JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Yuji TSUNO

Degeneration of the Kummer sequence in characteristic $p > 0$

Tome 22, nº 1 (2010), p. 219-257.

<http://jtnb.cedram.org/item?id=JTNB_2010__22_1_219_0>

Journal de Théorie des Nombres de Bordeaux **22** (2010), 219-257

Degeneration of the Kummer sequence in characteristic $p > 0$

par Yuji TSUNO

Résumé. Nous étudions une déformation de la suite de Kummer à la suite radicielle sur une $\mathbb{F}_p$-algèbre, qui est duale en un sens pour la déformation de la suite d'Artin-Schreier à la suite radicielle, étudiée par Saidi. Nous examinons aussi quelques relations entre nos suites et l'immersion d'un schéma en groupes commutatifs, fini et plat dans un schéma en groupes commutatifs, lisse, affine et connexe, construite par Grothendieck.

Abstract. We study a deformation of the Kummer sequence to the radicial sequence over an $\mathbb{F}_p$-algebra, which is somewhat dual for the deformation of the Artin-Schreier sequence to the radicial sequence, studied by Saidi. We also discuss some relations between our sequences and the embedding of a finite flat commutative group scheme into a connected smooth affine commutative group schemes, constructed by Grothendieck.

Introduction

Let p be a prime number. The Artin-Schreier sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{G}_{a,\mathbb{F}_p} \xrightarrow{F-I} \mathbb{G}_{a,\mathbb{F}_p} \longrightarrow 0$$

has an important role in algebraic geometry in characteristic p. Indeed we obtain a description of cyclic extensions of degree p over a field of characteristic p or more generally of cyclic coverings of a variety over a field of characteristic p, applying the theory of Galois cohomology or étale cohomology to the Artin-Schreier sequence.

Mohamed Saidi [4] studies the degeneration of cyclic coverings of a curve over a ring of characteristic p, using the exact sequence

$$(0) \qquad 0 \longrightarrow N_A \longrightarrow \mathbb{G}_{a,A} \xrightarrow{F-\mu I} \mathbb{G}_{a,A} \longrightarrow 0,$$

where A is an $\mathbb{F}_p$-algebra and $\mu \in A$. When $\mu = 0$, we obtain an exact sequence

$$0 \longrightarrow \boldsymbol{\alpha}_{p,A} \longrightarrow \mathbb{G}_{a,A} \xrightarrow{F} \mathbb{G}_{a,A} \longrightarrow 0,$$

Manuscrit reçu le 15 octobre 2008.

Classification math.. 13B05, 14L15, 12G05.

called the radicial sequence.

As is well known, the Cartier dual of $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to $\boldsymbol{\mu}_{p,A}$, the group scheme of p-th roots of unity, and $\boldsymbol{\alpha}_{p,A}$ is auto-dual for the Cartier duality. Hence the Cartier dual of N_A is a deformaion of $\boldsymbol{\mu}_{p,A}$ to $\boldsymbol{\alpha}_{p,A}$.

On the other hand, we have an exact sequence

$$0 \longrightarrow \boldsymbol{\mu}_{p,A} \longrightarrow \mathbb{G}_{m,A} \xrightarrow{F} \mathbb{G}_{m,A} \longrightarrow 0,$$

called the Kummer sequence. It would be interesting to consider an analogue of the sequence which combines the Artin-Schreier sequence and the radicial sequence.

The main results of this article are the following theorems:

Theorem 1 (= Theorem 2.6.) *Let A be an $\mathbb{F}_p$-algebra and $\lambda \in A$. Put $N_A = \mathrm{Ker}[F - \lambda^{p-1}I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$. Then there exists an exact sequnce of group A-schemes:*

$$0 \longrightarrow N_A^\vee \longrightarrow \mathcal{G}_A^{(\lambda)} \xrightarrow{F} \mathcal{G}_A^{(\lambda^p)} \longrightarrow 0. \tag{1}$$

Theorem 2 (= Theorem 2.9.) *Let A be an $\mathbb{F}_p$-algebra and $\lambda \in A$. Put $N_A = \mathrm{Ker}[F - \lambda^{(p-1)/2}I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$. Then there exists an exact sequence of group A-schemes:*

$$0 \longrightarrow N_A^\vee \longrightarrow G_{B/A} \xrightarrow{F} G_{\tilde{B}/A} \longrightarrow 0. \tag{2}$$

(For the notation, see Section 1. We owe the description of the group scheme $G_{B/A}$ to Waterhouse-Weisfeiler [14].)

Now we explain the contents of the article. In Section 1, we recall needed facts on group schemes. In Section 2, after giving a precise description of the Cartier dual of N_A, we prove Theorem 1 and Theorem 2. The exact sequence (1) gives a deformation of the Kummer sequence to the radicial sequence. Moreover, applying the cohomology theory of group schemes, we obtain an analogue of the classical Kummer theory:

Corollary 1 (= Corollary 2.11.) *Under the assumption of Theorem 1, suppose that $\mathrm{Spec}\, S$ has a structure of $N_A^\vee$-torsor over $\mathrm{Spec}\, R$. If R is a local ring or λ is nilpotent, then there exists a morphism $\mathrm{Spec}\, R \to \mathcal{G}_A^{(\lambda^p)}$ such that the square*

$$\begin{array}{ccc} \mathrm{Spec}\, S & \longrightarrow & \mathcal{G}_A^{(\lambda)} \\ \Big\downarrow & & \Big\downarrow F \\ \mathrm{Spec}\, R & \longrightarrow & \mathcal{G}_A^{(\lambda^p)} \end{array}$$

is cartesian.

Furthermore, the exact sequence (2) is a quadratic twist of (1), that is, after the base change by the quadratic extension $A[\sqrt{\lambda}]/A$, the sequence

(2) is isomorphic to a sequence of the form (1). We have also a similar assertion as above:

Corollary 2 (= Corollary 2.17.) *Under the assumption of Theorem 2, suppose that* $\operatorname{Spec} S$ *has a structure of* $N_A^\vee$*-torsor over* $\operatorname{Spec} R$*. If* R *is a local ring or* λ *is nilpotent, then there exists a morphism* $\operatorname{Spec} R \to G_{\tilde{B}/A}$ *such that the square*

$$\begin{array}{ccc} \operatorname{Spec} S & \longrightarrow & G_{B/A} \\ \downarrow & & \downarrow F \\ \operatorname{Spec} R & \longrightarrow & G_{\tilde{B}/A} \end{array}$$

is cartesian.

In Section 3, we compare our sequences and the exact sequence constructed by Grothendieck. In fact,

Theorem 3 (= Theorem 3.12.) *Let* A *be an* $\mathbb{F}_p$*-algebra and* $\lambda \in A$*. Put* $N_A = \operatorname{Ker}[F - \lambda^{p-1} I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$*. Then there exist commutative diagrams of group schemes*

$$\begin{array}{ccc} N_A^\vee & \longrightarrow & \prod_{N_A/A} \mathbb{G}_{m,N_A} \\ \| & & \downarrow \tilde{\chi} \\ N_A^\vee & \longrightarrow & \mathcal{G}_A^{(\lambda)} \end{array}$$

and

$$\begin{array}{ccc} N_A^\vee & \longrightarrow & \mathcal{G}_A^{(\lambda)} \\ \| & & \downarrow \tilde{\sigma} \\ N_A^\vee & \longrightarrow & \prod_{N_A/A} \mathbb{G}_{m,N_A}. \end{array}$$

Theorem 4 (= Theorem 3.15.) *Let* p *be a prime number* > 2*,* A *an* $\mathbb{F}_p$*-algebra and* $\lambda \in A$*. Put* $N_A = \operatorname{Ker}[F - \lambda^{\frac{p-1}{2}} I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$*. Then there exist commutative diagrams of group schemes*

$$\begin{array}{ccc} N_A^\vee & \longrightarrow & \prod_{N_A/A} \mathbb{G}_{m,N_A} \\ \downarrow \wr & & \downarrow \tilde{\chi} \\ N_A^\vee & \longrightarrow & G_{B/A} \end{array}$$

and

$$\begin{array}{ccc} N_A^\vee & \longrightarrow & G_{B/A} \\ \downarrow\wr & & \downarrow\tilde{\sigma} \\ N_A^\vee & \longrightarrow & \prod_{N_A/A} \mathbb{G}_{m,N_A}. \end{array}$$

It should be mentioned that the argument in Section 3 is an analogue of the statement for the unit group schemes of group algebras, developed in Suwa [10] after Serre [7, Ch.IV, 8].

Notation. Throughout the article, p denotes a prime number and $\mathbb{F}_p$ denotes the finite field of order p. Unless otherwise indicated, F denotes the Frobenius endomorphism.

For a scheme X and a commutative group scheme G over X, $H^*(X, G)$ denotes the cohomology group with respect to the fppf-topology. It is known that, if G is smooth over X, the fppf-cohomology group coincides with the étale cohomology group (Grothendieck [2], III.11.7). By the abbreviation, $H^*(R, G)$ denotes $H^*(\operatorname{Spec} R, G)$ when R is a ring.

For an A-algebra B, $\prod_{B/A}$ denotes the Weil restriction functor.

List of group schemes

$\mathbb{G}_{a,A}$: the additive group scheme over A
$\mathbb{G}_{m,A}$: the multiplicative group scheme over A
$\boldsymbol{\mu}_{n,A}$: $\operatorname{Ker}[n : \mathbb{G}_{m,A} \to \mathbb{G}_{m,A}]$
$\boldsymbol{\alpha}_{p,A}$: $\operatorname{Ker}[F : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$ when A is of characteristic p
$\mathcal{G}_A^{(\lambda)}$: recalled in 1.2
$G_{B/A}$: defined in 1.3

Acknowledgement. The author expresses his hearty gratitude to Professor Noriyuki Suwa for valuable advices and the patience. He is also grateful to Professors Tsutomu Sekiguchi, Fumiyuki Momose and Akira Masuoka for their useful suggestion. He thanks Dr. Michio Amano, Mr. Nobuhiro Aki and Dr. Yasuhiro Niitsuma for their warm encouragement. Finally is very grateful to the referee for useful remarks.

1. Preliminaries

Definition 1.1. Let A be a ring. The additive group scheme $\mathbb{G}_{a,A}$ over A is defined by

$$\mathbb{G}_{a,A} = \operatorname{Spec} A[T]$$

with

(a) the multiplication: $T \mapsto T \otimes 1 + 1 \otimes T$,
(b) the unit: $T \mapsto 0$,

(c) the inverse: $T \mapsto -T$.

On the other hand, the multiplicative group scheme $\mathbb{G}_{m,A}$ over A is defined by

$$\mathbb{G}_{m,A} = \operatorname{Spec} A[T, \frac{1}{T}]$$

with

(a) the multiplication: $T \mapsto T \otimes T$,
(b) the unit: $T \mapsto 1$,
(c) the inverse: $T \mapsto 1/T$.

Definition 1.2. Let A be a ring and $\lambda \in A$. A commutative group scheme $\mathcal{G}_A^{(\lambda)}$ over A is defined by

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

with

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

A homomorphism $\alpha^{(\lambda)} : \mathcal{G}_A^{(\lambda)} \to \mathbb{G}_{m,A}$ of group schemes over A is defined by

$$U \mapsto \lambda T + 1 : A[U, \frac{1}{U}] \longrightarrow A[T, \frac{1}{1+\lambda T}].$$

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

Definition 1.3. Let A be a ring and $\lambda \in A$. Put $B = A[\sqrt{\lambda}] = A[t]/(t^2 - \lambda)$. Then the functor from A-algebras to groups $R \mapsto (R \otimes_A B)^\times$ is represented by the group scheme

$$\prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 - \lambda V^2}]$$

with the multiplication

$$U \mapsto U \otimes U + \lambda V \otimes V,\ V \mapsto U \otimes V + V \otimes U.$$

Moreover, the canonical injection $R^\times \to (R \otimes_A B)^\times$ is represented by the homomorphism of group schemes

$$i : \mathbb{G}_{m,A} = \operatorname{Spec} A[T, \frac{1}{T}] \to \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 - \lambda V^2}]$$

defined by

$$U \mapsto T, V \mapsto 0.$$

On the other hand, the norm map $\mathrm{Nr} : (R \otimes_A B)^\times \to R^\times$ is represented by the homomorphism of group schemes

$$\mathrm{Nr} : \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 - \lambda V^2}] \to \mathbb{G}_{m,A} = \operatorname{Spec} A[T, \frac{1}{T}]$$

defined by

$$U \mapsto U^2 - \lambda V^2.$$

We define a group scheme $U_{B/A}$ over A by

$$U_{B/A} = \operatorname{Ker}[\mathrm{Nr} : \prod_{B/A} \mathbb{G}_{m,B} \to \mathbb{G}_{m,A}].$$

More precisely

$$U_{B/A} = \operatorname{Spec} A[U, V]/(U^2 - \lambda V^2 - 1)$$

with the multiplication

$$U \mapsto U \otimes U + \lambda V \otimes V,\ V \mapsto U \otimes V + V \otimes U.$$

If 2λ is invertible in A, then $U_{B/A}$ is an algebraic torus over A.

