Tohoku Math. J.
67 (2015), 495–505

GROUP ALGEBRAS AND NORMAL BASIS PROBLEM

NORIYUKI SUWA

(Received February 5, 2014, revised July 4, 2014)

Abstract. We formulate the notion of cleft extensions in the Hopf-Galois theory in the framework of algebraic geometry. The unit group scheme of the algebra of a finite flat group scheme plays a key role.

Introduction. The Kummer theory is an important item in the classical Galois theory to describe explicitly cyclic extensions of a field. We have an elementary way to verify the Kummer theory by the Lagrange resolvents. Serre [7, Ch.VI, 8] formulated this method, combining the normal basis theorem and the algebraic group representing the unit group of a group algebra. More precisely, the following assertion was proved:

— Let k be a field and Γ a finite group. Then any Galois extension K of k with group Γ is obtained by a cartesian diagram

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

Here $U(\Gamma)_k$ is the algebraic group over k representing the unit group $k[\Gamma]^\times$.

It is not difficult to formulate Serre's argument in the framework of group scheme theory over a ring as is done in [8]. In particular we have the following assertion:

— Let R be a ring, Γ a finite group and S an unramified Galois extension of R with group Γ. Then the Galois extension S/R has a normal basis if and only if there exists a cartesian diagram

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

Here $U(\Gamma)$ is the unit group scheme of the group algebra of Γ. (A definition of $U(\Gamma)$ is recalled in Example 2.8.)

In this article we generalize the above assertion to Hopf-Galois extensions as follows: Let R be a ring and C a commutative Hopf R-algebra such that C is a projective R-module of finite rank. Then a commutative C-comodule algebra S is cleft over R if and only if there

---

2010 *Mathematics Subject Classification.* Primary 13B05; Secondary 14L15, 12G05.

Key words and phrases. Group scheme, Hopf-Galois extension, cleft extension.

Partially supported by Grant-in-Aid for Scientific Research No. 23540027.

exists a cartesian diagram

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

Here $U(G)$ is the unit group scheme of the group algebra of the finite flat group scheme $G = \operatorname{Spec} C$(Theorem 3.2). For the definition of $U(G)$, see Definitions 2.5 and 2.7.

We state and prove our main result in a more general setting. It should be mentioned that, when C is cocommutative, the theorem is stated in Tsuno [10]. Indeed, the group scheme $U(G)$ is isomorphic to the Weil restriction $\prod_{C^\vee/R} \mathbb{G}_{m,C^\vee}$, where $C^\vee$ denotes the Cartier dual of C, as is verified in Example 2.9.

It should be mentioned also that the notion of a cleft C-comodule algebra was introduced by Doi and Takeuchi [4]. Here C is a Hopf R-algebra (not necessarily commutative). They proved that a C-comodule algebra S is cleft if and only if S/R is a C-Galois extension with normal basis [4, Th.9].

Now we explain the organization of the article. In Section 1, we recall needed facts on coalgebras, bialgebras and comodules. In Section 2, for a finite flat group S-scheme G, we define an affine group S-scheme $U(G)$, the unit group scheme of the group algebra of G. Our main result is mentioned and proved in Section 3.

It should be remarked that related results were estabished by Aljadeff-Kassel [1] and Kassel-Masuoka [5] in the framework of the Hopf-Galois theory over fields. It would be interseting to generalize our main result, including non-commutative cases and removing the assumption on Hopf algebras to be finite over a base ring, and to give a geometric interpretation of their works as is done in this article.

The author would like to express his hearty thanks to the hospitality of Università degli studi di Padova. In particular he is very grateful to Marco Garuti for valuable discussions. This work began with a conversation along a canal of Padova. The author thanks also Akira Masuoka for his introduction to trends in the Hopf-Galois theory. Finally he highly appreciates useful remarks by the referee.

NOTATION. For a ring R, $R^\times$ denotes the multiplicative group of invertible elements of R. A ring is commutative unless otherwise mentioned.

For a scheme X and a group scheme G over X, $H^1(X, G)$ denotes the set of isomorphism classes of right G-torsors over X. (For details we refer to Demazure-Gabriel [3, Ch.III, 4].)

1. Cleft extensions. In the section, A denotes a commutative ring. We refer to [4] and [6] for detailed argument on coalgebras, bialgebras and comodules.

DEFINITION 1.1. Let C be an A-module, and let $\varDelta : C \to C \otimes_A C$ and $\varepsilon : C \to A$ be homomorphisms of A-modules. The triple $(C, \varDelta, \varepsilon)$ is called an A-coalgebra if $(\varDelta \otimes I_C) \circ \varDelta = (I_C \otimes \varDelta) \circ \varDelta$ and $(\varepsilon \otimes I_C) \circ \varDelta = I_C = (I_C \otimes \varepsilon) \circ \varDelta$ hold. The maps $\varDelta$ and ε are called the comultiplication and the counit, respectively, of the coalgebra C.

