RIMS Kôkyûroku Bessatsu
B25 (2011), 53–74

Normal basis problem for torsors under a finite flat group scheme

By

Yuji Tsuno*

Abstract

Serre [12] mentions a remarkable observation that, for a finite group Γ and a field k, a universal Galois extension with group Γ over k is constructed by the unit group of the group algebra $k[\Gamma]$. We formulate this argument for finite flat group schemes, paraphrasing the reformulation in the framework of group schemes by Suwa [14]. Some examples are given concerning the argument.

Introduction

Let k be a field and Γ a finite group. Serre [12, Ch.IV, 8] observes that the unit group of the group algebra $k[\Gamma]$ has a structure of algebraic group over k, which we shall denote by $U(\Gamma)_k$, and verifies that any Galois extension of k with group Γ is obtained by a cartesian diagram

$$\begin{array}{ccc} \operatorname{Spec} K & \longrightarrow & U(\Gamma)_k \\ \downarrow & & \downarrow \\ \operatorname{Spec} k & \longrightarrow & U(\Gamma)_k/\Gamma \end{array}$$

as a consequence of the normal basis theorem. Moreover Serre verifies the Kummer theory, constructing a commutative diagram of algebraic groups with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Gamma & \longrightarrow & U(\Gamma)_k & \longrightarrow & U(\Gamma)_k/\Gamma & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \boldsymbol{\mu}_{n,k} & \longrightarrow & \mathbb{G}_{m,K} & \xrightarrow{n} & \mathbb{G}_{m,k} & \longrightarrow & 0, \end{array}$$

Received June 29, 2010. Revised November 18, 2010.
2000 Mathematics Subject Classification(s): Primary 13B05; Secondary 14L15, 12G05, 57T05.
Key Words: *Galois Theory, Group schemes, Galois cohomology, Hopf algebras.*
This research is partially supported by JSPS core-to-core program 18005.
*Department of Mathematics, Chuo University, 1-13-27 Kasuga,
Bunkyo-ku, Tokyo 112-8551, JAPAN.
e-mail: s18001@@gug.math.chuo-u.ac.jp

when Γ is a cyclic group of order n, invertible in k, and k contains all the n-th roots of unity. He verifies also the Artin-Schreier-Witt theory, constructing a commutative diagram of algebraic groups with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Gamma & \longrightarrow & U(\Gamma)_k & \longrightarrow & U(\Gamma)_k/\Gamma & \longrightarrow & 0 \\ & & \downarrow\wr & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & W_{n,k} & \xrightarrow{F-1} & W_{n,k} & \longrightarrow & 0, \end{array}$$

when Γ is a cyclic group of order p^n and k is of characteristic $p > 0$. Here $W_{n,k}$ denotes the additive group over k of Witt vectors of length n. Serre suggests even to twist the Kummer theory.

This argument can be generalized in the framework of group schemes over a ring as is done by Suwa [14]. For example, we have a following fact ([14, Prop.1.6]):
— *Let R be a ring and Γ a finite group. Then any unramified Galois extension S/R with group Γ and* with a normal basis *is obtained by a cartesian diagram*

$$\begin{array}{ccc} \operatorname{Spec} S & \longrightarrow & U(\Gamma) \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \longrightarrow & U(\Gamma)/\Gamma. \end{array}$$

Moreover two problems are raised in [14]: for a given embedding $i : \Gamma \to G$ of affine group schemes over R,

(1) if there exists a commutative diagram

$$\begin{array}{ccc} \Gamma & \longrightarrow & U(\Gamma)_R \\ \downarrow\wr & & \downarrow \\ \Gamma & \xrightarrow{i} & G; \end{array}$$

(2) if there exists a commutative diagram

$$\begin{array}{ccc} \Gamma & \xrightarrow{i} & G \\ \downarrow\wr & & \downarrow \\ \Gamma & \longrightarrow & U(\Gamma)_R. \end{array}$$

If both the problem are affimative, we obtain the following assertion ([14, Cor.1.7]):
— Let R be a ring and Γ a finite group. Then any unramified Galois extension S/R with group Γ and *with a normal basis* is obtained by a cartesian diagram

$$\begin{array}{ccc} \operatorname{Spec} S & \longrightarrow & G \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \longrightarrow & G/\Gamma. \end{array}$$

It would be interesting to consider such problems for a finite flat commutative group scheme Γ over R. In this article, we develop our argument, repalcing the embedding $\Gamma \to U(\Gamma)_R$ by the embedding

$$\Gamma = Hom_{S-\mathrm{gr}}(\Gamma^\vee, \mathbb{G}_{m,S}) \longrightarrow \prod_{\Gamma^\vee/R} \mathbb{G}_{m,\Gamma^\vee} = Hom_S(\Gamma^\vee, \mathbb{G}_{m,S}),$$

constructed by Grothendieck. It should be noted that the embedding $\Gamma \to \prod_{\Gamma^\vee/R} \mathbb{G}_{m,\Gamma^\vee}$ is nothing but $\Gamma \to U(\Gamma)_R$ when Γ is a finite commutative group. We need also employ the notion of cleft Hopf-Galois extensions. (For the definition, see Section 2.)

The main result is stated as follows (Theorem 3.5 and Corollary 3.6):

— *Let S be a scheme, Γ an affine commutative group scheme over S and X a Γ-torsor over S. Assume that $\mathcal{O}_\Gamma$ is a locally free $\mathcal{O}_S$-module of finite rank. Then X is cleft if and only if $[X] \in \mathrm{Ker}[H^1(S,\Gamma) \to \mathrm{Pic}(\Gamma^\vee)]$. Here the map $H^1(S,\Gamma) \to \mathrm{Pic}(\Gamma^\vee)$ is the composite*

$$H^1(S,\Gamma) \longrightarrow H^1(S, \prod_{\Gamma^\vee/R} \mathbb{G}_{m,\Gamma^\vee}) \xrightarrow{\sim} H^1(\Gamma^\vee, \mathbb{G}_{m,\Gamma^\vee}) = \mathrm{Pic}(\Gamma^\vee).$$

This implies a remarkable consequence (Corollary 3.8):

— *Under the assumption stated above, let G be a flat affine group scheme over S. Assume that $e : \Gamma \to G$ is a closed subgroup scheme of G and there exist commutative diagrams*

$$\begin{array}{ccc} \Gamma & \xrightarrow{i} & \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee} \\ \downarrow\wr & & \downarrow \\ \Gamma & \xrightarrow{e} & G \end{array}$$

and

$$\begin{array}{ccc} \Gamma & \xrightarrow{e} & G \\ \downarrow\wr & & \downarrow \\ \Gamma & \xrightarrow{i} & \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}. \end{array}$$

Then any cleft Γ-torsor X over S is obtained by a cartesian diagram

$$\begin{array}{ccc} X & \longrightarrow & G \\ \downarrow & & \downarrow \\ S & \longrightarrow & G/\Gamma. \end{array}$$

Now we explain the organization of the article. In Section 1 and Section 2, we recall the definition of affine group schemes used in the sequel and some fundamental terminologies in the Hopf-Galois theory, respectively. In Section 3, we state and prove the main theorem, after recalling the embedding of a finite flat commutative group scheme into a smooth affine commutative group schemes, constructed by Grothendieck. In Section 4, we give three examples for the argument in Section 3.