Moreover, we define a group scheme $G_{B/A}$ over A by

$$G_{B/A} = \operatorname{Spec} A[X, Y]/(X^2 - \lambda Y^2 - Y)$$

with

(a) the multiplication:

$$X \mapsto X\otimes 1+1\otimes X+2\lambda X\otimes Y+2\lambda Y\otimes X,\ Y \mapsto Y\otimes 1+1\otimes Y+2\lambda Y\otimes Y+2X\otimes X;$$

(b) the unit:

$$X \mapsto 0,\ Y \mapsto 0;$$

(c) the inverse:

$$X \mapsto -X,\ Y \mapsto Y.$$

Remark 1.4. We define a homomorphism of group A-schemes

$$r : \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 - \lambda V^2}] \\ \to G_{B/A} = \operatorname{Spec} A[X, Y]/(X^2 - \lambda Y^2 - Y)$$

by

$$X \mapsto \frac{UV}{U^2 - \lambda V^2},\ Y \mapsto \frac{V^2}{U^2 - \lambda V^2}$$

It is readily seen that the sequence

$$0 \longrightarrow \mathbb{G}_{m,A} \xrightarrow{i} \prod_{B/A} \mathbb{G}_{m,B} \xrightarrow{r} G_{B/A} \longrightarrow 0$$

is exact. If 2 is invertible in A, then $T \mapsto 2(X + \sqrt{\lambda}Y)$ defines an isomorphism over B:

$$\sigma : G_{B/A} \otimes_A B = \operatorname{Spec} B[X,Y]/(X^2 - \lambda Y^2 - Y) \xrightarrow{\sim} \mathcal{G}_B^{(\sqrt{\lambda})} = \operatorname{Spec} B[T, \frac{1}{1+\sqrt{\lambda}T}]$$

The inverse of σ is given by

$$X \mapsto \frac{2T + \sqrt{\lambda}T^2}{4(1+\sqrt{\lambda}T)},\ Y \mapsto \frac{T^2}{4(1+\sqrt{\lambda}T)}$$

Furthermore,

$$U \mapsto 1 + 2\lambda Y,\ V \mapsto 2X$$

define a homomorphism

$$\alpha : G_{B/A} = \operatorname{Spec} A[X,Y]/(X^2 - \lambda Y^2 - Y) \to U_{B/A} = \operatorname{Spec} A[U,V]/(U^2 - \lambda V^2 - 1)$$

If 2λ is invertible in A, then α is an isomorphism. Indeed, the inverse of α is given by

$$X \mapsto -\frac{V}{2},\ Y \mapsto -\frac{1-U}{2\lambda}$$

2. Deformations of the Kummer sequence

Throughout this section, A denotes an $\mathbb{F}_p$-algebra. We fix $\mu \in A$ and put $N_A = \operatorname{Ker}[F - \mu I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$ and $G = N_A^\vee$.

Defintion 2.1. Let A be an $\mathbb{F}_p$-algebra and $\mu \in A$. Put $N_A = \operatorname{Ker}[F - \mu I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$. Then N_A is a commutative group scheme, finite and flat of order p over A. Indeed, $N_A = \operatorname{Spec} A[T]/(T^p - \mu T)$ and the addition is given by $T \mapsto T \otimes 1 + 1 \otimes T$.

Lemma 2.2. *Under the notation of 2.1, let R be an A-algebra and $a \in R$. If $a^p = 0$, then*

$$U \mapsto \sum_{i=0}^{p-1} \frac{a^i}{i!} T^i$$

defines a homomorphism of group schemes

$$c : N_R = \operatorname{Spec} R[T]/(T^p - \mu T) \to \mathbb{G}_{m,R} = \operatorname{Spec} R[U, 1/U].$$

Furthermore, the map

$$a \mapsto \sum_{i=0}^{p-1} \frac{a^i}{i!} T^i$$

gives rise to a bijection between $\operatorname{Ker}[F : R \to R]$ *and* $\operatorname{Hom}_{R-\mathrm{gr}}(N_R, \mathbb{G}_{m,R})$.

Proof. Put $f(T)=\sum_{i=0}^{p-1}\frac{a^i}{i!}T^i$. If $a^p=0$, then $f(T)$ is inversible in $R[T]/(T^p-\mu T)$. Moreover, we obtain a functional equation $f(X+Y)=f(X)f(Y)$. Hence $U\mapsto f(T)$ defines a homomorphism of group R-schemes $c: N_R\to \mathbb{G}_{m,R}$. Conversely, assume that $U\mapsto f(T)=\sum_{i=0}^{p-1}a_iT^i$ defines a homomorphism of group R-schemes

$$c: N_R=\operatorname{Spec} R[T]/(T^p-\mu T)\to \mathbb{G}_{m,R}=\operatorname{Spec} R[U,1/U].$$

Then we obtain (1) $f(0)=1$, (2) $f(X+Y)=f(X)f(Y)$. By (1), $a_0=1$. Furthermore, comparing the coefficients of X^iY^j in

$$f(X+Y)=1+a_1(X+Y)+a_2(X+Y)^2+\cdots+a_{p-1}(X+Y)^{p-1}$$

and

$$\begin{aligned}f(X)f(Y)=(1&+a_1X+a_2X^2+\cdots+a_{p-1}X^{p-1})\\ &\times(1+a_1Y+a_2Y^2+\cdots+a_{p-1}Y^{p-1})\end{aligned}$$

for each i, j, we obtain

$$a_ia_j=\begin{cases}\binom{i+j}{i}a_{i+j} & (i+j<p)\\ 0 & (i+j\geq p)\end{cases}$$

In particular, we have $a_1a_{p-1}=0$ and $ia_i=a_1a_{i-1}$ for each $i\geq 1$. It follows that $a_i=\frac{a_1^i}{i!}$ for $1\leq i<p$ and $a_1^p=0$.

Notation 2.3. Let p be a prime number. We put

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

Definition 2.4. Let A be an $\mathbb{F}_p$-algebra and $\mu\in A$. Define a finite flat commutative group scheme G over A by $G=\operatorname{Spec} A[T]/(T^p)$ with

(a) the multiplication:

$$T\mapsto T\otimes 1+1\otimes T+\mu W(T\otimes 1,1\otimes T)=T\otimes 1+1\otimes T-\mu\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}T^{p-i}\otimes T^i,$$

(b) the unit: $T\mapsto 0$,

(c) the inverse: $T\mapsto -T$.

Proposition 2.5. *Let A be an $\mathbb{F}_p$-algebra and $\mu\in A$. Then the Cartier dual $N_A^\vee$ of $N_A=\operatorname{Ker}[F-\mu I:\mathbb{G}_{a,A}\to\mathbb{G}_{a,A}]$ is isomorphic to the group* *scheme*

$$G = \operatorname{Spec} A[T]/(T^p)$$

with the multiplication

$$\varDelta : T \mapsto T \otimes 1 + 1 \otimes T + \mu W(T \otimes 1, 1 \otimes T).$$

Proof. For an A-algebra R, we have $G(R) = \{a \in R \,;\, a^p = 0\}$. Therefore, the map $\eta : G(R) \to N^\vee(R) = \operatorname{Hom}_{R-\mathrm{gr}}(N_R, \mathbb{G}_{m,R})$ defined by

$$a \mapsto \sum_{i=0}^{p-1} \frac{a^i}{i!} T^i$$

is bijective by Lemma 2.4. Moreover, for any $a, b \in G(R)$, we have

$$\Big(\sum_{i=0}^{p-1} \frac{a^i}{i!} T^i\Big)\Big(\sum_{i=0}^{p-1} \frac{b^i}{i!} T^i\Big) = \sum_{i=0}^{p-1} \frac{c^i}{i!} T^i$$

for some $c \in G(R)$. Comparing the coefficients of T, we obtain

$$c = a + b + \mu \sum_{i=1}^{p-1} \frac{1}{(p-i)!i!} a^{p-i} b^i = a + b - \mu \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} a^{p-i} b^i$$

since $T^p = \mu T$ in $R[T]/(T^p - \mu T)$. Therefore the map $\eta : G(R) \to N_A^\vee(R) = \operatorname{Hom}_{R-\mathrm{gr}}(N_R, \mathbb{G}_{m,R})$ is an isomorphism of groups.

Remark 2.6. The Cartier duality asserts that the character group $\operatorname{Hom}_{R-\mathrm{gr}}(G \otimes_A R, \mathbb{G}_{m,R})$ is isomorphic to $N_A(R)$ for any A-algebra R. The assertion is verified directly as follows.

Let R be an A-algebra and $a \in R$. If $a^p = \mu a$, then

$$U \mapsto \sum_{i=0}^{p-1} \frac{a^i}{i!} T^i$$

defines a homomorphism of group schemes

$$G \otimes_A R = \operatorname{Spec} R[T]/(T^p) \to \mathbb{G}_{m,R} = \operatorname{Spec} R[U, 1/U]$$

since

$$\sum_{i=1}^{p-1} \frac{a^i}{i!} \Big\{X + Y + \mu W(X, Y)\Big\}^i \equiv \Big(\sum_{i=0}^{p-1} \frac{a^i}{i!} X^i\Big)\Big(\sum_{i=0}^{p-1} \frac{a^i}{i!} Y^i\Big) \mod (X^p, Y^p).$$

Furthermore,

$$a \mapsto \sum_{i=0}^{p-1} \frac{a^i}{i!} T^i$$

gives rise to a bijection

$$\xi : N_A(R) = \{a \in R \,;\, a^p = \mu a\} \xrightarrow{\sim} \operatorname{Hom}_{R-\mathrm{gr}}(G \otimes_A R, \mathbb{G}_{m,R}).$$

In fact, assume that $U \mapsto f(T) = \sum_{i=0}^{p-1} a_i T^i$ defines a homomorphism of group R-schemes

$$G \otimes_A R = \operatorname{Spec} R[T]/(T^p) \to \mathbb{G}_{m,R} = \operatorname{Spec} R[U, 1/U].$$

Then we obtain (1) $f(0) = 1$ and (2) $f(X + Y + \mu W(X,Y)) = f(X)f(Y)$. By (1), $a_0 = 1$. Furthermore, comparing the coefficients of $X^i Y^j$ in

$$\begin{aligned} f(X + Y + \mu W(X,Y)) = 1 &+ a_1\{X + Y + \mu W(X,Y)\} \\ &+ a_2\{X + Y + \mu W(X,Y)\}^2 + \cdots \\ &+ a_{p-1}\{X + Y + \mu W(X,Y)\}^{p-1} \end{aligned}$$

and

$$\begin{aligned} f(X)f(Y) = (1 &+ a_1 X + a_2 X^2 + \cdots + a_{p-1} X^{p-1}) \\ &\times (1 + a_1 Y + a_2 Y^2 + \cdots + a_{p-1} Y^{p-1}) \end{aligned}$$

for each i, j, we obtain

$$a_i a_j = \begin{cases} \dbinom{i+j}{i} a_{i+j} & (i + j < p) \\ -(i + j - p + 1)\dfrac{1}{p}(i + j - p + 1)\dbinom{i+j}{i} \mu a_{i+j-p+1} & (i + j \geq p) \end{cases}$$

In particular, we have $a_1 a_{p-1} = \mu a_1$ and $i a_i = a_1 a_{i-1}$ for each $i \geq 1$. It follows that $a_i = \dfrac{a_1^i}{i!}$ for $1 \leq i < p$ and $a_1^p = \mu a_1$. Hence ξ is surjective. It is readily seen that ξ is injective.

Moreover, for any $a, b \in N_A(R)$, we have

$$\Big(\sum_{i=0}^{p-1} \frac{a^i}{i!} T^i\Big)\Big(\sum_{i=0}^{p-1} \frac{b^i}{i!} T^i\Big) = \sum_{i=0}^{p-1} \frac{c^i}{i!} T^i$$

for some $c \in N_A(R)$. Comparing the coefficients of T, we obtain $c = a + b$ since $T^p = 0$ in $R[T]/(T^p)$. Therefore the map $\xi : N_A(R) \to G^\vee(R) = \operatorname{Hom}_{R-\mathrm{gr}}(G \otimes_A R, \mathbb{G}_{m,R})$ is an isomorphism of groups.

Theorem 2.7. *Let A be an $\mathbb{F}_p$-algebra and $\mu \in A$. If $\mu = \lambda^{p-1}$ for some $\lambda \in A$, then G is isomorphic to*

$$\operatorname{Ker}[F : \mathcal{G}_A^{(\lambda)} \to \mathcal{G}_A^{(\lambda^p)}] = \operatorname{Spec} A[X]/(X^p)$$

with the multiplication

$$\Delta : X \mapsto X \otimes 1 + 1 \otimes X + \lambda X \otimes X.$$

Here F denotes the absolute Frobenius map.