An A-coalgebra (C, Δ, ε) is called cocommutative if $T \circ \Delta = \Delta$ holds. Here $T : C \otimes_A C \to C \otimes_A C$ denotes the twist map defined by $T(a \otimes b) = b \otimes a$.

Let (C, Δ, ε) and $(C', \Delta', \varepsilon')$ be A-coalebras. A homomorphism of A-modules $\varphi : C \to C'$ is called a homomorphism of A-coalgebras if $(\varphi \otimes \varphi) \circ \Delta = \Delta' \circ \varphi$ and $\varepsilon = \varepsilon' \circ \varphi$ hold.

DEFINITION 1.2. Let (C, Δ, ε) be an A-coalgebra, M an A-module and $\rho : M \to M \otimes_A C$ a homomorphism of A-modules. The pair (M, ρ) is called a right C-comodule if $(\rho \otimes I_C) \circ \rho = (I_M \otimes \Delta) \circ \rho$ and $(I_M \otimes \varepsilon) \circ \rho = I_M$ hold.

Let (C, Δ, ε) be an A-coalgebra, and let (M, ρ) and (M', ρ') be right C-comodules. A homomorphism of A-modules $f : M \to M'$ is called a homomorphism of right C-comodules if $(f \otimes I_C) \circ \rho = \rho' \circ f$ holds.

DEFINITION 1.3. Let C be an A-coalgebra and B an A-algebra (not necessarily commutative). For $\varphi, \psi \in \mathrm{Hom}_A(C, B)$, the convolution product $\varphi * \psi$ is defined by $\varphi * \psi = \mu_B \circ (\varphi \otimes \psi) \circ \Delta_C$. Here $\mu_B : B \otimes_A B \to B$ denotes the multiplication of the algebra B. The A-module $\mathrm{Hom}_A(C, B)$ is an A-algebra equipped with the multiplication $*$. The neutral element of the algebra $\mathrm{Hom}_A(C, B)$ is given by the composite $u \circ \varepsilon : C \to B$, where $u : A \to B$ is the structure map.

DEFINITION 1.4. An A-coalgebra (C, Δ, ε) is called an A-bialgebra if C is an A-algebra (not necessarily commutative) and the maps $\Delta : C \to C \otimes_A C$ and $\varepsilon : C \to A$ are homomorphisms of A-algebras. Moreover, the bialgebra C is called an Hopf algebra over A if there exists an A-homomorphism $s : C \to C$ such that $\mu \circ (s \otimes I_C) \circ \Delta = u \circ \varepsilon = \mu \circ (I_C \otimes s) \circ \Delta$ holds. The map s is called the antipode of the Hopf algebra C.

Here is an important example of a bialgebra or a Hopf algebra.

EXAMPLE 1.5. Let Γ be a finite semi-group. Put $C = \mathrm{Hom}_A(A[\Gamma], A)$, where $A[\Gamma]$ denotes the semi-group algebra of Γ over A. Then C has a structure of A-bialgebra. More precisely, an addtion and a multiplication of C are defined by the addtion and the multiplication of A, respectively. On the other hand, a comultiplication and a counit of C are defined by the the multiplication of $A[\Gamma]$ and by the sturcure homomorphism $A \to A[\Gamma]$, repectively. The semi-group scheme $\mathrm{Spec}\, C$ is nothing but the constant semi-group scheme over A defined by Γ. By abbreviation we denote by Γ also the constant semi-group scheme $\mathrm{Spec}\, C$.

Assume now that Γ is a group. Then C has a structure of Hopf A-algebra. Indeed, the correspondence $\gamma \mapsto \gamma^{-1}$ gives rise to an automorphism of A-module $A[\Gamma]$, which defines an antipode of C. The group scheme $\mathrm{Spec}\, C$ is nothing but the constant group scheme over A defined by Γ.

DEFINITION 1.6. Let (C, Δ, ε) be an A-bialgebra and (B, ρ) a right C-comodule. We say that B is a C-comodule algebra or that C coacts to the right on B if B is an A-algebra (not necessarily commutative) and the map $\rho : B \to B \otimes_A C$ is a homomorphism of A-algebras. Put $B^C = \{b \in B \ ; \ \rho(b) = b \otimes 1\}$. Then B^C is a sub-A-algebra of B. B^C is called the invariant subring of the C-comodule algebra B.