List of group schemes

$\mathbb{G}_{a,R}$: the additive group scheme over R
$\mathbb{G}_{m,R}$: the multiplicative group scheme over R
$\boldsymbol{\mu}_{n,R} : \mathrm{Ker}[n : \mathbb{G}_{m,R} \to \mathbb{G}_{m,R}]$
$\boldsymbol{\alpha}_{p,R} : \mathrm{Ker}[F : \mathbb{G}_{a,R} \to \mathbb{G}_{a,R}]$ when R is of characteristic p
$\mathcal{G}_R^{(\lambda)}$: recalled in 1.2
$G_{R_1/R}$: defined in 1.3
$U(\Gamma)$: defined in 1.4

Acknowledgement. I would like to express my hearty thanks to Professor Noriyuki Suwa, my supervisor, for valuable advices and his patience. I cannot get any results in this paper without his support. Also I would like to express my thanks to Professor Akira Masuoka for his useful suggestion. In particular, he taught me the concept of normal bases in the framework of the Hopf-Galois theory. I am grateful to Professors Tsutomu Sekiguchi and Fumiyuki Momose for their warm advices. Finally he is very grateful to the referee for useful remarks.

§ 1. Group schemes

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

$$\mathbb{G}_{a,R} = \mathrm{Spec}\, R[T]$$

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 $\mathbb{G}_{m,R}$ over R is defined by

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

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

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

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

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

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

Definition 1.3. (Waterhouse-Weisfeiler [17, Th.3.1]) Let R be a ring and $\lambda \in R$. Put $R_1 = R[\sqrt{\lambda}] = R[t]/(t^2 - \lambda)$. A group scheme $G_{R_1/R}$ over R is defined by

$$G_{R_1/R} = \operatorname{Spec} R[U, V]/(U^2 - \lambda V^2 - V)$$

with
(a) the multiplication:

$$U \mapsto U \otimes 1 + 1 \otimes U + 2\lambda U \otimes V + 2\lambda U \otimes U, V \mapsto V \otimes 1 + 1 \otimes V + 2\lambda V \otimes V + 2U \otimes U;$$

(b) the unit:

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

(c) the inverse:

$$U \mapsto -U, V \mapsto V.$$

If 2 is invertible in R, then $T \mapsto 2(U + \sqrt{\lambda}V)$ defines an isomorphism over R_1

$$\sigma : G_{R_1/R} \otimes_R R_1 = \operatorname{Spec} R_1[U, V]/(U^2 - \lambda V^2 - V) \xrightarrow{\sim} \mathcal{G}_{R_1}^{(\sqrt{\lambda})} = \operatorname{Spec} R_1[T, \frac{1}{1+\sqrt{\lambda}T}].$$

The inverse of σ is given by

$$U \mapsto \frac{2T + \sqrt{\lambda}T^2}{4(1+\sqrt{\lambda}T)}, V \mapsto \frac{T^2}{4(1+\sqrt{\lambda}T)}.$$

Definition 1.4. Let Γ be a finite group. The functor $R \mapsto R[\Gamma]$ is represented by the ring scheme $A(\Gamma)$ defined by

$$A(\Gamma) = \operatorname{Spec} \mathbb{Z}[T_\gamma; \gamma \in \Gamma]$$

with
(a) the addition: $T_\gamma \mapsto T_\gamma \otimes 1 + 1 \otimes T_\gamma$;
(b) the multiplication: $T_\gamma \mapsto \sum_{\gamma'\gamma''=\gamma} T_{\gamma'} \otimes T_{\gamma''}$.

Put now

$$U(\Gamma) = \operatorname{Spec} \mathbb{Z}[T_\gamma, \frac{1}{\Delta_\Gamma}; \gamma \in \Gamma],$$

where $\Delta_\Gamma = \det(T_{\gamma'\gamma''})$ denotes the determinant of the matrix $(T_{\gamma'\gamma''})_{\gamma',\gamma'' \in \Gamma}$ (the group determinant of Γ). Then $U(\Gamma)$ is an open subscheme of $A(\Gamma)$, and the functer $\Gamma \mapsto R[\Gamma]^\times$ is represented by the group scheme $U(\Gamma)$.

We denote also by Γ, for the abbreviation, the constant group scheme defined by Γ. Moreprecisely, $\Gamma = \operatorname{Spec} \mathbb{Z}^\Gamma$ and the law of multiplication is defined by $e_\gamma \mapsto \sum_{\gamma'\gamma''=\gamma} e_{\gamma'} \otimes e_{\gamma''}$. Here $\mathbb{Z}^\Gamma$ denotes the functions from Γ to $\mathbb{Z}$, and $(e_\gamma)_{\gamma\in\Gamma}$ is a basis of $\mathbb{Z}^\Gamma$ over $\mathbb{Z}$ defined by

$$e_\gamma(\gamma') = \begin{cases} 1 & (\gamma' = \gamma) \\ 0 & (\gamma' \neq \gamma). \end{cases}$$

The canonical injection $\Gamma \mapsto R[\Gamma]^\times$ is represented by the homomorphism of group schemes $i : \Gamma \to U(\Gamma)$ defined by

$$T_\gamma \mapsto e_\gamma : \operatorname{Spec} \mathbb{Z}[T_\gamma, \frac{1}{\Delta_\Gamma}] \to \mathbb{Z}^\Gamma.$$

It is readily seen that $\Gamma \to U(\Gamma)$ is a closed immersion. If Γ is commutative, then $U(\Gamma)$ is isomorphic to the Weil restriction $\prod_{\Gamma^\vee/\mathbb{Z}} \mathbb{G}_{m,\Gamma^\vee}$.

Let R be a ring. Then the exact sequence

$$1 \longrightarrow \Gamma \longrightarrow U(\Gamma) \longrightarrow U(\Gamma)/\Gamma \longrightarrow 1$$

yields an exact sequence of pointed sets

$$U(\Gamma)(R) \longrightarrow (U(\Gamma)/\Gamma)(R) \longrightarrow H^1(R, \Gamma) \longrightarrow H^1(R, U(\Gamma)).$$

An unramified Galois extension S/R with group Γ has a normal basis if and only if $[S] \in \operatorname{Ker}[H^1(R, \Gamma) \to H^1(R, U(\Gamma))]$ (Suwa [14, Sect.1]).

§ 2. Hopf-Galois theory

We recall some terminologies of the Hopf-Galois theory. For details we refer to [8], [3], [2].

Definition 2.1. Let R be a commutative ring and C an R-bialgebra (necessarily neither commutative nor cocommutative). An R-algebra B (not necessarily commutative) is called a right C-comodule algebra over R if B is a right C-comodule and the comodule structure map $\rho_B : B \to B \otimes_R C$ is a homomorphism of R-algebras.

Definition 2.2. Let R be a commutative ring and C an R-bialgebra. An C-comodule algebra B over R is called an C-extension of a subalgebra of B if $A = \{a \in B \ ; \ \rho_B(a) = a \otimes 1\}$.

Notation 2.3. Let R be a commutative ring, C an R-bialgebra and B/A an C-extension of R-algebras. Then a homomorphism of left B-modules $r : B \otimes_A B \to B \otimes_R C$ is defined by $a \otimes b \mapsto (a \otimes 1)\rho_B(b)$. If B and C are commutative, then r is a homomorphism of B-algebras.

Definition 2.4. Let R be a commutative ring and C an R-bialgebra. An C-extension B/A of R-algebras is called Galois if the homomorphism $r : B \otimes_A B \to B \otimes_R C$ is bijective.

Example 2.5. Let R be a commutative ring, B a commutative R-algebra and C a commutative Hopf R-algebra. Put $S = \operatorname{Spec} R$, $Y = \operatorname{Spec} B$ and $G = \operatorname{Spec} C$. Then a right C-comodule algebra structure map $\rho : B \to B \otimes_R C$ over R corresponds to a right action ${}^a\rho : Y \times_S G \to Y$ of the group scheme G on Y over S. Put $A = \{a \in B \ ; \ \rho(a) = a \otimes 1\}$ and $X = \operatorname{Spec} A$. Assume that B is faithfully flat of finite presentation as an A-algebra. Then the C-extension B/A is Galois if and only if Y is a G-torsor over X.

