COMPOSITIO MATHEMATICA

TSUTOMU SEKIGUCHI
NORIYUKI SUWA

On the structure of the group scheme $\mathbb{Z}[\mathbb{Z}/p^n]^\times$

Compositio Mathematica, tome 97, nº 1-2 (1995), p. 253-271
<http://www.numdam.org/item?id=CM_1995__97_1-2_253_0>

Compositio Mathematica **97**: 253–271, 1995.

On the structure of the group scheme $\mathbb{Z}[\mathbb{Z}/p^n]^\times$

Dedicated to Frans Oort on the occasion of his 60th birthday

TSUTOMU SEKIGUCHI[1]* and NORIYUKI SUWA[2]**
[1]*Department of Mathematics, Faculty of Science and Engineering, Chuo University, Kasuga 1-13-27, Bunkyo-ku, Tokyo 112, Japan e-mail: sekigutimath.chuo-u.ac.jp*
[2]*Department of Mathematics, Tokyo Denki University, Kanda-Nishiki-cho 2-2, Chiyoda-ku, Tokyo 101, Japan e-mail: suwacck.dendai.ac.jp*

Received 6 February 1995; accepted in final form 28 March 1995

Introduction

Let A be a ring and G a finite group. It is an attractive problem to investigate the unit group of the group algebra $A[G]$. We find a lot of interesting results on this subject, for example in [3]. It seems, however, that an important remark given by Serre ([12], Ch. VI, 8–9) has not been paid regard to so much; he noticed that the unit group of $K[G]$ has a structure of algebraic group when K is a field. In this article, we study the structure of group scheme $U(G)$, which represents the unit group of $A[G]$, where G is a cyclic group of prime power order. It should be noted that a key of investigation is the group scheme $\mathcal{G}^{(\lambda)}$, which plays an important role in the theory unifying the Kummer and Artin–Schreier–Witt theories (cf. [11, 13, 7, 8, 9, 10]).

After a short review on Néron blow-ups of affine group schemes in Section 1, we establish some formalisms on $U(G)$ in Section 2. The structure of $U(\mathbb{Z}/p^n)$ is treated in Section 3. We conclude the article, by giving a relation with $U(\mathbb{Z}/p^n)$ and the Kummer–Artin–Schreier–Witt theories.

Our method can be applied without any difficulty to investigation of $U(G)$ for any finite commutative group G. We expect to describe detailed accounts in the sequel paper [11].

Notation

Throughout the article, p denotes a prime number.

$\mathbb{G}_{m,A}$ (resp. $\mathbb{G}_{a,A}$) denotes the multiplicative group (resp. additive group) over a ring A.

* Partially supported by Grant-in-Aid for Scientific Research #05640063.
** Partially supported by Grant-in-Aid for Scientific Research #01540077.

$\prod_{B/A} G$ denotes the Weil restriction of a B-scheme G to A when B is a ring, finite and locally free over A.

For a ring B (not necessarily commutative), $B^\times$ denotes the multiplicative group of invertible elements of B.

For an integer $\ell \geqslant 0$, we denote by $\binom{t}{\ell}$ the binomial polynomial

$$\frac{t(t-1)\cdots(t-\ell+1)}{\ell!}.$$

In particular $\binom{t}{0} = 1$.

By convention, $\sum_{i\in I} a_i = 0$ and $\prod_{i\in I} a_i = 1$ when $I = \emptyset$.

1. Preliminaries

We refer to [2], [4] or [15] on formalisms of affine group schemes.

1.1. Let A be a ring and $a \in A$. We define a group scheme $\mathcal{G}^{(a)}$ over A by $\mathcal{G}^{(a)} = \operatorname{Spec} A[X, 1/(aX+1)]$ with

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

Moreover, we define an A-homomorphism $\alpha^{(a)} \colon \mathcal{G}^{(a)} \to \mathbb{G}_{m,A}$ by

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

If a is invertible in A, $\alpha^{(a)}$ is an A-isomorphism. If $a = 0$, $\mathcal{G}^{(a)}$ is nothing but the additive group scheme $\mathbb{G}_{a,A}$.

1.2. Let A be a discrete valuation ring with maximal ideal $\mathfrak{m}$ and π a uniformizing parameter of A. Let K denote the field of fractions of A and $k = A/\mathfrak{m}$.

For a group scheme G over A, we denote by G_K (resp. G_k) the generic (resp. closed) fibre of G over A. Moreover, when G is affine, we denote by $A[G]$ (resp. $K[G]$) the coordinate rings of G (resp. G_K).

Now we recall the definition of Néron blow-ups. For details, see [1, 16].

Let G be a group scheme, flat and affine of finite type over A, and H a closed subgroup k-scheme of G_k. Let $J(H)$ be the inverse image in $A[G]$ of the defining ideal of H in $k[G]$. Then the structure of Hopf algebra on $K[G]$ induces a structure of Hopf A-algebra on the A-subalgebra $A[\pi^{-1}J(H)]$ of $K[G]$. Then $G^H = \operatorname{Spec} A[\pi^{-1}J(H)]$ is a group scheme, flat and affine of finite type over A. The injection $A[G] \subset A[G^H] = A[\pi^{-1}J(H)]$ induces an A-homomorphism $G^H \to G$. By the definition, the generic fibre $(G^H)_K \to G_K$ is an isomorphism.

We call the A-group G^H or the canonical A-homomorphism $G^H \to G$ the Néron blow-up of H in G.

PROPOSITION 1.3. *Let A be a discrete valuation ring and G, G' be commutative group schemes, flat and affine of finite type over A. Let $f\colon G' \to G$ be an A-homomorphism. Assume that the generic fibre $f_K : G'_K \to G_K$ is surjective. Then there exist a group scheme G'', flat and affine of finite type over A, an A-homomorphism $g\colon G'' \to G$ obtained by finite successive Néron blow-ups starting from G, and a surjective A-homomorphism $\tilde{f}\colon G' \to G''$ such that the diagram*

$$\begin{array}{ccc} G' & \xrightarrow{\tilde{f}} & G'' \\ & {}_f\searrow \quad \swarrow_g & \\ & G & \end{array}$$

is commutative.

Proof. Let $N = \mathrm{Ker}[f_K : G'_K \to G_K]$ and $\tilde{N}$ the flat closure of N in G'. Then by the uniqueness of the flat closure $\tilde{N}$ becomes a subgroup scheme of G'. We denote by $I_K(N) \subset K[G']$ (resp. $I(\tilde{N}) \subset A[G']$) the defining ideal of N (resp. $\tilde{N}$). Then we get $I(\tilde{N}) = I_K(N) \cap A[G']$. Note that

$$K[G'] \supset I_K(N) \quad \text{and} \quad A[G'] \supset I(\mathrm{Ker}\, f).$$

