ON ACTIONS OF INFINITESIMAL GROUP SCHEMES

GAETANA RESTUCCIA AND HANS-JÜRGEN SCHNEIDER

1. Introduction

Let k be a field of characteristic $p > 0$ and H a finite-dimensional commutative Hopf algebra over k with underlying algebra

$$(1.1) \quad H = k[X_1, \dots, X_n]/(X_1^{p^{s_1}}, \dots, X_n^{p^{s_n}}), n \geq 1, s_1 \geq \cdots \geq s_n \geq 1.$$

By the structure theorem of infinitesimal, that is finite and connected group schemes (see [W, 14.4]), any finite-dimensional, commutative and local Hopf algebra over a perfect field has this form.

Let A be a commutative algebra, and $\delta : A \to A \otimes H$, a right H-comodule algebra structure on A.

In other words, we are considering an action

$$X \times G \to X$$

of the infinitesimal group scheme represented by H on the affine scheme represented by A.

For any $a \in A$, we can write

$$\delta(a) = a \otimes 1 + \sum_{1 \leq i \leq n} D_i(a) \otimes x_i + \text{ terms of higher order in the } x_i,$$

where the x_i are the residue classes of the X_i in H, and where $D_i : A \to A, 1 \leq i \leq n$, are k-linear derivations of A.

Let $R = A^{coH}$ be the subalgebra of A of coinvariant elements under the coaction δ. The extension $R \subset A$ is called an H-Galois extension (see [M]) (and the projection $X \to Y$ represented by the inclusion $R \subset A$ is called a principal homogeneous space for G) if the canonical map

$$A \otimes_R A \to A \otimes H, a \otimes b \mapsto a\delta(b),$$

is bijective.

In Theorem 4.1 we prove a Jacobi criterion for H-Galois extensions. For local algebras A this criterion says that the following statements are equivalent:

1991 *Mathematics Subject Classification.* Primary: 17B37; Secondary: 16W30.

Key words and phrases. Hopf Galois extensions, infinitesimal group schemes.

Version of May 10, 2001.

This work was partially supported by the Graduiertenkolleg of the Math. Institut (Universität München)

.

- R $\subset A$ is an H-Galois extension.
- There are elements $y_1, \dots, y_n \in A$ such that the matrix $(D_i(y_j))$ is invertible over A.

By renumbering the y_i we can assume that for all $1 \leq m \leq n$ the matrices $(D_i(y_j))_{1 \leq i,j \leq m}$ are invertible. Assuming this stronger condition we show as an application of our criterion for H-Galois extensions that the elements

$$y_1^{\alpha_1} \cdots y_n^{\alpha_n}, 0 \leq \alpha_i < p^{s_i} - 1, 1 \leq i \leq n, \tag{1.2}$$

form an R-basis of A (Theorem 4.3).

Under the additional assumption that all the powers $y_i^{p^{s_i}}$ are H-coinvariant we obtain rather precise results about the structure of the ring extension $R \subset A$ for regular local rings A (Theorem 5.1). For example if A is local regular and complete, then the ring extension $R \subset A$ is isomorphic to the extension

$$F[[Y_1^{p^{s_1}}, \dots . Y_n^{p^{s_n}}, Z_{n+1}, \dots, Z_d]] \subset F[[Y_1, \dots . Y_n, Z_{n+1}, \dots, Z_d]]$$

of formal power series rings over a coefficient field $k \subset F \subset R$ of R and A.

Theorem 5.1 was known before in some special cases. The Lie algebra case, that is when $s_1 = \cdots = s_n = 1$, was shown in [RM] in analogy to a theorem of Lipman [L, Theorem 2] on invariants of derivations in characteristic zero. The case $n = 1$ of (1.1) but for cocommutative Hopf algebras H over separably closed fields was treated in [RT]. In this paper H was cocommutative in order to apply the theory of formal groups in an essential way. Then the results in [RT] were partially generalized in [RU] to the case when n is arbitrary and H is cocommutative.

The condition about the invertibility of the matrix $(D_i(y_j))_{1 \leq i,j \leq n}$ appears in all these papers. We explain this condition as a criterion for H-Galois extensions, and then we can use the properties of H-Galois extensions to achieve inductive arguments for arbitrary Hopf algebras satisfying (1.1).

