数理解析研究所講究録 1376 巻 2004 年 181-191

$\mathbb{F}_p$ 代数上の $\mathbb{G}_a$ の $\mathbb{G}_m$ による非可換な拡大について

中央大学・数学専攻（M２）原口　幸 (Yuki Haraguchi)
Department of Mathematics,
Chuo University

1．序

S をスキーム，G を S の上の群スキーム，H を G が作用する S の上の可換群スキームとする．G の H による拡大の同値類のなす群 $\mathrm{Ext}_S^1(G,H)$ を決定すること，あるいは，G と H が線型的である場合に $\mathrm{Ext}_S^1(G,H)$ の部分群である Hochschild cohomology 群 $H^2(G,H)$ を決定すること，さらに，G が可換で G の H の上への作用が自明である場合に $H^2(G,H)$ の部分群である対称 Hochschild cohomology 群 $H_0^2(G,H)$ を決定することは群スキームの理論の中でも重要な問題であるが，$S=\mathrm{Spec}\,K$（K は体）の場合，基本的な群スキームに対する結果が Demazure-Gabriel [1] に集大成されている．そこでは，例えば，加法群スキーム $\mathbb{G}_a$ の乗法群スキーム $\mathbb{G}_m$ による拡大は自明なものに限ることが示されている．

このような研究を一般の環 A の上で展開することは自然な試みであろうが，関口-諏訪 [2] で一般に $H^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})=0$ とは限らないことが注意され，A が $\mathbb{F}_p$ 代数である場合に $H_0^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$ の構造が解明された．これで，A が $\mathbb{F}_p$ 代数であるとき，$\mathbb{G}_{a,A}$ の $\mathbb{G}_{m,A}$ による可換な拡大が決定された訳であるが，非可換な拡大については一つ例が示されているだけで，それ以降非可換な拡大の研究は手付かずであった．

本稿では $\mathbb{G}_a$ の $\mathbb{G}_m$ による非可換な拡大について新たに得られた結果を提示した．その中で最も重要な定理は，A が $\mathbb{F}_p$ 代数である場合，$H^2(\widehat{\mathbb{G}}_{a,A},\widehat{\mathbb{G}}_{m,A})/H_0^2(\widehat{\mathbb{G}}_{a,A},\widehat{\mathbb{G}}_{m,A})$ と $H^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})/H_0^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$ の具体的で完全な記述である．その系として，A が $\mathbb{F}_p$ 代数であるときに，非可換な拡大も含めて $\widehat{\mathbb{G}}_a$ の $\widehat{\mathbb{G}}_m$ による，あるいは $\mathbb{G}_a$ の $\mathbb{G}_m$ による拡大がすべて決定された．

2．主定理

記号 2.1. p を素数，A を $\mathbb{F}_p$ 代数，$W(A)$ を A の元を成分に持つ Witt vector のなす群，$F:W(A)\to W(A)$ を Frobenius 準同型とする．また，

$$E_p(T)=\exp\left(\sum_{r=0}^{\infty}\frac{T^{p^r}}{p^r}\right)\in\mathbb{Z}_{(p)}[[T]] \qquad \text{: Artin-Hasse exponential series}$$

とし，$\boldsymbol{a}\in W(A)$ に対して，$E_p(\boldsymbol{a};T)=\prod_{r\geq 0}E_p(a_rT^{p^r})$ とおく．

2.2. A を環とする．乗法群 $Z^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$, $Z_0^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$, $B^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$ はそれ

それ

$$Z^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})=\left\{F(X,Y)\in A[X,Y]^\times\ ;\ \begin{aligned}&F(X,Y)F(X+Y,Z)\\&\quad=F(X,Y+Z)F(Y,Z)\end{aligned}\right\},$$

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

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

によって定義される．このとき，

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

であり，Hochschild cohomology 群と対称 Hochschild cohomology 群をそれぞれ

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

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

とおく．

加法群 $Z(\mathbb{G}_{a,A},\mathbb{G}_{a,A})$, $Z_0^2(\mathbb{G}_{a,A},\mathbb{G}_{a,A})$, $B^2(\mathbb{G}_{a,A},\mathbb{G}_{a,A})$ はそれぞれ

$$Z^2(\mathbb{G}_{a,A},\mathbb{G}_{a,A})=\left\{F(X,Y)\in A[X,Y]\ ;\ \begin{aligned}&F(X,Y)+F(X+Y,Z)\\&\quad=F(X,Y+Z)+F(Y,Z)\end{aligned}\right\},$$

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

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

によって定義される．このとき，

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

であり，Hochschild cohomology 群と対称 Hochschild cohomology 群をそれぞれ

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

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

とおく．

このとき，次のことが知られている：

1) $H^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$ は，$\mathbb{G}_{a,A}$ の $\mathbb{G}_{m,A}$ による A-scheme の拡大として split する中心拡

大の同値類のなす群と同型である.