Therefore we obtain $I(\tilde{N}) \supset I(\mathrm{Ker}\, f)$ and $\tilde{N} \subset \mathrm{Ker}\, f$. Moreover, $G'/\tilde{N}$ is represented by a group A-scheme, flat over A (cf. [1], Th. 4.C). Hence we obtain a homomorphism $G'/\tilde{N} \to G$ so that the diagram

$$\begin{array}{ccc} G' & \longrightarrow & G/\tilde{N} \\ & {}_f\searrow \quad \swarrow & \\ & G & \end{array}$$

is commutative. Since $(G'/\tilde{N})_K \to G_K$ is an isomorphism, there exist a successive Néron blow-up $G'' \to G$ and an isomorphism $G/\tilde{N} \xrightarrow{\sim} G''$ so that

$$\begin{array}{ccc} G'/\tilde{N} & \xrightarrow{\sim} & G'' \\ & \searrow \quad \swarrow & \\ & G & \end{array}$$

is commutative [16]. Hence the result. □

1.4. Let $a \in A$. Let G' be a group scheme, affine flat of finite type over A and $f : G' \to \mathcal{G}^{(a)}$ an A-homomorphism with surjective generic fibre. Suppose that $a \neq 0$ and that G'_k is connected. If f is not flat, the closed fibre of f is not surjective, and we have $\mathrm{Im}\, f_k = 0 \subset \mathcal{G}_k^{(a)} = \mathbb{G}_{a,k}$. Therefore, f factors through the Néron blow-up $\mathcal{G}^{(\pi a)} \to \mathcal{G}^{(a)}$ of $\mathcal{G}^{(a)}$ at the origin $\{0\}$ of the closed fibre, that is to say, there exists an A-homomorphism $g\colon G' \to \mathcal{G}^{(\pi a)}$ so that the diagram

$$\begin{array}{ccc} G' & \xrightarrow{g} & \mathcal{G}^{(\pi a)} \\ & {\scriptstyle f}\searrow \quad \swarrow & \\ & \mathcal{G}^{(a)} & \end{array}$$

is commutative. More precisely, g is defined by

$$g(x) = \begin{cases} \dfrac{f(x)-1}{\pi} & \text{if } a \in A^{\times}, \\ \dfrac{f(x)}{\pi} & \text{if otherwise.} \end{cases}$$

for any local section x of G'.

2. Formalisms on $U(G)$

2.1. Let G be a finite group. We denote by G, for the abbreviation, the constant group scheme representing G. More precisely, $G = \operatorname{Spec} \mathbb{Z}^G$ with the law of multiplication: $\mu^*(e_g) = \sum_{g_1 g_2 = g} e_{g_1} \otimes e_{g_2}$. Here $(e_g)_{g \in G}$ is a basis of $\mathbb{Z}^G$ over $\mathbb{Z}$ defined by $e_g(g') = \delta_{g,g'}$ (the Kronecker symbol).

Now we define a ring scheme $A(G)$ by $A(G) = \operatorname{Spec} \mathbb{Z}[T_g\,;\, g \in G]$ with

1. the addition: $\alpha^*(T_g) = T_g \otimes 1 + 1 \otimes T_g$, and
2. the multiplication: $\mu^*(T_g) = \sum_{g_1 g_2 = g} T_{g_1} \otimes T_{g_2}$,

where T_g are indeterminates. Then $A(G)$ represents the group algebra of G.

2.2. Let $\det(T_{gh}) \in \mathbb{Z}[T_g\,;\, g \in G]$ denote the determinant of the matrix $(T_{gh})_{g,h \in G}$, and let $U(G) = \operatorname{Spec} \mathbb{Z}[T_g, 1/\det(T_{gh})]$. Then $U(G)$ is an open subcheme of $A(G)$ and represents the unit group of the group algebra of G. The canonical injection $G \to U(G)$ is represented by the homomorphism $\mathbb{Z}[T_g, 1/\det(T_{gh})] \to \mathbb{Z}^G$ defined by $T_g \mapsto e_g$. The left multiplication by an element g of G on $A(G)$ or $U(G)$ is represented by the automorphism g^* of $\mathbb{Z}[T_g\,;\, g \in G]$ or $\mathbb{Z}[T_g, 1/\det(T_{gh})]$ defined by $T_h \mapsto T_{g^{-1}h}$.

If $G = \{1\}$, $U(G)$ is nothing but the multiplicative group $\mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[U, 1/U]$.

PROPOSITION 2.3 (cf. [13], Ch. VI, Prop. 5). *Let B be a local ring and C a local ring, étale and finite over B. Suppose that C/B is a Galois extension and $G = \operatorname{Gal}(C/B)$. Then there exists a cartesian diagram of B-schemes:*

$$\begin{array}{ccc} \operatorname{Spec} C & \longrightarrow & U(G)_B \\ \downarrow & & \downarrow \\ \operatorname{Spec} B & \longrightarrow & (U(G)/G)_B\,. \end{array} \qquad (1)$$

Proof. Let k (resp. ℓ) denote the residue field of B (resp. C). Then ℓ/k is a Galois extension of group G. By the normal basis theorem there exists $a \in \ell$ such that the $g(a)$ ($g \in G$) form a basis of ℓ over k. Let $\tilde{a} \in C$ such that $\tilde{a}$ maps on $a \in C \otimes_B k = \ell$. By Nakayama's lemma the $g(\tilde{a})$ form a basis of C over B. Define a homomorphism of B-algebras $\gamma : B[T_g, 1/\det T_{gh})] \to C$ by $\gamma(T_g) = g(\tilde{a})$. Then γ is G-equivariant and we have gotten a cocartesian diagram:

$$\begin{array}{ccc} C & \xleftarrow{\gamma} & B[T_g, 1/\det(T_{gh})] \\ \uparrow & & \uparrow \\ B & \longleftarrow & B[T_g, 1/\det(T_{gh})]^G, \end{array}$$

which defines the cartesian diagram (1). □

2.4. Let $\varphi: G \to H$ be a homomorphism of finite groups. We denote by $A(\varphi): A(G) \to A(H)$ and $U(\varphi): U(G) \to U(H)$ the homomorphism of ring schemes or the homomorphism of group schemes, respectively, induced by φ. We denote often $A(\varphi)$ and $U(\varphi)$ by $\tilde{\varphi}$ for simplicity. $\tilde{\varphi}$ is represented by the homomorphism of rings defined by

$$T_h \mapsto \sum_{\varphi(g)=h} T_g.$$

The canonical immersion $U(G) \to A(G)$ is factorized through $U(G) \to A(G) \times_{A(H)} U(H)$, which is also an open immersion. If φ is injective, $U(G) \to A(G) \times_{A(H)} U(H)$ is an isomorphism.

Moreover, we have a commutative diagram of group schemes with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & \operatorname{Ker}\varphi & \longrightarrow & G & \xrightarrow{\varphi} & H \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \operatorname{Ker}\tilde{\varphi} & \longrightarrow & U(G) & \xrightarrow{\tilde{\varphi}} & U(H). \end{array}$$

PROPOSITION 2.5. *Let $\varphi: G \to H$ be a homomorphism of finite groups. Then:*

(1) $\operatorname{Ker}[\tilde{\varphi}: A(G) \to A(H)]$ *and* $\operatorname{Ker}[\tilde{\varphi}: U(G) \to U(H)]$ *are smooth over* $\mathbb{Z}$.
(2) *If $\varphi: G \to H$ is injective, $\tilde{\varphi}: A(G) \to A(H)$ and $\tilde{\varphi}: U(G) \to U(H)$ are closed immersions.*
(3) *If $\varphi: G \to H$ is surjective, $\tilde{\varphi}: A(G) \to A(H)$ and $\tilde{\varphi}: U(G) \to U(H)$ are smooth and surjective.*
(4) $\operatorname{Im}[\tilde{\varphi}: A(G) \to A(H)] = A(\operatorname{Im}\varphi)$ *and* $\operatorname{Im}[\tilde{\varphi}: U(G) \to U(H)] = U(\operatorname{Im}\varphi)$.