EXAMPLE 1.7. Let Γ be a finite semi-group, $C = \mathrm{Hom}_A(A[\Gamma], A)$ and (B, ρ) a C-comodule algebra. For $\gamma \in \Gamma$ we define $e_\gamma \in C$ by

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

Then $\{e_\gamma\}_{\gamma \in \Gamma}$ is a basis of the A-module C.

Furhtermore, for $b \in B$ and $\gamma \in \Gamma$, we define $\gamma(b) \in B$ by

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

It is readily seen that $(\gamma, b) \mapsto \gamma(b) : \Gamma \times B \to B$ is a left action of Γ on B and that the invariant subring B^C of the C-comodule algebra B coincides with the invariant subring B^Γ of B by the action of Γ.

DEFINITION 1.8. Let C be an A-bialgebra. A C-comodule algebra B is called *cleft* if there exists $\varphi : C \to B$ a homomorphism of A-module which is compatible with the coactions by C and invertible for the convolution product.

EXAMPLE 1.9. Let Γ be a finite group, $C = \mathrm{Hom}_A(A[\Gamma], A)$ and (B, ρ) a C-comodule algebra (not nesessarily commutative). Then B is cleft if and only if B is a Γ-Galois extension with normal basis. (For detailed accounts, we refer to [6] and [4].) Recall that, by definiton, a Γ-Galois extension B/A admits a normal basis if there exists $b \in B$ such that $\{\gamma(b)\}_{\gamma \in \Gamma}$ is a basis of the A-module B.

Assume now that B is commutative. Then B is a Γ-Galois extension if and only if $\mathrm{Spec}\, B$ has a structure of Γ-torisor over $\mathrm{Spec}\, A$.

REMARK 1.10. Let S be a scheme. We can generalize the definitions mentioned above in the category of $\mathcal{O}_S$-modules. In particular, the functor $\mathcal{C} \mapsto \mathrm{Spec}\,\mathcal{C}$ gives rise to anti-equivalences of categories

$$\{\text{quasi-coherent commutative } \mathcal{O}_S\text{-bialgebras}\} \xrightarrow{\sim} \{\text{semi-group } S\text{-schemes affine over } S\}$$

and

$$\{\text{quasi-coherent commutative Hopf } \mathcal{O}_S\text{-algebras}\} \xrightarrow{\sim} \{\text{group } S\text{-schemes affine over } S\} \,.$$

DEFINITION 1.11. Let S be a scheme, G a group S-scheme affine over S and X a right G-torsor over S. We shall say that the G-torsor X is cleft if the $\mathcal{O}_G$-comodule algebra $\mathcal{O}_X$ is cleft.

2. $A(G)$ **and** $U(G)$**.** First we recall a definition of the group algebra $A(G)$ of an affine group scheme G. We refer to [2] for generalities on group algebras. We follow the notations of [3] and [11] concerning affine group schemes.

2.1. Let S be a scheme and $(\mathcal{C}, \Delta, \varepsilon)$ an $\mathcal{O}_S$-coalgebra. Let $S(\mathcal{C})$ denote the symmetric $\mathcal{O}_S$-algebra associated to the $\mathcal{O}_S$-module $\mathcal{C}$. Then $S(\mathcal{C})$ has a strucute of an $\mathcal{O}_S$-bialgebra.

Indeed, a comultiplication of $S(\mathcal{C})$ is given by the $\mathcal{O}_S$-algerbra homomorphism $S(\mathcal{C}) \to S(\mathcal{C}) \otimes_{\mathcal{O}_S} S(\mathcal{C})$, the unique extension of the $\mathcal{O}_S$-homomorphism

$$a \mapsto \Delta(a) : \mathcal{C} \to \mathcal{C} \otimes_{\mathcal{O}_S} \mathcal{C} \to S(\mathcal{C}) \otimes_{\mathcal{O}_S} S(\mathcal{C}),$$

and a counit of $S(\mathcal{C})$ by the $\mathcal{O}_S$-algerbra homomorphism $S(\mathcal{C}) \to \mathcal{O}_S$, the unique extension of the $\mathcal{O}_S$-homomorphism $\varepsilon : \mathcal{C} \to \mathcal{O}_S$. It is readily seen that the canonical inclusion $i : \mathcal{C} \to S(\mathcal{C})$ is a homomorphism of $\mathcal{O}_S$-coalgebras.

