive group scheme (resp. the additive formal group scheme) by the multiplicative group scheme (resp. the multiplicative formal group scheme) over an F_p-algebra.

Introduction

It is an interesting problem to determine the extensions of G by H, where G and H are elementary group schemes over a ring A. For example, when $G = G_{a,A}$ and $H = G_{m,A}$, it is well known that $\mathrm{Ext}^1_A(G_{a,A}, G_{m,A}) = 0$ if A is a field (cf. [1]) and $\mathrm{Ext}^1_A(\hat{G}_{a,A}, \hat{G}_{m,A}) = 0$ if A is a perfect field.

Sekiguchi and Suwa [3] gave an explicit description on the commutative extensions of $\hat{G}_{a,A}$ by $\hat{G}_{m,A}$ or of $G_{a,A}$ by $G_{m,A}$ when A is a ring of characteristic $p > 0$. More precisely, they have constructed isomorphisms

$$\mathrm{Coker}[F : W(A) \to W(A)] \xrightarrow{\sim} H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A})$$

and

$$\mathrm{Coker}[F : \hat{W}(A) \to \hat{W}(A)] \xrightarrow{\sim} H_0^2(G_{a,A}, G_{m,A}),$$

using the Artin-Hasse exponential series. Here $H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A})$ stands for the second symmetric Hochschild cohomology group of $\hat{G}_{a,A}$ with coefficients in $\hat{G}_{m,A}$, which describes commutative extensions of $\hat{G}_{a,A}$ by $\hat{G}_{m,A}$. However, there may exist a non-trivial extension of $G_{a,A}$ by $G_{m,A}$ if A has a nilpotent element. [3] gave also an example of non-commutative extensions of $G_{a,A}$ by $G_{m,A}$ (cf. [3, Remark 3.10]).

---

*) Partially supported by the Research on Security and Reliability in Electronic Society, Chuo University 21COE Program.
2000 Mathematics Subject Classification. Primary 14L05; Secondary 13K05, 20G10.
Received May 17, 2004.
Revised November 15, 2004.

In this article, we determine the non-commutative extensions of $\hat{G}_{a,A}$ by $\hat{G}_{m,A}$ and of $G_{a,A}$ by $G_{m,A}$ when A is of characteristic $p > 0$. More precisely, we can state the main theorem as follows:

THEOREM. *Let p be a prime number and A an F_p-algebra. Then the correspondence $(a_r)_{r\geq 1} \mapsto \prod_{r\geq 1} E_p(a_r; XY^{p^r})$ induces bijective homomorphisms*

$$(\mathrm{Ker}[F : W(A) \to W(A)])^N \xrightarrow{\sim} H^2(\hat{G}_{a,A}, \hat{G}_{m,A})/H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A})$$

and

$$(\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)])^{(N)} \xrightarrow{\sim} H^2(G_{a,A}, G_{m,A})/H_0^2(G_{a,A}, G_{m,A}).$$

Here $H^2(\hat{G}_{a,A}, \hat{G}_{m,A})$ stands for the second Hochschild cohomology group of $\hat{G}_{a,A}$ with coefficients in $\hat{G}_{m,A}$, which describes central extensions of $\hat{G}_{a,A}$ by $\hat{G}_{m,A}$. See Sect. 2 for further details concerning notations.

After a short review on Witt vectors and the Artin-Hasse exponential series, we state and prove the main theorem.

Acknowledgment

The author expresses her hearty thanks to Professor Noriyuki Suwa for his advices and suggestions. She is also grateful to Professors Tsutomu Sekiguchi and Fumiyuki Momose for their warm encouragement. Finally she thanks Doctors Noritsugu Endo, Mitsuaki Yato and Kazuyoshi Tsuchiya for their careful reading of the manuscript.

Notation

Throughout the article, p denotes a prime number.

$G_{a,Z}$: the additive group scheme over Z

$G_{m,Z}$: the multiplicative group scheme over Z

W_Z: the group scheme of Witt vectors over Z

$\hat{G}_{a,Z}$: the additive formal group scheme over Z

$\hat{G}_{m,Z}$: the multiplicative formal group scheme over Z

$\hat{W}_Z$: the formal group scheme of Witt vectors over Z

$H_0^2(G, H)$ 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 $G_{m,Z}(B)$.

For a commutative group M, M^N (resp. $M^{(N)}$) stands for $\prod_{i \in N} M_i$ (resp. $\bigoplus_{i \in N} M_i$) where $M_i = M$.

Contents

1. Recall: Witt Vectors and the Artin-Hasse Exponential Series

We start with reviewing necessary facts on Witt vectors. For details, see [1, Chap. V] or [2, 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

$$W_{\boldsymbol{Z}} = \operatorname{Spec} \boldsymbol{Z}[T_0, T_1, T_2, \ldots]$$

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

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

We denote by $\hat{W}_Z$ the formal completion of W_Z along the zero section. $\hat{W}_Z$ is considered as a subfunctor of W_Z. Indeed, if A is a ring,

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

1.2. Let A be an $\boldsymbol{F}_p$-algebra. The Verschiebung homomorphism $V : W(A) \to W(A)$ is defined by

$$(a_0, a_1, a_2, \dots) \mapsto (0, a_0, a_1, a_2, \dots),$$

and the Frobenius homomorphism $F : W(A) \to W(A)$ is defined by

$$(a_0, a_1, a_2, \dots) \mapsto (a_0^p, a_1^p, a_2^p, \dots).$$

Then it is verified without difficulty that F is a ring homomorphism. It is obvious that $\hat{W}(A)$ is stable under F.

1.3. Let A be an $\boldsymbol{F}_p$-algebra. Then we can verify without difficulty that:

(1) $FV = VF = p$;

(2) $V(F(\boldsymbol{a})\boldsymbol{b}) = \boldsymbol{a}V(\boldsymbol{b})$ for $\boldsymbol{a}, \boldsymbol{b} \in W(A)$.

Let A be a ring and $a \in A$. We denote the Witt vector $(a, 0, 0, \dots)$ by $[a]$. $[a]$ is called the Teichmüller lifting of a. It is readily seen:

(1) $[a][b] = [ab]$;

(2) $F[a] = [a^p]$;

(3) $(a_0, a_1, a_2, \dots) = \sum_{k=0}^{\infty} V^k[a_k]$.

1.4. Let $\boldsymbol{Z}_{(p)}$ denotes the localization of $\boldsymbol{Z}$ at the prime ideal (p). Recall now the definition of the Artin-Hasse exponential series

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

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

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

It is readily seen that

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

1.5. Let A be an $\boldsymbol{F}_p$-algebra and $\boldsymbol{a} = (a_r)_{r\geq 0} \in W(A)$. Then the correspondence $\boldsymbol{a} \mapsto E_p(\boldsymbol{a}; T)$ gives rise to isomorphisms

$$\mathrm{Ker}[F : W(A) \to W(A)] \xrightarrow{\sim} \mathrm{Hom}_{A\text{-gr}}(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$$

and

$$\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)] \xrightarrow{\sim} \mathrm{Hom}_{A\text{-gr}}(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}).$$

(cf. [1, Chap. II])

It should be remarked that if $\boldsymbol{a} = (a_r)_{r\geq 0} \in \mathrm{Ker}[F : W(A) \to W(A)]$, then

$$E_p(\boldsymbol{a}; T) = \prod_{r\geq 0} E_p(a_r T^{p^r}) = \prod_{r\geq 0}\left(\sum_{i=0}^{p-1} \frac{(a_r T^{p^r})^i}{i!}\right).$$

2. Statement of the Theorem

First we recall Hochschild cohomology groups. For details, see [1, Chap. II.5 and Chap. III.6].

2.1. Let A be a ring. We define the multiplicative groups $Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$, $Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$ and $B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$ by

$$Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) = \{F(X, Y) \in A[X, Y]^\times;$$
$$F(X, Y)F(X + Y, Z) = F(X, Y + Z)F(Y, Z)\},$$

$$Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) = \left\{F(X, Y) \in A[X, Y]^\times; \begin{array}{l} F(X, Y)F(X + Y, Z) = F(X, Y + Z)F(Y, Z), \\ F(X, Y) = F(Y, X) \end{array}\right\},$$

$$B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) = \left\{\frac{F(X)F(Y)}{F(X + Y)}; F(T) \in A[T]^\times\right\}.$$

Then we have

$$B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) \subset Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) \subset Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}).$$

We put

$$H^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) = Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})/B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}),$$

$$H_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) = Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})/B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}).$$

We define also the additive groups $Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$, $Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$ and $B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$ by

$$Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}) = \{F(X, Y) \in A[X, Y];\ F(X, Y) + F(X + Y, Z) = F(X, Y + Z) + F(Y, Z)\},$$

$$Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}) = \left\{F(X, Y) \in A[X, Y];\ \begin{matrix} F(X, Y) + F(X + Y, Z) = F(X, Y + Z) + F(Y, Z), \\ F(X, Y) = F(Y, X) \end{matrix}\right\},$$

$$B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}) = \{F(X) + F(Y) - F(X + Y); F(T) \in A[T]\}.$$

Then we have

$$B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}) \subset Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}) \subset Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}).$$

We put

$$H^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}) = Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})/B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}),$$

$$H_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}) = Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})/B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}).$$

It is well known that:

1) $H^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$ (resp. $H_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$) is isomorphic to the group of classes of central (resp. commutative) extensions of $\boldsymbol{G}_{a,A}$ by $\boldsymbol{G}_{m,A}$, which split as extensions of A-schemes.