Proof. Define a homomorphism of A-algebra $\tilde{\eta} : A[X]/(X^p) \to A[T]/(T^p)$ by

$$X \mapsto \sum_{i=1}^{p-1} \frac{\lambda^{i-1}}{i!} T^i.$$

Then $\tilde{\eta}$ is an isomorphism. Indeed, the inverse of $\tilde{\eta}$ is given by

$$T \mapsto \sum_{i=1}^{p-1} \frac{(-\lambda)^{i-1}}{i} X^i.$$

Hereafter we show that $\tilde{\eta}$ is a Hopf homomorphism. It is sufficient to verify that

$$\begin{aligned}\sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} \Big\{X+Y+\lambda^{p-1}W(X,Y)\Big\}^k &= \sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} X^k + \sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} Y^k \\ &\quad + \lambda\Big(\sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} X^k\Big)\Big(\sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} Y^k\Big)\end{aligned}$$

in $A[X,Y]/(X^p, Y^p)$. At first note that

$$\begin{aligned}&\sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} X^k + \sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} Y^k + \lambda\Big(\sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} X^k\Big)\Big(\sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} Y^k\Big) \\ &= \sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} X^k + \sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} Y^k + \sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} \Big\{\sum_{l=1}^{k-1} \binom{k}{l} X^{k-l} Y^l\Big\} \\ &\quad + \sum_{k=p}^{2p-2} \lambda^{k-1} \sum_{l=k-p+1}^{p-1} \frac{1}{l!(k-l)!} X^{k-l} Y^l \\ &= \sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} (X+Y)^k + \sum_{k=1}^{p-1} \lambda^{k+p-2} \Big(\sum_{l=k}^{p-1} \frac{1}{(k+p-1-l)!l!} X^{k+p-1-l} Y^l\Big).\end{aligned}$$

We have

$$\begin{aligned}&\sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} \Big\{X+Y+\lambda^{p-1}W(X,Y)\Big\}^k \\ &\qquad = \sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} \Big\{(X+Y)^k + k\lambda^{p-1}(X+Y)^{k-1}W(X,Y)\Big\} \\ &\qquad = \sum_{k=1}^{p-1} \frac{\lambda^{k-1}}{k!} (X+Y)^k + \sum_{k=1}^{p-1} \frac{\lambda^{k+p-2}}{(k-1)!} (X+Y)^{k-1} W(X,Y)\Big\}\end{aligned}$$

since $X^p = Y^p = 0$. Note now that we have a congruence relation

$$
\begin{aligned}
(X+Y)^{k-1}W(X,Y) &= (X+Y)^{k-1}\frac{X^p+Y^p-(X+Y)^p}{p} \\
&\equiv -\frac{1}{p}(X+Y)^{k+p-1} \\
&\equiv -\sum_{l=k}^{p-1}\frac{1}{p}\binom{k+p-1}{l}X^{k+p-1-l}Y^l \mod (X^p,Y^p)
\end{aligned}
$$

in $\mathbb{Q}[X,Y]$, and therefore

$$
(X+Y)^{k-1}W(X,Y) \equiv -\sum_{l=k}^{p-1}\frac{1}{p}\binom{k+p-1}{l}X^{k+p-1-l}Y^l \mod (X^p,Y^p)
$$

in $\mathbb{Z}[X,Y]$. Moreover, we have

$$
\begin{aligned}
&-\frac{1}{p}\binom{k+p-1}{l} \\
&\quad = -\frac{1}{p\,l!}(k+p-1)(k+p-2)\cdots \\
&\qquad \times (k+p-k+1)(k+p-k)(k+p-k-1)\cdots(k+p-l) \\
&\quad \equiv -\frac{(k-1)!(p-1)(p-2)\cdots(k+p-l)}{l!} \\
&\quad = -\frac{(k-1)!(p-1)!}{(k+p-l-1)!l!} \\
&\quad \equiv \frac{(k-1)!}{(k+p-l-1)!l!} \mod p
\end{aligned}
$$

in $\mathbb{Z}_{(p)}$. Hence the result.

Remark 2.8. We obtain an exact sequence of group A-schemes

$$
0 \longrightarrow G \xrightarrow{\eta} \mathcal{G}_A^{(\lambda)} \xrightarrow{F} \mathcal{G}_A^{(\lambda^p)} \longrightarrow 0. \tag{1}
$$

When $\lambda = 0$, the sequence (1) is nothing but the radicial sequence

$$
0 \longrightarrow \boldsymbol{\alpha}_{p,A} \longrightarrow \mathbb{G}_{a,A} \xrightarrow{F} \mathbb{G}_{a,A} \longrightarrow 0.
$$

On the other hand, if λ is invertible A, we have a commutative diagram of group A-schemes with exact rows

$$
\begin{tikzcd}
0 \arrow[r] & G \arrow[r, "\eta"] \arrow[d, "\wr"] & \mathcal{G}_A^{(\lambda)} \arrow[r, "F"] \arrow[d, "\wr\ \alpha^{(\lambda)}"] & \mathcal{G}_A^{(\lambda^p)} \arrow[r] \arrow[d, "\wr\ \alpha^{(\lambda^p)}"] & 0 \\
0 \arrow[r] & \boldsymbol{\mu}_{p,A} \arrow[r] & \mathbb{G}_{m,A} \arrow[r, "F"] & \mathbb{G}_{m,A} \arrow[r] & 0.
\end{tikzcd}
$$

Therefore, the exact sequence (1) gives a deformation of the Kummer sequence to the radicial sequence.

Corollary 2.9. *Let R be an A-algebra. If R is a local ring or λ is nilpotent, then $H^1(R, G)$ is isomorphic to* $\mathrm{Coker}[F : \mathcal{G}_A^{(\lambda)}(R) \to \mathcal{G}_A^{(\lambda^p)}(R)]$.

Proof. From the exact sequence of group schemes over R

$$0 \to G \to \mathcal{G}_A^{(\lambda)} \xrightarrow{F} \mathcal{G}_A^{(\lambda^p)} \to 0,$$

we obtain a long exact sequence

$$\mathcal{G}_A^{(\lambda)}(R) \xrightarrow{F} \mathcal{G}_A^{(\lambda^p)}(R) \longrightarrow H^1(R, G) \longrightarrow H^1(R, \mathcal{G}_A^{(\lambda)}) \xrightarrow{F} H^1(R, \mathcal{G}_A^{(\lambda^p)}).$$

We know that $H^1(R, \mathcal{G}_A^{(\lambda)}) = 0$ under the assumption ([5], Cor 1.3), which implies the assertion.

The above assertion is restated as follows :

Corollary 2.10. *Let R be an A-algebra and S an R-algebra. Assume that* $\mathrm{Spec}\, S$ *has a structure of G-torsor over* $\mathrm{Spec}\, R$*. If R is a local ring or λ is nilpotent, then there exists a morphism* $\mathrm{Spec}\, R \to \mathcal{G}_A^{(\lambda^p)}$ *such that the square*

$$\begin{array}{ccc} \mathrm{Spec}\, S & \longrightarrow & \mathcal{G}_A^{(\lambda)} \\ \big\downarrow & & \big\downarrow F \\ \mathrm{Spec}\, R & \longrightarrow & \mathcal{G}_A^{(\lambda^p)} \end{array}$$

is cartesian. More precisely, S is isomorphic to

$$R[X]/(X^p - a)$$

for some $a \in R$ with $1 + \lambda^p a \in R^\times$, and the action of G on $\mathrm{Spec}\, S$ *over R is defined by*

$$\begin{array}{ccc} R[X]/(X^p - a) & \to & R[T]/(T^p) \otimes_R R[X]/(X^p - a) \\ X & \mapsto & \displaystyle\sum_{i=1}^{p-1} \frac{\lambda^{i-1}}{i!} T^i \otimes 1 + \sum_{i=0}^{p-1} \frac{\lambda^i}{i!} T^i \otimes X. \end{array}$$

Hereafter we study a quadratic twist of the exact sequence (1).

Notation 2.11. Let A be a ring and $\lambda \in A$. Put $B = A[\sqrt{\lambda}] = A[t]/(t^2 - \lambda)$ and $\tilde{B} = A[\sqrt{\lambda}^p] = A[t]/(t^2 - \lambda^p)$. As is done in 1.4, we define group schemes $G_{B/A}$ and $G_{\tilde{B}/A}$ over A by

$$G_{B/A} = \mathrm{Spec}\, A[X, Y]/(X^2 - \lambda Y^2 - Y)$$

with the multiplication:

$$X \mapsto X \otimes 1 + 1 \otimes X + 2\lambda X \otimes Y + 2\lambda Y \otimes X, \ Y \mapsto Y \otimes 1 + 1 \otimes Y + 2\lambda Y \otimes Y + 2X \otimes X,$$

$$G_{\tilde{B}/A} = \operatorname{Spec} A[X,Y]/(X^2 - \lambda^p Y^2 - Y)$$

with the multiplication:

$$X \mapsto X \otimes 1 + 1 \otimes X + 2\lambda^p X \otimes Y + 2\lambda^p Y \otimes X,$$
$$Y \mapsto Y \otimes 1 + 1 \otimes Y + 2\lambda^p Y \otimes Y + 2X \otimes X.$$

Furthermore a homomorphism of group A-schemes

$$F : G_{B/A} = \operatorname{Spec} A[X,Y]/(X^2 - \lambda Y^2 - Y) \\ \to G_{\tilde{B}/A} = \operatorname{Spec} A[X,Y]/(X^2 - \lambda^p Y^2 - Y)$$

is defined by

$$X \mapsto X^p, \quad Y \mapsto Y^p.$$

It is readily seen that $F : G_{B/A} \to G_{\tilde{B}/A}$ is finite flat.

Theorem 2.12. *Let p be a prime number > 2, A an $\mathbb{F}_p$-algebra and $\mu \in A$. If $\mu = \lambda^{(p-1)/2}$ for some $\lambda \in A$, then G is isomorphic to*

$$\operatorname{Ker}[F : G_{B/A} \to G_{\tilde{B}/A}] = \operatorname{Spec} A[X,Y]/(X^2 - \lambda Y^2 - Y, X^p, Y^p)$$

with the multiplication

$$\Delta : X \mapsto X \otimes 1 + 1 \otimes X + 2\lambda X \otimes Y + 2\lambda Y \otimes X,$$
$$Y \mapsto Y \otimes 1 + 1 \otimes Y + 2\lambda Y \otimes Y + 2X \otimes X.$$

Here F denotes the absolute Frobenius map.

Proof. We verify that

$$X \mapsto \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}T^{2i-1}, \ Y \mapsto \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i)!}T^{2i}$$

defines a homomorphism of group schemes

$$\xi : G = \operatorname{Spec} A[X]/(T^p) \to G_{B/A} = \operatorname{Spec} A[X,Y]/(X^2 - \lambda Y^2 - Y)$$

Noting

$$\frac{\sinh \sqrt{\Lambda}T}{\sqrt{\Lambda}} = \sum_{i=1}^{\infty} \frac{\Lambda^{i-1}}{(2i-1)!}T^{2i-1}, \frac{\cosh \sqrt{\Lambda}T - 1}{\Lambda} = \sum_{i=1}^{\infty} \frac{\Lambda^{i-1}}{(2i)!}T^{2i},$$

and

$$\Big(\frac{1}{2}\,\frac{\sinh \sqrt{\Lambda}T}{\sqrt{\Lambda}}\Big)^2 - \Lambda\Big(\frac{1}{2}\,\frac{\cosh \sqrt{\Lambda}T - 1}{\Lambda}\Big)^2 - \frac{1}{2}\,\frac{\cosh \sqrt{\Lambda}T - 1}{\Lambda} = 0$$

we obtain an identity in $\mathbb{Q}[\Lambda][[T]]$

$$\Big\{\frac{1}{2}\sum_{i=1}^{\infty} \frac{\Lambda^{i-1}}{(2i-1)!}T^{2i-1}\Big\}^2 - \Lambda\Big\{\frac{1}{2}\sum_{i=1}^{\infty} \frac{\Lambda^{i-1}}{(2i)!}T^{2i}\Big\}^2 - \frac{1}{2}\sum_{i=1}^{\infty} \frac{\Lambda^{i-1}}{(2i)!}T^{2i} = 0,$$

and therefore an identity in $\mathbb{Q}[\varLambda][T]/(T^p)$

$$\Big\{\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\varLambda^{i-1}}{(2i-1)!}T^{2i-1}\Big\}^2-\varLambda\Big\{\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\varLambda^{i-1}}{(2i)!}T^{2i}\Big\}^2-\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\varLambda^{i-1}}{(2i)!}T^{2i}=0,$$

which reads as an identity in $\mathbb{F}_p[\varLambda][T]/(T^p)$

$$\Big\{\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\varLambda^{i-1}}{(2i-1)!}T^{2i-1}\Big\}^2-\varLambda\Big\{\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\varLambda^{i-1}}{(2i)!}T^{2i}\Big\}^2-\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\varLambda^{i-1}}{(2i)!}T^{2i}=0$$

since

$$\sum_{i=1}^{\frac{p-1}{2}}\frac{\varLambda^{i-1}}{(2i-1)!}T^{2i-1},\ \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\varLambda^{i-1}}{(2i)!}T^{2i}\in\mathbb{Z}_{(p)}[\varLambda][T].$$

Specializing $\varLambda$ to λ, we obtain

$$\Big\{\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\lambda^{i-1}}{(2i-1)!}T^{2i-1}\Big\}^2-\lambda\Big\{\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\lambda^{i-1}}{(2i)!}T^{2i}\Big\}^2-\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\lambda^{i-1}}{(2i)!}T^{2i}=0$$

in $A[T]/(T^p)$, which implies that

$$X\mapsto\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\lambda^{i-1}}{(2i-1)!}T^{2i-1},\ Y\mapsto\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\frac{\lambda^{i-1}}{(2i)!}T^{2i}$$

defines a homomorphism of A-algebras

$$\tilde{\xi}:A[X,Y]/(X^2-\lambda Y^2-Y,X^p,Y^p)\to A[T]/(T^p).$$

Furthermore, as is remarked in 1.4,

$$X\mapsto 2(X+\sqrt{\lambda}Y)$$

gives rise to an isomorphism of group scheme over $B=A[\sqrt{\lambda}]$

$$\begin{aligned}\sigma:G_{B/A}\otimes_A B=\operatorname{Spec}B[X,Y]/(X^2-\lambda Y^2-Y)&\\ \xrightarrow{\sim}\mathcal{G}_B^{(\sqrt{\lambda})}=\operatorname{Spec}B[X,\frac{1}{1+\sqrt{\lambda}X}].&\end{aligned}$$

On the other hand,

$$X\mapsto\sum_{i=1}^{p-1}\frac{\sqrt{\lambda}^{i-1}}{i!}T^i$$

gives an isomorphism of group scheme over B

$$\begin{aligned}\eta_B:G\otimes_A B=\operatorname{Spec}B[T]/(T^p)&\\ \xrightarrow{\sim}\operatorname{Ker}[F:\mathcal{G}_B^{(\sqrt{\lambda})}\to\mathcal{G}_B^{(\sqrt{\lambda}^p)}]=\operatorname{Spec}B[X]/(X^p).&\end{aligned}$$

Moreover, we have $\sigma \circ \eta_B = \xi_B$ since

$$2\Big\{\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}T^{2i-1} + \sqrt{\lambda}\,\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i)!}T^{2i}\Big\} = \sum_{i=1}^{p-1} \frac{\sqrt{\lambda}^{i-1}}{i!}T^{i}.$$

Hence, ξ_B is an homomorphism of group schemes over B. It follows that ξ is an homomorphism of group schemes over A since $B = A[\sqrt{\lambda}]$ is faithfully flat over A.