Theorem 2.6.(Doi-Takeuchi [3, Th.9]) *Let R be a commutative ring, C an R-bialgebra and B/A an C-extension of R-algebras. Then the following conditions are equivalent.*
(a) *There exists a homomorphism of R-modules $\varphi : C \to B$ which is also a homomorphism of right C-comodules and invertible for the convolution product in* $\operatorname{Hom}_R(C, B)$.
(b) *B/A is a Galois C-extension and there exists an isomorphism of left A-modules $A \otimes_R C \to B$ which is also a homomorphism of right C-comodules.*

We recall that the convolution product in $\operatorname{Hom}_R(C, B)$ is defined by $\varphi * \psi = \mu_B \circ (\varphi \otimes \psi) \circ \Delta_C$ for $\varphi, \psi \in \operatorname{Hom}_R(C, B)$. Here $\Delta_C : C \to C \otimes_R C$ denotes the comultiplication of C, and $\mu_B : B \otimes_R B \to B$ the multiplication of B.

Definition 2.7. Let R be a commutative ring and C an R-bialgebra. An C-extension B/A of R-algebras is called cleft if the equivalent conditions in Theorem 1.6 are satisfied.

Example 2.8.(Kreimer-Takeuchi [8, Example 1]) Let R be a commutative ring, B an R-algebra and Γ a finite group of R-algebra automorphisms of B. Let $C = R[\Gamma]^\vee$ denote the dual Hopf algebra of the group ring $R[\Gamma]$ and $\{e_\gamma\}_{\gamma\in\Gamma}$ the dual basis for $\{\gamma\}_{\gamma\in\Gamma}$. Then a right C-comodule algebra structure map $\rho_B : B \to B \otimes_R C$ over R is defined by

$$\rho_B(b) = \sum_{\gamma\in\Gamma} \gamma(b) \otimes e_\gamma,$$

Then we have

$$B^\Gamma = \{b \in B \ ; \ \gamma(b) = b \text{ for all } \gamma \in \Gamma\} = \{b \in B \ ; \ \rho_B(b) = b \otimes 1\}.$$

Put $A = B^\Gamma$. Then:
(a) B/A is a Galois C-extension if and only if there exist $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in B$ such that

$$\sum_{i=1}^{n} a_i\gamma(b_i) = \begin{cases} 1 & \text{if } \gamma = e \\ 0 & \text{if } \gamma \neq e. \end{cases}$$

(b) B/A is a cleft C-extension if and only if there exists $b \in B$ such that $\{\gamma(b)\}_{\gamma\in\Gamma}$ is a basis of the left A-module B.

If B is commutative, then $\operatorname{Spec} B$ is finite over $\operatorname{Spec} A$. The C-extension B/A is Galois if and only if $\operatorname{Spec} B$ is an étale covering of $\operatorname{Spec} A$ with Galois group Γ, that is to say, B/A is an unramified Galois extension with group Γ. The C-extension B/A is cleft if and only if the unramified Galois extension B/A has a normal basis.

Now we shall add the following definition.

Definition 2.9. Let S be a scheme, G an affine group S-scheme and X is a right G-torsor over S. We shall say that a right G-torsor X over S is cleft if there exists an isomomorphism of $\mathcal{O}_S$-modules $\mathcal{O}_G \to \mathcal{O}_X$ which is also a homomorphism of right $\mathcal{O}_G$-comodule.

§ 3. The main result

3.1. First we recall a resolution of a finite flat commutative group scheme by smooth affine commutative group schemes, constructed by Grothendieck (cf. [9. Sec 6]).

Let S be a scheme and Γ a finite commutative S-group scheme such that $\mathcal{O}_\Gamma$ is a locally free $\mathcal{O}_S$-module of finite rank. Then the functor $Hom_{S-\mathrm{gr}}(\Gamma, \mathbb{G}_{m,S})$ is represented by a commutative group scheme $\Gamma^\vee$, called the Cartier dual of Γ. The $\mathcal{O}_S$-module $\mathcal{O}_{\Gamma^\vee}$

is also locally free of finite rank. The Cartier duality asserts that $Hom_{S-\mathrm{gr}}(\Gamma^\vee, \mathbb{G}_{m,S})$ is isomorphic to Γ.

Furthermore the functor $Hom_S(\Gamma^\vee, \mathbb{G}_{m,S})$ is nothing but the Weil restriction $\prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}$, which is representable since $\mathcal{O}_{\Gamma^\vee}$ 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

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

(cf. [9, (5.1)]).

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

Moreover, in the case where Γ is finite commutative group, the exact sequence

$$0 \longrightarrow \Gamma \longrightarrow U(\Gamma) \longrightarrow U(\Gamma)/\Gamma \longrightarrow 0$$

coincides with the exact sequence induced by the Grothendieck resolution of Γ

$$0 \longrightarrow \Gamma \xrightarrow{i} \prod_{\Gamma^\vee/\mathbb{Z}} \mathbb{G}_{m,\Gamma^\vee} \longrightarrow \Big(\prod_{\Gamma^\vee/\mathbb{Z}} \mathbb{G}_{m,\Gamma^\vee}\Big)/\Gamma \longrightarrow 0.$$

Definition 3.2. Let S be a scheme and Γ a finite commutative group scheme over S. Assume that $\mathcal{O}_\Gamma$ is a locally free $\mathcal{O}_S$-module of finite rank.

Let X be a right Γ-torsor over S. Then there is defined an $\mathcal{O}_S$-homomorphism $\rho : \mathcal{O}_X \to \mathcal{O}_X \otimes_{\mathcal{O}_S} \mathcal{O}_\Gamma$, which makes $\mathcal{O}_X$ an $\mathcal{O}_\Gamma$-comodule algebra. Passing to the dual, we obtain an $\mathcal{O}_S$-homomorphism $\rho^\vee : \mathcal{O}_{\Gamma^\vee} \otimes_{\mathcal{O}_S} \mathcal{O}_X^\vee \to \mathcal{O}_X^\vee$, which makes $\mathcal{O}_X^\vee$ an $\mathcal{O}_{\Gamma^\vee}$-module.

By definition, there exists a faithfully flat morphism $T \to S$ such that the Γ-torsor $X_T = T \times_S X$ over T is isomorphic to $\Gamma_T = T \times_S \Gamma$. That is to say, the $\mathcal{O}_T$-algebra $\mathcal{O}_{X_T}$ is isomorphic to $\mathcal{O}_{\Gamma_T}$ as $\mathcal{O}_{\Gamma_T}$-comodule algebra. Hence the $\mathcal{O}_{X_T}^\vee$ is isomorphic to $\mathcal{O}_{\Gamma_T^\vee}$ as $\mathcal{O}_{\Gamma_T^\vee}$-module. It follows that $\mathcal{O}_X^\vee$ is an invertible $\mathcal{O}_{\Gamma^\vee}$-module. Furthermore, the Γ-torsor X is cleft if and only if $\mathcal{O}_X^\vee$ is isomorphic to $\mathcal{O}_{\Gamma^\vee}$ as $\mathcal{O}_{\Gamma^\vee}$-module. This follows from the argument developed by Kreimer and Takeuchi ([8, Sect. 1]).

On the other hand, the canonical map

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

is an isomorphism by the following lemma.

Lemma 3.3. *Let $f : T \to S$ be a finite morphism and G a commutative group scheme over T. Assume that $\mathcal{O}_T$ is locally free $\mathcal{O}_S$-module of finite ranks and that G is smooth and quasi-projective over T. Then the canonical homomorphism*

$$H^q(S, \prod_{T/S} G) \to H^q(T, G)$$

is bijective for $q \geq 0$.