2) $H^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$ (resp. $H_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$) is isomorphic to the group of classes of central (resp. commutative) extensions of $\boldsymbol{G}_{a,A}$ by $\boldsymbol{G}_{a,A}$.

2.2. Let A be a ring. We define the multiplicative formal groups $Z^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$, $Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ and $B^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ by

$$Z^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A}) = \left\{F(X, Y) \in A[[X, Y]]^\times;\ \begin{matrix} F(X, Y) \equiv 1 \mod \deg 1, \\ F(X, Y)F(X + Y, Z) = F(X, Y + Z)F(Y, Z) \end{matrix}\right\},$$

$$Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A}) = \left\{F(X, Y) \in A[[X, Y]]^\times;\ \begin{matrix} F(X, Y) \equiv 1 \mod \deg 1, \\ F(X, Y)F(X + Y, Z) = F(X, Y + Z)F(Y, Z), \\ F(X, Y) = F(Y, X) \end{matrix}\right\},$$

$$B^2(\hat{G}_{a,A}, \hat{G}_{m,A}) = \left\{\frac{F(X)F(Y)}{F(X+Y)}; F(T) \in A[[T]]^\times, F(T) \equiv 1 \mod \deg 1\right\}.$$

Then we have

$$B^2(\hat{G}_{a,A}, \hat{G}_{m,A}) \subset Z_0^2(\hat{G}_{a,A}, \hat{G}_{m,A}) \subset Z^2(\hat{G}_{a,A}, \hat{G}_{m,A}).$$

We put

$$H^2(\hat{G}_{a,A}, \hat{G}_{m,A}) = Z^2(\hat{G}_{a,A}, \hat{G}_{m,A})/B^2(\hat{G}_{a,A}, \hat{G}_{m,A}),$$

$$H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A}) = Z_0^2(\hat{G}_{a,A}, \hat{G}_{m,A})/B^2(\hat{G}_{a,A}, \hat{G}_{m,A}).$$

We define also the additive formal groups $Z^2(\hat{G}_{a,A}, \hat{G}_{a,A})$, $Z_0^2(\hat{G}_{a,A}, \hat{G}_{a,A})$ and $B^2(\hat{G}_{a,A}, \hat{G}_{a,A})$ by

$$Z^2(\hat{G}_{a,A}, \hat{G}_{a,A}) = \left\{ F(X, Y) \in A[[X, Y]]; \begin{array}{l} F(X, Y) \equiv 0 \mod \deg 1, \\ F(X, Y) + F(X+Y, Z) = F(X, Y+Z) + F(Y, Z) \end{array} \right\}.$$

$$Z_0^2(\hat{G}_{a,A}, \hat{G}_{a,A}) = \left\{ F(X, Y) \in A[[X, Y]]; \begin{array}{l} F(X, Y) \equiv 0 \mod \deg 1, \\ F(X, Y) + F(X+Y, Z) = F(X, Y+Z) + F(Y, Z), \\ F(X, Y) = F(Y, X) \end{array} \right\},$$

$$B^2(\hat{G}_{a,A}, \hat{G}_{a,A}) = \{F(X) + F(Y) - F(X+Y); F(T) \in A[[T]], F(T) \equiv 0 \mod \deg 1\}.$$

Then we have

$$B^2(\hat{G}_{a,A}, \hat{G}_{a,A}) \subset Z_0^2(\hat{G}_{a,A}, \hat{G}_{a,A}) \subset Z^2(\hat{G}_{a,A}, \hat{G}_{a,A}).$$

We put

$$H^2(\hat{G}_{a,A}, \hat{G}_{a,A}) = Z^2(\hat{G}_{a,A}, \hat{G}_{a,A})/B^2(\hat{G}_{a,A}, \hat{G}_{a,A}),$$

$$H_0^2(\hat{G}_{a,A}, \hat{G}_{a,A}) = Z_0^2(\hat{G}_{a,A}, \hat{G}_{a,A})/B^2(\hat{G}_{a,A}, \hat{G}_{a,A}).$$

It is well known that:

1) $H^2(\hat{G}_{a,A}, \hat{G}_{m,A})$ (resp. $H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A})$) is isomorphic to the group of classes of central (resp. commutative) extensions of $\hat{G}_{a,A}$ by $\hat{G}_{m,A}$, which split as extensions of formal A-schemes.

2) $H^2(\hat{G}_{a,A}, \hat{G}_{a,A})$ (resp. $H_0^2(\hat{G}_{a,A}, \hat{G}_{a,A})$) is isomorphic to the group of classes of central (resp. commutative) extensions of $\hat{G}_{a,A}$ by $\hat{G}_{a,A}$.

PROPOSITION 2.3. *Let A be an $\boldsymbol{F}_p$-algebra. If $P(X, Y) \in Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$, then $P(X, Y)$ is cohomologous to a cycle of the form*:

$$\sum_{r\geq 1} a_r \frac{(X+Y)^{p^r} - X^{p^r} - Y^{p^r}}{p} + \sum_{0\leq i<j} b_{ij} X^{p^i} Y^{p^j}, \quad a_r, b_{ij} \in A.$$

PROOF. The statement is proved in [1, Chap. II.3] when A is a field of characteristic p. However the argument works well for an arbitrary ring of characteristic p. We reproduce the proof presented in [loc.cit.] with a slight modification for the reader's convenience. For simplicity, we put

$$W(X, Y) = \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X^{p-i} Y^i = \frac{(X+Y)^p - X^p - Y^p}{p}.$$

Let $P(X, Y) \in Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}) \subset A[X, Y]$. We may assume that $P(X, Y)$ is homogeneous. Put

$$P(X, Y) = \sum_{i=0}^{n} a_i X^{n-i} Y^i, \quad n > 0. \tag{1}$$

By the assumption, we have

$$P(X, Y) + P(X+Y, Z) = P(X, Y+Z) + P(Y, Z). \tag{2}$$

Derivating (2) by X and substituting 0 for X, we obtain

$$\frac{\partial P}{\partial X}(0, Y) + \frac{\partial P}{\partial X}(Y, Z) = \frac{\partial P}{\partial X}(0, Y+Z),$$

and therefore

$$\frac{\partial P}{\partial X}(X, Y) = a_{n-1}\{(X+Y)^{n-1} - X^{n-1}\}.$$

Derivating (2) by Z and substituting 0 for Z, we obtain

$$\frac{\partial P}{\partial Z}(X+Y, 0) = \frac{\partial P}{\partial Z}(X, Y) + \frac{\partial P}{\partial Z}(Y, 0),$$

and therefore

$$\frac{\partial P}{\partial Y}(X, Y) = a_1\{(X+Y)^{n-1} - Y^{n-1}\}.$$

By Euler's formula, we obtain

$$\begin{aligned} nP(X, Y) &= X\frac{\partial P}{\partial X}(X, Y) + Y\frac{\partial P}{\partial Y}(X, Y) \\ &= a_1\{(X+Y)^n - X^n - Y^n\} + (a_{n-1} - a_1)\{X(X+Y)^{n-1} - X^n\}. \end{aligned}$$

Now we distinguish several cases.

Case 1: $a_{n-1} \neq a_1$. Put $c = a_{n-1} - a_1$ and $Q(X, Y) = c\{X(X+Y)^{n-1} - X^n\}$. Then

$$nP(X, Y) - Q(X, Y) \in B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}), \quad Q(X, Y) \in Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}).$$

Replacing X by $-Y$ in

$$Q(X, Y) + Q(X+Y, Z) = Q(X, Y+Z) + Q(Y, Z),$$

we obtain

$$cY\{(Y+Z)^{n-1} - Y^{n-1} - Z^{n-1}\} = 0. \tag{3}$$

Therefore

$$\binom{n-1}{k} \equiv 0 \bmod p \quad \text{for each } k \text{ with } 0 < k < n-1$$

since $c \neq 0$. Hence we can conclude that $n-1$ is a power of p. Put $n = 1 + p^r$. Then

$$Q(X, Y) = cXY^{p^r}$$

and therefore $P(X, Y)$ is cohomologous to $Q(X, Y)$.