2) $H_0^2(\mathbb{G}_{a,A}, \mathbb{G}_{m,A})$ は, $\mathbb{G}_{a,A}$ の $\mathbb{G}_{m,A}$ による A-scheme の拡大として split する可換な拡大の同値類のなす群と同型である.

3) $H^2(\mathbb{G}_{a,A}, \mathbb{G}_{a,A})$ は $\mathbb{G}_{a,A}$ の $\mathbb{G}_{a,A}$ による中心拡大の同値類のなす群と同型である.

4) $H_0^2(\mathbb{G}_{a,A}, \mathbb{G}_{a,A})$ は $\mathbb{G}_{a,A}$ の $\mathbb{G}_{a,A}$ による可換な拡大の同値類のなす群と同型である.

2.3. A を環とする. 乗法的形式群 $Z^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$, $Z_0^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$, $B^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$ はそれぞれ

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

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

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

によって定義される. このとき,

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

であり, Hochschild cohomology 群と対称 Hochschild cohomology 群をそれぞれ

$$H^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A}) = Z^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})/B^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A}),$$
$$H_0^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A}) = Z_0^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})/B^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$$

とおく.

加法的形式群 $Z(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{a,A})$, $Z_0^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{a,A})$, $B^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{a,A})$ はそれぞれ

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

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

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

によって定義される. このとき,

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

であり，Hochschild cohomology 群と対称 Hochschild cohomology 群をそれぞれ

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

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

とおく．

このとき，次のことが知られている：

1) $H^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$ は，$\widehat{\mathbb{G}}_{a,A}$ の $\widehat{\mathbb{G}}_{m,A}$ による形式的 A-scheme の拡大として split する中心拡大の同値類のなす群と同型である．
2) $H_0^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$ は，$\widehat{\mathbb{G}}_{a,A}$ の $\widehat{\mathbb{G}}_{m,A}$ による形式的 A-scheme の拡大として split する可換な拡大の同値類のなす群と同型である．
3) $H^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{a,A})$ は $\widehat{\mathbb{G}}_{a,A}$ の $\widehat{\mathbb{G}}_{a,A}$ による中心拡大の同値類のなす群と同型である．
4) $H_0^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{a,A})$ は $\widehat{\mathbb{G}}_{a,A}$ の $\widehat{\mathbb{G}}_{a,A}$ による可換な拡大の同値類のなす群と同型である．

2.4. ここで，$F(T) \in \mathrm{Hom}_{A\text{-gr}}(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$, $G(X,Y) \in Z^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{a,A})$ とする．このとき，$F(G(X,Y)) \in Z^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$ が成り立つことが分かる．例えば，$\boldsymbol{a} = (a_r)_{r\geq 0} \in \mathrm{Ker}[F : W(A) \to W(A)]$ に対して，

$$E_p(\boldsymbol{a}; T) = \prod_{r\geq 0} E_p(a_r T^{p^r}) = \prod_{r\geq 0}\left[\sum_{i=0}^{p-1} \frac{(a_r T^{p^r})^i}{i!}\right] \in \mathrm{Hom}_{A\text{-gr}}(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$$

が成り立つ．さらに，

$$XY^{p^r} \in Z^2(\mathbb{G}_{a,A}, \mathbb{G}_{a,A}) \subset Z^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{a,A}) \qquad (r > 0)$$

なので，

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

が成り立つ．

逆に，$\widehat{\mathbb{G}}_{m,A}$ に係数を持つ $\widehat{\mathbb{G}}_{a,A}$ の非対称な 2-cocycle は全て上記の方法で得られる．実際，

定理 2.5. A を $\mathbb{F}_p$ 代数とする．このとき，対応 $(\boldsymbol{a}_r)_{r\geq 1} \mapsto \prod_{r\geq 1} E_p(\boldsymbol{a}_r; XY^{p^r})$ によって定義される群の準同型

$$\xi : \left(\mathrm{Ker}[F : W(A) \to W(A)]\right)^{\mathbf{N}} \to H^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})/H_0^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A}),$$

$$\xi : \left(\mathrm{Ker}[F : \widehat{W}(A) \to \widehat{W}(A)]\right)^{(\mathbf{N})} \to H^2(\mathbb{G}_{a,A}, \mathbb{G}_{m,A})/H_0^2(\mathbb{G}_{a,A}, \mathbb{G}_{m,A})$$