Proof. The assertion seems to be a folklore for experts. This follows from the following three facts:
(a) Let $f : Y \to X$ be a finite morphism of schemes and F an abelian sheaf on Y_{et}. Then we have $R^j f_* F = 0$ for $j > 0$ ([5, exp 8. Cor.5.6]);
(b) Let X be a scheme and G be a commutative group scheme over X. Let $\varepsilon : X_{\mathrm{fl}} \to X_{\mathrm{et}}$ denote the canonical morphism of sites. If G is smooth and quasi-projective, then we have $R^j \varepsilon_* G = 0$ for $j > 0$ ([4, Th.11.7.]);
(c) Let $f : T \to S$ be a finite morphism and G a commutative group scheme over T. If $\mathcal{O}_T$ is a locally free $\mathcal{O}_S$-module of finite ranks and G is quasi-projective over T, then $\prod_{T/S} G = f_* G$ is representable by a quasi-projective commutative group scheme over S. Moreover, if G is smooth over T, then $\prod_{T/S} G$ is smooth over S (cf. [1, Ch.I, 1.6.6]).

We recall the definition of the contracted product for sheaves with group actions, before mentioning and proving our main result.

Notation 3.4. Let S be a scheme, and let G be a sheaf of groups on S_{fl}, X a right G-sheaf and Y a left G-sheaf on S_{fl}. Then a left action of G on the product $X \times Y$ is defined by $g(x, y) = (xg^{-1}, gy)$. We denote the quotient $X \times Y/G$ by $X \vee^G Y$, called the contracted product of X and Y. (For details we refer to Demazure-Gabriel [1, Ch.III, 4.3.1].)

Theorem 3.5. *Let S be a scheme and Γ an affine commutative group scheme over S such that $\mathcal{O}_\Gamma$ is a locally free $\mathcal{O}_S$-module of finite rank. Then the composite*

$$H^1(S, \Gamma) \xrightarrow{i} H^1(S, \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}) \xrightarrow{\sim} \mathrm{Pic}(\Gamma^\vee)$$

coincides with the map defined by $[X] \mapsto [\mathcal{O}_X^\vee]$, up to an automorphism of $\mathrm{Pic}(\Gamma^\vee)$. Here the map $i : H^1(S, \Gamma) \to H^1(S, \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee})$ is induced by the Grothendieck resolution

$$i : \Gamma = Hom_{S-gr}(\Gamma^\vee, \mathbb{G}_{m,S}) \to \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee} = Hom_S(\Gamma^\vee, \mathbb{G}_{m,S}).$$

Proof. It is known that the canonical homomorphism

$$H^1(S, \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}) \to H^1(\Gamma^\vee, \mathbb{G}_{m,\Gamma^\vee})$$

is the composite of the homomorphism

$$H^1(S, \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}) \to H^1(\Gamma^\vee, \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee})$$

induced by the structure morphism $\Gamma^\vee \to S$ and the homomorphism

$$H^1(\Gamma^\vee, \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}) \to H^1(\Gamma^\vee, \mathbb{G}_{m,\Gamma^\vee})$$

induced by the adjunction morphism $\Gamma^\vee \times_S \big(\prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee} \big) \to \mathbb{G}_{m,\Gamma^\vee}$, up to an automorphism of $H^1(\Gamma^\vee, \mathbb{G}_{m,\Gamma^\vee})$ (cf. [6, Ch.O, 12.1.7]).

Moreover we have a commutative diagram

$$\begin{array}{ccccc} H^1(S,\Gamma) & \xrightarrow{i} & H^1(S, \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}) & & \\ \downarrow & & \downarrow & & \\ H^1(\Gamma^\vee,\Gamma) & \xrightarrow{i} & H^1(\Gamma^\vee, \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}) & \longrightarrow & H^1(\Gamma^\vee, \mathbb{G}_{m,\Gamma^\vee}). \end{array}$$

Hence the composite

$$H^1(S,\Gamma) \xrightarrow{i} H^1(S, \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}) \xrightarrow{\sim} H^1(\Gamma^\vee, \mathbb{G}_{m,\Gamma^\vee})$$

is given by $[X] \mapsto [X_{\Gamma^\vee} \vee^{\Gamma_{\Gamma^\vee}} \mathbb{G}_{m,\Gamma^\vee}]$.

We remark here that the compsoite

$$\chi : \Gamma_{\Gamma^\vee} = \Gamma^\vee \times_S \Gamma \xrightarrow{i} \Gamma^\vee \times_S \big(\prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee} \big) \longrightarrow \mathbb{G}_{m,\Gamma^\vee}$$

is the scalar extension of the Cartier paring

$$\Gamma^\vee \times_S \Gamma \to \mathbb{G}_{m,S}$$

by the structure morphism $\Gamma^\vee \to S$.

On the other hand, the sheaf $Isom_{\mathcal{O}_{\Gamma^\vee}}(\mathcal{O}_{\Gamma^\vee}, \mathcal{O}_X^\vee)$ on $\Gamma^\vee$ for the fppf-topology is a $\mathbb{G}_{m,\Gamma^\vee}$-torsor over $\Gamma^\vee$. Moreover the correspondence $\mathcal{L} \mapsto Isom_{\mathcal{O}_{\Gamma^\vee}}(\mathcal{O}_{\Gamma^\vee}, \mathcal{L})$ gives

rise to an isomorphism $\mathrm{Pic}(\Gamma^\vee) \xrightarrow{\sim} H^1(\Gamma^\vee, \mathbb{G}_{m,\Gamma^\vee})$ (cf. Demazure-Gabriel [1, Ch.III, 4.4.4]).

Now we verify that, for a Γ-torsor X over S, the contracted product $X_{\Gamma^\vee} \vee^{\Gamma_{\Gamma^\vee}} \mathbb{G}_{m,\Gamma^\vee}$ is isomorphic to $Isom_{\mathcal{O}_{\Gamma^\vee}}(\mathcal{O}_{\Gamma^\vee}, \mathcal{O}_X^\vee)$ as $\mathbb{G}_{m,\Gamma^\vee}$-torsors over $\Gamma^\vee$, which implies the assertion by the above argument.

Let X be a right Γ-torsor over S and T a scheme affine over $\Gamma^\vee$. Then the right $\Gamma(T)$-set $X(T) = \mathrm{Hom}_S(T, X) = \mathrm{Hom}_T(T, T \times_S X)$ is identified to the set of Γ-equivariant T-isomorphisms $\Gamma_T \to X_T$. Take $\xi \in X(T)$. We denote by $\xi : \Gamma_T \xrightarrow{\sim} X_T$ also the corresponding Γ-equivariant T-isomorphism. Moreover let $\tilde{\xi} : \mathcal{O}_{X_T} \xrightarrow{\sim} \mathcal{O}_{\Gamma_T}$ denote the isomorphism of $\mathcal{O}_{\Gamma_T}$-comodule algebras, which defines $\xi : \Gamma_T \xrightarrow{\sim} X_T$. Passing to the dual, we obtain an $\mathcal{O}_{\Gamma_T^\vee}$-isomorphism $\tilde{\xi}^\vee : \mathcal{O}_{\Gamma_T^\vee} \xrightarrow{\sim} \mathcal{O}_{X_T}^\vee$. Moreover we consider the composite of $\mathcal{O}_T$-homomorphisms

$$\begin{aligned}\eta(\widetilde{\xi^\vee}) : \mathcal{O}_T &\xrightarrow{i} \mathcal{O}_T \otimes_{\mathcal{O}_S} \mathcal{O}_{\Gamma^\vee} = \mathcal{O}_T \otimes_{\mathcal{O}_{\Gamma^\vee}} (\mathcal{O}_{\Gamma^\vee} \otimes_{\mathcal{O}_S} \mathcal{O}_{\Gamma^\vee}) \\ &\xrightarrow{\xi^\vee} \mathcal{O}_T \otimes_{\mathcal{O}_S} \mathcal{O}_X^\vee = \mathcal{O}_T \otimes_{\mathcal{O}_{\Gamma^\vee}} (\mathcal{O}_{\Gamma^\vee} \otimes_{\mathcal{O}_S} \mathcal{O}_X^\vee) \xrightarrow{\mathrm{Id}\otimes\mu} \mathcal{O}_T \otimes_{\mathcal{O}_S} \mathcal{O}_X^\vee\end{aligned}$$

Here $i : \mathcal{O}_T \to \mathcal{O}_T \otimes_{\mathcal{O}_S} \mathcal{O}_{\Gamma^\vee}$ is locally defined by $a \mapsto a \otimes 1$, and $\mu : \mathcal{O}_{\Gamma^\vee} \otimes_{\mathcal{O}_S} \mathcal{O}_X^\vee \to \mathcal{O}_X^\vee$ by $a \otimes b \mapsto ab$. Then $\eta(\xi^\vee)$ is an isomorphism since $\mathcal{O}_T \otimes_{\mathcal{O}_S} \mathcal{O}_{\Gamma^\vee}$ is faithfully flat over $\mathcal{O}_T$.