In Section 3 we consider coactions of the additive group where the x_i are primitive elements of the Hopf algebra H. In this Section the algebra A is an arbitrary not necessarily commutative algebra. For a general Hopf algebra H satisfying (1.1) we do not know whether our results can be generalized to coactions on non-commutative algebras.

2. Preliminaries on Hopf Galois extensions and free actions

Let H be a Hopf algebra over the field k with comultiplication $\Delta : H \to H \otimes H$, counit $\varepsilon : H \to k$ and antipode $S : H \to H$. We will use the Sweedler notation $\Delta(x) = x_{(1)} \otimes x_{(2)}$ for $x \in H$. If V is a right H-comodule with structure map $\delta : V \to V \otimes H$, we will use the notation $\delta(v) = v_{(0)} \otimes v_{(1)}$ for all $v \in V$. The augmentation ideal of H will be denoted by $H^+ = \ker(\varepsilon)$.

Let us first recall some notions and results from Hopf algebra theory [M].

Definition 2.1. Let A be an algebra, and

$$\delta : A \to A \otimes H$$

an algebra map and a right H-comodule structure on A. Then (A, δ) is called a right **H-comodule algebra**, and

$$A^{coH} = \{a \in A \mid \delta(a) = a \otimes 1\}$$

is the subalgebra of H-coinvariant elements.

Let (A, δ) be a right H-comodule algebra, and $R := A^{coH}$. The extension $R \subset A$ is called an **H-Galois extension** and δ is called H-Galois, if the canonical map

$$\mathrm{can} : A \otimes_R A \to A \otimes H, x \otimes y \mapsto x\delta(y) = xy_{(0)} \otimes y_{(1)},$$

is bijective.

Let now H be a finite-dimensional Hopf algebra.

By a fundamental theorem of Larson and Sweedler [M, 2.1.3] the space of left integrals of H is one-dimensional. A left integral Λ of H is an element of H such that $x\Lambda = \varepsilon(x)\Lambda$ for all $x \in H$.

Theorem 2.2. *[Kreimer and Takeuchi] Let Λ be a non-zero integral of H, and $\delta : A \to A \otimes H$ a right H-comodule algebra with $R = A^{coH}$. Then the following are equivalent:*

(1) *$R \subset A$ is an H-Galois extension.*
(2) *The canonical map $can : A \otimes_R A \to A \otimes H$ is surjective.*
(3) *$1 \otimes \Lambda \in A \otimes H$ is in the image of the canonical map.*

In this case, A is a finitely generated and projective R-left and R-right module. In particular, A is faithfully flat over R if R is commutative.

Proof. The equivalence of (1) and (2), and the fact that A is finitely generated and projective over R on both sides is a result of Kreimer and Takeuchi (see [M, 8.3.1]). Since $\mathrm{can} : A \otimes_R A \to A \otimes H$ is left A-linear and right H-colinear with the obvious structure maps, and Λ generates H as a left H^*-module or as a right H-comodule, (2) and (3) are equivalent. Finally, if R is commutative, then A is faithfully flat over R, since $A_{\mathfrak{m}}$ is non-zero and free over $R_{\mathfrak{m}}$ for any maximal ideal $\mathfrak{m}$ of R.

□

The next result is useful for induction arguments on the order of H. A Hopf subalgebra $K \subset A$ is called normal if for all $x \in H$, and $y \in K$, $x_{(1)}yS(x_{(2)}) \in K$ (or equivalently $S(x_{(1)})yx_{(2)} \in K$). Note that any

Hopf subalgebra is trivially normal if H is commutative. If $K \subset H$ is normal, then $\overline{H} = H/HK^+$ is a quotient Hopf algebra of H.

We will say that an H-Galois extension $R \subset A$ is faithfully flat if A is faithfully flat over R as a left (or equivalently right) module over R.

Theorem 2.3. [MS, 6.1, 6.2] *Let $K \subset H$ be a normal Hopf subalgebra, and $R \subset A$ a faithfully flat H- Galois extension with structure map $\delta : A \to A \otimes H$. Let $\pi : H \to \overline{H} = H/HK^+$ be the quotient map, and $\overline{\delta} = (id \otimes \pi)\delta : A \to A \otimes \overline{H}$ the induced $\overline{H}$-module algebra structure. Define $B = A^{co\overline{H}}$.*

Then $R \subset B$ is a faithfully flat K-Galois extension where the coaction isthe restriction of δ, and $B \subset A$ is a faithfully flat $\overline{H}$-Galois extension with coaction $\overline{\delta}$.