The correspondence $\mathcal{C} \mapsto S(\mathcal{C})$ defines a covariant functor from the category of $\mathcal{O}_S$-coalgebras to that of commutative $\mathcal{O}_S$-bialgebras, which is left-adjoint of the forgetful functor. More precisely, let $\mathcal{B}$ be a commutative $\mathcal{O}_S$-bialgebra and $\varphi : \mathcal{C} \to \mathcal{B}$ a homomorhism of $\mathcal{O}_S$-coalgebras. Then φ is extended to a homomorhism $\mathcal{O}_S$-bialgebras $\tilde{\varphi} : S(\mathcal{C}) \to \mathcal{B}$ by

$$\tilde{\varphi}(a_1 \otimes a_2 \otimes \cdots \otimes a_r) = \varphi(a_1)\varphi(a_2) \cdots \varphi(a_r)\,.$$

Moreover $\varphi \mapsto \tilde{\varphi}$ gives rise to a bijection $\mathrm{Hom}_{\mathcal{O}_S-\mathrm{coalg}}(\mathcal{C}, \mathcal{B}) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_S-\mathrm{bialg}}(S(\mathcal{C}), \mathcal{B})$. Indeed, the inverse is given by $\psi \mapsto \psi \circ i$.

2.2. Assume now $\mathcal{C}$ is a quasi-coherent commutaive $\mathcal{O}_S$-bialgebra. Then $G = \operatorname{Spec} \mathcal{C}$ is an semigroup scheme affine over S.

Furthermore $S(\mathcal{C})$ is a quasi-coherent commutative $\mathcal{O}_S$-algebra. Put now $A(G) = \operatorname{Spec} S(\mathcal{C})$. Then $A(G)$ is equipped with a ring structure. Indeed, the multiplication of $A(G)$ is defined by the comultiplication $\Delta : S(\mathcal{C}) \to S(\mathcal{C}) \otimes_{\mathcal{O}_S} S(\mathcal{C})$. Moreover the addition of $A(G)$ is defined by the $\mathcal{O}_S$-algebra homomorphism $S(\mathcal{C}) \to S(\mathcal{C}) \otimes_{\mathcal{O}_S} S(\mathcal{C})$, the unique extension of the $\mathcal{O}_S$-homomorphism

$$a \mapsto a \otimes 1 + 1 \otimes a : \mathcal{C} \to S(\mathcal{C}) \otimes_{\mathcal{O}_S} S(\mathcal{C})\,.$$

We call the ring S-scheme $A(G)$ the group algebra of the group scheme $G = \operatorname{Spec} \mathcal{C}$.

Let $\pi : S(\mathcal{C}) \to \mathcal{C}$ denote the homomorphism of $\mathcal{O}_S$-algebras defined by $s_1 \otimes s_2 \otimes \cdots \otimes s_j \mapsto s_1 s_2 \cdots s_j$. Then π is surjective. Let $\iota : G \to A(G)$ denote the closed immersion defined by π. The morphism $\iota : G \to A(G)$ is a homomorphism of multiplicative semigroups.

The comultiplication $S(\mathcal{C}) \to S(\mathcal{C}) \otimes_{\mathcal{O}_S} S(\mathcal{C})$ induces the right coaction $S(\mathcal{C}) \to S(\mathcal{C}) \otimes_{\mathcal{O}_S} \mathcal{C}$. The canonical injection of $\mathcal{O}_S$-modules $i : \mathcal{C} \to S(\mathcal{C})$ is a homomorphism of $\mathcal{C}$-comodules.

REMARK 2.3. The ring S-scheme $A(G)$ represents the functor defined by $T \mapsto \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{C}, \mathcal{O}_T)$ equipped with the convolution product.

More precisely, let T be an affine S-scheme. Then we have

$$A(G)(T) = \mathrm{Hom}_{\mathcal{O}_S-\mathrm{alg}}(S(\mathcal{C}), \mathcal{O}_T) = \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{C}, \mathcal{O}_T)\,.$$

It is readily seen that the addition of $A(G)(T)$ coincide with the addition of $\mathrm{Hom}_{\mathcal{O}_S}(\mathcal{C}, \mathcal{O}_T)$. On the other hand, the multiplication of $A(G)(T)$ is the convolution of $\mathrm{Hom}_{\mathcal{O}_S}(\mathcal{C}, \mathcal{O}_T)$ since, for $\varphi, \psi \in \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{C}, \mathcal{O}_T)$, the convolution product $\varphi * \psi$ is defined by $\varphi * \psi = \mu \circ (\varphi \otimes \psi) \circ \Delta$.

Furthermore the map $\iota : G(T) \to A(G)(T)$ is nothing but the inclusion $\mathrm{Hom}_{\mathcal{O}_S-\mathrm{alg}}(\mathcal{C}, \mathcal{O}_T) \to \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{C}, \mathcal{O}_T)$.