Remark 2.13. We obtain an exact sequence of group schemes

$$0 \to G \xrightarrow{\xi} G_{B/A} \xrightarrow{F} G_{\tilde{B}/A} \to 0. \tag{2}$$

In the proof of 2.12, we obtained an isomorphism of exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & G \otimes_A B \arrow[r, "\xi_B"] \arrow[d, equal] & G_{B/A} \otimes_A B \arrow[r, "F"] \arrow[d, "\wr\ \sigma"] & G_{\tilde{B}/A} \otimes_A B \arrow[r] \arrow[d, "\wr\ \tilde{\sigma}"] & 0 \\
0 \arrow[r] & G \otimes_A B \arrow[r, "\eta_B"] & \mathcal{G}_B^{(\sqrt{\lambda})} \arrow[r, "F"] & \mathcal{G}_B^{(\sqrt{\lambda^p})} \arrow[r] & 0.
\end{tikzcd}$$

That is to say, the sequence (2) is a quadratic twist of (1).

Corollary 2.14. *Let R be an A-algebra. If R is a local ring or λ is nilpotent, then $H^1(R, G)$ is isomorphic to* $\mathrm{Coker}[F : G_{B/A}(R) \to G_{\tilde{B}/A}(R)]$.

Proof. From the exact sequence of group schemes over R

$$0 \to G \to G_{B/A} \xrightarrow{F} G_{\tilde{B}/A} \to 0,$$

we obtain a long exact sequence

$$G_{B/A}(R) \xrightarrow{F} G_{\tilde{B}/A}(R) \longrightarrow H^1(R, G) \longrightarrow H^1(R, G_{B/A}) \xrightarrow{F} H^1(R, G_{\tilde{B}/A}).$$

We know that $H^1(R, G_{B/A})$ is annihilated by 2 under the assumption ([9], Prop 4.3.) and that $H^1(R, G)$ is annihilated by p, which imply the assertion.

The above assertion is restated as follows :

Corollary 2.15. *Let R be an A-algebra and S an R-algebra. Assume that* $\mathrm{Spec}\, S$ *has a structure of G-torsor over* $\mathrm{Spec}\, R$*. If R is a local ring or λ is nilpotent, then there exists a morphism* $\mathrm{Spec}\, R \to G_{\tilde{B}/A}$ *such that the square*

$$\begin{tikzcd}
\mathrm{Spec}\, S \arrow[r] \arrow[d] & G_{B/A} \arrow[d, "F"] \\
\mathrm{Spec}\, R \arrow[r] & G_{\tilde{B}/A}
\end{tikzcd}$$

is cartesian. More precisely, S is isomorphic to

$$R[X, Y]/(X^p - a, Y^p - b, X^2 - \lambda Y^2 - Y)$$

for some $a, b \in R$ with $a^2-\lambda^p b^2-b=0$, and the action of G on $\operatorname{Spec} S$ *over R is defined by*

$$
\begin{aligned}
& R[X, Y]/(X^p-a, Y^p-b, X^2-\lambda Y^2-Y) \\
& \qquad \rightarrow R[T]/(T^p) \otimes_R R[X, Y]/(X^p-a, Y^p-b, X^2-\lambda Y^2-Y):
\end{aligned}
$$

$$
\begin{aligned}
& X \mapsto \frac{1}{2} \sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!} T^{2i-1} \otimes 1+\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^i}{(2i-1)!} T^{2i-1} \otimes Y+\sum_{i=0}^{\frac{p-1}{2}} \frac{\lambda^i}{(2i)!} T^{2i} \otimes X, \\
& Y \mapsto \frac{1}{2} \sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i)!} T^{2i} \otimes 1+\sum_{i=0}^{\frac{p-1}{2}} \frac{\lambda^i}{(2i)!} T^{2i} \otimes Y+\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!} T^{2i-1} \otimes X .
\end{aligned}
$$

Remark 2.16. The Artin-Hasse exponential series $E_p(T) \in \mathbb{Z}_{(p)}[[T]]$ is defined by

$$
E_p(T)=\exp\Big(\sum_{r=0}^{\infty} \frac{T^{p^r}}{p^r}\Big).
$$

For an $\mathbb{Z}_{(p)}$-algebra R and $\boldsymbol{a}=(a_k)_{k \geq 0} \in R^{\mathbb{N}}$, we define $E_p(\boldsymbol{a}; T) \in A[[T]]$ by

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

It is known that

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

where + denotes the addition of Witt vectors.

Let $\widehat{W}$ denote the formal completion of the additive group scheme of Witt vectors. Then, if R is an $\mathbb{F}_p$ -algebra, we have

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

Moreover,

$$
\boldsymbol{a}=(a_k)_{k \geq 0} \mapsto E_p(\boldsymbol{a}; T)=\prod_{k=0}^{\infty}\Big(\sum_{i=0}^{p-1} \frac{a_k^i}{i!} T^{p^k i}\Big)
$$

gives rise to an isomorphism

$$
\eta :{}_F \widehat{W}(R)=\operatorname{Ker}[F: \widehat{W}(R) \rightarrow \widehat{W}(R)] \xrightarrow{\sim} \operatorname{Hom}_{R-\mathrm{gr}}(\mathbb{G}_{a, R}, \mathbb{G}_{m, R})
$$

(cf. [1, Ch II, Sec 2, 2.7]). Under this identification,

$$
F-\mu I: \mathbb{G}_{a, R} \rightarrow \mathbb{G}_{a, R}
$$

induces

$$
V-[\mu] I :{}_F \widehat{W}(R) \rightarrow{}_F \widehat{W}(R).
$$

In fact, if $\boldsymbol{a} \in_F \widehat{W}(R)$, we have

$$\begin{aligned} E_p(\boldsymbol{a}; T^p - \mu T) &= \prod_{k=0}^{\infty} \Big(\sum_{i=0}^{p-1} \frac{{a_k}^i}{i!} (T^p - \mu T)^{p^k i} \Big) \\ &= \prod_{k=0}^{\infty} \Big(\sum_{i=0}^{p-1} \frac{{a_k}^i}{i!} (T^{p^{k+1}} - \mu^{p^k} T^{p^k})^i \Big). \end{aligned}$$

Now, by the functional equation of the exponential series, we obtain

$$\sum_{i=0}^{p-1} \frac{{a_k}^i}{i!} (T^{p^{k+1}} - \mu^{p^k} T^{p^k})^i = \Big(\sum_{i=0}^{p-1} \frac{{a_k}^i}{i!} (T^{p^{k+1}})^i \Big) \Big(\sum_{i=0}^{p-1} \frac{(\mu^{p^k} a_k)^i}{i!} (T^{p^k})^i \Big)^{-1}$$

for each k since we have ${a_k}^p = 0$. Therefore, we have gotten

$$\begin{aligned} E_p(\boldsymbol{a}; T^p - \mu T) &= \prod_{k=0}^{\infty} \Big(\sum_{i=0}^{p-1} \frac{{a_k}^i}{i!} (T^{p^{k+1}})^i \Big) \Big(\sum_{i=0}^{p-1} \frac{(\mu^{p^k} a_k)^i}{i!} (T^{p^k})^i \Big)^{-1} \\ &= E_p(V\boldsymbol{a}; T) E_p([\mu]\boldsymbol{a}; T)^{-1} \\ &= E_p((V - [\mu])\boldsymbol{a}; T). \end{aligned}$$

Moreover, we obtain a commutative diagram with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & \operatorname*{Hom}_{R-\mathrm{gr}}(\mathbb{G}_{a,R}, \mathbb{G}_{m,R}) \arrow[r, "(F-[\mu]I)^*"] \arrow[d, "\wr\ \eta"] & \operatorname*{Hom}_{R-\mathrm{gr}}(\mathbb{G}_{a,R}, \mathbb{G}_{m,R}) \arrow[r] \arrow[d, "\wr\ \eta"] & \operatorname*{Hom}_{R-\mathrm{gr}}(N, \mathbb{G}_{m,R}) \arrow[r] \arrow[d, "\wr\ \eta"] & 0 \\ 0 \arrow[r] & {}_F\widehat{W}(R) \arrow[r, "V-[\mu]I"] & {}_F\widehat{W}(R) \arrow[r] & G(R) \arrow[r] & 0. \end{tikzcd}$$

Remark 2.17. Put $\Lambda_p = \mathbb{Z}[\zeta, 1/p(p-1)] \cap \mathbb{Z}_p$, where ζ is a primitive $(p-1)$-th root of unity in the ring of p-adic integers. For any scheme S over Λ_p. In [11] Tate and Oort defined a commutative group scheme $G^L_{a,b}$ over S, where L is an invertible $\mathcal{O}_S$-module and $a \in \Gamma(S, L^{\otimes(p-1)}), b \in \Gamma(S, L^{\otimes(1-p)})$ with $a \otimes b = p$. The group scheme $G^L_{a,b}$ is finite flat of order p over S, and the Cartier dual $(G^L_{a,b})^\vee$ is isomorphisc to $G^{L^\vee}_{b,a}$. If A is an $\mathbb{F}_p$-algebra, $S = \operatorname{Spec} A$ and $L = \mathcal{O}_S$, then we have $ab = 0$ and

$$G^L_{a,b} = \operatorname{Spec} A[T]/(T^p - aT)$$

with the multiplication

$$\Delta : T \mapsto T \otimes 1 + 1 \otimes T + bW(T \otimes 1, 1 \otimes T).$$

In particular, we have $N = G^A_{\mu,0}$ and $G = G^A_{0,\mu}$.

3. Relations with the Grothendieck resolution

Throughtout the section, A denotes an $\mathbb{F}_p$-algebra.

3.1. First we recall a resolution of a finite flat commutative group scheme by smooth affine commutative group schemes, constructed by Grothendieck (cf. [3. Sec 6]). Let S be a scheme and F an affine commutative S-group scheme such that $\mathcal{O}_F$ is a locally free $\mathcal{O}_S$-module of finite rank. Then the functor $Hom_{S-\mathrm{gr}}(F, \mathbb{G}_{m,S})$ is represented by a commutative group scheme $F^\vee$, called the Cartier dual of F. The $\mathcal{O}_S$-module $\mathcal{O}_{F^\vee}$ is also locally free of finite rank. The Cartier duality asserts that $Hom_{S-\mathrm{gr}}(F^\vee, \mathbb{G}_{m,S})$ is isomorphic to F.

Furthermore the functor $Hom_{S-\mathrm{sch}}(F^\vee, \mathbb{G}_{m,S})$ is nothing but the Weil restriction $\prod_{F^\vee/S} \mathbb{G}_{m,F^\vee}$, which is representable since $\mathcal{O}_{F^\vee}$ is a locally free $\mathcal{O}_S$-module of finite rank (cf. [1, Ch.I, Sec.1,6.6]). Then we obtain an exact sequence of commutative group schemes:

$$0 \to F \xrightarrow{i} \prod_{F^\vee/S} \mathbb{G}_{m,F^\vee} \to \Big(\prod_{F^\vee/S} \mathbb{G}_{m,F^\vee}\Big)/F \to 0.$$

The Weil restriction $\prod_{F^\vee/S} \mathbb{G}_{m,F^\vee}$ is smooth over S since $\mathbb{G}_{m,F^\vee}$ is smooth over $F^\vee$, and therefore the quotient $\Big(\prod_{F^\vee/S} \mathbb{G}_{m,F^\vee}\Big)/F$ is also smooth over S.

The canonical map

$$H^1\Big(S, \prod_{F^\vee/S} \mathbb{G}_{m,F^\vee}\Big) \to H^1\Big(F^\vee, \mathbb{G}_{m,F^\vee}\Big) = \mathrm{Pic}\,(F^\vee)$$

is an isomorphism since $F^\vee$ is finite over S and $\mathbb{G}_{m,F^\vee}$ is is smooth over $F^\vee$. Let X be an F-torsor over S. Then the inclusion $F \to \prod_{F^\vee/S} \mathbb{G}_{m,F^\vee}$ defines a class $[X]$ in $\mathrm{Pic}\,(F^\vee)$.

First we treat the sequence: (0) $\quad 0 \longrightarrow N_A \longrightarrow \mathbb{G}_{a,A} \stackrel{F-\mu I}{\longrightarrow} \mathbb{G}_{a,A} \longrightarrow 0.$

3.2. Let A be an $\mathbb{F}_p$-algebra, and $B = A[T]/(T^p)$. Then $\prod_{B/A} \mathbb{G}_{m,B}$ is represented by

$$\mathrm{Spec}\, A[T_0, T_1, \dots, T_{p-1}, \frac{1}{T_0}]$$

with the multiplication

$$T_k \mapsto \sum_{i=0}^{k} T_{k-1} \otimes T_i \ (0 \leq k \leq p-1)$$

with the unit

$$T_0 \mapsto 1, \ T_k \mapsto 0 \ (1 \leq k \leq p-1)$$

In fact, let R be an A-algebra. The multiplication of $R[T]/(T^p) = R \otimes_A A[T]/(T^p)$ is given by

$$\Big(\sum_{i=0}^{p-1} a_i T^i\Big)\Big(\sum_{i=0}^{p-1} b_i T^i\Big) = \sum_{k=1}^{p-1} (\sum_{i=0}^{k} a_{k-i} b_i) T^k.$$

It is now sufficient to note that $\sum_{k=0}^{p-1} a_k T^k$ is invertible in $R[T]/(T^p)$ if and only if a_0 is invertible in R.