One ingredient of the proof of Theorem 4.2 is the basic Theorem of Nichols and Zoeller ([M, 3.1.5]) which says that H is free over any Hopf subalgebra.

We will apply Theorem 2.3 in the case when H is commutative, and k has characteristic $p > 0$. Then

$$H^{[1]} := k[H^p],$$

the subalgebra generated by all $x^p, x \in H$, is a Hopf subalgebra, and $H/(x^p \mid x \in H^+)$ is the quotient Hopf algebra.

Remark 2.4. Let H be commutative, and A a commutative H-comodule algebra with structure map $\delta : A \to A \otimes H$. In the language of affine schemes and affine group schemes (see [DG], [W]), H defines a functor G from commutative k-algebras to groups, A defines a functor X from commutative k-algebras to sets represented by H resp. A, and δ describes an action

$$\mu : X \times G \to X,$$

that is for all commutative algebras T an action of the group $G(T)$ on the set $X(T)$. We will write $\mu(x, g) = xg$ for all $x \in X(T), g \in G(T)$.

Recall that for all commutative algebras T, the group structure in $G(T) = \mathrm{Alg}(H, T)$ is defined by $(f \cdot g)(h) = f(h_{(1)})g(h_{(2)})$, and the action is given by $(xg)(a) = x(a_{(0)})g(a_{(1)})$, for all $f, g \in G(T), x \in X(T) = \mathrm{Alg}(A, T), t \in T$.

Then can : $A \otimes_R A \to A \otimes H$ is surjective if and only if the **action** of G on X is (fixed point) **free** in the sense that for all commutative algebras T, and all $g \in G(T), x \in X(T)$ the equality $xg = x$ is only possible for $g = 1$.

The subgroup $G_{(1)}$ of G represented by the quotient Hopf algebra $H/(x^p \mid x \in H^+)$ is called the first Frobenius kernel of G.

Theorem 2.2 in the commutative case is the fundamental result on free actions of finite affine group schemes on affine schemes which goes back to Grothendieck.

Let us now fix some **notations** and assumptions.

In this paper we assume that k is a field of characteristic $p > 0$, and H will always be a commutative Hopf algebra with underlying algebra

$$(2.1) \quad H = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}}), n \geq 1, s_1 \geq \cdots \geq s_n \geq 1.$$

By the structure theorem of infinitesimal, that is finite and connected group schemes (see [W, 14.4]), any finite-dimensional, commutative and local Hopf algebra over a perfect field has this form.

Let $\mathbb{A}$ be the set of all multi-indices $\alpha = (\alpha_1, \ldots, \alpha_n)$ with $0 \leq \alpha_i < p^{s_i}, 1 \leq i \leq n$.

For $\beta = (\beta_1, \ldots, \beta_n), \gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}^n$ we define

$$\beta + \gamma = (\beta_1 + \gamma_1, \ldots, \beta_n + \gamma_n), \text{ and } |\beta| = \beta_1 + \cdots + \beta_n.$$

For all i, we denote the residue class of X_i in H by x_i. Then

$$x^\alpha := x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \alpha \in \mathbb{A},$$

is a k-basis of H. Note that $\varepsilon(x_i) = 0$ for all i, where $\varepsilon : H \to k$ is the counit of H, since H is local with maximal ideal $(x_1, \ldots, x_n)$. Let $\Lambda := x_1^{p^{s_1}-1} \ldots x_n^{p^{s_n}-1}$. Then $\Lambda \neq 0$ and $\Lambda x_i = 0$ for all $1 \leq i \leq n$. Hence Λ is a non-zero integral in H.