Case 2: $a_{n-1} = a_1 \neq 0$. If $n \not\equiv 0 \bmod p$, then

$$P(X, Y) = \frac{a_1\{(X+Y)^n - X^n - Y^n\}}{n} \in B^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}).$$

On the other hand, assume that $n \equiv 0 \bmod p$. Then we have a congruence

$$\binom{n-1}{p-1} = \frac{(n-1)(n-2)\cdots(n-p+1)}{1\cdot 2\cdots(p-1)} \equiv 1 \bmod p.$$

If $n \neq p$, it follows that $a_1\{(X+Y)^{n-1} - Y^{n-1}\}$ contains the term $a_1X^{n-p}Y^{p-1}$, which is a contradiction to $a_1 \neq 0$ since

$$\frac{\partial P}{\partial Y}(X, Y) = a_1\{(X+Y)^{n-1} - Y^{n-1}\}.$$

Therefore $n = p$, we obtain

$$\frac{\partial P}{\partial X}(X, Y) = a_1\{(X+Y)^{p-1} - Y^{p-1}\} = a_1 \frac{\partial W}{\partial X}(X, Y)$$

and

$$\frac{\partial P}{\partial Y}(X, Y) = a_1\{(X+Y)^{p-1} - Y^{p-1}\} = a_1 \frac{\partial W}{\partial Y}(X, Y).$$

Derivating $P(X, Y) - a_1 W(X, Y)$ by X and by Y respectively, we obtain

$$\frac{\partial P}{\partial X}(X, Y) - a_1 \frac{\partial W}{\partial X}(X, Y) = \frac{\partial P}{\partial Y}(X, Y) - a_1 \frac{\partial W}{\partial Y}(X, Y) = 0.$$

Hence we obtain

$$P(X, Y) = a_1 W(X, Y) + a_0 X^p + a_p Y^p,$$

and $a_0 = a_p = 0$ since $a_0 X^p + a_p Y^p \in Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$.

Case 3: $a_{n-1} = a_1 = 0$. Then we have

$$\frac{\partial P}{\partial X}(X, Y) = \frac{\partial P}{\partial Y}(X, Y) = 0.$$

Hence we obtain $P(X, Y) = P_1(X^p, Y^p)$, where $P_1(X, Y)$ is a 2-cocycle of degree $n/p < n$ if $P(X, Y) \neq 0$.

Replacing $P(X, Y)$ by $P_1(X, Y)$ and repeating the same argument as above, we can obtain the required result.

Now we define symmetric 2-cocycles of $\hat{\boldsymbol{G}}_{a,A}$ with coefficients in $\hat{\boldsymbol{G}}_{m,A}$, using the Artin-Hasse exponential series. For details, see [3, 2.2].

2.4. A formal power series

$$F_p(U; X, Y) = \exp\left(\sum_{i \geq 1} U^{p^{i-1}} \frac{X^{p^i} + Y^{p^i} - (X+Y)^{p^i}}{p^i}\right) \in \boldsymbol{Z}_{(p)}[U][[X, Y]]$$

is defined in [3, 2.2].

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

$$F_p(\boldsymbol{U}; X, Y) = \prod_{r \geq 0} F_p(U_r; X^{p^r}, Y^{p^r}) \in \boldsymbol{Z}_{(p)}[\boldsymbol{U}][[X, Y]].$$

It is readily seen that

$$F_p(S(U, V); X, Y) = F_p(U; X, Y)F_p(V; X, Y).$$

2.5. Assume now that A is an F_p-algebra. Let $\boldsymbol{a} = (a_r)_{r\geq 0} \in W(A)$. Define a formal power series by

$$F_p(\boldsymbol{a}; X, Y) = \prod_{r\geq 0} F_p(a_r; X^{p^r}, Y^{p^r}) \in A[[X, Y]].$$

The following assertion was proved in [3, 3.4]:

Let A be an F_p-algebra. Then the correspondence $\boldsymbol{a} \mapsto F_p(\boldsymbol{a}; X, Y)$ gives rise to isomorphisms

$$\mathrm{Coker}[F : W(A) \to W(A)] \xrightarrow{\sim} H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A})$$

and

$$\mathrm{Coker}[F : \hat{W}(A) \to \hat{W}(A)] \xrightarrow{\sim} H_0^2(G_{a,A}, G_{m,A}).$$

Remark 2.6. Let A be an F_p-algebra. If $G(X, Y) \in Z_0^2(G_{a,A}, G_{a,A})$ and $G(X, Y)$ is a homogeneous polynomial of degree l, then there exists $F(X, Y) \in Z_0^2(G_{a,A}, G_{m,A})$ such that

$$F(X, Y) \equiv 1 + G(X, Y) \mod \deg(l + 1).$$

(cf. [3, Proof of Lemma 3.1])

2.7. Now we observe the following facts:

If $F(T) \in \mathrm{Hom}_{A\text{-gr}}(\hat{G}_{a,A}, \hat{G}_{m,A})$ and $G(X, Y) \in Z^2(\hat{G}_{a,A}, \hat{G}_{a,A})$, then

$$F(G(X, Y)) \in Z^2(\hat{G}_{a,A}, \hat{G}_{m,A}).$$

For example, $E_p(\boldsymbol{a}; T) \in \mathrm{Hom}_{A\text{-gr}}(\hat{G}_{a,A}, \hat{G}_{m,A})$ for $\boldsymbol{a} = (a_r)_{r\geq 0} \in \mathrm{Ker}[F : W(A) \to W(A)]$ (see 1.5) and

$$XY^{p^r} \in Z^2(G_{a,A}, G_{a,A}) \subset Z^2(\hat{G}_{a,A}, \hat{G}_{a,A}) \quad (r > 0).$$

Then

$$E_p(\boldsymbol{a}; XY^{p^r}) \in Z^2(\hat{G}_{a,A}, \hat{G}_{m,A}).$$

Any non-symmetric 2-cocycle of $\hat{G}_{a,A}$ with coefficients in $\hat{G}_{m,A}$ is obtained in the above way. In fact, we have the following:

THEOREM 2.8. *Let A be an $\boldsymbol{F}_p$-algebra. Then the correspondence $(\boldsymbol{a}_r)_{r\geq 1} \mapsto \prod_{r\geq 1} E_p(\boldsymbol{a}_r; XY^{p^r})$ gives rise to isomorphisms*

$$(\mathrm{Ker}[F : W(A) \to W(A)])^N \xrightarrow{\sim} H^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})/H_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$$

and

$$(\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)])^{(N)} \xrightarrow{\sim} H^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})/H_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}).$$

COROLLARY 2.9. *Let A be an $\boldsymbol{F}_p$-algebra. If $P(X, Y) \in Z^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ (resp. $Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$), then $P(X, Y)$ is cohomologous to a 2-cocycle of the form:*

$$F_p(\boldsymbol{b}; X, Y) \prod_{r\geq 1} E_p(\boldsymbol{a}_r; XY^{p^r}),$$

where $\boldsymbol{b} \in W(A)$ and $(\boldsymbol{a}_r)_{r\geq 1} \in (\mathrm{Ker}[F : W(A) \to W(A)])^N$ (resp. $\boldsymbol{b} \in \hat{W}(A)$ and $(\boldsymbol{a}_r)_{r\geq 1} \in (\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)])^{(N)}$).

3. Proof of the Theorem

Now we start proving necessary lemmas for our proof of Theorem 2.8.

LEMMA 3.1. *Let A be an $\boldsymbol{F}_p$-algebra and $F(X, Y) \in Z^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$. If*

$$F(X, Y) \equiv 1 \mod \deg(p^r + 1) \quad (r > 0),$$

then there exists $\tilde{F}(X, Y) \in Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ and $a_{r,0}, a_{r-1,1}, \dots, a_{1,r-1} \in A$ such that

$$F(X, Y)\tilde{F}(X, Y)^{-1} \equiv \sum_{k=0}^{p-1} \frac{1}{k!}\{a_{r,0}XY^{p^r} + a_{r-1,1}X^pY^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}}Y^{p^r}\}^k \mod \deg(p^{r+1} + 1).$$

PROOF. We shall prove that there exist $\tilde{F}(X, Y) \in Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ and $a_{r,0}, a_{r-1,1}, \dots, a_{1,r-1} \in A$ such that

$$F(X, Y)\tilde{F}(X, Y)^{-1} \equiv \sum_{k=0}^{l+1} \frac{1}{k!}\{a_{r,0}XY^{p^r} + a_{r-1,1}X^pY^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}}Y^{p^r}\}^k \mod \deg(l + 2)(p^r + 1)$$

by the induction on l $(0 \leq l \leq p - 3)$.

Step 1. Assume that

$$F(X, Y) \equiv 1 + H(X, Y) \mod \deg 2(p^r + 1),$$

where

$$H(X, Y) = \sum_{i=p^r+1}^{2(p^r+1)-1} H_i(X, Y),$$

here $H_i(X, Y)$ is the homogeneous part of degree i. It is readily seen that $H_i(X, Y)$ satisfies the functional equation

$$H_i(X, Y) + H_i(X + Y, Z) = H_i(X, Y + Z) + H_i(Y, Z).$$

Hence we obtain that $H(X, Y)$ satisfies the functional equation

$$H(X, Y) + H(X + Y, Z) = H(X, Y + Z) + H(Y, Z).$$

By Proposition 2.3, there exists $\tilde{H}(X, Y) \in Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$ and $a_{r,0}, a_{r-1,1}, \dots, a_{1,r-1} \in A$ such that

$$H(X, Y) = \tilde{H}(X, Y) + \{a_{r,0}XY^{p^r} + a_{r-1,1}X^p Y^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}} Y^{p^r}\}.$$

Note that $\tilde{H}(X, Y)$ is the sum of homogeneous polynomials. By Remark 2.6, there exists $\tilde{F}(X, Y) \in Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ such that

$$\tilde{F}(X, Y) \equiv 1 + \tilde{H}(X, Y) \mod \deg 2(p^r + 1).$$

Hence, we obtain

$$F(X, Y)\tilde{F}(X, Y)^{-1} \equiv 1 + \{a_{r,0}XY^{p^r} + a_{r-1,1}X^p Y^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}} Y^{p^r}\} \mod \deg 2(p^r + 1).$$