Theorem 3.3. *Let A be an $\mathbb{F}_p$-algebra and $\mu \in A$. Put $N_A = \operatorname{Ker}[F - \mu I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$ and $B = A[T]/(T^p)$. Then:*
(1) *A homomorphism of group schemes*

$$\tilde{\chi} : \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[T_0, T_1, \ldots, T_{p-1}, \frac{1}{T_0}] \to \mathbb{G}_{a,A} = \operatorname{Spec} A[T]$$

is defined by

$$T \mapsto \frac{T_1}{T_0}.$$

Moreover, the diagram of group schemes

$$\begin{array}{ccc} N_A & \xrightarrow{i} & \prod_{B/A} \mathbb{G}_{m,B} \\ \Big\| & & \Big\downarrow \tilde{\chi} \\ N_A & \xrightarrow[\xi]{} & \mathbb{G}_{a,A} \end{array}$$

is commutative.
(2) *A homomorphism of group schemes*

$$\tilde{\sigma} : \mathbb{G}_{a,A} = \operatorname{Spec} A[T] \to \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[T_0, T_1, \ldots, T_{p-1}, \frac{1}{T_0}]$$

is defined by

$$T_0 \mapsto 1, \ T_k \mapsto \frac{1}{k!} T^k \ (1 \leq k \leq p-1).$$

Moreover, the diagram of group schemes

$$\begin{tikzcd} N_A \arrow[r, "\xi"] \arrow[d, equal] & \mathbb{G}_{a,A} \arrow[d, "\tilde{\sigma}"] \\ N_A \arrow[r, "i"'] & \prod_{B/A} \mathbb{G}_{m,B} \end{tikzcd}$$

is commutative, and $\tilde{\sigma}$ is a section of $\tilde{\chi}$.

Proof. The addition of $\mathbb{G}_{a,A}$ is given by

$$T \mapsto T \otimes 1 + 1 \otimes T.$$

On the other hand, we have

$$\frac{T_1}{T_0} \mapsto \frac{T_1 \otimes T_0 + T_0 \otimes T_1}{T_0 \otimes T_0} = \frac{T_1}{T_0} \otimes 1 + 1 \otimes \frac{T_1}{T_0}$$

by the definition of multiplication of $\prod\limits_{B/A} \mathbb{G}_{m,B}$. Therefore $\tilde{\chi}$ is a homomorphism of group. Futhermore, comparing

$$\frac{1}{k!}T^k \mapsto \frac{1}{k!}(T \otimes 1 + 1 \otimes T)^k = \sum_{i=1}^{k} \frac{1}{(k-i)!}T^{k-i} \otimes \frac{1}{i!}T^i$$

and

$$T_k \mapsto \sum_{i=0}^{k} T_{k-i} \otimes T_i,$$

we find that $\tilde{\sigma}$ is group homomorphism.

We obtain the commutativity of the two squares, noting that

$$i : N_A \to \prod_{B/A} \mathbb{G}_{m,B}$$

is defined by

$$\begin{aligned} A[T_0, T_1, \ldots, T_{p-1}, \frac{1}{T_0}] &\to A[T]/(T^p - \mu T) \\ T_0 &\mapsto 1, \\ T_k &\mapsto \frac{1}{k!}T^k \ (1 \leq k \leq p-1). \end{aligned}$$

Next we examine the exact sequence: (1) $\quad 0 \longrightarrow G \xrightarrow{\eta} \mathcal{G}_A^{(\lambda)} \xrightarrow{F} \mathcal{G}_A^{(\lambda^p)} \longrightarrow 0.$

Notation 3.4. Let A be an $\mathbb{F}_p$-algebra and $\mu \in A$. Put

$$\Delta(\mu; T_0, T_1, \ldots, T_{p-1}) = \begin{vmatrix} T_0 & 0 & 0 & \ldots & 0 & O \\ T_1 & T_0 + \mu T_{p-1} & \mu T_{p-2} & \ldots & \mu T_2 & \mu T_1 \\ T_2 & T_1 & T_0 + \mu T_{p-1} & \ldots & \mu T_3 & \mu T_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ T_{p-2} & T_{p-3} & T_{p-4} & \ldots & T_0 + \mu T_{p-1} & \mu T_{p-2} \\ T_{p-1} & T_{p-2} & T_{p-3} & \ldots & T_1 & T_0 + \mu T_{p-1} \end{vmatrix}.$$

Proposition 3.5. *Let A be an $\mathbb{F}_p$-algebra and $\mu \in A$. Then $f(T) = \sum_{k=0}^{p-1} a_k T^k$ is invertible in $A[T]/(T^p - \mu T)$ if and only if $\Delta(\mu; a_0, a_1, \ldots, a_{p-1})$ is invertible in A.*

Proof. The A-module $A[T]/(T^p - \mu T)$ has a basis $\{1, T, T^2, \ldots, T^{p-1}\}$. Moreover, we have

$$(1\ T\ T^2\ \ldots\ T^{p-1})(a_0 + a_1 T + a_2 T^2 + \cdots + a_{p-1} T^{p-1}) = (1\ T\ T^2\ \ldots\ T^{p-1})$$
$$\times \begin{pmatrix} a_0 & 0 & 0 & \ldots & 0 & 0 \\ a_1 & a_0 + \mu a_{p-1} & \mu a_{p-2} & \ldots & \mu a_2 & \mu a_1 \\ a_2 & a_1 & a_0 + \mu a_{p-1} & \ldots & \mu a_3 & \mu a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{p-2} & a_{p-3} & a_{p-4} & \ldots & a_0 + \mu a_{p-1} & \mu a_{p-2} \\ a_{p-1} & a_{p-2} & a_{p-3} & \ldots & a_1 & a_0 + \mu a_{p-1} \end{pmatrix}.$$

Hence the result.

Corollary 3.6. *Let A be an $\mathbb{F}_p$-algebra, $\mu \in A$ and $B = A[T]/(T^p - \mu T)$. Then $\prod_{B/A} \mathbb{G}_{m,B}$ is represented by*

$$\operatorname{Spec} A[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta(\mu; T_0, T_1, \ldots, T_{p-1})}]$$

with

(a) the multiplication : $T_0 \mapsto T_0 \otimes T_0$, $T_k \mapsto \sum_{i=0}^{k} T_i \otimes T_{k-i} + \mu \sum_{i=k}^{p-1} T_i \otimes T_{k+p-i-1}$ $(1 \le k \le p-1)$,

(b) the unit : $T_0 \mapsto 1$, $T_k \mapsto 0$ $(1 \le k \le p-1)$.

Proof. Let R be an A-algebra. The multiplication of $R[T]/(T^p-\mu T) = R\otimes_A A[T]/(T^p-\mu T)$ is given by

$$\Bigl(\sum_{i=0}^{p-1} a_iT^i\Bigr)\Bigl(\sum_{i=0}^{p-1} b_iT^i\Bigr) = a_0b_0 + \sum_{k=1}^{p-1}\Bigl(\sum_{i=0}^{k} a_ib_{k-i} + \mu\sum_{i=k}^{p-1} a_ib_{k+p-i-1}\Bigr)T^k.$$

Lemma 3.7. *Let A be an $\mathbb{F}_p$-algebra and $\lambda\in A$. Then we have*

$$\varDelta(\lambda^{p-1};a_0,a_1,\dots,a_{p-1}) = a_0\prod_{k=1}^{p-1}\Bigl\{\sum_{l=0}^{p-1}(k\lambda)^l a_l\Bigr\}$$

for $a_0,a_1,\dots,a_{p-1}\in A$.

Proof. We define $e_k(T)\in A[\varLambda,\varLambda^{-1}][T]$ $(0\le k<p)$ by

$$\begin{aligned}
&e_0(T) = 1-\varLambda^{-p+1}T^{p-1},\\
&e_k(T) = 1-\varLambda^{-p+1}(T-k\varLambda)^{p-1} = -\sum_{l=1}^{p-1}(k\varLambda)^{-l}T^l \ (0<k<p).
\end{aligned}$$

Then we obtain

$$e_k(j\varLambda) = \begin{cases} 1 & (j=k)\\ 0 & (j\ne k).\end{cases}$$

Therefore $\{e_0(T),e_1(T),e_2(T),\dots,e_{p-1}(T)\}$ is a basis over $A[\varLambda,\varLambda^{-1}]$ of $A[\varLambda,\varLambda^{-1}][T]/(T^p-\varLambda^{p-1}T)$. Moreover, we have

$$\begin{aligned}
1 &= e_0(T)+e_1(T)+e_2(T)+\cdots+e_{p-1}(T),\\
T &= \varLambda e_1(T)+2\varLambda e_2(T)+\cdots+(p-1)\varLambda e_{p-1}(T),\\
T^2 &= (\varLambda)^2e_1(T)+(2\varLambda)^2e_2(T)+\cdots+((p-1)\varLambda)^2e_{p-1}(T),\\
&\ \ \vdots\\
T^{p-1} &= \varLambda^{p-1}e_1(T)+(2\varLambda)^{p-1}e_2(T)+\cdots+((p-1)\varLambda)^{p-1}e_{p-1}(T).
\end{aligned}$$

Hence we obtain

$$(e_0(T)\ e_1(T)\ e_2(T)\ \ldots\ e_{p-1}(T))(a_0 + a_1T + a_2T^2 + \cdots + a_{p-1}T^{p-1}) = (e_0(T)\ e_1(T)\ e_2(T)\ \ldots\ e_{p-1}(T)) \times \begin{pmatrix} a_0 & 0 & 0 & \ldots & 0 \\ 0 & \sum_{k=0}^{p-1} \Lambda^k a_k & 0 & \ldots & 0 \\ 0 & 0 & \sum_{k=0}^{p-1} (2\Lambda)^k a_k & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \sum_{k=0}^{p-1} ((p-1)\Lambda)^k a_k \end{pmatrix}.$$

Therefore we obtain an identity in $A[\Lambda]$

$$\Delta(\Lambda^{p-1}; a_0, a_1, \ldots, a_{p-1}) = a_0 \prod_{k=1}^{p-1} \Big\{ \sum_{l=0}^{p-1} (k\Lambda)^l a_l \Big\}.$$

Furthermore, we obtain the required result, specializing Λ to λ.

Combining the above assertion with Proposition 3.5, we obtain the following:

Corollary 3.8. *Let A be an $\mathbb{F}_p$-algebra, $\lambda \in A$ and $f(T) \in A[T]/(T^p - \lambda^{p-1}T)$. Then $f(T)$ is invertible if and only if $f(j\lambda) \in A^\times$ for $0 \le j < p$.*

Notation 3.9. Let A be an $\mathbb{F}_p$-algebra and $\lambda, a \in A$. We put

$$F_p(\lambda, a; T) = 1 + aT + \frac{a^2}{2!}T(T-\lambda) + \frac{a^3}{3!}T(T-\lambda)(T-2\lambda) + \cdots \\ \cdots + \frac{a^{p-1}}{(p-1)!}T(T-\lambda)\cdots(T-(p-2)\lambda).$$

Notation 3.10. Recall now the definition of the Stirling number $S_{k,l}$ of first kind:

$$T(T-1)\ldots(T-(k-1)) = \sum_{l=1}^{k} S_{k,l} T^l$$

For example, we have

$$\begin{array}{lllll} S_{1,1} = 1, & & & & \\ S_{2,1} = -1, & S_{2,2} = 1, & & & \\ S_{3,1} = 2, & S_{3,2} = -3, & S_{3,3} = 1, & & \\ S_{4,1} = -6, & S_{4,2} = 11, & S_{4,3} = -6, & S_{4,4} = 1, & \\ S_{5,1} = 24, & S_{5,2} = -50, & S_{5,3} = 35, & S_{5,4} = -10, & S_{5,5} = 1. \end{array}$$

Lemma 3.11. *Let A be an $\mathbb{F}_p$-algebra and $\lambda, a \in A$. Then $F_p(\lambda, a; T)$ is invertible in $A[T]/(T^p - \lambda^{p-1}T)$ if and only if $1+\lambda a$ is invertible in A.*

Proof. By Corollary 3.8, we obtain the result since $F_p(\lambda, a; j\lambda) = (1+\lambda a)^j$ for $1 \leq j < p$.

Theorem 3.12. *Let A be an $\mathbb{F}_p$-algebra, $\lambda \in A$, $N_A = \mathrm{Ker}[F - \lambda^{p-1}I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$ and $G = N_A^\vee$. Then:*

(1) *A homomorphism of group schemes*

$$\tilde{\chi} : \prod_{N_A/A} \mathbb{G}_{m,N_A} = \mathrm{Spec}\, A[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta(\lambda^{p-1}; T_0, T_1, \ldots, T_{p-1})}] \\ \to \mathcal{G}_A^{(\lambda)} = \mathrm{Spec}\, A[X, \frac{1}{1+\lambda X}]$$

is defined by

$$X \mapsto \sum_{l=1}^{p-1} \lambda^{l-1} T_l \Big/ T_0.$$

Moreover, the diagram of group schemes

$$\begin{array}{ccc} G & \xrightarrow{i} & \prod_{N_A/A} \mathbb{G}_{m,N_A} \\ \| & & \downarrow \tilde{\chi} \\ G & \xrightarrow[\eta]{} & \mathcal{G}_A^{(\lambda)} \end{array}$$

is commutative.