On the other hand, the sheaf $Aut_{\mathcal{O}_{\Gamma^\vee}}(\mathcal{O}_{\Gamma^\vee})$ is represented by $\mathbb{G}_{m,\Gamma^\vee}$. Take $h \in \mathbb{G}_m(T)$. We denote by $h : \mathcal{O}_T \xrightarrow{\sim} \mathcal{O}_T$ also the corresponding $\mathcal{O}_T$-automorphism. Then $(\xi, h) \mapsto \eta(\tilde{\xi}^\vee) \circ h$ defines a morphism of right $\mathbb{G}_{m,\Gamma^\vee}$-sheaves $\mu : X_{\Gamma^\vee} \times_{\Gamma^\vee} \mathbb{G}_{m,\Gamma^\vee} \to Isom_{\mathcal{O}_{\Gamma^\vee}}(\mathcal{O}_{\Gamma^\vee}, \mathcal{O}_X^\vee)$.

Furthermore the left action by $\Gamma_{\Gamma^\vee}$ on $X_{\Gamma^\vee} \times_{\Gamma^\vee} \mathbb{G}_{m,\Gamma^\vee}$ is defined by

$$\gamma(\xi, h) = (\xi\gamma^{-1}, \chi(\gamma)h).$$

for $\gamma \in \Gamma_{\Gamma^\vee}(T)$.

Note now that the Cartier duality asserts the equality $\eta(\tilde{\gamma}^\vee) = \chi(\gamma) : \mathcal{O}_T \xrightarrow{\sim} \mathcal{O}_T$. It follows that the morphism $\mu : X_{\Gamma^\vee} \times_{\Gamma^\vee} \mathbb{G}_{m,\Gamma^\vee} \to Isom_{\mathcal{O}_{\Gamma^\vee}}(\mathcal{O}_{\Gamma^\vee}, \mathcal{O}_X^\vee)$ is compatible with the left action by $\Gamma_{\Gamma^\vee}$ on $X_{\Gamma^\vee} \times_{\Gamma^\vee} \mathbb{G}_{m,\Gamma^\vee}$. Therefore μ defines a morphism of right $\mathbb{G}_{m,\Gamma^\vee}$-sheaves $X_{\Gamma^\vee} \vee^{\Gamma_{\Gamma^\vee}} \mathbb{G}_{m,\Gamma^\vee} \to Isom_{\mathcal{O}_{\Gamma^\vee}}(\mathcal{O}_{\Gamma^\vee}, \mathcal{O}_X^\vee)$, which is an isomorphism of right $\mathbb{G}_{m,\Gamma^\vee}$-torsors.

Corollary 3.6. *Under the assumption of Theorem 3.5, let X be a Γ torsor over S. Then the Γ-torsor X is cleft if and only if $[X] \in \mathrm{Ker}[H^1(S, \Gamma) \to \mathrm{Pic}(\Gamma^\vee)]$.*

Corollary 3.7. *Under the assumption of Theorem 3.5, let G be a flat affine group scheme over S.*
(1) *Assume that $e : \Gamma \to G$ is a closed subgroup scheme of G and there exists a commutative diagram*

$$\begin{array}{ccc} \Gamma & \xrightarrow{i} & \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee} \\ \downarrow \wr & & e \downarrow \\ \Gamma & \longrightarrow & G. \end{array}$$

Then, if a Γ-torsor X over S is cleft, there exists morphisms $X \to G$ and $S \to G/\Gamma$ such that the diagram

$$\begin{array}{ccc} X & \longrightarrow & G \\ \downarrow & & \downarrow \\ S & \longrightarrow & G/\Gamma \end{array}$$

is cartesian.

(2) *Assume that $e : \Gamma \to G$ is a closed subgroup scheme of G and there exists a commutative diagram*

$$\begin{array}{ccc} \Gamma & \xrightarrow{e} & G \\ \downarrow \wr & & \downarrow \\ \Gamma & \xrightarrow{i} & \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}. \end{array}$$

Then, if a Γ-torsor X over S is defined by a cartesian diagram

$$\begin{array}{ccc} X & \longrightarrow & G \\ \downarrow & & \downarrow \\ S & \longrightarrow & G/\Gamma, \end{array}$$

X is a cleft Γ-torsor.

Proof. Under the assumption of (1) we obtain

$$\mathrm{Ker}[H^1(S,\Gamma) \to \mathrm{Pic}(\Gamma^\vee)] \subset \mathrm{Ker}[H^1(S,\Gamma) \to H^1(S,G)],$$

and under the assumption of (2) we obtain

$$\mathrm{Ker}[H^1(S,\Gamma) \to H^1(S,G)] \subset \mathrm{Ker}[H^1(S,\Gamma) \to \mathrm{Pic}(\Gamma^\vee)].$$

There imply the assertions.

Corollary 3.8. *Under the assumption of Theorem 3.5, let G be a flat affine group scheme over S. Assume that $e : \Gamma \to G$ is a closed subgroup scheme of G and there exist commutative diagrams*

$$\begin{array}{ccc} \Gamma & \xrightarrow{i} & \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee} \\ \downarrow{\scriptstyle \wr} & & \downarrow \\ \Gamma & \longrightarrow & G \end{array}$$

and

$$\begin{array}{ccc} \Gamma & \longrightarrow & G \\ \downarrow{\scriptstyle \wr} & & \downarrow \\ \Gamma & \xrightarrow{i} & \prod_{\Gamma^\vee/S} \mathbb{G}_{m,\Gamma^\vee}. \end{array}$$

Then, a Γ-torsor X over S is cleft if and only if X is defined by a cartesian diagram

$$\begin{array}{ccc} X & \longrightarrow & G \\ \downarrow & & \downarrow \\ S & \longrightarrow & G/\Gamma. \end{array}$$

§ 4. Examples

Example 4.1. Let p be a prime number, R an $\mathbb{F}_p$-algebra and $\mu \in R$. Put

$$N = \mathrm{Ker}[F - \mu I : \mathbb{G}_{a,R} \to \mathbb{G}_{a,R}].$$

Then there exist commutative diagrams of group schemes

$$\begin{array}{ccc} N & \longrightarrow & \prod_{N^\vee/R} \mathbb{G}_{m,N^\vee} \\ \| & & \downarrow{\scriptstyle \tilde{\chi}} \\ N & \longrightarrow & \mathbb{G}_{a,R} \end{array}$$

and

$$\begin{array}{ccc} N & \longrightarrow & \mathbb{G}_{a,R} \\ \| & & \downarrow{\scriptstyle \tilde{\sigma}} \\ N & \longrightarrow & \prod_{N^\vee/R} \mathbb{G}_{m,N^\vee} \end{array}$$

([16, Th.3.3]). Therefore we obtain

$$\mathrm{Ker}[H^1(R,N) \to \mathrm{Pic}(N^\vee)] = \mathrm{Ker}[H^1(R,N) \to H^1(R,\mathbb{G}_{a,R})].$$

Moreover it is known that $H^1(R,\mathbb{G}_{a,R}) = 0$. It follows that all the N-torsor X over $\mathrm{Spec}\, R$ is cleft.