は同型である．

2.6. [2] で，$\boldsymbol{U} = (U_0, U_1, U_2, \ldots)$ に対して形式的巾級数 $F_p(\boldsymbol{U}; X, Y) \in \mathbb{Z}_{(p)}[\boldsymbol{U}][[X,Y]]$ が

$$F_p(\boldsymbol{U}; X, Y) = \prod_{r\geq 0} F_p(U_r; X^{p^r}, Y^{p^r})$$

によって定義されている．ただし，

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

とする．[2] の主結果と合わせて次の結論を得る．

系 2.7. A を $\mathbb{F}_p$ 代数，$P(X,Y)\in Z^2(\widehat{\mathbb{G}}_{a,A},\widehat{\mathbb{G}}_{m,A})$ (resp. $Z^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$) とする．このとき，$P(X,Y)$ は，

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

の形の 2-cocycle に cohomologous である．ただし，$\boldsymbol{b}\in W(A)$, $(\boldsymbol{a}_r)_{r\geq 1}\in\left(\mathrm{Ker}[F:W(A)\to W(A)]\right)^{\mathbb{N}}$ (resp. $\boldsymbol{b}\in\widehat{W}(A)$, $(\boldsymbol{a}_r)_{r\geq 1}\in\left(\mathrm{Ker}[F:\widehat{W}(A)\to\widehat{W}(A)]\right)^{(\mathbb{N})}$) とする．

3．主定理の証明

3.1. まず，本稿で鍵となる 3 つの事項を引用する．

[1] では，A が体の場合に $H^2(\mathbb{G}_{a,A},\mathbb{G}_{a,A})$ の具体的な記述が与えられている．この証明を追ってみると，A が $\mathbb{F}_p$ 代数であっても同じ結果が得られることが分かる：

(A) A を $\mathbb{F}_p$ 代数とする．$P(X,Y)\in Z^2(\mathbb{G}_{a,A},\mathbb{G}_{a,A})$ であるとき，$P(X,Y)$ は，

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

の形の 2-cocycle に cohomologous である．

[2] では，A が $\mathbb{F}_p$ 代数の場合に $H_0^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$ の具体的な記述が与えられている：

(B) A を $\mathbb{F}_p$ 代数とする．このとき，対応 $\boldsymbol{a}\mapsto F_p(\boldsymbol{a};X,Y)$ は群の同型

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

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

を誘導する．

さらに，上の結果を得る際，次のような事実が得られている：

(C) A を $\mathbb{F}_p$ 代数とする．このとき，$G(X,Y)\in Z_0^2(\mathbb{G}_{a,A},\mathbb{G}_{a,A})$ で $G(X,Y)$ が次数 l の斉次多項式であるとき，

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

をみたす $F(X,Y)\in Z_0^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$ が存在する．

次に，定理の証明に必要となる補題を準備する．

補題 3.2. A を $\mathbb{F}_p$ 代数とし，$F(X,Y)\in Z^2(\widehat{\mathbb{G}}_{a,A},\widehat{\mathbb{G}}_{m,A})$ とする．このとき，

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

ならば，

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

となる $\widetilde{F}(X,Y)\in Z_0^2(\widehat{\mathbb{G}}_{a,A},\widehat{\mathbb{G}}_{m,A})$ と $a_{r,0}$, $a_{r-1,1}$, $\cdots$, $a_{1,r-1}\in A$ が存在する．

証明.

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

を満たす $\widetilde{F}(X,Y)\in Z_0^2(\widehat{\mathbb{G}}_{a,A},\widehat{\mathbb{G}}_{m,A})$ と $a_{r,0}$, $a_{r-1,1}$, $\cdots$, $a_{1,r-1}\in A$ が存在することを，l $(0\le l\le p-2)$ に関する帰納法によって証明する．

Step 1.