Proof. We verify the assertions on $\tilde{\varphi}: A(G) \to A(H)$. It is easy to apply the argument for $\tilde{\varphi}: U(G) \to U(H)$.

(1) Ker[$\tilde{\varphi}$: $A(G) \to A(H)$] is defined by the ideal generated by $\sum_{\varphi(g)=h} T_g$ ($h \in H$), that is, Ker[$\tilde{\varphi}$: $A(G) \to A(H)$] is a linear subspace. It follows that Ker[$\tilde{\varphi}$: $A(G) \to A(H)$] is smooth over $\mathbb{Z}$.
(2) $A(G)$ is isomorphic to the closed subscheme of $A(H)$ defined by the ideal generated by T_h, $h \in H - \varphi(G)$.
(3) Let $\pi : A(G) \to \operatorname{Ker}\tilde{\varphi}$ be a linear projection. Then $(\tilde{\varphi}, \pi) : A(G) \to A(H) \times \operatorname{Ker}\tilde{\varphi}$ is an isomorphism. It follows that $\tilde{\varphi} : A(G) \to A(H)$ is smooth and surjective.
(4) follows from (2) and (3). □

EXAMPLE 2.6. The canonical injection $\{1\} \to G$ induces an injective homomorphism $\mathbb{G}_{m,\mathbb{Z}} \to U(G)$, represented by

$$\mathbb{Z}[T_g, 1/\det(T_{gh})] \to \mathbb{Z}\left[U, \frac{1}{U}\right] : \; T_g \mapsto \begin{cases} U & \text{if } g = 1 \\ 0 & \text{if } g \neq 1. \end{cases}$$

EXAMPLE 2.7. The canonical surjection $G \to \{1\}$ induces a surjective homomorphism $\varepsilon : U(G) \to \mathbb{G}_{m,\mathbb{Z}}$, called the augmentation homomorphism and represented by

$$\mathbb{Z}\left[U, \frac{1}{U}\right] \to \mathbb{Z}[T_g, 1/\det(T_{gh})] : \; U \mapsto \sum_{g \in G} T_g.$$

2.8. We denote by $V(G)$ the kernel of the augmentation homomorphism $\varepsilon : U(G) \to \mathbb{G}_{m,\mathbb{Z}}$. The exact sequence of group schemes

$$1 \to V(G) \to U(G) \xrightarrow{\varepsilon} \mathbb{G}_{m,\mathbb{Z}} \to 1$$

splits. $V(G)$ is represented by the Hopf subalgebra $\mathbb{Z}[T_g/\sum_{g\in G} T_g]$ of $\mathbb{Z}[T_g, 1/\det(T_{gh})]$, and a splitting map of $V(G) \to U(G)$ is given by $T_g \mapsto T_g/\sum_{g\in G} T_g$. Moreover, the canonical injection $G \to U(G)$ is factorized through the canonical injection $V(G) \to U(G)$.

If $\varphi : G \to H$ is a homomorphism of finite groups, we have a commutative diagram of group schemes with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V(G) & \longrightarrow & U(G) & \xrightarrow{\varepsilon} & \mathbb{G}_{m,\mathbb{Z}} & \longrightarrow & 1 \\ & & \downarrow \tilde{\varphi} & & \downarrow \tilde{\varphi} & & \downarrow \mathrm{id} & & \\ 1 & \longrightarrow & V(H) & \longrightarrow & U(H) & \xrightarrow{\varepsilon} & \mathbb{G}_{m,\mathbb{Z}} & \longrightarrow & 1. \end{array}$$

Hence we obtain Ker[$\tilde{\varphi}$: $V(G) \to V(H)$] = Ker[$\tilde{\varphi}$: $U(G) \to U(H)$]. Moreover, we have a commutative diagram of group schemes with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \operatorname{Ker}\varphi & \longrightarrow & G & \xrightarrow{\varphi} & H \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \operatorname{Ker}\tilde{\varphi} & \longrightarrow & V(G) & \xrightarrow{\tilde{\varphi}} & V(H). \end{array}$$

REMARK 2.9. It is easily seen that, under the hypothesis of 2.3, there exists a cartesian diagram of B-schemes

$$\begin{array}{ccc} \operatorname{Spec} C & \longrightarrow & V(G)_B \\ \downarrow & & \downarrow \\ \operatorname{Spec} B & \longrightarrow & (V(G)/G)_B . \end{array} \tag{2}$$

3. Structure of $U(\mathbb{Z}/p^n)$

Let p be a prime number, and let ζ_k be a primitive p^kth root of unity, chosen so that $\zeta_{k+1}^p = \zeta_k$ for each $k \geqslant 1$. Put $\zeta = \zeta_1$ and $\lambda = \zeta - 1$. Then (λ) is a prime ideal of $\mathbb{Z}[\zeta]$ and $(\lambda)^{p-1} = (p)$.

3.1. Let $G = \mathbb{Z}/p^n$. Then $\mathbb{Z}[G]$ is isomorphic to $\mathbb{Z}[T]/(T^{p^n} - 1)$. Hereafter we identify $A(G)$ and $U(G)$ with the functor $A \mapsto A[T]/(T^{p^n} - 1)$ or $A \mapsto (A[T]/(T^{p^n} - 1))^\times$, respectively. The homomorphisms $\tilde{p}^r : A(G) \to A(G)$ and $\tilde{p}^r : U(G) \to U(G)$ are given by $T \mapsto T^{p^r}$.

Now put

$$V_k(G) = \operatorname{Ker}[\tilde{p}^{n-k+1} : U(G) \to U(G)] = \operatorname{Ker}[\tilde{p}^{n-k+1} : V(G) \to V(G)],$$

for $k = 0, 1, \ldots, n$. Then we have gotten a filtration of $U(G)$ of closed subgroups:

$$V_{n+1}(G) = 0 \subset V_n(G) \subset \cdots \subset V_1(G) = V(G) \subset U(G).$$

LEMMA 3.2. *Let n, m, ℓ be integers with $0 \leqslant \ell < m < n$. Then:*

(1) $V_{m+1}(\mathbb{Z}/p^n) = \operatorname{Ker}[\tilde{p}^{n-m} : U(\mathbb{Z}/p^n) \to U(\mathbb{Z}/p^m)]$;
(2) $V_{\ell+1}(\mathbb{Z}/p^n)/V_{m+1}(\mathbb{Z}/p^n)$ *is isomorphic to* $V_{\ell+1}(\mathbb{Z}/p^m)$.

Proof. (1) The assertion follows from 2.5. (4), since $\operatorname{Im}(p^{n-m} : \mathbb{Z}/p^n \to \mathbb{Z}/p^n) = \mathbb{Z}/p^m$.