Let A be an algebra, and $\delta : A \to A \otimes H$, a right H-comodule algebra structure on A. We will always write

$$\delta(a) = \sum_{\alpha \in \mathbb{A}} D_\alpha(a) \otimes x^\alpha, \text{ for all } a \in A.$$

Thus for all $\alpha \in \mathbb{A}$ and $a, b \in A$,

$$D_\alpha(ab) = \sum_{\substack{\beta+\gamma=\alpha \\ \beta,\gamma \in \mathbb{A}}} D_\beta(a) D_\gamma(b), \text{ and } D_{(0,\ldots,0)} = \mathrm{id}.$$

For all i, let $\delta_i = (\delta_{ij})_{1 \leq j \leq n} \in \mathbb{A}$, where $\delta_{ij} = 1$, if $j = i$, and $\delta_{ij} = 0$, otherwise. We define $D_i = D_{\delta_i}, 1 \leq i \leq n$. Thus the linear maps $D_i : A \to A$ are derivations of the algebra A, and for all $a \in A$ we have

$$(2.2) \qquad \delta(a) = a \otimes 1 + \sum_{1 \leq i \leq n} D_i(a) \otimes x_i + \sum_{\substack{\alpha \in \mathbb{A} \\ |\alpha| \geq 2}} D_\alpha(a) \otimes x_\alpha.$$

Let H^* be the dual Hopf algebra of H and $\mathfrak{g} = P(H^*)$ the p-Lie algebra of the primitive elements in H^*. Thus $\mathfrak{g}$ is the Lie algebra of the group scheme represented by H. Recall that the primitive elements in H^* are the ε-derivations $d : H \to k$, that is the linear functions satisfying $d(xy) = \varepsilon(x)d(y) + d(x)\varepsilon(y)$ for all $x, y \in H$. For all i, let $d_i : H \to k$ be the ε-derivation with $d_i(x_j) = \delta_{ij}, 1 \leq i, j \leq n$ (Kronecker δ). Then $d_1, \ldots, d_n$ is a basis of $\mathfrak{g}$. The coaction $\delta : A \to A \otimes H$ defines a left H^*-module algebra structure on A, and the action of d_i is given by the derivation D_i. Thus

$$\mathfrak{g} \to \mathrm{Der}(A, A), d_i \mapsto D_i, 1 \leq i \leq n,$$

is a map of p-Lie algebras. In particular,

$$[D_i, D_j], D_i^p \in \sum_{1 \le l \le n} kD_l, 1 \le i, j \le n. \tag{2.3}$$

In the case when $s_1 = \cdots = s_n = 1$, H^* is the restricted enveloping algebra of $\mathfrak{g}$, and the action is determined by the action of $\mathfrak{g}$. Hence in this case $A^{coH} = A^{\{D_1,\dots,D_n\}}$, where

$$A^{\{D_1,\dots,D_n\}} := \{a \in A \mid D_i(a) = 0 \text{ for all } 1 \le i \le n\}. \tag{2.4}$$

3. The additive group

The Hopf algebra H_a with underlying algebra

$$H_a = k[X_1, \dots, X_n]/(X_1^{p^{s_1}}, \dots, X_n^{p^{s_n}}), n \ge 1, s_1 \ge \cdots \ge s_n \ge 1, \tag{3.1}$$

and comultiplication given by

$$\Delta(x_i) = x_i \otimes 1 + 1 \otimes x_i, 1 \le i \le n, \tag{3.2}$$

will be called the Hopf algebra of the additive group (where n and $s_1, \dots, s_n$ are fixed).

Note that for any commutative algebra T, $G_a(T) := \mathrm{Alg}(H_a, T) \simeq \{(t_1, \dots, t_n) \in k^n \mid t^{p^{s_i}} = 0, 1 \le i \le n\}$, where the group structure is componentwise addition.

We consider coactions of H_a on arbitrary, not necessarily commutative algebras A. However in all the later results about H-comodule algebras A for our general Hopf algebra H satisfying (2.1) we assume that A is commutative.

Theorem 3.1. *Let H_a be the Hopf algebra defined by* (3.1), (3.2), *and A a right H-comodule algebra with structure map $\delta : A \to A \otimes H_a$. Define the derivations $D_1, \dots, D_n$ by* (2.2) *and let $R = A^{coH_a}$.*

Then the following are equivalent:

1. *$R \subset A$ is a faithfully flat H_a-Galois extension.*
2. *There are $y_1, \dots, y_n \in A$ with $\delta(y_i) = y_i \otimes 1 + 1 \otimes x_i$, for all $1 \le i \le n$.*

Suppose (2) holds. Define $y^\alpha = y_1^{\alpha_1} \cdots y_n^{\alpha_n}, \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{A}$. Then

$$R \otimes H_a \to A, r \otimes x^\alpha \mapsto ry^\alpha, r \in R, \alpha \in \mathbb{A},$$

is a left R-linear and right H_a-colinear isomorphism. In particular, the elements

$$y^\alpha, \alpha \in \mathbb{A},$$

form an R-basis of A as a left R-module.