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

と仮定する．ただし，

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

$H_i(X,Y)$ は i 次斉次多項式とする．多項式 $F(X,Y)$ は関数等式

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

を満たすので，$H_i(X,Y)$ は

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

を満たす．したがって，

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

を得る．このとき，(A) より

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

を満たす $\widetilde{H}(X,Y)\in Z_0^2(\mathbb{G}_{a,A},\mathbb{G}_{a,A})$ と $a_{r,0}$, $a_{r-1,1}$, $\cdots$, $a_{1,r-1}\in A$ が存在する．ここで，$\widetilde{H}(X,Y)$ は斉次多項式の和であることに注意する．(C) より

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

を満たす $\widetilde{F}(X,Y) \in Z_0^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$ が存在するので,

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

を得る.

Step 2. 帰納法の仮定より, $l \leq p-2$ に対して

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

とおける. ただし,

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

$H_i(X,Y)$ は i 次斉次多項式とし,

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

とする. ここで,

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

が成り立つので,

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

と

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

を得る. 一方, 多項式 $F(X,Y)$ は関数等式

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

を満たすので,

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

が成り立つ. ここで, $i\ \big((l+1)(p^r+1)\le i\le(l+2)(p^r+1)-1\big)$ 次の項を比較すると,

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

を得る. 多項式 $G(X,Y)$ は関数等式

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

を満たすので,

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

を得る. このことから,

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

が従う. 以下, Step 1 と同様の議論により,

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

を満たす $\widetilde{F}(X,Y)\in Z_0^2(\widehat{\mathbb{G}}_{a,A},\widehat{\mathbb{G}}_{m,A})$ が存在することが従う.

補題 3.3. A を $\mathbb{F}_p$ 代数とし, $F(X,Y)\in Z^2(\widehat{\mathbb{G}}_{a,A},\widehat{\mathbb{G}}_{m,A})$ とする. このとき, $r>0$, $a_{r,0}$, $a_{r-1,1}$, $\cdots$, $a_{1,r-1}\in A$ に対して,

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

ならば，

$$a^p_{r,0} = a^p_{r-1,1} = \cdots = a^p_{1,r-1} = 0.$$

証明． 証明は初等的な議論を重ねて出来るが，幾分長いので詳細は割愛する．要点は，

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

の両辺を展開して，$XY^{p-1}Z^{p^{r-l}}$, $XY^{p^{r-l}}Z^{p-1}$, $X^{p^{r-l}}YZ^{p-1}$ $(0 \leq l \leq r-1)$ の項に着目して係数を比較することである．

3.4. 形式的群スキームの場合について，定理 2.5 を証明する．ξ の全射性を示せば十分である．以下，証明の概略を述べる．

$F(X,Y) \in Z^2(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$ とする．これを定数項で割って，$F(X,Y) \equiv 1 \mod \deg 1$ と仮定してよい．このとき，補題 3.2 と同じ議論により，

$$F(X,Y)\widetilde{F}(X,Y)^{-1} \equiv 1 \mod \deg 2p$$

をみたす $\widetilde{F}(X,Y) \in Z^2_0(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$ が存在することが分かる．$F(X,Y)\widetilde{F}(X,Y)^{-1}$ を $F(X,Y)$ で置き換えて，

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

と仮定する．ここで，補題 3.2 の $r=1$ の場合を適用して，

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

をみたす $\widetilde{F}(X,Y) \in Z^2_0(\widehat{\mathbb{G}}_{a,A}, \widehat{\mathbb{G}}_{m,A})$ と $a_{1,0} \in A$ が存在することが分かる．さらに，補題 3.3 の $r=1$ の場合を適用して，

$$a^p_{1,0} = 0$$

を得る．したがって，

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

であるので，

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

を得る．ここで，

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

であることに注意する．$F(X,Y)\widetilde{F}(X,Y)^{-1}E_p(a_{1,0}XY^p)^{-1}$ を $F(X,Y)$ で置き換えて，

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

と仮定する.

この議論を続けていくと,

$$
\begin{aligned}
&F(X,Y)\widetilde{F}(X,Y)^{-1}\\
&\quad=\prod_{r=1}^{\infty}\prod_{j=0}^{r-1}E_p(a_{r-j,j}X^{p^j}Y^{p^r})=\prod_{r=1}^{\infty}\prod_{j=0}^{\infty}E_p(a_{r,j}X^{p^j}Y^{p^{r+j}})=\prod_{r=1}^{\infty}E_p(\boldsymbol{a}_r;XY^{p^r})
\end{aligned}
$$

をみたす $\widetilde{F}(X,Y)\in Z_0^2(\widehat{\mathbb{G}}_{a,A},\widehat{\mathbb{G}}_{m,A})$ が見つかる. 以上のことから, ξ が全射であることが従う.