Step 2. By the assumption of the induction, we can put

$$F(X, Y) \equiv \sum_{k=0}^{l} \frac{1}{k!} G(X, Y)^k + H(X, Y) \mod \deg (l + 2)(p^r + 1) \tag{4}$$

for some $l \leq p - 3$, where

$$H(X, Y) = \sum_{i=(l+1)(p^r+1)}^{(l+2)(p^r+1)-1} H_i(X, Y),$$

here $H_i(X, Y)$ is homogeneous part of degree i and

$$G(X, Y) = a_{r,0}XY^{p^r} + a_{r-1,1}X^p Y^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}} Y^{p^r}.$$

Since

$$\left(\sum_{k=0}^{l}\frac{1}{k!}X^k\right)\left(\sum_{k=0}^{l}\frac{1}{k!}Y^k\right)\equiv\sum_{k=0}^{l}\frac{1}{k!}(X+Y)^k$$
$$+\frac{1}{(l+1)!}\{(X+Y)^{l+1}-X^{l+1}-Y^{l+1}\}\ \operatorname{mod}\deg(l+2), \tag{5}$$

we have

$$\left\{\sum_{k=0}^{l}\frac{1}{k!}G(X,Y)^k\right\}\left\{\sum_{k=0}^{l}\frac{1}{k!}G(X+Y,Z)^k\right\}\equiv\sum_{k=0}^{l}\frac{1}{k!}(G(X,Y)+G(X+Y,Z))^k$$
$$+\frac{1}{(l+1)!}\{(G(X,Y)+G(X+Y,Z))^{l+1}-G(X,Y)^{l+1}-G(X+Y,Z)^{l+1}\}$$
$$\operatorname{mod}\deg(l+2)(p^r+1)$$

and

$$\left\{\sum_{k=0}^{l}\frac{1}{k!}G(X,Y+Z)^k\right\}\left\{\sum_{k=0}^{l}\frac{1}{k!}G(Y,Z)^k\right\}\equiv\sum_{k=0}^{l}\frac{1}{k!}(G(X,Y+Z)+G(Y,Z))^k$$
$$+\frac{1}{(l+1)!}\{(G(X,Y+Z)+G(Y,Z))^{l+1}-G(X,Y+Z)^{l+1}-G(Y,Z)^{l+1}\}$$
$$\operatorname{mod}\deg(l+2)(p^r+1).$$

On the other hand, since

$$F(X,Y)F(X+Y,Z)=F(X,Y+Z)F(Y,Z),$$

we have

$$\left\{\sum_{k=0}^{l}\frac{1}{k!}G(X,Y)^k+H(X,Y)\right\}\left\{\sum_{k=0}^{l}\frac{1}{k!}G(X+Y,Z)^k+H(X+Y,Z)\right\}$$
$$\equiv\left\{\sum_{k=0}^{l}\frac{1}{k!}G(X,Y+Z)^k+H(X,Y+Z)\right\}\left\{\sum_{k=0}^{l}\frac{1}{k!}G(Y,Z)^k+H(Y,Z)\right\}$$
$$\operatorname{mod}\deg(l+2)(p^r+1).$$

Comparing the terms of degree i with $(l+1)(p^r+1)\le i\le(l+2)(p^r+1)-1$, we have

$$H(X, Y) + H(X+Y, Z)$$
$$+\frac{1}{(l+1)!}\{(G(X, Y) + G(X+Y, Z))^{l+1} - G(X, Y)^{l+1} - G(X+Y, Z)^{l+1}\}$$
$$= H(X, Y+Z) + H(Y, Z)$$
$$+\frac{1}{(l+1)!}\{(G(X, Y+Z) + G(Y, Z))^{l+1} - G(X, Y+Z)^{l+1} - G(Y, Z)^{l+1}\}.$$

Since we see that $G(X, Y) \in Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$, and so

$$H(X, Y) + H(X+Y, Z) - \frac{1}{(l+1)!}G(X, Y)^{l+1} - \frac{1}{(l+1)!}G(X+Y, Z)^{l+1}$$
$$= H(X, Y+Z) + H(Y, Z) - \frac{1}{(l+1)!}G(X, Y+Z)^{l+1} - \frac{1}{(l+1)!}G(Y, Z)^{l+1},$$

it follows that

$$\tilde{H}(X, Y) := H(X, Y) - \frac{1}{(l+1)!}G(X, Y)^{l+1} \in Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}). \tag{6}$$

Noting that $\tilde{H}(X, Y)$ has only terms of degree i with $(l+1)(p^r+1) \leq i \leq (l+2)(p^r+1) - 1$, we can conclude by Proposition 2.3 that

$$\tilde{H}(X, Y) \in Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A}).$$

By Remark 2.6, there exist $\tilde{F}(X, Y) \in Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ such that

$$\tilde{F}(X, Y) \equiv 1 + \tilde{H}(X, Y) \mod \deg(l+2)(p^r+1).$$

Hence we have

$$F(X, Y)\tilde{F}(X, Y)^{-1} \equiv \left\{\sum_{k=0}^{l}\frac{1}{k!}G(X, Y)^k + H(X, Y)\right\}\{1 - \tilde{H}(X, Y)\}$$
$$\equiv \sum_{k=0}^{l}\frac{1}{k!}G(X, Y)^k + \frac{1}{(l+1)!}G(X, Y)^{l+1}$$
$$\mod \deg(l+2)(p^r+1)$$

by (4) and (6).

Step 3. Assume that

$$F(X, Y) \equiv \sum_{k=0}^{p-2}\frac{1}{k!}G(X, Y)^k + H(X, Y) \mod \deg(p^{r+1}+1), \tag{7}$$

where

$$H(X, Y) = \sum_{i=(p-1)(p^r+1)}^{p^{r+1}} H_i(X, Y),$$

here $H_i(X, Y)$ is homogeneous part of degree i and

$$G(X, Y) = a_{r,0}XY^{p^r} + a_{r-1,1}X^p Y^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}} Y^{p^r}.$$

By (5), we obtain that

$$\left\{\sum_{k=0}^{p-2} \frac{1}{k!} G(X, Y)^k\right\}\left\{\sum_{k=0}^{p-2} \frac{1}{k!} G(X+Y, Z)^k\right\} \equiv \sum_{k=0}^{p-2} \frac{1}{k!}(G(X, Y) + G(X+Y, Z))^k$$
$$+ \frac{1}{(p-1)!}\{(G(X, Y) + G(X+Y, Z))^{p-1} - G(X, Y)^{p-1} - G(X+Y, Z)^{p-1}\}$$
$$\mod \deg p(p^r+1)$$

and

$$\left\{\sum_{k=0}^{p-2} \frac{1}{k!} G(X, Y+Z)^k\right\}\left\{\sum_{k=0}^{p-2} \frac{1}{k!} G(Y, Z)^k\right\} \equiv \sum_{k=0}^{p-2} \frac{1}{k!}(G(X, Y+Z) + G(Y, Z))^k$$
$$+ \frac{1}{(p-1)!}\{(G(X, Y+Z) + G(Y, Z))^{p-1} - G(X, Y+Z)^{p-1} - G(Y, Z)^{p-1}\}$$
$$\mod \deg p(p^r+1).$$

On the other hand, since

$$F(X, Y)F(X+Y, Z) = F(X, Y+Z)F(Y, Z),$$

we have

$$\left\{\sum_{k=0}^{p-2} \frac{1}{k!} G(X, Y)^k + H(X, Y)\right\}\left\{\sum_{k=0}^{p-2} \frac{1}{k!} G(X+Y, Z)^k + H(X+Y, Z)\right\}$$
$$\equiv \left\{\sum_{k=0}^{p-2} \frac{1}{k!} G(X, Y+Z)^k + H(X, Y+Z)\right\}\left\{\sum_{k=0}^{p-2} \frac{1}{k!} G(Y, Z)^k + H(Y, Z)\right\}$$
$$\mod \deg(p^{r+1}+1).$$

Comparing the terms of degree i with $(p-1)(p^r+1) \le i \le p^{r+1}$, we have

$$H(X,Y)+H(X+Y,Z)$$
$$+\frac{1}{(p-1)!}\{(G(X,Y)+G(X+Y,Z))^{p-1}-G(X,Y)^{p-1}-G(X+Y,Z)^{p-1}\}$$
$$=H(X,Y+Z)+H(Y,Z)$$
$$+\frac{1}{(p-1)!}\{(G(X,Y+Z)+G(Y,Z))^{p-1}-G(X,Y+Z)^{p-1}-G(Y,Z)^{p-1}\}.$$

Since we see that $G(X,Y)\in Z^2(\boldsymbol{G}_{a,A},\boldsymbol{G}_{a,A})$, and so

$$H(X,Y)+H(X+Y,Z)-\frac{1}{(p-1)!}G(X,Y)^{p-1}-\frac{1}{(p-1)!}G(X+Y,Z)^{p-1}$$
$$=H(X,Y+Z)+H(Y,Z)-\frac{1}{(p-1)!}G(X,Y+Z)^{p-1}-\frac{1}{(p-1)!}G(Y,Z)^{p-1},$$

it follows that

$$\tilde{H}(X,Y):=H(X,Y)-\frac{1}{(p-1)!}G(X,Y)^{p-1}\in Z^2(\boldsymbol{G}_{a,A},\boldsymbol{G}_{a,A}). \tag{8}$$