EXAMPLE 2.4. Let Γ be a finite semigroup. Put $C = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\Gamma], \mathbb{Z})$. Then $\mathrm{Spec}\, C$ is the constant semigroup scheme Γ over $\mathbb{Z}$.

Now let $\{e_\gamma\}_{\gamma\in\Gamma}$ denote the dual basis for the basis $\{\gamma\}_{\gamma\in\Gamma}$ of $\mathbb{Z}[\Gamma]$. The comultiplication on C is given by

$$\Delta(e_\gamma) = \sum_{\gamma'\gamma''=\gamma} e_{\gamma'} \otimes e_{\gamma''} .$$

Furthermore we have $A(\Gamma) = \mathrm{Spec}\, \mathbb{Z}[T_\gamma; \gamma \in \Gamma]$, where the addition of $A(\Gamma)$ is given by

$$T_\gamma \mapsto T_\gamma \otimes 1 + 1 \otimes T_\gamma$$

and the multiplication by

$$T_\gamma \mapsto \sum_{\gamma'\gamma''=\gamma} T_{\gamma'} \otimes T_{\gamma''} .$$

For a ring R, $A(\Gamma)(R)$ is nothing but the semigroup algebra $R[\Gamma]$.

DEFINITION 2.5. Let S be a scheme and G an affine group scheme over S. Define a functor $U(G)$ by $U(G)(T) = A(G)(T)^\times$. Then $U(G)$ is a sheaf of groups for the fppf-topolgy over S. The morphism $\iota : G \to A(G)$ is factorized as $G \to U(G) \to A(G)$. We denote also by ι the morphism of sheaves $G \to U(G)$. Then $\iota : G \to U(G)$ is a homomorphism of groups.

THEOREM 2.6. *Let S be a scheme and G an affine group scheme over S. Assume that $\mathcal{O}_G$ is a locally free $\mathcal{O}_S$-module of finite rank. Then:*
(1) $A(G)$ is smooth over S;
(2) $U(G)$ is represented by an affine open subscheme of $A(G)$, and therefore smooth over S.
(3) $\iota : G \to U(G)$ is a closed immersion.

PROOF. (1) By locality of the problem, we may assume that $S = \mathrm{Spec}\, A$, $G = \mathrm{Spec}\, C$ and C is a free A-module of finite rank. Take a basis $\{e_1, e_2, \dots, e_n\}$ of C over A. For each j, let T_j denote the image of e_j by the canonical injection $C \to S_A(C)$. Then $S_A(C)$ is isomorphic to the polynomial algebra $A[T_1, T_2, \dots, T_n]$, which implies that $A(G) = \mathrm{Spec}\, S_A(C)$ is smooth over A.
(2) Define a linear form $R_{ij}(e_1, e_2, \dots, e_n) = \sum_{k=1}^n a_{ijk} e_k$ $(a_{ijk} \in A)$ for each (i, j) by

$$\Delta_C(e_j) = \sum_{i=1}^n e_i \otimes R_{ij}(e_1, e_2, \dots, e_n) .$$

The matrix $(R_{ij})_{1\le i,j\le n}$ is nothing but the right regular representation of the bialgebra C with respect to the basis $\{e_1, e_2, \dots, e_n\}$.

The multiplication of $A(G) = \mathrm{Spec}\, A[T_1, T_2, \dots, T_n]$ is defined by

$$T_j \mapsto \sum_{j=1}^n T_i \otimes R_{ij}(T_1, T_2, \dots, T_n) ,$$

where $R_{ij}(T_1, T_2, \dots, T_n) = \sum_{k=1}^n c_{ijk} T_k$.

More precisely, let R be an A-algebra. Then the additive group $A(G)(R)$ is isomorphic to the direct sum R^n, and the multiplication of $A(G)(R)$ is given by

$$\begin{aligned}&(a_1, a_2, \dots ,a_n)(b_1, b_2, \dots ,b_n)\\ &= \left(\sum_{i=1}^{n} a_i R_{i1}(b_1, b_2, \dots, b_n), \sum_{i=1}^{n} a_i R_{i2}(b_1, b_2, \dots, b_n), \dots, \sum_{i=1}^{n} a_i R_{in}(b_1, b_2, \dots, b_n)\right).\end{aligned}$$

By the coassociativity of Δ_C, we have also

$$\begin{aligned}&(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n)\\ &= \left(\sum_{j=1}^{n} R_{1j}(a_1, a_2, \dots, a_n) b_j, \sum_{j=1}^{n} R_{2j}(a_1, a_2, \dots, a_n) b_j, \dots, \sum_{j=1}^{n} R_{nj}(a_1, a_2, \dots, a_n) b_j\right).\end{aligned}$$

Hence $(a_1, a_2, \dots, a_n) \in A(G)(R)$ is invertible if and only if $\det(R_{ij}(a_1, a_2, \dots, a_n))$ is invertible in R.