(2) We obtain an isomorphism $V_{\ell+1}(\mathbb{Z}/p^n)/V_{m+1}(\mathbb{Z}/p^n) \xrightarrow{\sim} V_{\ell+1}(\mathbb{Z}/p^m)$, applying the snake lemma to the commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V_{m+1}(\mathbb{Z}/p^n) & \longrightarrow & V(\mathbb{Z}/p^n) & \longrightarrow & V(\mathbb{Z}/p^m) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow \mathrm{id} & & \downarrow & & \\ 1 & \longrightarrow & V_{\ell+1}(\mathbb{Z}/p^n) & \longrightarrow & V(\mathbb{Z}/p^n) & \longrightarrow & V(\mathbb{Z}/p^l) & \longrightarrow & 1. \end{array}$$

3.3. We have a commutative diagram of group schemes with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/p^{n-m} & \longrightarrow & \mathbb{Z}/p^n & \longrightarrow & \mathbb{Z}/p^m & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & V_{m+1}(\mathbb{Z}/p^n) & \longrightarrow & V(\mathbb{Z}/p^n) & \longrightarrow & V(\mathbb{Z}/p^m) & \longrightarrow & 0. \end{array}$$

THEOREM 3.4. *Let* $0 < k \leqslant n$. *Then* $V_k(\mathbb{Z}/p^n)/V_{k+1}(\mathbb{Z}/p^n)$ *is isomorphic to*

$$\prod_{\mathbb{Z}[\zeta_k]/\mathbb{Z}} \mathcal{G}^{(\lambda)}.$$

Proof. By 3.2. (2), $V_k(\mathbb{Z}/p^n)/V_{k+1}(\mathbb{Z}/p^n)$ is isomorphic to $V_k(\mathbb{Z}/p^k)$. Hence it is sufficient to verify that $V_n(\mathbb{Z}/p^n)$ is isomorphic to

$$\prod_{\mathbb{Z}[\zeta_n]/\mathbb{Z}} \mathcal{G}^{(\lambda)}.$$

Let A be a ring and $f(T) = \sum_{k=0}^{p^n-1} a_k T^k \in A[T]/(T^{p^n} - 1)$. Then we can verify without difficulty that:

$$\tilde{p}(f) = 1 \iff \sum_{i=0}^{p-1} a_{ip^{n-1}+j} = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{if } 0 < j < p^{n-1} \end{cases}$$

$$\iff f(T) \text{ is written in the form}$$

$$1 + \sum_{i=1}^{p-1} \sum_{j=0}^{p^{n-1}-1} a_{ip^{n-1}+j} T^j (T^{ip^{n-1}} - 1).$$

Now assume that $f(T) = \sum_{k=0}^{p^n-1} a_k T^k \in V_n(G)(A) \subset \left(A[T]/(T^{p^n} - 1)\right)^\times$. Then

$$f(1 \otimes \zeta_n) = \sum_{k=0}^{p^n-1} a_k \otimes \zeta_n^k \in (A \otimes \mathbb{Z}[\zeta_n])^\times,$$

and therefore,

$$\sum_{i=1}^{p-1} \sum_{j=0}^{p^{n-1}-1} a_{ip^{n-1}+j} \otimes \zeta_n^j \frac{\zeta^i - 1}{\zeta - 1} \in \mathcal{G}^{(\lambda)}(A \otimes \mathbb{Z}[\zeta_n]).$$

We define a homomorphism $\eta_A : V_n(G)(A) \to \mathcal{G}^{(\lambda)}(A \otimes \mathbb{Z}[\zeta_n]) = \left(\prod_{\mathbb{Z}[\zeta_n]/\mathbb{Z}} \mathcal{G}^{(\lambda)}\right)(A)$ by

$$\eta_A \left(1 + \sum_{k=1}^{p^n-1} a_k T^k\right) = \sum_{i=1}^{p-1} \sum_{j=0}^{p^{n-1}-1} a_{ip^{n-1}+j} \otimes \zeta_n^j \frac{\zeta^i - 1}{\zeta - 1}.$$

It is clear that η_A is functorial. Since $\zeta_n^j \frac{\zeta^i-1}{\zeta-1}$ $(0 \leqslant i \leqslant p^{n-1} - 1,\ 1 \leqslant i \leqslant p - 1)$ form a basis of $\mathbb{Z}[\zeta_n]$ over $\mathbb{Z}$, η_A is injective.

Now let

$$\sum_{i=1}^{p-1}\sum_{j=0}^{p^{n-1}-1} a_{ip^{n-1}+j}\otimes \zeta_n^j\frac{\zeta^i-1}{\zeta-1}\in \mathcal{G}^{(\lambda)}(A\otimes\mathbb{Z}[\zeta_n]).$$

We define a_j for $0\leqslant j<p^{n-1}$ by

$$a_j=\begin{cases} 1-\sum_{i=1}^{p-1}a_{ip^{n-1}+j} & \text{if } j=0\\ -\sum_{i=1}^{p-1}a_{ip^{n-1}+j} & \text{if } 0<j<p^{n-1}.\end{cases}$$

By the definition,

$$\sum_{k=0}^{p^n-1}a_k\otimes\zeta_n^k=1+\sum_{i=1}^{p-1}\sum_{j=0}^{p^{n-1}-1}a_{ip^{n-1}+j}\otimes\zeta_n^j(\zeta^i-1)\in(A\otimes\mathbb{Z}[\zeta_n])^\times,$$

and therefore, if j is prime to p,

$$\sum_{k=0}^{p^n-1}a_k\otimes\zeta_n^{jk}\in(A\otimes\mathbb{Z}[\zeta_n])^\times.$$

On the other hand, if j is divisible by p, we have

$$\sum_{k=0}^{p^n-1}a_k\otimes\zeta_n^{jk}=1.$$

It follows that

$$\begin{vmatrix} a_0 & a_1 & \cdots & a_{p^n-1}\\ a_1 & a_2 & \cdots & a_0\\ \vdots & \vdots & \ddots & \vdots\\ a_{p^n-1} & a_0 & & a_{p^n-2}\end{vmatrix}\otimes 1 = (-1)^{(p^n-1)(p^n-2)/2}\prod_{j=0}^{p^n-1}\left(\sum_{k=0}^{p^n-1}a_k\otimes\zeta_n^{jk}\right)$$
$$\in(A\otimes\mathbb{Z}[\zeta_n])^\times,$$

and therefore,

$$\begin{vmatrix} a_0 & a_1 & \cdots & a_{p^n-1}\\ a_1 & a_2 & \cdots & a_0\\ \vdots & \vdots & \ddots & \vdots\\ a_{p^n-1} & a_0 & & a_{p^n-2}\end{vmatrix}\in A^\times.$$

Hence $f(T)=\sum_{k=0}^{p^n-1}a_kT^k$ is invertible in $A[T]/(T^{p^n}-1)$. It is easy to see that $\eta_A(f)=\sum_{i=1}^{p-1}\sum_{j=0}^{p^{n-1}-1}a_{ip^{n-1}+j}\otimes\zeta_n^j\frac{\zeta^i-1}{\zeta-1}$. Therefore η_A is surjective. Thus we have gotten the assertion. □

REMARK 3.5. $\left(\prod_{\mathbb{Z}[\zeta_k]/\mathbb{Z}} \mathcal{G}^{(\lambda)}\right) \otimes \mathbb{Z}[\frac{1}{p}]$ is isomorphic to the algebraic torus

$$\prod_{\mathbb{Z}[1/p,\zeta_k]/\mathbb{Z}[1/p]} \mathbb{G}_{m,\mathbb{Z}[1/p,\zeta_k]}.$$

Moreover, the sequence of group schemes

$$0 \to V_{m+1}(\mathbb{Z}/p^n) \to V(\mathbb{Z}/p^n) \to V(\mathbb{Z}/p^m) \to 0$$

splits over $\mathbb{Z}[1/p]$. It follows that $U(\mathbb{Z}/p^n) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ is isomorphic to

$$\prod_{0\leqslant k\leqslant p} \left(\prod_{\mathbb{Z}[1/p,\zeta_k]/\mathbb{Z}[1/p]} \mathbb{G}_{m,\mathbb{Z}[1/p,\zeta_k]} \right),$$

as is well known.