More precisely, we have $N = \mathrm{Spec}\, R[T]/(T^p - \mu T)$ equipped with the addition defined by $T \mapsto T \otimes 1 + 1 \otimes T$. There exists $a \in A$ such that X is isomorphic to $\mathrm{Spec}\, R[X]/(X^p - \mu X - a)$ and the action of N on X over R is defined by

$$R[X]/(X^p - \mu X - a) \to R[X]/(X^p - \mu X - a) \otimes_R R[T]/(T^p - \mu T) : X \mapsto X \otimes 1 + 1 \otimes T.$$

We can verify directly that $R[X]/(X^p - \mu X - a)$ with the coaction $X \mapsto X \otimes 1 + 1 \otimes T$ is a cleft Hopf comodule algebra. Put $C = R[T]/(T^p - \mu T)$ and $B = R[X]/(X^p - \mu X - a)$. Define a homomorphism of R-modules $\varphi : C \to B$ by

$$T^i \mapsto X^i \ (0 \leq i < p).$$

Then φ is bijective and a homomorphism of right C-comodules. Furthermore φ is invertible for the convolution product in $\mathrm{Hom}_R(C,B)$. Indeed, the convolution inverse of φ is given by

$$T^i \mapsto (-X)^i \ (0 \leq i < p).$$

Example 4.2. Let p be a prime number, R an $\mathbb{F}_p$-algebra and $\lambda \in R$. The Frobenius morphism

$$F : \mathcal{G}^{(\lambda)} = \mathrm{Spec}\, R[T, \frac{1}{1+\lambda T}] \to \mathcal{G}^{(\lambda^p)} = \mathrm{Spec}\, R[T, \frac{1}{1+\lambda^p T}]$$

is defined by $T \mapsto T^p$. Put $G = \mathrm{Ker}[F : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}]$. Then $G = \mathrm{Spec}\, R[T]/(T^p)$ is equipped with the multiplication defined by $T \mapsto T \otimes 1 + 1 \otimes T + \lambda T \otimes T$.

Moreover there exist commutative diagrams of group schemes

$$\begin{array}{ccc} G & \longrightarrow & \prod\limits_{G^\vee/R} \mathbb{G}_{m,G^\vee} \\ \| & & \downarrow \tilde{\chi} \\ G & \longrightarrow & \mathcal{G}^{(\lambda)} \end{array}$$

and

$$\begin{array}{ccc} G & \longrightarrow & \mathcal{G}^{(\lambda)} \\ \| & & \downarrow \tilde{\sigma} \\ G & \longrightarrow & \prod\limits_{G^\vee/R} \mathbb{G}_{m,G^\vee} \end{array}$$

([16], Th.3.12). This implies

$$\mathrm{Ker}[H^1(R,G) \to \mathrm{Pic}(G^\vee)] = \mathrm{Ker}[H^1(R,G) \to H^1(R,\mathcal{G}^{(\lambda)})].$$

Furthemore, we obtain the following corollaries.

Corollary 4.3. *Under the notations of Example 4.2, let S/R be an extension of ring. Then* $\mathrm{Spec}\, S$ *is a cleft G-torsor over* $\mathrm{Spec}\, R$ *if and only if there exist morphisms* $\mathrm{Spec}\, S \to \mathcal{G}^{(\lambda)}$ *and* $\mathrm{Spec}\, R \to \mathcal{G}^{(\lambda^p)}$ *such that the diagram*

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

is cartesian.

Corollary 4.4. *Under the notations of Example 4.2, the following conditions are equivalent:*
(a) *Any G-torsor over R is cleft* ;
(b) *The homomorphism $\mathcal{G}^{(\lambda^p)}(R) \to H^1(R,G)$ induced by the exact sequence*

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

is surjective ;
(c) *The homomorphism $H^1(R,\mathcal{G}^{(\lambda)}) \to H^1(R,\mathcal{G}^{(\lambda^p)})$ induced by the Frobenius morphism $F : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}$ is injective.*

Remark 4.5. Assume that R is a local ring or λ is nilpotent. Then we have $H^1(R,\mathcal{G}^{(\lambda)}) = 0$ ([11], Cor 1.3]). It follows that all the G-torsor over $\mathrm{Spec}\, R$ is cleft.

Example 4.6. There exists an $\mathbb{F}_p$-algebra R and $\lambda \in R$ such that the homomorphism $H^1(R,\mathcal{G}^{(\lambda)}) \to H^1(R,\mathcal{G}^{(\lambda^p)})$ induced by the Frobenius morphism is not injective. Here is an example. Let p be a prime number, and put

$$R = \mathbb{F}_p[X, Y, \frac{1}{Y^p + (X+1)^p Y + X^p}]$$

and $\lambda = X + 1$. Then $H^1(R,\mathcal{G}^{(\lambda)})$ is a cyclic group of order p, and $F : H^1(R,\mathcal{G}^{(\lambda)}) \to H^1(R,\mathcal{G}^{(\lambda^p)})$ is trivial. Moreover, we have $H^1(R,G) = H^1(R,\mathcal{G}^{(\lambda)})$.

In fact, we have an exact sequence of abelian sheaves on the étale site of $\mathrm{Spec}\, R$

$$0 \longrightarrow \mathcal{G}^{(\lambda)} \xrightarrow{\alpha^{(\lambda)}} \mathbb{G}_{m,R} \longrightarrow i_* \mathbb{G}_{m,R_0} \longrightarrow 0$$

([11, Theorem.1.2]) since $\lambda = X + 1$ is a non zero divisor of R. Here $R_0 = R/(\lambda)$, and $i : \mathrm{Spec}\, R_0 \to \mathrm{Spec}\, R$ denotes the canonical closed immersion. Therefore we obtain a

long exact sequence of cohomology groups

$$0 \longrightarrow \mathcal{G}^{(\lambda)}(R) \longrightarrow R^{\times} \longrightarrow {R_0}^{\times} \longrightarrow H^1(R, \mathcal{G}^{(\lambda)}) \longrightarrow \mathrm{Pic}(R).$$

Now we have

$$R^{\times} = \Big\{ c\{Y^p + (X+1)^p Y + X^p\}^n ; c \in \mathbb{F}_p^{\times},\ n \in \mathbb{Z} \Big\}$$

since the polynomial $Y^p + (X+1)^p Y + X^p$ is irreducible in $\mathbb{F}_p[X, Y]$. Moreover, under the identification $R_0 = \mathbb{F}_p[Y, 1/(Y-1)]$, we have

$$R_0^{\times} = \Big\{ c(Y-1)^n ; c \in \mathbb{F}_p^{\times},\ n \in \mathbb{Z} \Big\},$$

and $c\{Y^p + (X+1)^p Y + X^p\}^n \in R^{\times}$ is mapped to $c(Y-1)^{pn} \in R_0^{\times}$. Hence we obtain $\mathcal{G}^{(\lambda)}(R) = 0$, and $\mathrm{Coker}[R^{\times} \to R_0^{\times}]$ is a cyclic group of order p and generated by the class of $Y + X$ in R_0. On the other hand, we have $\mathrm{Pic}(R) = 0$ since R is a unique factorization domain. This implies that the map $\mathrm{Coker}[R^{\times} \to R_0^{\times}] \to H^1(R, \mathcal{G}^{\lambda})$ is bijective.