Thus we obtain

$$U(G) = \operatorname{Spec} A\left[T_1, T_2, \dots, T_n, \frac{1}{\Delta}\right],$$

where $\Delta = \det(R_{ij}(T_1, T_2, \dots, T_n))$. This implies the assertion.

(3) We obtain the conclusion, noting that the composite $G \xrightarrow{\iota} U(G) \to A(G)$ is a closed immersion and the embedding $U(G) \to A(G)$ is an affine morphism. □

DEFINITION 2.7. We shall call the group S-scheme $U(G)$ the unit group scheme of the group algebra of the finite flat group scheme $G = \operatorname{Spec} \mathcal{C}$.

EXAMPLE 2.8. Let Γ be a finite group. Then $U(\Gamma)$ is nothing but the unit group scheme of the group algebra of Γ. That is to say, for a ring R, we have $U(\Gamma)(R) = R[\Gamma]^\times$.

More explicitly, we have

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

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).

EXAMPLE 2.9. Let G be an affine commutative group scheme over S such that $\mathcal{O}_G$ is a locally free $\mathcal{O}_S$-module of finite rank. Then $U(G)$ is isomorphic to the Weil restriction $\prod_{G^\vee/S} \mathbb{G}_{m,G^\vee}$.

Indeed, let T be an S-scheme affine over S. Then we have functorial isomorphisms of $\mathcal{O}_S$-algebras

$$\operatorname{Hom}_{\mathcal{O}_S}(\mathcal{O}_G, \mathcal{O}_T) \xrightarrow{\sim} \operatorname{Hom}_{\mathcal{O}_S}(\mathcal{O}_G, \mathcal{O}_S) \otimes_{\mathcal{O}_S} \mathcal{O}_T \xrightarrow{\sim} \mathcal{O}_{G^\vee} \otimes_{\mathcal{O}_S} \mathcal{O}_T$$

since $\mathcal{O}_G$ is a locally free $\mathcal{O}_S$-module of finite rank. It is now sufficient to note that the functors $T \mapsto \operatorname{Hom}_{\mathcal{O}_S}(\mathcal{O}_G, \mathcal{O}_T)^\times$ and $T \mapsto (\mathcal{O}_{G^\vee} \otimes_{\mathcal{O}_S} \mathcal{O}_T)^\times$ are represented by $U(G)$ and $\prod_{G^\vee/S} \mathbb{G}_{m,G^\vee}$, respectively.

REMARK 2.10. Let k be a field. Takeuchi constructed in [9] a covariant functor $C \mapsto H(C)$ from the category of k-coalgebras to that of commutative Hopf k-algebras, which is a left adjoint of the forgetful functor. The Hopf algebra $H(C)$ is called the free Hopf algebra generated by C. Aljadeff and Kassel gave a different description of $H(C)$ in [1, Appendix B]. They denote by $S(C)_\Theta$ the free Hopf algebra generated by C. (We employ here a slightly different notation from theirs.) It is not difficult to verify that, if C is a finite dimensional Hopf k-algebra and $G = \operatorname{Spec} C$, the affine ring of $U(G)$ coincides with $H(C)$.

3. Main theorem.

PROPOSITION 3.1. *Let S be a scheme and G an affine group scheme over S. Assume that $\mathcal{O}_G$ is a locally free $\mathcal{O}_S$-module of finite rank. Then $U(G)$ is a cleft G-torsor over $U(G)/G$.*

PROOF. Let $S(\mathcal{O}_G)[1/\Delta]$ denote the quasi-coherent $\mathcal{O}_S$-algebra with $\operatorname{Spec} S(\mathcal{O}_G)[1/\Delta] = U(G)$. We denote by $i : \mathcal{O}_G \to S(\mathcal{O}_G)[1/\Delta]$ also the composite of the canonical injections of $\mathcal{O}_S$-modules $\mathcal{O}_G \to S(\mathcal{O}_G)$ and $S(\mathcal{O}_G) \to S(\mathcal{O}_G)[1/\Delta]$. Then i is a homomorphism of $\mathcal{O}_G$-comodules. Futhermore i is invertible for the convolution products.

Now we give a detailed account for the reader's convenience though it would be a standard fact that $s \circ i$ is the inverse of i for the convolution products. Here s is the antipode of the Hopf $\mathcal{O}_S$-algebra $S(\mathcal{O}_G)[1/\Delta]$.