REMARK 3.6. Let A be a ring of characteristic p. Then $A[T]/(T^{p^n} - 1) = A[T]/(T-1)^{p^n}$. Put $U = T - 1$. We can consider the additive group $W_n(A)$ of Witt vectors of length n as a subgroup of $V(\mathbb{Z}/p^n)$ by the identification

$$\begin{aligned} W_n(A) &= \left\{ \prod_{j=0}^{n-1} E_p(a_j U^{p^j}) \bmod U^{p^n};\ a_j \in A \right\} \\ &\subset \left(A[T]/(T^{p^n} - 1)\right)^{\times}, \end{aligned}$$

where $E_p(X)$ denotes the Artin–Hasse exponential (cf. [13], Ch. V, no. 16).

Hence we obtain an injective homomorphism $W_{n,\mathbb{F}_p} \to V(\mathbb{Z}/p^n)\otimes_{\mathbb{Z}}\mathbb{F}_p$ of group schemes over $\mathbb{F}_p$. Moreover, we have a commutative diagram of group schemes with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/p^{n-m} & \longrightarrow & \mathbb{Z}/p^n & \longrightarrow & \mathbb{Z}/p^m & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & W_{n-m,\mathbb{F}_p} & \longrightarrow & W_{n,\mathbb{F}_p} & \longrightarrow & W_{m,\mathbb{F}_p} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & V_{m+1}(\mathbb{Z}/p^n)\otimes_{\mathbb{Z}}\mathbb{F}_p & \longrightarrow & V(\mathbb{Z}/p^n)\otimes_{\mathbb{Z}}\mathbb{F}_p & \longrightarrow & V(\mathbb{Z}/p^m)\otimes_{\mathbb{Z}}\mathbb{F}_p & \longrightarrow & 0. \end{array}$$

REMARK 3.7. Let A be a local ring. Then

$$\mathrm{H}^1_{\mathrm{et}}\left(A, \prod_{\mathbb{Z}[\zeta_k]/\mathbb{Z}} \mathcal{G}^{(\lambda)}\right) = \mathrm{H}^1_{\mathrm{et}}(A \otimes \mathbb{Z}[\zeta_k], \mathcal{G}^{(\lambda)}) = 0$$

(cf. [9]). Hence we have a filtration of $U(G)(A) = A[\mathbb{Z}/p^n]^{\times}$ of subgroups:

$$V_{n+1}(G)(A) = 0 \subset V_n(G)(A) \subset \cdots \subset V_1(G)(A) = V(G) \subset U(G)$$

with $V_k(G)(A)/V_{k+1}(G)(A)$ isomorphic to $\mathcal{G}^{(\lambda)}(A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_k])$.

REMARK 3.8. Let A be a ring. When p is not invertible in A and $\mathrm{H}^1_{\mathrm{et}}(A \otimes \mathbb{Z}[\zeta_k], \mathcal{G}^{(\lambda)}) \neq 0$, it is a subtle problem to determine the image of $V_k(G)(A)/V_{k+1}(G)(A) \to \mathcal{G}^{(\lambda)}(A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_k])$. For example, when $A = \mathbb{Z}$, the obstruction for surjectivity of $V_k(G)(\mathbb{Z})/V_{k+1}(G)(\mathbb{Z}) \to \mathcal{G}^{(\lambda)}(\mathbb{Z}[\zeta_k])$ is given by elements of $\mathrm{H}^1_{\mathrm{et}}(\mathbb{Z}[\zeta_k], \mathcal{G}^{(\lambda)})$, which is isomorphic to the ray class group of $\mathbb{Q}(\zeta_k)$ modulo λ. We refer to [3], Ch. IV, 15 for related topics.

Hereafter we investigate the structure of

$$V_n(\mathbb{Z}/p^n) \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_n] \simeq \left(\prod_{\mathbb{Z}[\zeta_n]/\mathbb{Z}} \mathcal{G}^{(\lambda)}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_n].$$

3.9. Let $I = \{0, 1, \ldots, p-1\}$ and $D = I^{(\mathbb{N})}$. For $\boldsymbol{i} = (i_0, i_1, \ldots,) \in D$, we put

$$S(\boldsymbol{i}) = \sum_{k \geqslant 0} i_k p^k$$

and

$$\zeta(\boldsymbol{i}) = \prod_{k \geqslant 0} \zeta_{k+1}^{i_k}.$$

Define polynomials $s_k(T)$ by

$$s_k(T) = \prod_{\substack{\boldsymbol{i} \in D \\ S(\boldsymbol{i}) < k}} (T - \zeta(\boldsymbol{i})).$$

If $k \leqslant p^n$, $s_k(T) \in \mathbb{Z}[\zeta_n][T]$. It is clear that $s_0(T) = 1$ and $s_{p^r}(T) = T^{p^r} - 1$ for $r \geqslant 0$. Put $\tilde{\lambda}_k = s_k(\zeta(\boldsymbol{i}))$, where $k = S(\boldsymbol{i})$. It is clear that $\tilde{\lambda}_{p^r} = \lambda$ for $r \geqslant 0$.

LEMMA 3.10. $s_k(T)$ $(0 \leqslant k \leqslant p^n - 1)$ *form a basis of* $\mathbb{Z}[\zeta_n][T]/(T^{p^n} - 1)$ *over* $\mathbb{Z}[\zeta_n]$.

Proof. Note that

$$\begin{pmatrix} s_0(T) \\ s_1(T) \\ \vdots \\ s_{p^n-1}(T) \end{pmatrix} = Q \begin{pmatrix} 1 \\ T \\ \vdots \\ T^{p^n-1} \end{pmatrix},$$

where Q is a lower triangular matrix with the diagonal entries 1. □

3.11. Let A be a $\mathbb{Z}[\zeta_n]$-algebra. For $\ell = 1, 2, \dots, p^n - 1$, we define a subfunctor $\tilde{V}_\ell$ of $U(\mathbb{Z}/p^n)$ by

$$\tilde{V}_\ell(A) = \left\{ f(T) = 1 + \sum_{k=\ell}^{p^n-1} a_k s_k(T)\,;\ f(T) \text{ is invertible} \right\}.$$

LEMMA 3.12. *$\tilde{V}_{p^r} = V_{r+1}$ for $r \geqslant 0$.*

Proof. Let A be a ring and $f(T) \in (A[T]/(T^{p^n} - 1))^\times$. Assume that $f(T) \in \tilde{V}_{p^r}(A)$. Since $s_k(T) \equiv 0 \bmod T^{p^r} - 1$ for $k \geqslant p^r$, $f(T) \equiv 1 \bmod T^{p^r} - 1$, that is to say, $f(T) \in V_{r+1}(A)$.