Proof. (1) $\Rightarrow$ (2): By (1), A is an injective H_a-comodule (see for example [S, Theorem I]). Hence the right H_a-colinear map $k \to A, 1 \mapsto 1$, can be extended to an H_a-colinear map $\gamma : H_a \to A$. Then for all i,

$$\delta(\gamma(x_i)) = (\gamma \otimes \mathrm{id})\Delta(x_i) = \gamma(x_i) \otimes 1 + 1 \otimes x_i,$$

since γ is H_a-colinear and $\gamma(1) = 1$, and the claim follows with $y_i := \gamma(x_i)$ for all $1 \leq i \leq n$.

Suppose (2) holds. Then we define a k-linear map $\gamma : H_a \to A$ by $\gamma(x^\alpha) := y^\alpha$ for all $\alpha \in \mathbb{A}$. Since Δ and δ are algebra maps, and for all i,

$$\Delta(x_i) = x_i \otimes 1 + 1 \otimes x_i, \delta(y_i) = y_i \otimes 1 + 1 \otimes x_i,$$

γ is right H_a-colinear.

Since H_a as an algebra is generated by the group-like element 1 and the primitive elements x_i, k is the only simple subcoalgebra of H_a ([M, 5.5.1]). Therefore the map γ is convolution invertible (cf. [M, 5.2.10]). Thus the H_a-extension $R \subset A$ is H_a-cleft, hence H_a-Galois, and

$$R \otimes H_a \to A, r \otimes x^\alpha \mapsto ry^\alpha, r \in R, \alpha \in \mathbb{A},$$

is bijective (see [M, 8.2.4, 7.2.3]). □

Example 3.2. We consider the Lie algebra case of the additive group

$$H_a = k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p).$$

In this case coactions of H_a are given by derivations $D_1, \ldots, D_n \in \mathrm{Der}(A, A)$ with

$$D_i D_j = D_j D_i, \text{ and } D_i^p = 0, 1 \leq i, j \leq n,$$

where

$$D_\alpha = \frac{D_1^{\alpha_1}}{\alpha_1!} \cdots \frac{D_n^{\alpha_n}}{\alpha_n!}, \alpha = (\alpha_1, \ldots, \alpha_n), 0 \leq \alpha_i < p, 1 \leq i \leq n.$$

Proof. This follows easily from the fact that $e_\alpha = \frac{x^{\alpha_1}}{\alpha_1!} \cdots \frac{x^{\alpha_n}}{\alpha_n!}, \alpha \in \mathbb{A}$, is a k-basis of H_a with

$$\Delta(e_\alpha) = \sum_{\substack{\beta+\gamma=\alpha \\ \beta,\gamma\in\mathbb{A}}} e_\beta \otimes e_\gamma.$$

□

Corollary 3.3. *Assume $s_1 = \cdots = s_n = 1$. Let A be an algebra, and $\delta : A \to A \otimes H_a$ a coaction. Define the derivations $D_1, \ldots, D_n$ by (2.2) and let $R = A^{coH}$.*

Then the following are equivalent:

(1) *$R \subset A$ is a faithfully flat H_a-Galois extension.*
(2) *There are $y_1, \ldots, y_n \in A$ with $D_i(y_j) = \delta_{ij}$ for all $1 \leq i, j \leq n$.*

Suppose (2) holds. Then

$$R \otimes H_a \to A, r \otimes x^\alpha \mapsto ry^\alpha, r \in R, \alpha \in \mathbb{A},$$

is a left R-linear and right H_a-colinear isomorphism.

Proof. This follows from Theorem 3.1 and Example 3.2

□

The next Lemma shows that under certain conditions the coinvariant elements in the Lie algebra case are the coinvariant elements under some action of the additive group. The idea of this Lemma appears several times in the literature (see [L] resp. [RM] when the characteristic of the field is 0 resp. $p > 0$.) We include the proof for completeness.