Noting that $\tilde{H}(X,Y)$ has only terms of degree i with $(p-1)(p^r+1)\le i\le p^{r+1}$, we can conclude by Proposition 2.3 that

$$\tilde{H}(X,Y)\in Z_0^2(\boldsymbol{G}_{a,A},\boldsymbol{G}_{a,A}).$$

By Remark 2.6, there exist $\tilde{F}(X,Y)\in Z_0^2(\hat{\boldsymbol{G}}_{a,A},\hat{\boldsymbol{G}}_{m,A})$ such that

$$\tilde{F}(X,Y)\equiv 1+\tilde{H}(X,Y)\mod\deg(p^{r+1}+1).$$

Hence we have

$$F(X,Y)\tilde{F}(X,Y)^{-1}\equiv\left\{\sum_{k=0}^{p-2}\frac{1}{k!}G(X,Y)^k+H(X,Y)\right\}\{1-\tilde{H}(X,Y)\}$$
$$\equiv\sum_{k=0}^{p-2}\frac{1}{k!}G(X,Y)^k+\frac{1}{(p-1)!}G(X,Y)^{p-1}\mod\deg(p^{r+1}+1)$$

by (7) and (8).

Lemma 3.2. *Let A be an $\boldsymbol{F}_p$-algebra and $F(X,Y)\in Z^2(\hat{\boldsymbol{G}}_{a,A},\hat{\boldsymbol{G}}_{m,A})$. If*

$$F(X,Y)\equiv\sum_{k=0}^{p-1}\frac{1}{k!}\{a_{r,0}XY^{p^r}+a_{r-1,1}X^pY^{p^r}+\cdots+a_{1,r-1}X^{p^{r-1}}Y^{p^r}\}^k$$
$$\mod\deg(p^{r+1}+1)$$

with $r > 0$ *and* $a_{r,0}, a_{r-1,1}, \dots, a_{1,r-1} \in A$, *then*

$$a_{r,0}^p = a_{r-1,1}^p = \cdots = a_{1,r-1}^p = 0.$$

PROOF. We shall prove $a_{r-l,l}^p = 0$ by the induction on l $(0 \le l \le r-1)$.
Step 1. Assume that

$$F(X,Y) \equiv \sum_{k=0}^{p-1} \frac{1}{k!} G(X,Y)^k + H(X,Y) \mod \deg(p(p^r+1)+1),$$

where

$$H(X,Y) = \sum_{i=p^{r+1}+1}^{p(p^r+1)} H_i(X,Y),$$

here $H_i(X,Y)$ is homogeneous part of degree i and

$$G(X,Y) = a_{r,0}XY^{p^r} + a_{r-1,1}X^pY^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}}Y^{p^r}.$$

Now put

$$W(X,Y) = \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X^{p-i}Y^i = \frac{(X+Y)^p - X^p - Y^p}{p}$$

as in the proof of Proposition 2.3. By (5), we obtain that

$$\left\{\sum_{k=0}^{p-1} \frac{1}{k!} G(X,Y)^k\right\}\left\{\sum_{k=0}^{p-1} \frac{1}{k!} G(X+Y,Z)^k\right\}$$
$$\equiv \sum_{k=0}^{p-1} \frac{1}{k!}\{G(X,Y) + G(X+Y,Z)\}^k - W(G(X,Y), G(X+Y,Z))$$
$$\mod \deg(p+1)(p^r+1)$$

and

$$\left\{\sum_{k=0}^{p-1} \frac{1}{k!} G(X,Y+Z)^k\right\}\left\{\sum_{k=0}^{p-1} \frac{1}{k!} G(Y,Z)^k\right\}$$
$$\equiv \sum_{k=0}^{p-1} \frac{1}{k!}\{G(X,Y+Z) + G(Y,Z)\}^k - W(G(X,Y+Z), G(Y,Z))$$
$$\mod \deg(p+1)(p^r+1)$$

since $(p-1)! \equiv -1 \bmod p$. On the other hand, since

$$F(X, Y)F(X+Y, Z) = F(X, Y+Z)F(Y, Z),$$

we have

$$\left\{\sum_{k=0}^{p-1} \frac{1}{k!} G(X, Y)^k + H(X, Y)\right\}\left\{\sum_{k=0}^{p-1} \frac{1}{k!} G(X+Y, Z)^k + H(X+Y, Z)\right\}$$
$$\equiv \left\{\sum_{k=0}^{p-1} \frac{1}{k!} G(X, Y+Z)^k + H(X, Y+Z)\right\}\left\{\sum_{k=0}^{p-1} \frac{1}{k!} G(Y, Z)^k + H(Y, Z)\right\}$$
$$\bmod \deg(p(p^r+1)+1).$$

Hence we obtain

$$\sum_{k=0}^{p-1} \frac{1}{k!}\{G(X, Y) + G(X+Y, Z)\}^k - W(G(X, Y), G(X+Y, Z))$$
$$+ H(X, Y) + H(X+Y, Z)$$
$$\equiv \sum_{k=0}^{p-1} \frac{1}{k!}\{G(X, Y+Z) + G(Y, Z)\}^k - W(G(X, Y+Z), G(Y, Z))$$
$$+ H(X, Y+Z) + H(Y, Z) \bmod \deg(p(p^r+1)+1).$$

Since we see that $G(X, Y) \in Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{a,A})$, we obtain

$$-W(G(X, Y), G(X+Y, Z)) + H(X, Y) + H(X+Y, Z)$$
$$\equiv -W(G(X, Y+Z), G(Y, Z)) + H(X, Y+Z) + H(Y, Z)$$
$$\bmod \deg(p(p^r+1)+1).$$

Now noting that

$$W(G(X, Y), G(X+Y, Z))$$
$$\equiv W(a_{r,0}XY^{p^r}, a_{r,0}(X+Y)Z^{p^r}) \bmod \deg(p(p^r+1)+1)$$

and

$$W(G(X, Y+Z), G(Y, Z))$$
$$\equiv W(a_{r,0}X(Y+Z)^{p^r}, a_{r,0}YZ^{p^r}) \bmod \deg(p(p^r+1)+1),$$

we obtain

$$H_{p(p^r+1)}(X, Y) + H_{p(p^r+1)}(X + Y, Z) - a_{r,0}^p W(XY^{p^r}, XZ^{p^r} + YZ^{p^r})$$
$$= H_{p(p^r+1)}(X, Y + Z) + H_{p(p^r+1)}(Y, Z) - a_{r,0}^p W(XY^{p^r} + XZ^{p^r}, YZ^{p^r}). \tag{9}$$

Put now

$$H_{p(p^r+1)}(X, Y) = \sum_{i+j=p(p^r+1)} c_{ij} X^i Y^j.$$

It is easily varified that

$$\begin{aligned} W(XY^{p^r}, XZ^{p^r} + YZ^{p^r}) &= \frac{1}{p}\sum_{l=1}^{p-1}\binom{p}{l}(XY^{p^r})^{p-l}(XZ^{p^r} + YZ^{p^r})^l \\ &= \sum_{\substack{i+j+k=p \\ i\geq 1, j+k\geq 1}} \frac{(p-1)!}{i!j!k!} X^{i+j} Y^{ip^r+k} Z^{(j+k)p^r} \end{aligned}$$

and

$$\begin{aligned} W(XY^{p^r} + XZ^{p^r}, YZ^{p^r}) &= \frac{1}{p}\sum_{l=1}^{p-1}\binom{p}{l}(XY^{p^r} + XZ^{p^r})^{p-l}(YZ^{p^r})^l \\ &= \sum_{\substack{i+j+k=p \\ k\geq 1, i+j\geq 1}} \frac{(p-1)!}{i!j!k!} X^{i+j} Y^{ip^r+k} Z^{(j+k)p^r}. \end{aligned}$$

Equating coefficients of $XY^{p-1}Z^{p^{r+1}}$, $XY^{p^{r+1}}Z^{p-1}$, $X^{p^{r+1}}YZ^{p-1}$ on (9) gives

$$\begin{cases} 0 = c_{1,p(p^r+1)-1} - a_{r,0}^p, \\ c_{p^{r+1}+1,p-1} = c_{1,p(p^r+1)-1}, \\ c_{p^{r+1}+1,p-1} = 0. \end{cases}$$

Hence we obtain

$$a_{r,0}^p = 0.$$

Step 2. Let $r \geq 2$. Assume that

$$a_{r,0}^p = a_{r-1,1}^p = \cdots = a_{r-l,l}^p = 0 \quad (l < r-1).$$

Then

$$E_p(a_{r,0}XY^{p^r}) \cdots E_p(a_{r-l,l}X^{p^l}Y^{p^r}) \in Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) \subset Z^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$$

and then

$$F(X, Y)E_p(a_{r,0}XY^{p^r})^{-1}E_p(a_{r-1,1}X^pY^{p^r})^{-1}\cdots E_p(a_{r-l,l}X^{p^l}Y^{p^r})^{-1} \in Z^2(\hat{G}_{a,A}, \hat{G}_{m,A}).$$