(2) *A homomorphism of group schemes*

$$\tilde{\sigma} : \mathcal{G}_A^{(\lambda)} = \mathrm{Spec}\, A[X, \frac{1}{1+\lambda X}] \to \\ \prod_{N_A/A} \mathbb{G}_{m,N_A} = \mathrm{Spec}\, A[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta(\lambda^{p-1}; T_0, T_1, \ldots, T_{p-1})}].$$

is defined by

$$T_0 \mapsto 1,\ T_l \mapsto \sum_{k=l}^{p-1} \frac{S_{k,l}}{k!} \lambda^{k-l} X^k \ (1 \leq l \leq p-1).$$

Moreover, the diagram of group schemes

$$\begin{array}{ccc} G & \xrightarrow{\eta} & \mathcal{G}_A^{(\lambda)} \\ \| & & \downarrow \tilde{\sigma} \\ G & \xrightarrow[i]{} & \prod_{N_A/A} \mathbb{G}_{m,N_A} \end{array}$$

is commutative, and $\tilde{\sigma}$ is a section of $\tilde{\chi}$

Proof. (1) At first we consider the case where $A=\mathbb{F}_p[\Lambda]$ and $\lambda=\Lambda$. Let R be an A-algebra and $f(T)=\sum_{k=0}^{p-1} a_k T_k \in \prod_{N_A/A} \mathbb{G}_{m,N_A}(R)=(R[T]/(T^p-\Lambda^{p-1}T))^\times$. Then we obtain

$$\tilde{\chi}(f(T))=\sum_{k=0}^{p-1} a_k \Lambda^{k-1}=\frac{1}{\Lambda}\Big\{\frac{f(\Lambda)}{f(0)}-1\Big\}$$

by the definition of $\tilde{\chi}$. Moreover, we obtain

$$\begin{aligned}\frac{1}{\Lambda}\Big\{\frac{f(\Lambda)}{f(0)}-1\Big\}+\frac{1}{\Lambda}\Big\{\frac{g(\Lambda)}{g(0)}-1\Big\}+\Lambda\,\frac{1}{\Lambda}\Big\{\frac{f(\Lambda)}{f(0)}-1\Big\}\frac{1}{\Lambda}\Big\{\frac{g(\Lambda)}{g(0)}-1\Big\}&\\ =\frac{1}{\Lambda}\Big\{\frac{f(\Lambda)g(\Lambda)}{f(0)g(0)}-1\Big\}&\end{aligned}$$

for $f(T),g(T)\in(R[T]/(T^p-\Lambda^{p-1}T))^\times$, which means that $\tilde{\chi}$ is a group homomorphism. In the general case, we see that $\tilde{\chi}$ is a group homomorphism, specializing Λ to λ.

Let R be an A-algebra. By definition,

(a) $i: G(R)\to(\prod_{N_A/A}\mathbb{G}_{m,N_A})(R)=\big(R[T]/(T^p-\Lambda^{p-1}T)\big)^\times$ is given by

$$a\mapsto\sum_{i=1}^{p-1}\frac{a^i}{i!}T^i;$$

(b) $\tilde{\chi}:(\prod_{N_A/A}\mathbb{G}_{m,N_A})(R)=\big(R[T]/(T^p-\Lambda^{p-1}T)\big)^\times\to\mathcal{G}_A^{(\lambda)}(R)$ is given by

$$\sum_{i=0}^{p-1}a_iT^i\mapsto\sum_{i=0}^{p-1}\lambda^{i-1}a_i\Big/a_0;$$

(c) $\eta: G(R)\to\mathcal{G}_A^{(\lambda)}(R)$ is given by

$$a\mapsto\sum_{i=1}^{p-1}\lambda^{i-1}a^i.$$

These imply the commutativity of the first square.

(2) Let R be an A-algebra. Then, by definition, we have

$$\begin{aligned} F_p(\lambda, a; T) &= 1 + aT + \frac{a^2}{2!}T(T-\lambda) + \cdots \\ &\quad + \frac{a^{p-1}}{(p-1)!}T(T-\lambda)\cdots(T-(p-2)\lambda) \\ &= 1 + \sum_{l=1}^{p-1}\Big(\sum_{k=l}^{p-1}\frac{S_{k,l}}{k!}\lambda^{k-l}a^k\Big)T^l \end{aligned}$$

for $a \in R$. If $a \in \mathcal{G}_A^{(\lambda)}(R)$, then $1+\lambda a$ is invertible in R, and therefore $F_p(\lambda, a; T)$ is invertible in $R[T]/(T^p - \lambda^{p-1}T)$.

At first we consider the case where $A = \mathbb{F}_p[\Lambda]$ and $\lambda = \Lambda$. We define a ring homomorphism

$$\varphi : R[\Lambda][T]/(T^p - \Lambda^{p-1}T) \to R[\Lambda]^p$$

by

$$f(T) \mapsto (f(0), f(\Lambda), f(2\Lambda), \ldots, f(p-1)\Lambda)).$$

Then,

$$\varphi \otimes_{R[\Lambda]} R[\Lambda, \Lambda^{-1}] : R[\Lambda, \Lambda^{-1}][T]/(T^p - \Lambda^{p-1}T) \to R[\Lambda, \Lambda^{-1}]^p$$

is an isomorphism of $R[\Lambda, \Lambda^{-1}]$-algebra since we have

$$T^p - \Lambda^{p-1}T = T(T-\Lambda)(T-2\Lambda)\cdots(T-(p-1)\Lambda).$$

Therefore the map $\varphi : R[\Lambda][T]/(T^p - \Lambda^{p-1}T) \to R[\Lambda]^p$ is injective. Now we have

$$\varphi(F_p(\Lambda, a : T)) = (1, 1+\Lambda a, (1+\Lambda a)^2, \ldots, (1+\Lambda a)^{p-1}).$$

Moreover, we have an identity in $R[\Lambda][T]/(T^p - \Lambda^{p-1}T)$

$$F_p(\Lambda, a; T)F_p(\Lambda, b; T) = F_p(\Lambda, a+b+\Lambda ab; T)$$

since $(1+\Lambda a)(1+\Lambda b) = 1 + \Lambda(a+b+\Lambda ab)$. Therefore $\tilde{\sigma}$ is a group homomorphism.

By the definition of $\tilde{\chi}$, we have also

$$\tilde{\chi}(\tilde{\sigma}((a)) = \tilde{\chi}(F_p(\Lambda, a; T)) = a$$

for $f(T) \in (R[T]/(T^p - \Lambda^{p-1}T))^\times$. It follows that $\tilde{\sigma}$ is a section of $\tilde{\chi}$.

Now we verify the commutativity of the second square. As is known, we have an identity in $\mathbb{Q}[[U]]$

$$\sum_{k=l}^{\infty}\frac{S_{k,l}}{k!}U^k = \frac{1}{l!}\{\log(1+U)\}^l$$

for each $l \geq 1$ (cf.[8, 1.1.11]). Then we obtain in $\mathbb{Q}[\Lambda, T][[U]]$

$$\sum_{k=l}^{p-1} \frac{S_{k,l}}{k!} \Lambda^{k-l} U^k \equiv \frac{1}{l!} \Big\{ \frac{\log(1+\Lambda U)}{\Lambda} \Big\}^l \quad \bmod U^p$$

for $1 \leq l \leq p-1$, and therefore,

$$\begin{aligned} 1 + \sum_{l=1}^{p-1} \Big(\sum_{k=l}^{p-1} \frac{S_{k,l}}{k!} \Lambda^{k-l} U^k \Big) T^l &\equiv 1 + \sum_{l=0}^{\infty} \frac{1}{l!} \Big\{ \frac{T \log(1+\Lambda U)}{\Lambda} \Big\}^l \\ &= \exp\Big[\frac{T}{\Lambda} \log(1+\Lambda U) \Big] \quad \bmod U^p. \end{aligned}$$

Furthermore we obtain

$$1 + \sum_{l=1}^{p-1} \Big\{ \sum_{k=l}^{p-1} \frac{S_{k,l}}{k!} \Lambda^{k-l} \Big(\sum_{i=1}^{p-1} \frac{\Lambda^{i-1}}{i!} U^i \Big)^k \Big\} T^l \equiv \exp TU \quad \bmod U^p,$$

noting that

$$\sum_{i=1}^{p-1} \frac{\Lambda^{i-1}}{i!} U^i \equiv \frac{\exp \Lambda U - 1}{\Lambda} \quad \bmod U^p.$$

At last we have gotten an identity in $\mathbb{Z}_{(p)}[\Lambda, U, T]/(U^p)$

$$1 + \sum_{l=1}^{p-1} \Big\{ \sum_{k=l}^{p-1} \frac{S_{k,l}}{k!} \Lambda^{k-l} \Big(\sum_{i=1}^{p-1} \frac{\Lambda^{i-1}}{i!} U^i \Big)^k \Big\} T^l = \sum_{i=0}^{p-1} \frac{U^i}{i!} T^i,$$

which reads as an identity in $\mathbb{F}_p[\Lambda, U, T]/(U^p)$. This implies the commutativity of the second square.

In the general case, we obtain the required results, specializing Λ to λ.

Corollary 3.13. *Let S be an A-scheme and X a G-torsor over S. Then the class $[X]$ belongs to* $\mathrm{Ker}[H^1(S, G) \to H^1(S, \mathcal{G}_A^{(\lambda)})]$ *if and only if $[X]$ is trivial in* $\mathrm{Pic}(S \times_A N_A)$.

Proof. By Theorem 3.12.(1), we obtain a commutative diagram of cohomology groups

$$\begin{array}{ccc} H^1(S, G) & \xrightarrow{\ i\ } & H^1(S, \prod_{N_A/A} \mathbb{G}_{m,N_A}) \\ \| & & \downarrow \tilde{\chi} \\ H^1(S, G) & \xrightarrow[\eta]{} & H^1(S, \mathcal{G}_A^{(\lambda)}) \end{array}.$$

Hence we obtain an implication

$$[X] \text{ is trivial in } \mathrm{Pic}(S \times_A N_A) \Rightarrow [X] \in \mathrm{Ker}[H^1(S, G) \to H^1(S, \mathcal{G}_A^{(\lambda)})].$$

On the other hand, by Theorem 3.12. (2), we obtain a commutative diagram of cohomology groups

$$\begin{array}{ccc} H^1(S,G) & \xrightarrow{\eta} & H^1(S,\mathcal{G}_A^{(\lambda)}) \\ \| & & \downarrow{\scriptstyle \tilde{\sigma}} \\ H^1(S,G) & \xrightarrow[i]{} & H^1(S,\prod_{N_A/A}\mathbb{G}_{m,N_A}) \end{array}.$$

Hence we obtain an implication

$$[X] \in \mathrm{Ker}[H^1(S,G) \to H^1(S,\mathcal{G}^{(\lambda)}) \Rightarrow [X] \text{ is trivial in } \mathrm{Pic}(S \times_A N).$$

Remark 3.14. Let A be an $\mathbb{F}_p$-algebra, $\lambda \in A$ and $B = A[T]/(T^p - \lambda^{p-1}T)$. We define a homomorphism of group schemes

$$\varepsilon : \prod_{B/A} \mathbb{G}_{m,B} \to \mathbb{G}_{m,A}$$

by

$$U \mapsto T_0.$$

We define also a homomorphism of group schemes

$$\chi_k : \prod_{B/A} \mathbb{G}_{m,B} \to \mathbb{G}_{m,A}$$

by

$$U \mapsto \sum_{l=0}^{p-1} k^l \lambda^l T_l$$

for $0 < k < p$.

If λ is invertible in A,

$$(\varepsilon, \chi_1, \ldots, \chi_{p-1}) : \prod_{B/A} \mathbb{G}_{m,B} \to (\mathbb{G}_{m,A})^{p-1}$$

is an isomorphism. The inverse of $(\varepsilon, \chi_1, \ldots, \chi_{p-1})$ is given by

$$T_0 \mapsto U_0,\ T_l \mapsto -\lambda^{-l} \sum_{k=1}^{p-1} k^{-l} U_k \ (1 \le l \le p-2),\ T_{p-1} = -\lambda^{-p+1} \sum_{k=0}^{p-1} U_k.$$

Furthermore the homomorphism

$$\sigma_0 : \mathbb{G}_{m,A} \to \prod_{B/A} \mathbb{G}_{m,B}$$

defined by

$$T_0 \mapsto U,\ T_l \mapsto 0 \ (1 \le l \le p-2),\ T_{p-1} \mapsto \lambda^{-p+1}(1-U)$$

is a section of ε. For $1 \leq k \leq p-1$, the homomorphism

$$\sigma_k : \mathbb{G}_{m,A} \to \prod_{B/A} \mathbb{G}_{m,B}$$

defined by

$$T_0 \mapsto 1,\ T_l \mapsto (k\lambda)^{-1}(1-U)\ (1 \leq l \leq p-1)$$

is section of χ_k.

The composition $\alpha^{(\lambda)} \circ \tilde{\chi}$ coincides with the homomorphism χ_1/ε. Moreover, if λ is invertible in A, then the homomorphism $\tilde{\sigma}$ coincides with the composition $(\sigma_1\sigma_2^2 \cdots \sigma_{p-1}^{p-1}) \circ \alpha^{(\lambda)}$.

We conclude the section, examining the sequence: (2) $0 \to G \xrightarrow{\xi} G_{B/A} \xrightarrow{F} G_{\tilde{B}/A} \to 0$.