Conversely, assume that $f(T) \in V_{r+1}(A)$. Let $f(T) = 1 + \sum_{k=1}^{p^n-1} a_k s_k(T)$. Then $\sum_{k=1}^{p^r-1} a_k s_k(T) \equiv 0 \bmod T^{p^r} - 1$. Since $s_k(T)$ $(1 \leqslant k \leqslant p^r - 1)$ are free over A, then $a_k = 0$ for $1 \leqslant k \leqslant p^r - 1$, that is to say, $f(T) \in \tilde{V}_{p^r}(A)$. □

LEMMA 3.13. *$s_\ell(T)^2 \equiv \tilde{\lambda}_\ell s_\ell(T) \bmod s_{\ell+1}(T)$.*

Proof. Let $\boldsymbol{i} \in D$ with $S(\boldsymbol{i}) = \ell$. Then

$$\begin{aligned} s_\ell(T)^2 &= s_\ell(T) \prod_{\substack{\boldsymbol{j} \in D \\ S(\boldsymbol{j}) < \ell}} (T - \zeta(\boldsymbol{i}) + \zeta(\boldsymbol{i}) - \zeta(\boldsymbol{j})) \\ &\equiv s_\ell(T) \prod_{\substack{\boldsymbol{j} \in D \\ S(\boldsymbol{j}) < \ell}} (\zeta(\boldsymbol{i}) - \zeta(\boldsymbol{j})) \bmod s_{\ell+1}(T). \end{aligned}$$

Note that

$$\prod_{\substack{\boldsymbol{j} \in D \\ S(\boldsymbol{j}) < \ell}} (\zeta(\boldsymbol{i}) - \zeta(\boldsymbol{j})) = s_\ell(\zeta(\boldsymbol{i})) = \tilde{\lambda}_k.$$

□

THEOREM 3.14. *$\tilde{V}_l/\tilde{V}_{l+1}$ is isomorphic to $\mathcal{G}^{(\tilde{\lambda}_l)}$.*

Proof. Let $\boldsymbol{i} \in D$ with $S(\boldsymbol{i}) = \ell$. Let A be a ring and

$$f(T) = 1 + \sum_{k=\ell}^{p^n-1} a_k s_k(T) \in \tilde{V}_\ell(A) \subset \left(A[T]/(T^{p^n} - 1)\right)^\times.$$

Then $f(\zeta(\boldsymbol{i})) = 1 + \tilde{\lambda}_\ell a_\ell \in A^\times$, and therefore $a_\ell \in \mathcal{G}^{(\tilde{\lambda}_\ell)}(A)$. Now define a homomorphism $\xi_A : \tilde{V}_\ell(A) \to \mathcal{G}^{(\tilde{\lambda}_\ell)}(A)$ by $\xi_A(f) = a_\ell$. It is clear that ξ_A is functorial and $\operatorname{Ker} \xi_A = \tilde{V}_{\ell+1}(A)$. □

4. Relations with Kummer–Artin–Schreier–Witt theories

We keep the notations used in the previous sections.

4.1. Let $A = \mathbb{Z}_{(p)}[\zeta_n]$. Then there exists an exact sequence of affine group A-schemes which unifies the Kummer and Artin–Schreier–Witt theories. More precisely, there exists an exact sequence of group A-schemes

$$0 \to \mathbb{Z}/p^n \longrightarrow \mathcal{W}_n \xrightarrow{\Psi} \mathcal{V}_n \to 0 \tag{\#}$$

such that

(1) the generic fibre of (#) is isomorphic to the sequence

$$0 \to \boldsymbol{\mu}_{p^n,K} \to (\mathbb{G}_{m,K})^n \xrightarrow{\Theta} (\mathbb{G}_{m,K})^n \to 0,$$

where

$$\begin{aligned}\Theta : (\mathbb{G}_{m,\mathbb{Z}})^n &= \operatorname{Spec} \mathbb{Z}[U_0, \dots, U_{n-1}, U_0^{-1}, \dots, U_{n-1}^{-1}] \\ &\to (\mathbb{G}_{m,\mathbb{Z}})^n = \operatorname{Spec} \mathbb{Z}[U_0, \dots, U_{n-1}, U_0^{-1}, \dots, U_{n-1}^{-1}]\end{aligned}$$

is defined by

$$(U_0, U_1, \dots, U_{n-1}) \mapsto (U_0^p, U_0^{-1}U_1^p, \dots, U_{n-2}^{-1}U_{n-1}^p);$$

(2) the closed fibre of (#) is isomorphic to the Artin–Schreier–Witt sequence

$$0 \to \mathbb{Z}/p^n \longrightarrow W_{n,\mathbb{F}_p} \xrightarrow{F-1} W_{n,\mathbb{F}_p} \to 0;$$

(3) (Hilbert 90) if B is a local A-algebra,

$$\mathrm{H}^1_{\mathrm{et}}(B, \mathcal{W}_{n,B}) = \mathrm{H}^1_{\mathrm{et}}(B, \mathcal{V}_{n,B}) = 0.$$

(cf. [8]. For details see [10]). As a corollary, we have the assertion analogous to Proposition 2.3: Let B a local A-algebra and C a local ring, étale and finite over B. Suppose that C/B is a cyclic extension of degree p^n. Then there exists a cartesian diagram of B-schemes:

$$\begin{array}{ccc} \operatorname{Spec} C & \longrightarrow & \mathcal{W}_{n,B} \\ \downarrow & & \downarrow \\ \operatorname{Spec} B & \longrightarrow & \mathcal{V}_{n,B}. \end{array}$$

This suggests that there should be some relations between $U(\mathbb{Z}/p^n)$ and $\mathcal{W}_n$. In fact, when $n = 1$, (#) is nothing but the Kummer–Artin–Schreier sequence

$$0 \to \mathbb{Z}/p \longrightarrow \mathcal{G}^{(\lambda)} \xrightarrow{\Psi} \mathcal{G}^{(\lambda^p)} \to 0, \tag{\#}$$

and the diagram of group schemes over $\mathbb{Z}[\zeta]$

$$\begin{array}{ccc} V(\mathbb{Z}/p) & \longrightarrow & \mathcal{G}^{(\lambda)} \\ \downarrow & & \downarrow \Psi \\ V(\mathbb{Z}/p)/(\mathbb{Z}/p) & \longrightarrow & \mathcal{G}^{(\lambda^p)} \end{array}$$

is cartesian. Here $V(\mathbb{Z}/p) \to \mathcal{G}^{(\lambda)}$ is the canonical surjection defined in 3.14 ([7]).

When $p = 2$ and $n = 2$, $V(\mathbb{Z}/4)/\tilde{V}_3(\mathbb{Z}/4)$ is isomorphic to $\mathcal{W}_2$ and the diagram

$$\begin{array}{ccc} V(\mathbb{Z}/4) & \longrightarrow & \mathcal{W}_2 \\ \downarrow & & \downarrow \Psi \\ V(\mathbb{Z}/4)/(\mathbb{Z}/4) & \rightarrow & \mathcal{V}_2 \end{array}$$

is cartesian.