We have also

$$F(X, Y)E_p(a_{r,0}XY^{p^r})^{-1}E_p(a_{r-1,1}X^pY^{p^r})^{-1}\cdots E_p(a_{r-l,l}X^{p^l}Y^{p^r})^{-1}$$

$$\equiv \sum_{k=0}^{p-1}\frac{1}{k!}\{a_{r-(l+1),l+1}X^{p^{l+1}}Y^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}}Y^{p^r}\}^k \mod \deg(p^{r+1}+1).$$

Replacing $F(X, Y)E_p(a_{r,0}XY^{p^r})^{-1}E_p(a_{r-1,1}X^pY^{p^r})^{-1}\cdots E_p(a_{r-l,l}X^{p^l}Y^{p^r})^{-1}$ by $F(X, Y)$, we may assume that

$$F(X, Y) \equiv \sum_{k=0}^{p-1}\frac{1}{k!}\{a_{r-(l+1),l+1}X^{p^{l+1}}Y^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}}Y^{p^r}\}^k$$

$$\mod \deg(p^{r+1}+1).$$

Assume that

$$F(X, Y) \equiv \sum_{k=0}^{p-1}\frac{1}{k!}G(X, Y)^k + H(X, Y) \mod \deg(p(p^r+p^l)+1),$$

where

$$H(X, Y) = \sum_{i=p^{r+1}+1}^{p(p^r+p^l)} H_i(X, Y),$$

here $H_i(X, Y)$ is homogeneous part of degree i and

$$G(X, Y) = a_{r-(l+1),l+1}X^{p^{l+1}}Y^{p^r} + \cdots + a_{1,r-1}X^{p^{r-1}}Y^{p^r}.$$

Now put $W(X, Y)$ as in the proof of Proposition 2.3. By (5), we obtain that

$$\left\{\sum_{k=0}^{p-1}\frac{1}{k!}G(X, Y)^k\right\}\left\{\sum_{k=0}^{p-1}\frac{1}{k!}G(X+Y, Z)^k\right\}$$

$$\equiv \sum_{k=0}^{p-1}\frac{1}{k!}\{G(X, Y) + G(X+Y, Z)\}^k - W(G(X, Y), G(X+Y, Z))$$

$$\mod \deg(p+1)(p^r+1)$$

and

$$\left\{\sum_{k=0}^{p-1}\frac{1}{k!}G(X,Y+Z)^k\right\}\left\{\sum_{k=0}^{p-1}\frac{1}{k!}G(Y,Z)^k\right\}$$

$$\equiv \sum_{k=0}^{p-1}\frac{1}{k!}\{G(X,Y+Z)+G(Y,Z)\}^k - W(G(X,Y+Z),G(Y,Z))$$

$$\bmod \deg(p+1)(p^r+1).$$

On the other hand, since

$$F(X,Y)F(X+Y,Z) = F(X,Y+Z)F(Y,Z),$$

we have

$$\left\{\sum_{k=0}^{p-1}\frac{1}{k!}G(X,Y)^k + H(X,Y)\right\}\left\{\sum_{k=0}^{p-1}\frac{1}{k!}G(X+Y,Z)^k + H(X+Y,Z)\right\}$$

$$\equiv \left\{\sum_{k=0}^{p-1}\frac{1}{k!}G(X,Y+Z)^k + H(X,Y+Z)\right\}\left\{\sum_{k=0}^{p-1}\frac{1}{k!}G(Y,Z)^k + H(Y,Z)\right\}$$

$$\bmod \deg(p(p^r+p^l)+1).$$

Hence we obtain

$$\sum_{k=0}^{p-1}\frac{1}{k!}\{G(X,Y)+G(X+Y,Z)\}^k - W(G(X,Y),G(X+Y,Z))$$

$$+H(X,Y)+H(X+Y,Z)$$

$$\equiv \sum_{k=0}^{p-1}\frac{1}{k!}\{G(X,Y+Z)+G(Y,Z)\}^k - W(G(X,Y+Z),G(Y,Z))$$

$$+H(X,Y+Z)+H(Y,Z) \bmod \deg(p(p^r+p^l)+1).$$

Since we see that $G(X,Y) \in Z^2(\boldsymbol{G}_{a,A},\boldsymbol{G}_{a,A})$, we obtain

$$-W(G(X,Y),G(X+Y,Z)) + H(X,Y) + H(X+Y,Z)$$

$$\equiv -W(G(X,Y+Z),G(Y,Z)) + H(X,Y+Z) + H(Y,Z)$$

$$\bmod \deg(p(p^r+p^l)+1).$$

Now noting that

$$W(G(X,Y),G(X+Y,Z)) \equiv W(a_{r-(l+1),l+1}X^{p^{l+1}}Y^{p^r}, a_{r-(l+1),l+1}(X+Y)^{p^{l+1}}Z^{p^r}) \mod \deg(p(p^r+p^l)+1)$$

and

$$W(G(X,Y+Z),G(Y,Z)) \equiv W(a_{r-(l+1),l+1}X^{p^{l+1}}(Y+Z)^{p^r}, a_{r-(l+1),l+1}Y^{p^{l+1}}Z^{p^r}) \mod \deg(p(p^r+p^l)+1),$$

we obtain

$$\begin{aligned}
&H_{p(p^r+p^{l+1})}(X,Y)+H_{p(p^r+p^{l+1})}(X+Y,Z)\\
&\quad - a^p_{r-(l+1),l+1}W(X^{p^{l+1}}Y^{p^r}, X^{p^{l+1}}Z^{p^r}+Y^{p^{l+1}}Z^{p^r})\\
&= H_{p(p^r+p^{l+1})}(X,Y+Z)+H_{p(p^r+p^{l+1})}(Y,Z)\\
&\quad - a^p_{r-(l+1),l+1}W(X^{p^{l+1}}Y^{p^r}+X^{p^{l+1}}Z^{p^r}, Y^{p^{l+1}}Z^{p^r}).
\end{aligned}$$

Note that $X^{p^{l+1}}Y^{p^r}=(XY^{p^{r-l-1}})^{p^{l+1}}$. Replacing $X^{p^{l+1}}Y^{p^r}$ by $XY^{p^{r-l-1}}$, we see

$$\begin{aligned}
&H_{p(p^{r-l-1}+1)}(X,Y)+H_{p(p^{r-l-1}+1)}(X+Y,Z)\\
&\quad - a^p_{r-(l+1),l+1}W(XY^{p^{r-l-1}}, XZ^{p^{r-l-1}}+YZ^{p^{r-l-1}})\\
&= H_{p(p^{r-l-1}+1)}(X,Y+Z)+H_{p(p^{r-l-1}+1)}(Y,Z)\\
&\quad - a^p_{r-(l+1),l+1}W(XY^{p^{r-l-1}}+XZ^{p^{r-l-1}}, YZ^{p^{r-l-1}}).
\end{aligned} \tag{10}$$

Put now

$$H_{p(p^{r-l-1}+1)}(X,Y)=\sum_{i+j=p(p^{r-l-1}+1)} c_{ij}X^iY^j.$$

It is easily varified that

$$\begin{aligned}
W(XY^{p^{r-l-1}}, XZ^{p^{r-l-1}}+YZ^{p^{r-l-1}}) &= \frac{1}{p}\sum_{u=1}^{p-1}\binom{p}{u}(XY^{p^{r-l-1}})^{p-u}(XZ^{p^{r-l-1}}+YZ^{p^{r-l-1}})^u\\
&= \sum_{\substack{i+j+k=p\\ i\geq 1, j+k\geq 1}} \frac{(p-1)!}{i!j!k!}X^{i+j}Y^{ip^{r-l-1}+k}Z^{(j+k)p^{r-l-1}}
\end{aligned}$$

and

$$W(XY^{p^{r-l-1}}+XZ^{p^{r-l-1}}, YZ^{p^{r-l-1}}) = \frac{1}{p}\sum_{u=1}^{p-1}\binom{p}{u}(XY^{p^{r-l-1}}+XZ^{p^{r-l-1}})^{p-u}(YZ^{p^{r-l-1}})^{u}$$

$$= \sum_{\substack{i+j+k=p\\ k\geq 1, i+j\geq 1}} \frac{(p-1)!}{i!j!k!} X^{i+j} Y^{ip^{r-l-1}+k} Z^{(j+k)p^{r-l-1}}.$$

Equating coefficients of $XY^{p-1}Z^{p^{r-l}}$, $XY^{p^{r-l}}Z^{p-1}$, $X^{p^{r-l}}YZ^{p-1}$ on (10) gives

$$\begin{cases} 0 = c_{1,p^{r-l}+p-1} - a^{p}_{r-(l+1),l+1}, \\ c_{p^{r-l}+1,p-1} = c_{1,p^{r-l}+p-1}, \\ c_{p^{r-l}+1,p-1} = 0. \end{cases}$$

Hence we obtain

$$a^{p}_{r-(l+1),l+1} = 0.$$

COROLLARY 3.3. *Under the assumption of Lemma* 3.2, *we have*

$$F(X,Y)E_p(a_{r,0}XY^{p^r})^{-1}\cdots E_p(a_{1,r-1}X^{p^{r-1}}Y^{p^r})^{-1} \in Z^2(\hat{G}_{a,A},\hat{G}_{m,A})$$

and

$$F(X,Y)E_p(a_{r,0}XY^{p^r})^{-1}\cdots E_p(a_{1,r-1}X^{p^{r-1}}Y^{p^r})^{-1} \equiv 1 \mod \deg(p^{r+1}+1).$$

3.4. Now we prove the first result of Theorem 2.8 for formal group schemes, that is, the bijectivity of the homomorphism

$$(\mathrm{Ker}[F : W(A) \to W(A)])^N \to H^2(\hat{G}_{a,A},\hat{G}_{m,A})/H_0^2(\hat{G}_{a,A},\hat{G}_{m,A})$$

which was explicitly given in the theorem. It is enough to prove the surjectivity since the injectivity is obvious.