As in the proof of Theorem 2.6, we may assume that $S = \operatorname{Spec} A$, $G = \operatorname{Spec} C$ and C is a free A-module of finite rank. Take a basis $\{e_1, e_2, \dots, e_n\}$ of C over A. Let T_j denote the image of e_j by $i : \mathcal{O}_G \to S(\mathcal{O}_G)[1/\Delta]$ or equivalently $i : C \to S_A(C)[1/\Delta]$.

Furthermore we may assume that $e_1 = 1$ and $\varepsilon_C(e_j) = 0$ for $j > 1$ since the A-module C is a direct sum of A and $\operatorname{Ker} \varepsilon_C$. Then we obtain $R_{1j}(T_1, \dots, T_n) = T_j$ for each j since we have

$$e_j = (\varepsilon_C \otimes I_C)(\Delta_C(e_j)) = (\varepsilon_C \otimes I_C)\left(\sum_{i=1}^{n} e_i \otimes R_{ij}(e_1, \dots, e_n)\right) = R_{1j}(e_1, \dots, e_n)\,.$$

For each i, let Δ_i denote the $(i, 1)$-cofactor of the matrix $(R_{ij}(T_1, \dots, T_n))_{i,j}$. Then we obtain

$$\sum_{i=1}^{n} \Delta_j R_{ij}(T_1, \dots, T_n) = \begin{cases} \Delta & (j = 1) \\ 0 & (i \neq 1) \end{cases}.$$

Now define a homomorphism of A-modules $\psi : C \to S_A(C)[1/\Delta]$ by

$$\psi(e_i) = \frac{\Delta_i}{\Delta}\ (1 \leq i \leq n)\,.$$

Then we have $\psi * i = i * \psi = I_C$. □

THEOREM 3.2. *Let S be a scheme and G an affine group scheme over S. Assume that $\mathcal{O}_G$ is a locally free $\mathcal{O}_S$-module of finite rank. Then a G-torsor X over S is cleft if and only if* *there exists a cartesian diagram*

$$\begin{array}{ccc} X & \longrightarrow & U(G) \\ \downarrow & & \downarrow \\ S & \longrightarrow & U(G)/G\,. \end{array}$$

PROOF. Assume that there exists a cartesian diagram

$$\begin{array}{ccc} X & \longrightarrow & U(G) \\ \downarrow & & \downarrow \\ S & \longrightarrow & U(G)/G\,. \end{array}$$

Then X is a cleft G-torsor over S since $U(G)$ is a cleft G-torsor over $U(G)/G$.

Conversely assume that the G-torsor X is cleft. Then there exists a homomorphism of $\mathcal{O}_G$-comodules $\varphi : \mathcal{O}_G \to \mathcal{O}_X$ which invertible for the convolution product in $\mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_G, \mathcal{O}_X)$. By the universality, the homomorphism of $\mathcal{O}_S$-modules φ is extented to a homomorphism of $\mathcal{O}_S$-algebras $\tilde{\varphi} : S(\mathcal{O}_G) \to \mathcal{O}_X$. It is readily seen that $\tilde{\varphi}$ is compatible with the coactions by $\mathcal{O}_G$. We will prove that the homomorphism $\tilde{\varphi} : S(\mathcal{O}_G) \to \mathcal{O}_X$ is extended to a homomorphism of $\mathcal{O}_S$-algebras $\tilde{\varphi} : S(\mathcal{O}_G)[1/\varDelta] \to \mathcal{O}_X$.

Let $\psi : \mathcal{O}_G \to \mathcal{O}_X$ denote the inverse of φ. Then we have

$$\sum_{k=1}^{n} \varphi(R_{ik})\psi(R_{kj}) = \begin{cases} 1 & (i = j) \\ 0 & (i \neq j) \end{cases}$$

since

$$\varDelta_{\mathcal{O}_G}(R_{ij}) = \sum_{k=1}^{n} R_{ik} \otimes R_{kj}$$

and

$$\varepsilon_{\mathcal{O}_G}(R_{ij}) = \begin{cases} 1 & (i = j) \\ 0 & (i \neq j) \end{cases}.$$

Then the matrix $(\varphi(R_{ij}))$ is invertible with inverse $(\psi(R_{ij}))$. This implies that $\tilde{\varphi} : S(\mathcal{O}_G) \to \mathcal{O}_X$ is extended to a homomorphism of $\mathcal{O}_S$-algebras $\tilde{\varphi} : S(\mathcal{O}_G)[1/\varDelta] \to \mathcal{O}_X$. Hence we obtain a cartesian diagram

$$\begin{array}{ccc} X & \longrightarrow & U(G) \\ \downarrow & & \downarrow \\ S & \longrightarrow & U(G)/G\,. \end{array}$$

□

REMARK 3.3. Under the assumption of Theorem 3.1, the sequence of sheaves over S with values in pointed sets

$$1 \longrightarrow G \xrightarrow{\iota} U(G) \longrightarrow U(G)/G \longrightarrow 1\,,$$

is exact with respect to the fppf-topology. Then we obtain an exact sequence of pointed sets

$$U(G)(S) \longrightarrow (U(G)/G)(S) \longrightarrow H^1(S,G) \longrightarrow H^1(S,U(G))$$

(cf. Demazure-Gabriel [3, Ch.III, Prop.4.6].)