When $p > 2$ or $n > 2$, it is hard to define a homomorphism of group schemes $V(\mathbb{Z}/p^n) \to \mathcal{W}_n$. In this section, we construct a homomorphism $V(\mathbb{Z}/p^2) \to \mathcal{W}_2$. For this we prepare several lemmas.

LEMMA 4.2. *Let k and a be integers with $k \geqslant 1$ and $1 \leqslant a \leqslant k$. Then we have the equalities:*

(1) $\sum_{\ell=1}^{k}(-1)^{k-\ell}\ell^a\binom{t+k-\ell-1}{k-\ell}\binom{t+k}{\ell} = (t+k)^a$;

(2) $\sum_{\ell=1}^{k}(-1)^{k-\ell}\binom{t+k-\ell-1}{k-\ell}\binom{t+k}{\ell} = 1 + (-1)^{k+1}\binom{t+k-1}{k}$.

Proof. Put

$$G(t) = \sum_{\ell=1}^{k}(-1)^{k-\ell}\ell^a\binom{t+k-\ell-1}{k-\ell}\binom{t+k}{\ell}.$$

Since $G(t)$ is of degree $\leqslant k$, it is sufficient to verify the equalities, substituting $t = 0, -1, \dots, -k$ to $G(t)$.

Let c be an integer $\leqslant 0$. Then

$$\binom{c+k-\ell-1}{k-\ell} = 0 \quad \text{if } \ell \leqslant c+k-1$$

and

$$\binom{c+k}{\ell} = 0 \quad \text{if } \ell \geqslant c+k+1.$$

Moreover,

$$\binom{c+k-\ell-1}{k-\ell}\binom{c+k}{\ell} = \binom{-1}{-c}\binom{c+k}{c+k} = (-1)^{-c} \quad \text{if } \ell = c+k.$$

It follows that

(1) $G(c) = (c+k)^a$ when $1 \leqslant a \leqslant k$;

(2) $G(c) = \begin{cases} 1 & \text{if } -k+1 \leqslant c \leqslant 0 \\ 0 & \text{if } c = -k, \end{cases}$

when $a = 0$. Hence the results. □

COROLLARY 4.3. *Let k and a be integers with $k \geqslant 0$ and $1 \leqslant a \leqslant k$. Then we have the equalities:*

(1) $\sum_{\ell=1}^{k}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}\ell^{a+1} = (k+1)^{a+1}$;

(2) $\sum_{\ell=1}^{k}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}\ell = \left\{1+(-1)^{k+1}\right\}(k+1)$.

Proof. We obtain the equalities, substituting $t = 1$ to

(1) $\sum_{\ell=1}^{k}(-1)^{k-\ell}\frac{t+k}{\ell}\binom{t+k-\ell-1}{k-\ell}\binom{t+k}{\ell}\ell^{a+1} = (t+k)^{a+1}$ when $1 \leqslant a \leqslant k$;

(2) $\sum_{\ell=1}^{k}(-1)^{k-\ell}\frac{t+k}{\ell}\binom{t+k-\ell-1}{k-\ell}\binom{t+k}{\ell}\ell = \left\{1+(-1)^{k+1}\binom{t+k-1}{k}\right\}(t+k)$. □

COROLLARY 4.4. *Let A be a $\mathbb{Q}$-algebra and $g(\ell) = \sum_{j=1}^{k+1} b_j\ell^j$ with $b_j \in A$. Then we have the equality:*

$$\sum_{\ell=1}^{k}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}g(\ell) = g(k+1) + (-1)^{k+1}(k+1)b_1.$$

In particular, if $b_1 = 0$,

$$\sum_{\ell=1}^{k}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}g(\ell) = g(k+1).$$

COROLLARY 4.5. *For an integer a with $1 \leqslant a \leqslant k+1$, we have*

$$\sum_{\ell=1}^{k+1}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}\binom{\ell}{a} = (-1)^{k+a}\frac{k+1}{a}.$$

Proof. Apply 4.4 to $g(\ell) = \binom{\ell}{a}$. □

Let K be a $\mathbb{Q}$-algebra and $f(T) \in K[[T]]$. When $f(0) = 0$, we define a formal power series $\log(1 + f(T)) \in K[[T]]$ by

$$\log(1+f(T)) = \sum_{k=1}^{\infty}\frac{(-1)^{k-1}}{k}f(T)^k.$$

LEMMA 4.6. *Let k be an integer $\geqslant 1$. Then we have*

$$\sum_{\ell=1}^{k+1}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}\left\{(1+T)^\ell - 1\right\}$$
$$\equiv (-1)^{k+1}(k+1)\log(1+T) \bmod \deg k+2.$$

Proof. Noting that

$$\frac{k+1}{\ell}\binom{k+1}{\ell}\left\{(1+T)^\ell - 1\right\} = \sum_{a=1}^{\ell} \frac{k+1}{\ell}\binom{k+1}{\ell}\binom{\ell}{a}T^a,$$

we obtain

$$\begin{aligned}
&\sum_{\ell=1}^{k+1}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}\left\{(1+T)^\ell - 1\right\} \\
&= \sum_{\ell=1}^{k+1}\sum_{a=1}^{\ell}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}\binom{\ell}{a}T^a \\
&= \sum_{a=1}^{k+1}\left\{\sum_{\ell=1}^{k+1}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}\binom{\ell}{a}\right\}T^a \\
&= \sum_{a=1}^{k+1}\left\{(-1)^{k+a}\frac{k+1}{a}\right\}T^a \\
&= (-1)^{k+1}(k+1)\sum_{a=1}^{k+1}\frac{(-1)^{a-1}}{a}T^a. \qquad \square
\end{aligned}$$

LEMMA 4.7. *Let K be a $\mathbb{Q}$-algebra and $g(T) = \Sigma_{j=2}^{\infty} a_j T^j$. For an integer $\ell \geqslant 1$, put $G_\ell(T) = \sum_{j=2}^{\infty} a_j \left\{(1+T)^\ell - 1\right\}^j$. Then we have a congruence*

$$G_{k+1}(T) \equiv \sum_{\ell=1}^{k+1}(-1)^{k-\ell}\frac{k+1}{\ell}\binom{k+1}{\ell}G_\ell(T) \bmod T^{k+2}.$$

Proof. Note first that

$$\begin{aligned}
G_\ell(T) &= \sum_{j=2}^{\infty} a_j \left\{\sum_{a=1}^{\ell}\binom{\ell}{a}T^a\right\}^j \\
&= \sum_{j=2}^{\infty} a_j \left\{\sum_{\substack{e_1a_1+e_2a_2+\cdots+e_\ell a_\ell = j \\ e_i \geqslant 0,\ a_i \geqslant 1,\ \sum e_i \geqslant 2}} \frac{(\sum e_i)!}{e_1!\cdots e_\ell!}\binom{\ell}{a_1}^{e_1}\binom{\ell}{a_2}^{e_2}\cdots\binom{\ell}{a_\ell}^{e_\ell}\right\}T^j
\end{aligned}$$