Let $F(X,Y) \in Z^2(\hat{G}_{a,A},\hat{G}_{m,A})$. By 2.2, $F(X,Y) \equiv 1 \mod \deg 1$. Assume that

$$F(X,Y) \equiv 1 + H(X,Y) \mod \deg 2,$$

where

$$H(X,Y) = c_{1,0}X + c_{0,1}Y.$$

Since

$$F(X,Y)F(X+Y,Z) = F(X,Y+Z)F(Y,Z),$$

we have

$$c_{1,0} = c_{0,1} = 0.$$

Moreover, we obtain the following fact by the same argument as in Lemma 3.1.

If $F(X, Y) \equiv 1 \mod \deg 2$, then there exists $\tilde{F}(X, Y) \in Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ such that

$$F(X, Y)\tilde{F}(X, Y)^{-1} \equiv 1 \mod \deg(p+1).$$

Replacing $F(X, Y)\tilde{F}(X, Y)^{-1}$ by $F(X, Y)$, we may assume that

$$F(X, Y) \equiv 1 \mod \deg(p+1).$$

By Lemma 3.1, there exists $\tilde{F}(X, Y) \in Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ and $a_{1,0} \in A$ such that

$$F(X, Y)\tilde{F}(X, Y)^{-1} \equiv \sum_{k=0}^{p-1} \frac{1}{k!}\{a_{1,0}XY^p\}^k \mod \deg(p^2+1).$$

By Lemma 3.2,

$$a_{1,0}^p = 0.$$

Hence

$$F(X, Y)\tilde{F}(X, Y)^{-1} \equiv E_p(a_{1,0}XY^p) \mod \deg(p^2+1),$$

and therefore

$$F(X, Y)\tilde{F}(X, Y)^{-1}E_p(a_{1,0}XY^p)^{-1} \equiv 1 \mod \deg(p^2+1).$$

Note that

$$F(X, Y)\tilde{F}(X, Y)^{-1}E_p(a_{1,0}XY^p)^{-1} \in Z^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$$

by Corollary 3.3. Replacing $F(X, Y)\tilde{F}(X, Y)^{-1}E_p(a_{1,0}XY^p)^{-1}$ by $F(X, Y)$, we may assume that

$$F(X, Y) \equiv 1 \mod \deg(p^2+1).$$

Continuing this process, we find $\tilde{F}(X, Y) \in Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A})$ such that

$$F(X, Y)\tilde{F}(X, Y)^{-1} = \prod_{r=1}^{\infty}\prod_{j=0}^{r-1} E_p(a_{r-j,j}X^{p^j}Y^{p^r}) = \prod_{r=1}^{\infty}\prod_{j=0}^{\infty} E_p(a_{r,j}X^{p^j}Y^{p^{r+j}})$$

$$= \prod_{r=1}^{\infty} E_p(\boldsymbol{a}_r; XY^{p^r}).$$

This proves the desired surjectivity. The second result of Theorem 2.8 for group schemes follows by the next:

LEMMA 3.5. *Let A be an $\boldsymbol{F}_p$-algebra and $F(X,Y) \in Z^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A}) \subset A[X,Y]^{\times}$. Then there exists $\tilde{F}(X,Y) \in Z_0^2(\boldsymbol{G}_{a,A}, \boldsymbol{G}_{m,A})$ and $(\boldsymbol{a}_r)_{r\geq 1} \in (\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)])^{(N)}$ such that*

$$F(X,Y)\tilde{F}(X,Y)^{-1} = \prod_{r\geq 1} E_p(\boldsymbol{a}_r; XY^{p^r}).$$

PROOF. Let $\boldsymbol{P} = \{p^r; r \geq 0\}$. Dividing $F(X,Y)$ by its constant term, we may assume that $F(X,Y) \equiv 1 \bmod \deg 1$. By 3.4, there exists $\tilde{F}(X,Y) \in Z_0^2(\hat{\boldsymbol{G}}_{a,A}, \hat{\boldsymbol{G}}_{m,A}) \subset A[[X,Y]]^{\times}$ and $a_{r,j} \in A$ $(0 \leq j < r)$ such that

$$F(X,Y)\tilde{F}(X,Y)^{-1} = \prod_{r\geq 1} E_p(\boldsymbol{a}_r; XY^{p^r}).$$

By a result of [3, 3.4], there exist $a_k \in A$ $(k \notin \boldsymbol{P})$, $\boldsymbol{b} = (b_l)_{l\geq 0} \in W(A)$ such that

$$\tilde{F}(X,Y) = \prod_{k\notin \boldsymbol{P}} \{E_p(a_k X^k) E_p(a_k Y^k) E_p(a_k (X+Y)^k)^{-1}\} F_p(\boldsymbol{b}; X, Y).$$

Hence we obtain a factorization:

$$\begin{aligned} F(X,Y) = & \prod_{k\notin \boldsymbol{P}} \{E_p(a_k X^k) E_p(a_k Y^k) E_p(a_k (X+Y)^k)^{-1}\} \\ & \times \prod_{l\geq 0} F_p(b_l; X^{p^l}, Y^{p^l}) \prod_{r=1}^{\infty} \prod_{j=0}^{r-1} E_p(a_{r-j,j} X^{p^j} Y^{p^r}). \end{aligned}$$

Now we prove that a_k is nilpotent for all k $(k \notin \boldsymbol{P})$ and is zero for all but finite number of k, $\boldsymbol{b} = (b_l)_{l\geq 0} \in \hat{W}(A)$ and $(\boldsymbol{a}_r)_{r\geq 1} \in (\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)])^{(N)}$.

We now observe that:

(1) Putting

$$E_p(X^k) E_p(Y^k) E_p((X+Y)^k)^{-1} = 1 + \sum_{l=1}^{\infty} \sum_{i+j=l} c_{ij} X^{ki} Y^{kj} \in \boldsymbol{Z}_{(p)}[[X,Y]],$$

we have, for $a \in A$,

$$E_p(aX^k) E_p(aY^k) E_p(a(X+Y)^k)^{-1} = 1 + \sum_{l=1}^{\infty} a^l \left(\sum_{i+j=l} c_{ij} X^{ki} Y^{kj} \right) \in A[[X,Y]]$$

and

$$E_p(aX^k)E_p(aY^k)E_p(a(X+Y)^k)^{-1} \equiv 1 + a\{X^k + Y^k - (X+Y)^k\} \mod \deg(k+1).$$

(2) Putting

$$F_p(1; X^{p^r}, Y^{p^r}) = 1 + \sum_{\substack{l>0 \\ p^{r+1}|l}} \sum_{i+j=l} c_{ij} X^i Y^j \in \boldsymbol{Z}_{(p)}[[X, Y]],$$

we have, for $a \in A$,

$$F_p(a; X^{p^r}, Y^{p^r}) = 1 + \sum_{\substack{l>0 \\ p^{r+1}|l}} a^{l/p^{r+1}} \left(\sum_{i+j=l} c_{ij} X^i Y^j \right) \in A[[X, Y]]$$

and

$$F_p(a; X^{p^r}, Y^{p^r}) \equiv 1 + a \frac{X^{p^{r+1}} + Y^{p^{r+1}} - (X+Y)^{p^{r+1}}}{p} \mod \deg(p^{r+1} + 1).$$

(3) Putting

$$E_p(X^{p^j} Y^{p^r}) = 1 + \sum_{l=1}^{\infty} c_l (X^{p^j} Y^{p^r})^l \in \boldsymbol{Z}_{(p)}[[X, Y]],$$

we have, for $a \in A$,

$$E_p(aX^{p^j} Y^{p^r}) = 1 + \sum_{l=1}^{\infty} c_l a^l (X^{p^j} Y^{p^r})^l \in A[[X, Y]]$$

and

$$E_p(aX^{p^j} Y^{p^r}) \equiv 1 + aX^{p^j} Y^{p^r} \mod \deg(p^j + p^r + 1).$$

Let N be the degree of $F(X, Y)$ and let $\mathfrak{a}$ denote the ideal of A generated by the coefficients of terms of degree ≥ 1 in $F(X, Y)$. Since the polynomial $F(X, Y)$ is invertible, $\mathfrak{a}$ is nilpotent.