Furthermore, we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{G}^{(\lambda)} & \xrightarrow{\alpha^{(\lambda)}} & \mathbb{G}_{m,R} & \longrightarrow & i_* \mathbb{G}_{m,R_0} & \longrightarrow & 0 \\
 & & \downarrow F & & \downarrow F & & \downarrow F & & \\
0 & \longrightarrow & \mathcal{G}^{(\lambda^p)} & \xrightarrow{\alpha^{(\lambda^p)}} & \mathbb{G}_{m,R} & \longrightarrow & {i'}_* \mathbb{G}_{m,R_1} & \longrightarrow & 0,
\end{array}$$

where $R_1 = A/(\lambda^p)$ and $i' : \mathrm{Spec}\, R_1 \to \mathrm{Spec}\, R$ is the canonical closed immersions. Therefore we obtain a commutative diagram of cohomology groups with exact rows

$$\begin{array}{ccccccc}
R^{\times} & \longrightarrow & R_0^{\times} & \longrightarrow & H^1(R, \mathcal{G}^{(\lambda)}) & \longrightarrow & 0 \\
\downarrow p & & \downarrow p & & \downarrow F & & \\
R^{\times} & \longrightarrow & R_1^{\times} & \longrightarrow & H^1(R, \mathcal{G}^{(\lambda^p)}) & \longrightarrow & 0.
\end{array}$$

Here the class of $c(Y+X)^n$ in R_0 ($c \in \mathbb{F}_p^{\times},\ n \in \mathbb{Z}$) is mapped to the class of $c^p(Y^p + X^p)^n$ in R_1 by the homomorphism $p : R_0^{\times} \to R_1^{\times}$.

Note now $[Y^p + X^p] \in \mathrm{Im}[R^{\times} \to R_1^{\times}]$ since $Y^p + X^p \equiv Y^p + (X+1)^p Y + X^p \mod (X+1)^p$. Hence we can conclude that $F : H^1(R, \mathcal{G}^{(\lambda)}) \to H^1(R, \mathcal{G}^{(\lambda^p)})$ is a trivial map.

Remark 4.7. We can describe more concretely Corollary 4.3 as follows.

Let p be a prime number, R an $\mathbb{F}_p$-algebra and $\lambda, a \in R$. Let C denote the Hopf R-algebra $R[T]/(T^p)$ with the comultiplication $T \mapsto T \otimes 1 + 1 \otimes T + \lambda T \otimes T$. Put $B = R[X]/(X^p - a)$. Then a structure of right C-comodule algebra is defined on B by

$$B \to B \otimes_R C : X \mapsto X \otimes 1 + 1 \otimes T + \lambda X \otimes T.$$

Define now a homomorphism of R-modules $\varphi : C \to B$ by

$$T^i \mapsto X^i \ (0 \leq i < p).$$

Then φ is a homomorphism of right C-comodules. Furthermore, if $1 + \lambda^p a$ is invertible in R, then φ is invertible for the convolution product in $\mathrm{Hom}_R(C, B)$, and therefore B is a cleft right C-comodule algebra. The convolution inverse of φ is given by

$$T^i \mapsto \Big(\frac{-X}{1+\lambda X}\Big)^i \ (0 \leq i < p).$$

Conversely, any cleft right C-comodule commutative algebra is isomorphic to a right C-comodule algebra of the form $B = R[X]/(X^p - a)$ with $a \in R$ such that $1 + \lambda^p a \in R^\times$.

Remark 4.8. Under the notations of Example 4.2, taking $\lambda = 1$, we obtain

$$\mathrm{Ker}[H^1(R, \boldsymbol{\mu}_p) \to \mathrm{Pic}(\boldsymbol{\mu}_{p,R}^\vee)] = \mathrm{Ker}[H^1(R, \boldsymbol{\mu}_p) \to \mathrm{Pic}(R)].$$

It should be mentioned that, for a scheme S, we have

$$\mathrm{Ker}[H^1(S, \boldsymbol{\mu}_n) \to \mathrm{Pic}(\boldsymbol{\mu}_{n,S}^\vee)] = \mathrm{Ker}[H^1(S, \boldsymbol{\mu}_n) \to \mathrm{Pic}(S)].$$

which is more or less known for a long time. For the reader's convenience, we recall an outline of the argument given by [1, Ch.III, 4.5.6].

Let S be a scheme. For an integer $n > 0$, put

$$\Gamma(S, \mathcal{O}_S)^\times / n = \mathrm{Coker}[n : \Gamma(S, \mathcal{O}_S)^\times \to \Gamma(S, \mathcal{O}_S)^\times],$$

$${}_n\mathrm{Pic}(S) = \mathrm{Ker}[n : \mathrm{Pic}(S) \to \mathrm{Pic}(S)].$$

Then the Kummer sequence

$$0 \longrightarrow \boldsymbol{\mu}_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \longrightarrow 0$$

induces an exact sequence

$$0 \longrightarrow \Gamma(S, \mathcal{O}_S)^\times / n \longrightarrow H^1(S, \boldsymbol{\mu}_n) \longrightarrow {}_n\mathrm{Pic}(S) \longrightarrow 0.$$

Now let $\mathcal{L}$ be an invertible $\mathcal{O}_S$-module. Assume that there exists an isomorphism of $\mathcal{O}_S$-modules $\alpha : \mathcal{L}^{\otimes n} \xrightarrow{\sim} \mathcal{O}_S$. Let $\mathcal{I}$ denote the ideal of the symmetric algebra $S_{\mathcal{O}_S}(\mathcal{L})$, generated by the local sections of the form $s - \alpha(s)$, where s is a local section of $\mathcal{L}^{\otimes n}$. Put $\mathcal{O}_{(\mathcal{L},\alpha)} = S_{\mathcal{O}_S}(\mathcal{L})/\mathcal{I}$. Then the $\mathcal{O}_S$-algebra $\mathcal{O}_{(\mathcal{L},\alpha)}$ is locally free of finite rank as an $\mathcal{O}_S$-module. Moreover an action of $\boldsymbol{\mu}_n$ on the $\mathcal{O}_S$-module $\mathcal{L}$ is defined by $(\zeta, s) \mapsto \zeta s$ and uniquely extended to an action $\boldsymbol{\mu}_n$ on the $\mathcal{O}_S$-algebra $\mathcal{O}_{(\mathcal{L},\alpha)}$.

Put $X_{(\mathcal{L},\alpha)} = \operatorname{Spec}\mathcal{O}_{(\mathcal{L},\alpha)}$. Then $X_{(\mathcal{L},\alpha)}$ is a $\boldsymbol{\mu}_n$-torsor over S. Moreover we have

$$H^1(S,\boldsymbol{\mu}_n) = \left\{ [X_{(\mathcal{L},\alpha)}] \; ; \begin{array}{l} \mathcal{L} \text{ is an invertible } \mathcal{O}_S\text{-module with } [\mathcal{L}] \in {}_n\mathrm{Pic}(S), \\ \alpha : \mathcal{L}^{\otimes n} \to \mathcal{O}_S \text{ is an isomorphism of } \mathcal{O}_S\text{-module} \end{array} \right\}.$$

It is verified also that the map $H^1(S,\boldsymbol{\mu}_n) \to {}_n\mathrm{Pic}(S)$ is given by $[X_{(\mathcal{L},\alpha)}] \mapsto [\mathcal{L}]$.