Put

$$g_j(\ell) = \sum_{\substack{e_1a_1+e_2a_2+\cdots+e_\ell a_\ell = j \\ e_i \geqslant 0,\ a_i \geqslant 1,\ \sum e_i \geqslant 2}} \frac{(\sum e_i)!}{e_1!\cdots e_\ell!}\binom{\ell}{a_1}^{e_1}\binom{\ell}{a_2}^{e_2}\cdots\binom{\ell}{a_\ell}^{e_\ell}.$$

Applying 4.4 to $g_j(\ell)$ for $2 \leqslant j \leqslant k$, we obtain the assertion. □

4.8. Let $V = V(\mathbb{Z}/p^2)$ and $\mathcal{K} = \tilde{V}_2(\mathbb{Z}/p^2)$. We define $\xi \colon V \to \mathbb{G}_{m,A}$ by

$$\xi(f(T)) = \prod_{\ell=1}^{p-1} f(\zeta_2^\ell)^{(-1)^{p-\ell}(p-1)!\frac{p-1}{\ell}\binom{p-1}{\ell}}.$$

Then we have

$$\xi(T^p) = \zeta.$$

Next we will show that $\xi \colon \mathcal{K} \to \mathbb{G}_{m,A}$ is factorized by the Néron blow-up $\mathcal{G}^{(\lambda)} \to \mathbb{G}_{m,A}$, that is to say, there exists a faithfully flat homomorphism $\tilde{\xi} \colon \mathcal{K} \to \mathcal{G}^{(\lambda)}$ so that the diagram

$$\begin{array}{ccc} \mathcal{K} & \xrightarrow{\tilde{\xi}} & \mathcal{G}^{(\lambda)} \\ & \searrow \quad \swarrow & \\ & \mathbb{G}_{m,A} & \end{array}$$

is commutative. More precisely, we check that the map $\xi \colon \mathcal{K} \to \mathcal{G}^{(\lambda)}$ given by $\tilde{\xi}(f) = \{\xi(f) - 1\}/\lambda$ is well defined and flat.

Let

$$f(T) = 1 + \sum_{k=2}^{p^2-1} a_k s_k(T) \in V(\mathbb{Z}/p^2)(A) \subset \left(A[T]/(T^{p^2} - 1)\right)^\times.$$

Put

$$F_\ell(T) = 1 + \sum_{k=2}^{p^2-1} a_k \{(T+1)^\ell - 1\}^k$$

for $\ell \geqslant 1$ and

$$F(T) = \prod_{\ell=1}^{p-1} F_\ell(T)^{(-1)^{p-\ell}(p-1)!\frac{p-1}{\ell}\binom{p-1}{\ell}}.$$

Then we have

$$f(\zeta_2^\ell) \equiv F_\ell(\lambda_2) \bmod \lambda.$$

for each $\ell \geqslant 1$.

In fact, if $k \geqslant p$, $s_k(\zeta_2^\ell) = 0$. On the other hand, if $1 < k < p$, $s_k(T) \equiv (T-1)^k \bmod \lambda$, and therefore $s_k(\zeta_2^\ell) \equiv ((\lambda_2 + 1)^\ell - 1)^k$. It follows that

$$\xi(f(T)) \equiv F(\lambda_2) \bmod \lambda.$$

Furthermore, we can verify by 4.7 that

$$\log F_{p-1}(T) \equiv \sum_{\ell=1}^{p-1}(-1)^{p-\ell}\frac{p-1}{\ell}\binom{p-1}{\ell}\log F_\ell(T) \bmod T^p.$$

Hence $\mathrm{ord}_T \log F(T) \geqslant p$, and therefore, $F(T) \equiv 1 \bmod T^p$. This implies that

$$F(\lambda_2) \equiv 1 \bmod \lambda.$$

Thus we have got

$$\xi(f(T)) \equiv 1 \bmod \lambda.$$

That is to say, $\tilde{\xi}(f) = \{\xi(f) - 1\}/\lambda$ is defined over A.

Furthermore, $\tilde{\xi}(T^p) = 1$ and $\tilde{\xi}_{\mathbb{F}_p}\colon \mathcal{K} \otimes_A \mathbb{F}_p \to \mathcal{G}^{(\lambda)} \otimes_A \mathbb{F}_p = \mathbb{G}_{a,\mathbb{F}_p}$ is not trivial. Since $\mathcal{K} \otimes_A \mathbb{F}_p$ is connected, $\tilde{\xi}_{\mathbb{F}_p}$ is surjective, and therefore, $\xi\colon \mathcal{K} \to \mathcal{G}^{(\lambda)}$ is flat.

Now we define a group A-scheme $\mathcal{W}_2$ by the cocartesian diagram

$$\begin{array}{ccc} \mathcal{K} & \longrightarrow & U \\ \downarrow & & \downarrow \\ \mathcal{G}^{(\lambda)} & \longrightarrow & \mathcal{W}_2. \end{array}$$

Then we obtain an exact sequence of group A-schemes

$$0 \to \mathcal{G}^{(\lambda)} \to \mathcal{W}_2 \to \mathcal{G}^{(\lambda)} \to 0.$$

It is similarly seen that $\mathcal{W}_2 \otimes_A \mathbb{F}_p$ is isomorphic to $W_{2,\mathbb{F}_2}$.

References

[1] S. Annantharaman, 'Schémas en groupes, espaces homogénes et espaces algébriques sur une base de dimension 1', *Bull. Soc. Math. France, Mémoire* 33 (1973).

[2] M. Demazure and P. Gabriel, *Groupes algébriques, Tome 1*, Masson–North-Holland, 1970.

[3] G. Karpilovsky, *Unit groups of group rings*, Longman Scientific and Technical, 1989.

[4] F. Oort, *Commutative group schemes*, Lecture Notes in Math. Springer, Vol. 15, 1966.

[5] T. Sekiguchi, 'On the deformation of Witt groups to torilI' *J. of Algebra* 138 (1991) 273–297.

[6] T. Sekiguchi and N. Suwa, 'A case of extensions of group schemes over a discrete valuation ring', *Tsukuba J. Math.* 14 (1990) 459–487.

[7] T. Sekiguchi and N. Suwa, 'Théorie de Kummer–Artin–Schreier', *C.R. Acad. Sci. Paris*, 312 (1991) 417–420.

[8] T. Sekiguchi and N. Suwa, 'Théories de Kummer–Artin–Schreier–Witt', *C.R. Acad. Sci. Paris* 319 (1994) 105–110.

[9] T. Sekiguchi and N. Suwa, 'Théorie de Kummer–Artin–Schreier et applications', (to appear in the Proceedings of Journées Arithmétiques Bordeaux 1993).

[10] T. Sekiguchi and N. Suwa, 'On the unified Kummer–Artin–Schreier–Witt theory', *Preprint series, Chuo-Math.* 41 (1994).

[11] T. Sekiguchi and N. Suwa, 'On the unit group schemes of commutative group algebras' (in preparation).

[12] T. Sekiguchi, F. Oort and N. Suwa, 'On the deformation of Artin–Schreier to Kummer', *Ann. Scient. Ec. Normale Sup.* 22 (1989) 345–375.

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

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

[15] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Math, Vol. 66, Springer, 1979.

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

[17] A. Grothendieck et A. Dieudonné, *Eléments de géométrie algébriques I*, Springer, 1971.