For the simplicity, we put $a_{p^{l+1}} = b_l$ and

$$F_k(X, Y) = \begin{cases} F_p(a_{p^{l+1}}; X^{p^l}, Y^{p^l}) & \text{if } k = p^{l+1} \ (l \geq 0) \\ \dfrac{E_p(a_k X^k) E_p(a_k Y^k)}{E_p(a_k (X+Y)^k)} E_p(a_{r-j,j} X^{p^j} Y^{p^r}) & \text{if } k = p^j + p^r \ (0 \leq j < r) \\ \dfrac{E_p(a_k X^k) E_p(a_k Y^k)}{E_p(a_k (X+Y)^k)} & \text{otherwise.} \end{cases}$$

Then we have

$$F(X, Y) = \prod_{k=2}^{\infty} F_k(X, Y)$$

and, up to $\deg(k+1)$,

$$F_k(X, Y) \equiv \begin{cases} 1 + a_{p^{l+1}} \dfrac{X^{p^{l+1}} + Y^{p^{l+1}} - (X+Y)^{p^{l+1}}}{p} & \text{if } k = p^{l+1} \ (l \geq 0) \\ 1 + a_k\{X^k + Y^k - (X+Y)^k\} + a_{r-j,j} X^{p^j} Y^{p^r} & \text{if } k = p^j + p^r \\ & \quad (0 \leq j < r) \\ 1 + a_k\{X^k + Y^k - (X+Y)^k\} & \text{otherwise.} \end{cases}$$

Furthermore, let

$$F_k(X, Y) = 1 + \sum_{l \geq k} \sum_{i+j=l} b_{ij} X^i Y^j, \quad b_{ij} \in A.$$

Then we can conclude that if $b_{ij} \in \mathfrak{a}^s$ for all (i, j) with $i + j = k$, then $b_{ij} \in \mathfrak{a}^{s+[(i+j)/k]-1}$ for all (i, j) with $i + j > k$.

Step 1. We shall prove that

$$a_k \in \mathfrak{a} \quad \text{if } k \leq N$$

and

$$a_{r-j,j} \in \mathfrak{a} \quad \text{if } p^j + p^r \leq N$$

by the induction on k and (r, j) with $0 \leq j < r$.

Let k be an integer $< N$. Assume that

$$a_i \in \mathfrak{a} \quad \text{if } i < k$$

and

$$a_{r-j,j} \in \mathfrak{a} \quad \text{if } p^j + p^r < k.$$

Then we obtain

$$F(X, Y) \equiv F_k(X, Y) \bmod(\mathfrak{a}, \deg(k+1)).$$

Case 1: When $k = p^{l+1}$ $(l \geq 0)$,

$$\frac{1}{p}\binom{p^{l+1}}{p^h} a_{p^{l+1}} \in \mathfrak{a} \quad \text{for } 1 \leq h \leq l.$$

Since $\frac{1}{p}\binom{p^{l+1}}{p^h} \not\equiv 0 \bmod p$, we obtain $a_{p^{l+1}} \in \mathfrak{a}$.

Case 2: When $k = p^j + p^r$ $(0 \leq j < r)$,

$$\binom{p^j + p^r}{p^j} a_k + a_{r-j,j} \in \mathfrak{a}.$$

Since $\binom{p^j + p^r}{p^j} \not\equiv 0 \bmod p$, we obtain $a_k \in \mathfrak{a}$ and $a_{r-j,j} \in \mathfrak{a}$.

Case 3: Otherwise,

$$ka_k \in \mathfrak{a}.$$

Since $(k, p) = 1$, we obtain $a_k \in \mathfrak{a}$.

Step 2. We shall prove that

$$a_k \in \mathfrak{a}^s \quad \text{if } (s-1)N < k \leq sN$$

and

$$a_{r-j,j} \in \mathfrak{a}^s \quad \text{if } (s-1)N < p^j + p^r \leq sN$$

by the induction on k and (r, j) with $0 \leq j < r$.

Let k be an integer $< sN$. Assume that

$$a_i \in \mathfrak{a}^s \quad \text{if } (s-1)N < i < k$$

and

$$a_{r-j,j} \in \mathfrak{a}^s \quad \text{if } (s-1)N < p^j + p^r < k.$$

Then we obtain

$$F(X, Y)\left\{\prod_{i<k} F_i(X, Y)\right\}^{-1} \equiv F_k(X, Y) \equiv 1 + \sum_{i+j=k} c_{ij} X^i Y^j \mod(\mathfrak{a}^s, \deg(k+1)).$$

Now we put

$$F(X, Y) = 1 + \sum \alpha_{ij} X^i Y^j,$$

$$\left\{\prod_{i<k} F_i(X, Y)\right\}^{-1} = 1 + \sum \beta_{ij} X^i Y^j$$

and

$$F(X, Y)\left\{\prod_{i<k} F_i(X, Y)\right\}^{-1} = 1 + \sum \gamma_{ij} X^i Y^j.$$

By the assumption,

$$\alpha_{ij}, \beta_{ij} \in \mathfrak{a}^s \quad \text{if} \quad (s-1)N < i+j \le sN.$$

Hence, we obtain

$$\gamma_{ij} \in \mathfrak{a}^s \quad \text{if} \quad (s-1)N < i+j \le sN.$$

Since $(s-1)N < k < sN$, we obtain $c_{ij} \in \mathfrak{a}^s$.

Hence, a_k and $a_{r-j,j}$ are nilpotent for all k and (r,j) with $0 \le j < r$, and are zero for all but a finite number of k and (r,j) with $0 \le j < r$.

REMARK 3.6. We establish some functorialities. For example,

(1) The diagrams

$$\begin{tikzcd}
(\mathrm{Ker}[F : W(A) \to W(A)])^N \arrow[r, "V"] \arrow[d, "\wr"'] & (\mathrm{Ker}[F : W(A) \to W(A)])^N \arrow[d, "\wr"] \\
H^2(\hat{G}_{a,A}, \hat{G}_{m,A})/H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A}) \arrow[r, "F^*"'] & H^2(\hat{G}_{a,A}, \hat{G}_{m,A})/H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A})
\end{tikzcd}$$

and

$$\begin{tikzcd}
(\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)])^{(N)} \arrow[r, "V"] \arrow[d, "\wr"'] & (\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)])^{(N)} \arrow[d, "\wr"] \\
H^2(G_{a,A}, G_{m,A})/H_0^2(G_{a,A}, G_{m,A}) \arrow[r, "F^*"'] & H^2(G_{a,A}, G_{m,A})/H_0^2(G_{a,A}, G_{m,A})
\end{tikzcd}$$

are commutative.

(2) Let $a \in A$. Then the diagrams

$$\begin{tikzcd}
(\mathrm{Ker}[F : W(A) \to W(A)])^N \arrow[r, "{[a^{p^r+1}]\cdot}"] \arrow[d, "\wr"'] & (\mathrm{Ker}[F : W(A) \to W(A)])^N \arrow[d, "\wr"] \\
H^2(\hat{G}_{a,A}, \hat{G}_{m,A})/H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A}) \arrow[r, "{[a]^*}"'] & H^2(\hat{G}_{a,A}, \hat{G}_{m,A})/H_0^2(\hat{G}_{a,A}, \hat{G}_{m,A})
\end{tikzcd}$$

and

$$\begin{tikzcd}
(\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)])^{(N)} \arrow[r, "{[a^{p^r+1}]\cdot}"] \arrow[d, "\wr"'] & (\mathrm{Ker}[F : \hat{W}(A) \to \hat{W}(A)])^{(N)} \arrow[d, "\wr"] \\
H^2(G_{a,A}, G_{m,A})/H_0^2(G_{a,A}, G_{m,A}) \arrow[r, "{[a]^*}"'] & H^2(G_{a,A}, G_{m,A})/H_0^2(G_{a,A}, G_{m,A})
\end{tikzcd}$$

are commutative. Here $[a^{p^r+1}] = (a^{p^r+1}, 0, 0, \ldots)$ and $[a]^*$ denotes the maps induced by the endomorphism of $\hat{G}_{a,A}$ or of $G_{a,A}$, defined by $T \mapsto aT$.

REMARK 3.7. Let A be a Q-algebra. It is well known that $H^2(\hat{G}_{a,A}, \hat{G}_{a,A}) = 0$ and $H^2(G_{a,A}, G_{a,A}) = 0$ (cf. [1, Chap. II]), from which we can deduce that $H^2(\hat{G}_{a,A}, \hat{G}_{m,A}) = 0$ and $H^2(G_{a,A}, G_{m,A}) = 0$ by the same argument as Theorem 2.8 from Proposition 2.3.

References

[1] M. Demazure and P. Gabriel, Groupes algébriques, Tome1, Masson-North-Holland, Paris-Amsterdam, 1970.
[2] M. Hazewinkel, Formal groups and applications, Academic Press, New York, 1978.
[3] T. Sekiguchi and N. Suwa, A note on extensions of algebraic and formal groups I, Math. Z. **206** (1991), 567–575.

Department of Mathematics
Chuo University
1-13-27 Kasuga, Bunkyo-ku
Tokyo 112-8551, JAPAN
E-mail address: haraguti@gug.math.chuo-u.ac.jp