群スキームの場合には, 上の結果に次の補題を組み合わせて定理を証明できる.

補題 3.5. A を $\mathbb{F}_p$ 代数とし, $F(X,Y)\in Z^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})\subset A[X,Y]^\times$ とする. このとき,

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

を満たす $\widetilde{F}(X,Y)\in Z_0^2(\mathbb{G}_{a,A},\mathbb{G}_{m,A})$ と $(\boldsymbol{a}_r)_{r\geq1}\in\left(\mathrm{Ker}[F:\widehat{W}(A)\to\widehat{W}(A)]\right)^{(\mathbb{N})}$ が存在する.

証明. 証明の概略を述べる. [2] の主結果を得る過程と合わせて

$$
\begin{aligned}
&F(X,Y)\\
&=\prod_{k\notin\mathbb{P}}\{E_p(a_kX^k)E_p(a_kY^k)E_p(a_k(X+Y)^k)^{-1}\}\prod_{l\geq0}F_p(b_l;X^{p^l},Y^{p^l})\prod_{r=1}^{\infty}\prod_{j=0}^{r-1}E_p(a_{r-j,j}X^{p^j}Y^{p^r})
\end{aligned}
$$

と表せることにまず注意する. ただし, $\mathbb{P}=\{p^r;r\geq0\}$ とする. $F(X,Y)$ が多項式であることから, a_k が巾零元で有限個を除いて 0, $\boldsymbol{b}=(b_l)_{l\geq0}\in\widehat{W}(A)$, $(\boldsymbol{a}_r)_{r\geq1}\in\left(\mathrm{Ker}[F:\widehat{W}(A)\to\widehat{W}(A)]\right)^{(\mathbb{N})}$ であることを示せばよい.

$F(X,Y)$ の次数を N, $F(X,Y)$ の 1 次以上の項の係数で生成される A のイデアルを $\mathfrak{a}$ とする. このとき, 多項式 $F(X,Y)$ は可逆であるので, $\mathfrak{a}$ は巾零イデアルである.

簡単のために, $a_{p^{l+1}}=b_l$,

$$
F_k(X,Y)=\begin{cases}
F_p(a_{p^{l+1}};X^{p^l},Y^{p^l}) & \text{if } k=p^{l+1}\ (l\geq0)\\[2mm]
\dfrac{E_p(a_kX^k)E_p(a_kY^k)}{E_p(a_k(X+Y)^k)}E_p(a_{r-j,j}X^{p^j}Y^{p^r}) & \text{if } k=p^j+p^r\ (0\leq j<r)\\[2mm]
\dfrac{E_p(a_kX^k)E_p(a_kY^k)}{E_p(a_k(X+Y)^k)} & \text{otherwise}
\end{cases}
$$

とおく. このとき,

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

$k+1$ 次以上を除いて，

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

となる．さらに，

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

とすると，$i+j=k$ である全ての組 (i,j) に対して $b_{ij} \in \mathfrak{a}^s$ ならば，$i+j>k$ である全ての組 (i,j) に対して $b_{ij} \in \mathfrak{a}^{s+[(i+j)/k]-1}$ が成り立つ．

このとき，次のことが従う：

$$(1) \begin{cases} k \leq N \text{ ならば } a_k \in \mathfrak{a} \\ p^j + p^r \leq N \text{ ならば } a_{r-j,j} \in \mathfrak{a} \end{cases};$$

$$(2) \begin{cases} (s-1)N < k \leq N \text{ ならば } a_k \in \mathfrak{a}^s \\ (s-1)N < p^j + p^r \leq N \text{ ならば } a_{r-j,j} \in \mathfrak{a}^s. \end{cases}$$

したがって，a_k と $a_{r-j,j}$ は全ての k と組 (r,j) $(0 \leq j < r)$ に対して巾零元で，有限個を除いて $a_k = 0$, $a_{r-j,j} = 0$ である．

最後に． 詳しくは [3] を参照して下さい．

参考文献

[1] M.Demazure and P.Gabriel, *Groupes algébriques, Tome1,* Masson-North-Holland, Paris-Amsterdam, 1970 .
[2] T.Sekiguchi and N.Suwa, *A note on extensions of algebraic and formal groups I,* Math.Z.206 (1991), 567-575.
[3] Y.Haraguchi, *On non-commutative extensions of* $\mathbb{G}_a$ *by* $\mathbb{G}_m$ *over an* $\mathbb{F}_p$*-algebra,* Preprint (2004).