Lemma 3.15. *Let p be a prime number > 2, A an $\mathbb{F}_p$-algebra and $\lambda \in A$. Put $N_A = \mathrm{Ker}[F - \lambda^{\frac{p-1}{2}} I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$ and $B = A[T]/(T^2 - \lambda)$. Then a homomorphism of group schemes*

$$\pi : \prod_{N_A/A} \mathbb{G}_{m,N_A} = \operatorname{Spec} A[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta(\lambda^{(p-1)/2}; T_0, T_1, \ldots, T_{p-1})}]$$
$$\to \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 - \lambda V^2}$$

is defined by

$$U \mapsto \sum_{l=0}^{(p-1)/2} \lambda^l T_{2l},\ V \mapsto \sum_{l=1}^{(p-1)/2} \lambda^{l-1} T_{2l-1}.$$

Proof. Let R be an A-algebra. Then a homomorphism of R-algebra

$$\pi : R[T]/(T^p - \lambda^{\frac{p-1}{2}} T) \to R[T]/(T^2 - \lambda)$$

is defined by $\pi(f(T)) = f(\sqrt{\lambda})$ since the polynomial $T^{p-1} - \lambda^{\frac{p-1}{2}} T$ is divisible by $T^2 - \lambda$. Hence we obtain a homomorphism of multiplicative groups

$$\pi : \big(R[T]/(T^p - \lambda^{\frac{p-1}{2}} T)\big)^\times \to \big(R[T]/(T^2 - \lambda)\big)^\times,$$

which is represented by a homomorphism of group A-schemes

$$\pi : \prod_{N_A/A} \mathbb{G}_{m,N_A} = \operatorname{Spec} A[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta(\lambda^{(p-1)/2}; T_0, T_1, \ldots, T_{p-1})}]$$
$$\to \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 - \lambda V^2}].$$

In fact, for $f(T) = \sum_{k=0}^{p-1} a_k T^k \in \big(R[T]/(T^p - \lambda^{\frac{p-1}{2}})\big)^\times$, we have

$$\pi(f(T)) = F(\sqrt{\lambda}) = (\sum_{k=0}^{\frac{p-1}{2}} a_{2k}\lambda^k) + \Big(\sum_{k=0}^{\frac{p-1}{2}} a_{2k-1}\lambda^{k-1}\Big)\sqrt{\lambda}.$$

Lemma 3.16. *Let p be a prime number > 2. Put*

$$F_p(\Lambda, U; T) = 1+UT+\frac{U^2}{2!}T(T-\Lambda)+\cdots+\frac{U^{p-1}}{(p-1)!}T(T-\Lambda)\cdots(T-(p-2)\Lambda)$$

and

$$G_p(\Lambda, X, Y; T) = F_p(\sqrt{\Lambda}, 2(X+Y\sqrt{\Lambda}); T)F_p(-\sqrt{\Lambda}, 2(X-Y\sqrt{\Lambda}); T).$$

Then $G_p(\Lambda, X, Y, T) \in \mathbb{Z}_{(p)}[\Lambda, X, Y, T]$.

Proof. The field $\mathbb{Q}(\sqrt{\Lambda}, X, Y, T)$ is a quadratic extension of $\mathbb{Q}(\Lambda, X, Y, T)$, and the Galois group is generated by $\sqrt{\Lambda} \mapsto -\sqrt{\Lambda}$. Hence we have $G_p(\Lambda, X, Y; T) \in \mathbb{Q}(\Lambda, X, Y, T)$ since $G_p(\Lambda, X, Y; T)$ is invariant under the action $\sqrt{\Lambda} \mapsto -\sqrt{\Lambda}$.

We obtain the result, noting $\mathbb{Z}_{(p)}[\sqrt{\Lambda}, X, Y, T] \cap \mathbb{Q}(\Lambda, X, Y, T) = \mathbb{Z}_{(p)}[\Lambda, X, Y, T]$.

Notation 3.17. For each $l \geq 1$, we define $c_{p,l}(\Lambda; X, Y) \in \mathbb{Z}_{(p)}[\Lambda; X, Y]$ by

$$G_p(\Lambda, X, Y; T) = 1 + \sum_{l\geq 1} c_{p,l}(\Lambda; X, Y)T^l.$$

Example 3.18. When $p = 3$, we have

$$\begin{aligned}
c_{3,1}(\Lambda; X, Y) &= 4X - 48XY\Lambda,\\
c_{3,2}(\Lambda; X, Y) &= 28X^2 - 144X^4\Lambda\\
&\qquad - 48X^2Y\Lambda + 20Y^2\Lambda + 288X^2Y^2\Lambda^2 + 48Y^3\Lambda^2 - 144Y^4\Lambda^3,\\
c_{3,3}(\Lambda; X, Y) &= 48X^3 - 48XY^2\Lambda,\\
c_{3,4}(\Lambda; X, Y) &= 144X^4 - 288X^2Y^2\Lambda + 144Y^4\Lambda^2.
\end{aligned}$$

Example 3.19. When $p = 5$, we have

$$
\begin{aligned}
c_{5,1}(\Lambda; X, Y) &= 4X + 32X^3\Lambda - 48XY\Lambda - 3072X^3Y\Lambda^2 + 96XY^2\Lambda^2 \\
&\quad - 3072XY^3\Lambda^3, \\
c_{5,2}(\Lambda; X, Y) &= 28X^2 + 1328X^4\Lambda - 192X^2Y\Lambda + 20Y^2\Lambda - 8960X^6\Lambda^2 \\
&\quad - 4224X^4Y\Lambda^2 + 8736X^2Y^2\Lambda^2 - 147456X^8\Lambda^3 \\
&\quad - 12288X^6Y\Lambda^3 + 8448X^4Y^2\Lambda^3 + 2304X^2Y^3\Lambda^3 \\
&\quad + 1200Y^4\Lambda^3 + 589824X^6Y^2\Lambda^4 + 36864X^4Y^3\Lambda^4 \\
&\quad + 9984X^2Y^4\Lambda^4 + 1920Y^5\Lambda^4 - 884736X^4Y^4\Lambda^5 \\
&\quad - 36864X^2Y^5\Lambda^5 - 9472Y^6\Lambda^5 + 589824X^2Y^6\Lambda^6 \\
&\quad + 12288Y^7\Lambda^6 - 147456Y^8\Lambda^7, \\
c_{5,3}(\Lambda; X, Y) &= 64X^3 + 2624X^5\Lambda - 3264X^3Y\Lambda + 4096X^7\Lambda^2 \\
&\quad + 15360X^5Y\Lambda^2 + 6016X^3Y^2\Lambda^2 - 2880XY^3\Lambda^2 \\
&\quad - 12288X^5Y^2\Lambda^3 - 30720X^3Y^3\Lambda^3 - 8640XY^4\Lambda^3 \\
&\quad + 12288X^3Y^4\Lambda^4 + 15360XY^5\Lambda^4 - 4096XY^6\Lambda^5, \\
c_{5,4}(\Lambda; X, Y) &= 304X^4 + 7360X^6\Lambda - 4992X^4Y\Lambda + 480X^2Y^2\Lambda \\
&\quad + 200704X^8\Lambda^2 + 15360X^6Y\Lambda^2 - 6720X^4Y^2\Lambda^2 \\
&\quad + 3840X^2Y^3\Lambda^2 + 240Y^4\Lambda^2 - 802816X^6Y^2\Lambda^3 \\
&\quad - 46080X^4Y^3\Lambda^3 - 8640X^2Y^4\Lambda^3 + 1152Y^5\Lambda^3 \\
&\quad + 1204224X^4Y^4\Lambda^4 + 46080X^2Y^5\Lambda^4 + 8000Y^6\Lambda^4 \\
&\quad - 802816X^2Y^6\Lambda^5 - 15360Y^7\Lambda^5 + 200704Y^8\Lambda^6, \\
c_{5,5}(\Lambda; X, Y) &= 448X^5 - 5120X^7\Lambda - 15360X^5Y\Lambda + 128X^3Y^2\Lambda \\
&\quad + 15360X^5Y^2\Lambda^2 + 30720X^3Y^3\Lambda^2 - 576XY^4\Lambda^2 \\
&\quad - 15360X^3Y^4\Lambda^3 - 15360XY^5\Lambda^3 + 5120XY^6\Lambda^4, \\
c_{5,6}(\Lambda; X, Y) &= 1600X^6 - 57344X^8\Lambda - 3072X^6Y\Lambda - 1728X^4Y^2\Lambda \\
&\quad + 229376X^6Y^2\Lambda^2 + 9216X^4Y^3\Lambda^2 - 1344X^2Y^4\Lambda^2 \\
&\quad - 344064X^4Y^4\Lambda^3 - 9216X^2Y^5\Lambda^3 + 1472Y^6\Lambda^3 \\
&\quad + 229376X^2Y^6\Lambda^4 + 3072Y^7\Lambda^4 - 57344Y^8\Lambda^5, \\
c_{5,7}(\Lambda; X, Y) &= 1024X^7\Lambda - 3072X^5Y^2\Lambda + 3072X^3Y^4\Lambda^2 - 1024XY^6\Lambda^3, \\
c_{5,8}(\Lambda; X, Y) &= 4096X^8 - 16384X^6Y^2\Lambda + 24576X^4Y^4\Lambda^2 - 16384X^2Y^6\Lambda^3 \\
&\quad + 4096Y^8\Lambda^4.
\end{aligned}
$$

Theorem 3.20. *Let p be a prime number >2, A an $\mathbb{F}_p$-algebra and $\lambda \in A$. Put $N_A = \mathrm{Ker}[F - \lambda^{\frac{p-1}{2}} I : \mathbb{G}_{a,A} \to \mathbb{G}_{a,A}]$ and $G = N_A^\vee$. Then:*
(1) *A homomorphism of group schemes*

$$\tilde{\chi} : \prod_{N_A/A} \mathbb{G}_{m,N_A} = \mathrm{Spec}\, A[T_0, T_1, \dots, T_{p-1}, \frac{1}{\Delta(\lambda^{(p-1)/2}; T_0, T_1, \dots, T_{p-1})}] \\ \to G_{B/A} = \mathrm{Spec}\, A[X,Y]/(X^2 - \lambda Y^2 - Y)$$

is defined by

$$X \mapsto \frac{\Big(\sum_{l=0}^{(p-1)/2} \lambda^l T_{2l}\Big)\Big(\sum_{l=1}^{(p-1)/2} \lambda^{l-1} T_{2l-1}\Big)}{\Big(\sum_{l=0}^{(p-1)/2} \lambda^l T_{2l}\Big)^2 - \lambda\Big(\sum_{l=1}^{(p-1)/2} \lambda^{l-1} T_{2l-1}\Big)^2},$$

$$Y \mapsto \frac{\Big(\sum_{l=1}^{(p-1)/2} \lambda^{l-1} T_{2l-1}\Big)^2}{\Big(\sum_{l=0}^{(p-1)/2} \lambda^l T_{2l}\Big)^2 - \lambda\Big(\sum_{l=1}^{(p-1)/2} \lambda^{l-1} T_{2l-1}\Big)^2}.$$

Moreover, the diagram of group schemes

$$\begin{tikzcd} G \arrow[r, "i"] \arrow[d, "\wr"', "\text{square map}"'] & \prod_{N_A/A} \mathbb{G}_{m,N_A} \arrow[d, "\tilde{\chi}"] \\ G \arrow[r, "\xi"'] & G_{B/A} \end{tikzcd}$$

is commutative.
(2) *A homomorphism of group schemes*

$$\tilde{\sigma} : G_{B/A} = \mathrm{Spec}\, A[X,Y]/(X^2 - \lambda Y^2 - Y) \to \\ \prod_{N_A/A} \mathbb{G}_{m,N_A} = \mathrm{Spec}\, A[T_0, T_1, \dots, T_{p-1}, \frac{1}{\Delta(\lambda^{(p-1)/2}; T_0, T_1, \dots, T_{p-1})}]$$

is defined by

$$T_0 \mapsto 1,\ T_l \mapsto c_{p,l}(\lambda; X, Y) + \lambda^{\frac{p-1}{2}} c_{p,l+p-1}(\lambda; X, Y)\ (1 \le l \le p-1).$$

Moreover, the diagram of group schemes

$$\begin{tikzcd} G \arrow[r, "\xi"] \arrow[d, "\wr", "\text{square map}"'] & G_{B/A} \arrow[d, "\tilde{\sigma}"] \\ G \arrow[r, "i"'] & \prod_{N_A/A} \mathbb{G}_{m,N_A} \end{tikzcd}$$

is commutative.

Proof. (1) At first recall that a homomorphism of group schemes

$$r : \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 - \lambda V^2}] \\ \to G_{B/A} = \operatorname{Spec} A[X, Y]/(X^2 - \lambda Y^2 - Y)$$

is defined by

$$X \mapsto \frac{UV}{U^2 - \lambda V^2},\ Y \mapsto \frac{V^2}{U^2 - \lambda V^2}.$$

Then $\tilde{\chi}$ is nothing but the composite

$$r \circ \pi : \prod_{N_A/A} \mathbb{G}_{m,N_A} \to \prod_{B/A} \mathbb{G}_{m,B} \to G_{B/A}.$$

Now we verify the commutativity of the first square. First note that the square map on $G = \operatorname{Spec} A[T]/(T^p)$ is given by $T \mapsto 2T$ since the multiplication of G is defined by

$$\varDelta : T \mapsto T \otimes 1 + 1 \otimes T - \mu \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} T^{p-i} \otimes T^i.$$

Let R be an A-algebra. Then by the definition,
(a) $i : G(R) \to (\prod_{N_A/A} \mathbb{G}_{m,N_A})(R) = \big(R[T]/(T^p - \lambda^{\frac{p-1}{2}} T)\big)^{\times}$ is given by

$$a \mapsto \sum_{i=0}^{p-1} \frac{a^i}{i!} T^i;$$

(b) $\tilde{\chi} : (\prod_{N_A/A} \mathbb{G}_{m,N_A})(R) = \big(R[T]/(T^p - \lambda^{\frac{p-1}{2}})\big)^{\times} \to G_{B/A}(R)$ is given by

$$\sum_{i=0}^{p-1} a_i T^i \mapsto \left(\frac{\Big(\sum_{i=0}^{\frac{p-1}{2}} \lambda^i a_{2i}\Big)\Big(\sum_{i=1}^{\frac{p-1}{2}} \lambda^{i-1} a_{2i-1}\Big)}{\Big(\sum_{i=0}^{\frac{p-1}{2}} \lambda^i a_{2i}\Big)^2 - \lambda\Big(\sum_{i=1}^{\frac{p-1}{2}} \lambda^{i-1} a_{2i-1}\Big)^2}, \frac{\Big(\sum_{i=1}^{\frac{p-1}{2}} \lambda^{i-1} a_{2i-1}\Big)^2}{\Big(\sum_{i=0}^{\frac{p-1}{2}} \lambda^i a_{2i}\Big)^2 - \lambda\Big(\sum_{i=1}^{\frac{p-1}{2}} \lambda^{i-1} a_{2i-1}\Big)^2} \right);$$