Example 4.9. Let p be a prime number > 2, R an $\mathbb{F}_p$-algebra, and $\lambda \in R$. Put $R_1 = R[\sqrt{\lambda}] = R[t]/(t^2-\lambda)$ and $\tilde{R}_1 = R[\sqrt{\lambda^p}] = R[t]/(t^2-\lambda^p)$. The Frobenius morphism

$$F : G_{R_1/R} = \operatorname{Spec} R[U,V]/(U^2 - \lambda V^2 - V) \to G_{\tilde{R}_1/R} = \operatorname{Spec} R[U,V]/(U^2 - \lambda^p V^2 - V)$$

is defined by $(U,V) \mapsto (U^p, V^p)$. Put $G = \mathrm{Ker}[F : G_{R_1/R} \to G_{\tilde{R}_1/R}]$. Then

$$\operatorname{Spec} R[U,V]/(U^2 - \lambda V^2 - V, U^p, V^p)$$

is equipped with the multiplication defined by

$$U \mapsto U\otimes 1 + 1\otimes U + 2\lambda U\otimes V + 2\lambda V\otimes U,\ V \mapsto V\otimes 1 + 1\otimes V + 2\lambda V\otimes V + 2U\otimes U.$$

Moreover there exist commutative diagrams of group schemes

$$\begin{array}{ccc} G & \longrightarrow & \displaystyle\prod_{G^\vee/R} \mathbb{G}_{m,G^\vee} \\ \big\downarrow \wr \text{ square} & & \big\downarrow \tilde{\chi} \\ G & \longrightarrow & G_{R_1/R} \end{array}$$

and

$$\begin{array}{ccc} G & \longrightarrow & G_{R_1/R} \\ \big\downarrow \wr \text{ square} & & \big\downarrow \tilde{\sigma} \\ G & \longrightarrow & \displaystyle\prod_{G^\vee/R} \mathbb{G}_{m,N} \end{array}$$

([16, Th.3.18]). This implies

$$\mathrm{Ker}[H^1(R,G) \to \mathrm{Pic}(G^\vee)] = \mathrm{Ker}[H^1(R,G) \to H^1(R, G_{R_1/R})].$$

Furthemore, we obtain the following corollaries.

Corollary 4.10. *Under the notations of Example 4.9, let S/R be an extension of ring. Then* $\operatorname{Spec} S$ *is a cleft G-torsor over* $\operatorname{Spec} R$ *if and only if there exist morphisms* $\operatorname{Spec} S \to G_{R_1/R}$ *and* $\operatorname{Spec} R \to G_{\tilde{R}_1/R}$ *such that the diagram*

$$\begin{array}{ccc} \operatorname{Spec} S & \longrightarrow & G_{R_1/R} \\ \downarrow & & \downarrow F \\ \operatorname{Spec} R & \longrightarrow & G_{\tilde{R}_1/R} \end{array}$$

is cartesian.

Corollary 4.11. *Under the notations of Example 4.9, the following are equivalent:*
(a) *Any G-torsor over R is cleft*;
(b) *The homomorphism $G_{\tilde{R}_1/R}(R) \to H^1(R, G)$ induced by the exact sequence*

$$0 \longrightarrow G \longrightarrow G_{R_1/R} \xrightarrow{F} G_{\tilde{R}_1/R} \longrightarrow 0.$$

is surjective;
(c) *The homomorphism $H^1(R, G_{R_1/R}) \to H^1(R, G_{\tilde{R}_1/R})$ induced by the Frobenius map $F : G_{R_1/R} \to G_{\tilde{R}_1/R}$ is injective.*

Remark 4.12. Assume that R is a local ring or λ is nilpotent, Then $H^1(R, G_{R_1/R})$ is annihilated by 2 (Suwa [13, Prop 4.3]). Moreover $H^1(R, G)$ is annihilated by p. It follows that all the G-torsor over $\operatorname{Spec} R$ is cleft.

Lemma 4.13. We can describe more concretely Corollary 4.10 as follows.

Let p be a prime number > 2, R an $\mathbb{F}_p$-algebra and $\lambda \in R$. Let C denote the Hopf R-algebra $R[U, V]/(U^2 - \lambda V^2 - V, U^p, V^p)$ with the comultiplication

$$U \mapsto U \otimes 1 + 1 \otimes U + 2\lambda U \otimes V + 2\lambda V \otimes U,\ V \mapsto V \otimes 1 + 1 \otimes V + 2\lambda V \otimes V + 2U \otimes U.$$

Note that $\{1, U, U^2, \ldots, U^{p-1}\}$ is a basis of R-module C.

In fact, an isomorphism of R_1-algebra

$$R_1[U, V]/(U^2 - \lambda V^2 - V, U^p, V^p) \xrightarrow{\sim} R_1[T](T^p)$$

is induced by

$$U \mapsto \frac{2T + \sqrt{\lambda}T^2}{4(1 + \sqrt{\lambda}T)},\ V \mapsto \frac{T^2}{4(1 + \sqrt{\lambda}T)}.$$

It follows that $\{1, U, U^2, \ldots, U^{p-1}\}$ is a basis of $R_1 \otimes_R C = R_1[U, V]/(U^2 - \lambda V^2 - V, U^p, V^p)$ over R_1. Hence we obtain the conclusion since R_1 is faithfully flat over R. It is verified also that $U^i V^j = 0$ for $i + 2j \geq p$.

Take now $a, b \in R$, and put $B = R[X, Y]/(X^2 - \lambda Y^2 - Y, X^p - a, Y^p - b)$. Then a structure of right C-comodule algebra is defined on B by

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

Furthermore a homomorphism of R-modules $\varphi : C \to B$ is defined by

$$U^i \mapsto X^i \ (0 \leq i < p).$$

Then φ is a homomorphism of right C-comodules. Furthermore, if $a^2 - \lambda^p b^2 - b = 0$, then φ is invertible for the convolution product in $\mathrm{Hom}_R(C, B)$, and therefore B is a cleft right C-comodule algebra. The convolution inverse of φ is given by

$$U^i \mapsto (-X)^i \ (0 \leq i < p).$$

Conversely, any cleft right C-comodule commutative algebra is isomorphic to a right C-comodule algebra of the form $B = R[X, Y]/(X^2 - \lambda Y^2 - Y, X^p - a, Y^p - b)$ with $a, b \in R$ such that $a^2 - \lambda^p b^2 - b = 0$.

Remark 4.14. It should be mentioned that Kreimer [7] proves the following assertion.

Let R be a local ring, C a Hopf R-algebra (not necessarily commutative) and B a right C-comodule algebra. Assume that (1) C is a free R-module of finite rank, (2) B/R is a Galois extension and R is contained in the center of B. Then B is a cleft right C-comodule algebra.

References

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

[2] Y. Doi, Equivalent crossed products for a Hopf algebra, Comm. Alg. **17** (1989), 3053–3085.

[3] Y. Doi, M. Takeuchi, Cleft comodule algebras for a bialgebra, Comm. Alg. **14** (1986), 801–817.

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

[5] A. Grothendieck, et al, Séminaire de Géométrie Algébrique 4, *Théorie des Topos et cohomologie étale*, Lecture Notes in Math. **269**, **270** (1972), and **305** (1973), Springer.

[6] A. Grothendieck, J. Dieudonné, *Éléments de géométrie algébrique* III, *premiére Partie,* Publ. Math. Inst. HES, no **11**, 1961.

[7] H. F. Kreimer, *Normal bases for Hopf algebras and Galois algebras*, Proc. Amer. Math. Soc. **130** (2002), 2853–2856.

[8] H. F. Kreimer, M. Takeuchi, *Hopf algebras and Galois extensions of an algebra*, Indiana Univ. Math. J. **30** (1981), 675–692.

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

[10] T. Sekiguchi and N. Suwa, *Some cases of extensions of group schemes over a discrete valuation ring*, I. J. Fac. Sci. Univ. Tokyo Sect. IA, Math. **38** (1991), 1–45.

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

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

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

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

[15] M. E. Sweedler, *Cohomology of algebras over Hopf algebras*, Trans. Amer. Math. Soc. **133** (1968), 205–239.
[16] Y. Tsuno, *Degeneration of the Kummer sequence in characteristic $p > 0$*, J. Théor. Nombres Bordeaux. **22**, (2010), 219–257.
[17] W. C. Waterhouse and B. Weisfeiler, *One-dimensional affine group schemes*, J. Algebra **66** (1980), 550–568.