Let X be a G-torsor over S. Then $[S] \in \mathrm{Im}[(U(G)/G)(S) \to H^1(S,G)]$ if and only if there exists a cartesian diagram

$$\begin{tikzcd} X \arrow[r] \arrow[d] & U(G) \arrow[d] \\ S \arrow[r] & U(G)/G\,. \end{tikzcd}$$

Hence it follows from Corollary 3.2 that the G-torsor X over S is cleft if and only if $[X] \in \mathrm{Ker}[H^1(S,G) \to H^1(S,U(G))]$.

REMARK 3.4. We conclude the article, mentioning related results in the Hopf-Galois theory.

Let k be a field and C a Hopf k-algebra. Aljadeff and Kassel introduced a subalgebra $\mathcal{B}_C$ of $S(C)_\Theta = H(C)$ in [1, Sect.5] and a cleft Hopf-Galois extension $\mathcal{A}_C$ of $\mathcal{B}_C$ with Hopf algebra C in [1, Sect.6]. (We employ again slightly different notations from theirs.)

Kassel and Masuoka proved remarkable theorems as follow.

(1) ([5, Th.3.6]) If C is of finite dimension over k, then $S(C)_\Theta$ is a projective $\mathcal{B}_C$-module of finite rank.

(2) ([5, Th.3.8]) If C is cocommutative, then $S(C)_\Theta$ is faithfully flat over $\mathcal{B}_C$.

(3) ([5, Th.3.13]) If C is commutative, then $S(C)_\Theta = \mathcal{A}_C$ and $S(C)_\Theta$ is a free $\mathcal{B}_C$-module.

They asserted also an important remark in the last phrase of [5, Sect.1] as follows:

— Let K be an extension field of k. Assume that $S(C)_\Theta$ is faithfully flat over $\mathcal{B}_C$. Then any cleft C-Galois extension R of K is obtained by a cocartesian diagram of k-algebras

$$\begin{tikzcd} R & \mathcal{A}_C \arrow[l] \\ K \arrow[u] & \mathcal{B}_C\,. \arrow[l] \arrow[u] \end{tikzcd}$$

Theorem 3.2 gives a geometric interpretation of the above results when $\mathcal{C}$ is a commutaitve Hopf $\mathcal{O}_S$-algebra and a locally free $\mathcal{O}_S$-module of finite rank.

REFERENCES

[1] E. ALJADEFF and C. KASSEL, Polynomial identities and noncommutative verasal torsors, Adv. Math. 218 (2008), 1453–1495.

[2] A. ÁLVAREZ, C. SANCHO and P. SANCHO, Algebra schemes and their representations, J. Alg. 296 (2006), 110–144.

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

[4] Y. DOI and M. TAKEUCHI, Cleft comodule algebras for a bialgebra, Comm. Alg. 14 (1986), 3053–3085.

[5] C. KASSEL and A. MASUOKA, Flatness and freeness properties of the generic Hopf Galois extensions, Revista de la Unión Mathemática Argentina 51 (2010), 79–94.

[6] H. F. KREIMER and M. TAKEUCHI, Hopf algebras and Galois extensions of an algebra, Indiana Univ. Math. J. 30 (1981), 675–692.

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

[8] N. SUWA, Around Kummer theories. RIMS Kôkyûroku Bessatsu B12 (2009), 115–148.

[9] M. TAKEUCHI, Free Hopf algebras generated by coalgebras, J. Math. Soc. Japan 23 (1971), 561–582.

[10] Y. TSUNO, Normal basis problem for torsors under a finite flat group scheme, RIMS Kôkyûroku Bessatsu, B25, Res. Inst. Math. Sci. (RIMS), Kyoto, 2011.

[11] W. C. WATERHOUSE, *Introduction to affine group schemes*, Springer, 1979.

DEPARTMENT OF MATHEMATICS
CHUO UNIVERSITY
1–13–27 KASUGA
BUNKYO-KU
TOKYO 112–8551
JAPAN

E-mail address: suwa@@math.chuo-u.ac.jp