(c) $\xi : G(R) \to G_{B/A}(R)$ is given by

$$a \mapsto \Big(\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}a^{2i-1}, \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i)!}a^{2i}\Big).$$

Hence the map $\tilde{\chi} \circ i : G(R) \to G_{B/A}(R)$ is given by

$$\sum_{i=0}^{p-1} a_i T^i \mapsto$$

$$\left(\frac{\Big\{\sum_{i=0}^{\frac{p-1}{2}} \frac{\lambda^i}{(2i)!}a^{2i}\Big\}\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}a^{2i-1}\Big\}}{\Big\{\sum_{i=0}^{\frac{p-1}{2}} \frac{\lambda^i}{(2i)!}a^{2i}\Big\}^2 - \lambda\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}a^{2i-1}\Big\}^2}, \frac{\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}a^{2i-1}\Big\}^2}{\Big\{\sum_{i=0}^{\frac{p-1}{2}} \frac{\lambda^i}{(2i)!}a_{2i}\Big\}^2 - \lambda\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}a^{2i-1}\Big\}^2}\right)$$

and the map $\xi \circ \text{square} : G(R) \to G_{B/A}(R)$ is given by

$$a \mapsto \Big(\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}(2a)^{2i-1}, \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i)!}(2a)^{2i}\Big).$$

Then it is sufficient to verify that, for $a \in R$ with $a^p = 0$, we have

$$\frac{\Big\{\sum_{i=0}^{(p-1)/2} \frac{\lambda^i}{(2i)!}a^{2i}\Big\}\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}a^{2i-1}\Big\}}{\Big\{\sum_{i=0}^{\frac{p-1}{2}} \frac{\lambda^i}{(2i)!}a^{2i}\Big\}^2 - \lambda\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}a^{2i-1}\Big\}^2} = \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}(2a)^{2i-1}$$

and

$$\frac{\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}a^{2i-1}\Big\}^2}{\Big\{\sum_{i=0}^{\frac{p-1}{2}} \frac{\lambda^i}{(2i)!}a^{2i}\Big\}^2 - \lambda\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i-1)!}a^{2i-1}\Big\}^2} = \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\lambda^{i-1}}{(2i)!}(2a)^{2i}.$$

In fact, we have two identities in $\mathbb{Q}[\sqrt{\Lambda}][[U]]$:

$$\cosh\sqrt{\Lambda}U \equiv \sum_{i=0}^{\frac{p-1}{2}} \frac{\Lambda^i}{(2i)!}U^{2i} \mod U^p,$$

$$\frac{\sinh\sqrt{\Lambda}U}{\sqrt{\Lambda}} \equiv \sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i-1)!}U^{2i-1} \mod U^p$$

These imply that

$$\Big\{\sum_{i=0}^{\frac{p-1}{2}} \frac{\Lambda^i}{(2i)!}U^{2i}\Big\}^2 - \Lambda\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i-1)!}U^{2i-1}\Big\}^2 \equiv (\cosh\sqrt{\Lambda}U)^2 - \Lambda\Big(\frac{\sinh\sqrt{\Lambda}U}{\sqrt{\Lambda}}\Big) \\ = 1 \mod U^p,$$

$$\begin{aligned}\Big\{\sum_{i=0}^{\frac{p-1}{2}} \frac{\Lambda^i}{(2i)!}U^{2i}\Big\}\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i-1)!}U^{2i-1}\Big\} &\equiv \cosh\sqrt{\Lambda}U\, \frac{\sinh\sqrt{\Lambda}U}{\sqrt{\Lambda}} \\ &= \frac{1}{2}\,\frac{\sinh 2\sqrt{\Lambda}U}{2\sqrt{\Lambda}} \\ &\equiv \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i-1)!}(2U)^{2i-1} \mod U^p,\end{aligned}$$

$$\begin{aligned}\Big(\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i-1)!}U^{2i-1}\Big)^2 &\equiv \Big(\frac{\sinh\sqrt{\Lambda}U}{\sqrt{\Lambda}}\Big)^2 \\ &= \frac{1}{2}\,\frac{\cosh 2\sqrt{\Lambda}U - 1}{\Lambda} \\ &\equiv \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i)!}(2U)^{2i} \mod U^p.\end{aligned}$$

Then we obtain identities in $\mathbb{Z}_{(p)}[\Lambda, U]/(U^p)$:

$$\Big\{\sum_{i=0}^{\frac{p-1}{2}} \frac{\Lambda^i}{(2i)!}U^{2i}\Big\}^2 - \Lambda\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i-1)!}U^{2i-1}\Big\}^2 = 1,$$

$$\Big\{\sum_{i=0}^{\frac{p-1}{2}} \frac{\Lambda^i}{(2i)!}U^{2i}\Big\}\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i-1)!}U^{2i-1}\Big\} = \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i-1)!}(2U)^{2i-1},$$

$$\Big\{\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i-1)!}U^{2i-1}\Big\}^2 = \frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}} \frac{\Lambda^{i-1}}{(2i)!}(2U)^{2i}.$$

(2) As is remarked in 1.4, an isomorphism of group schemes over B

$$s_1 : G_{B/A} \otimes_A B = \operatorname{Spec} B[X,Y]/(X^2 - \lambda Y^2 - Y) \\ \xrightarrow{\sim} \mathcal{G}_B^{(\sqrt{\lambda})} = \operatorname{Spec} B[T, \frac{1}{1+\sqrt{\lambda}T}]$$

is defined by

$$T \mapsto 2(X+\sqrt{\lambda}Y).$$

Then we obtain a homomorphism of group schemes over B

$$\sigma_1 = \tilde{\sigma}_1 \circ s_1 : G_{B/A} \otimes_A B \xrightarrow{\sim} \mathcal{G}_B^{(\sqrt{\lambda})} \to \big(\prod_{N_A/A} \mathbb{G}_{m,N_A}\big) \otimes_A B,$$

where $\tilde{\sigma}_1 : \mathcal{G}_B^{(\sqrt{\lambda})} \to \big(\prod_{N_A/A} \mathbb{G}_{m,N_A}\big) \otimes_A B$ is the homomorphism defined as in the statement of in Theorem 3.12. For a B-algebra R, the map $\sigma_1 : G_{B/A}(R) \to \big(\prod_{N_A/A} \mathbb{G}_{m,N_A}\big)(R) = \big(R[T]/(T^p - \lambda^{\frac{p-1}{2}}T)\big)^\times$ is given by

$$(a,b) \mapsto F_p(\sqrt{\lambda}, 2(a+b\sqrt{\lambda}); T).$$

Similarly an isomorphism of group schemes over B

$$\begin{aligned} s_2 : G_{B/A} \otimes_A B = \operatorname{Spec} B[X,Y]/(X^2 - \lambda Y^2 - Y) \\ \xrightarrow{\sim} \mathcal{G}_B^{(-\sqrt{\lambda})} = \operatorname{Spec} B[T, \frac{1}{1-\sqrt{\lambda}T}] \end{aligned}$$

is defined by

$$T \mapsto 2(X-\sqrt{\lambda}Y).$$

Then we obtain a homomorphism of group schemes over B

$$\sigma_2 = \tilde{\sigma}_2 \circ s_2 : G_{B/A} \otimes_A B \xrightarrow{\sim} \mathcal{G}_B^{(-\sqrt{\lambda})} \to \big(\prod_{N_A/A} \mathbb{G}_{m,N_A}\big) \otimes_A B.$$

For a B-algebra R, the map $\sigma_2 : G_{B/A}(R) \to \big(\prod_{N_A/A} \mathbb{G}_{m,N_A}\big)(R) = \big(R[T]/(T^p - \lambda^{\frac{p-1}{2}}T)\big)^\times$ is given by

$$(a,b) \mapsto F_p(-\sqrt{\lambda}, 2(a-b\sqrt{\lambda}); T).$$

Hence, by the definition, the morphism

$$\tilde{\sigma}_B : G_{B/A} \otimes_A B \to \big(\prod_{N_A/A} \mathbb{G}_{m,N_A}\big) \otimes_A B$$

is the product of σ_1 and σ_2. It follows that $\tilde{\sigma}_B$ is a homomorphism of group schemes over B. Furtheremore $\tilde{\sigma} : G_{B/A} \to \prod_{N_A/A} \mathbb{G}_{m,N_A}$ is a homomorphism of group schemes over A since B is faithfully flat over A.

We verify now the commutativity of the second square. Consider the composite of homomorphisms

$$G \otimes_A B \xrightarrow{\xi_B} G_{B/A} \otimes_A B \xrightarrow{s_1} \mathcal{G}_B^{(\sqrt{\lambda})} \xrightarrow{\tilde{\sigma}_1} \big(\prod_{N/A} \mathbb{G}_{m,N}\big) \otimes_A B.$$

As is shown in 2.12, we have

$$\eta_B = s_1 \circ \xi_B : G \otimes_A B \to G_{B/A} \otimes_A B \xrightarrow{\sim} \mathcal{G}_B^{(\sqrt{\lambda})}.$$

Hence, by Theorem 3.12(2), we have $\tilde{\sigma}_1 \circ \eta_B = \xi_B$, and therefore $\sigma_1 \circ \xi_B = \tilde{\sigma}_1 \circ s_1 \circ \xi_B = i_B$. Similary we obtain $\sigma_2 \circ \xi_B = i_B$. These imply that $(\tilde{\sigma} \circ \xi)_B = i_B \circ \text{square}$. At last we obtain the required result since B is faithfully flat over A.

Corollary 3.21. *Let S be an A-scheme and X a G-torsor over S. Then the class $[X]$ belongs to* $\mathrm{Ker}[H^1(S,G) \to H^1(S,G_{B/A})]$ *if and only if $[X]$ is trivial in* $\mathrm{Pic}(S \times_A N_A)$.

Proof. By Theorem 3.18 (1), we obtain a commutative diagram of cohomology groups

$$\begin{array}{ccc} H^1(S,G) & \xrightarrow{i} & H^1(S, \prod_{N_A/A} \mathbb{G}_{m,N_A}) \\ {\scriptstyle \text{square map}}\big\downarrow\wr & & \big\downarrow \tilde{\chi} \\ H^1(S,G) & \xrightarrow[\xi]{} & H^1(S, G_{B/A}) \end{array}.$$

Hence we obtain an implication

$$[X] \text{ is trivial in } \mathrm{Pic}(S \times_A N_A) \Rightarrow [X] \in \mathrm{Ker}[H^1(S,G) \to H^1(S,G_{B/A})].$$

On the other hand, by Theorem 3.18 (2), we obtain a commutative diagram of cohomology groups

$$\begin{array}{ccc} H^1(S,G) & \xrightarrow{\xi} & H^1(S, G_{B/A}) \\ {\scriptstyle \text{square map}}\big\downarrow\wr & & \big\downarrow \tilde{\sigma} \\ H^1(S,G) & \xrightarrow[i]{} & H^1(S, \prod_{N_A/A} \mathbb{G}_{m,N_A}) \end{array}.$$

Hence we obtain an implication

$$[X] \in \mathrm{Ker}[H^1(S,G) \to H^1(S,G_{B/A}) \Rightarrow [X] \text{ is trivial in } \mathrm{Pic}(S \times_A N_A).$$

References

[1] M. Demazure and P. Gabriel, *Groupes algébriques, Tome I.* Masson & Cie, Editeur, Paris; North-Holland Publishing, Amsterdam, 1970.

[2] A. Grothendieck, *Le groupe de Brauer.* Dix exposés sur la cohomologie des schémas, 46–188. North-Holland, 1968.

[3] B. Mazur, L. Roberts, *Local Euler Characteristics.* Invent. math. **9** (1970), 201–234.

[4] M. Saidi, *On the degeneration of étale $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z}$-torsors in equal characteristic $p > 0$.* Hiroshima. Math. J. **37** (2007), 315–341.

[5] T. Sekiguchi and N. Suwa, *Théorie de Kummer-Artin-Schreier et applications.* J. Théor. Nombres Bordeaux **7** (1995), 177–189.

[6] T. Sekiguchi, F. Oort and N. Suwa, *On the deformation of Artin-Schreier to Kummer.* Ann. Sci. École Norm. Sup. (4) **22** (1989), 345–375.

[7] J. P. Serre, *Groupes algébriques et corps de classes*. Hermann, Paris, 1959.

[8] R. P. Stanley, *Enumerative Combinatorics, vol. 1*. Cambridge Stud. Adv. Math. vol. **49**, Cambridge University Press, Cambridge, 1997.

[9] N. Suwa, *Twisted Kummer and Kummer-Artin-Schreier theories*. Tôhoku Math. J. **60** (2008), 183–218.

[10] N. Suwa, *Around Kummer theories*. RIMS Kôkyûroku Bessatsu **B12** (2009), 115–148.

[11] J. Tate and F. Oort, *Group scheme of prime order*. Ann. Sci. Éc. Norm. Sup. (4) **3** (1970), 1–21.

[12] W. C. Waterhouse, *Introduction to affine group schemes*. Springer, 1979.

[13] W. C. Waterhouse, *A unified Kummer-Artin-Schreier sequence*. Math. Ann. **277** (1987), 447–451.

[14] W. C. Waterhouse and B. Weisfeiler, *One-dimensional affine group schemes*. J. Algebra **66** (1980), 550–568.

Yuji Tsuno
Department of Mathematics
Chuo University
1-13-27 Kasuga
Bunkyo-ku, Tokyo 112-8551, JAPAN
E-mail: `s18001@@gug.math.chuo-u.ac.jp`