Lemma 3.4. *Let A be a commutative algebra, H a Hopf algebra satisfying* (2.1) *with $s_1 = \cdots = s_n = 1$, and δ a right H-comodule algebra structure on A with derivations $D_1, \ldots, D_n$ defined by* (2.2).

Assume $y_1, \ldots, y_n \in A$ such that the matrix $(D_i(y_j))_{1 \leq i,j \leq n}$ is invertible.

Then there are derivations $\partial_1, \ldots, \partial_n \in Der(A, A)$ such that

$$[\partial_i, \partial_j] = 0, \partial_i^p = 0, \partial_i(y_j) = \delta_{ij}, 1 \leq i, j \leq n, \text{ and } A^{coH} = A^{\{\partial_1, \ldots, \partial_n\}}.$$

In particular, the elements

$$y_1^{\alpha_1} \cdots y_n^{\alpha_n}, 0 \leq \alpha_i < p, 1 \leq i \leq n,$$

form a basis of A over R.

Proof. Let (a_{ij}) be the inverse matrix of $(D_i(y_j))$. Define

$$\partial_i = \sum_{1 \leq j \leq n} a_{ij} D_j, 1 \leq i \leq n.$$

Then $\partial_i(y_l) = \delta_{il}$ for all $1 \leq i, l \leq n$, and $\sum_{1 \leq i \leq n} AD_i = \sum_{1 \leq i \leq n} A\partial_i$. In particular, using (2.4),

$$A^{\{\partial_1, \ldots, \partial_n\}} = A^{\{D_1, \ldots, D_n\}} = A^{coH}.$$

Since A is commutative it is easy to see by (2.3) that

$$[\partial_i, \partial_j] \in \sum_{1 \leq i \leq n} AD_i = \sum_{1 \leq i \leq n} A\partial_i.$$

By Hochschild's formula [Ma, 25.5], for any $a \in A$ and any derivation $D \in \mathrm{Der}(A, A)$, $(aD)^p$ is an A-linear combination of D^p and D. Hence for all i by (2.3),

$$\partial_i^p \in \sum_{1 \leq i \leq n} AD_i = \sum_{1 \leq i \leq n} A\partial_i.$$

Since an A-linear combination of $\partial_1, \ldots, \partial_n$ is zero if its evaluation on all $y_j, 1 \leq j \leq n$, vanishes, we see that $[\partial_i, \partial_j] = 0, \partial_i^p = 0, 1 \leq i, j \leq n$.

Finally, the statement about the R-basis of A follows from Corollary 3.3 and Example 3.2. □

4. A Jacobi-criterion for free actions

Theorem 4.1. *Let H be a Hopf algebra satisfying* (2.1), *and A a commutative right H-comodule algebra with structure map $\delta : A \to A \otimes H$. Define the derivations $D_1, \ldots, D_n$ by* (2.2) *and let $R = A^{coH}$.*

Then the following are equivalent:

(1) *$R \subset A$ is an H-Galois extension.*

(2) *There are $N \in \mathbb{N}$ and $y_1, \dots, y_N \in A$ such that the matrix $(D_i(y_j))$ is right invertible, that is there are $a_{jl} \in A, 1 \le j \le N, 1 \le l \le n$, with $\sum_{1\le j\le N} D_i(y_j)a_{jl} = \delta_{il}$, for all $1 \le i, l \le n$.*
(3) *If A is local: There are $y_1, \dots, y_n \in A$ such that for all $1 \le m \le n$, the $m \times m$ matrix $(D_i(y_j))_{1\le i,j\le m}$ over A is invertible.*

Proof. (1) $\Rightarrow$ (2): By (1), $1 \otimes x_l$ is in the image of the canonical map $A \otimes_R A \to A \otimes H$ for all $1 \le l \le n$. Hence there are elements $y_j \in A, 1 \le j \le N$, for some $N \in \mathbb{N}$ such that there are $a_{jl} \in A, 1 \le j \le N, 1 \le l \le n$, with

$$\sum_{\substack{1\le j\le N\\ \alpha\in\mathbb{A}}} a_{jl} D_\alpha(y_j) \otimes x^\alpha = 1 \otimes x_l, 1 \le l \le n.$$

In particular, for all $1 \le i, l \le n$, $\sum_{1\le j\le N} a_{jl} D_i(y_j) = \delta_{il}$.

(2) $\Rightarrow$ (1): By Theorem 2.2 it is enough to show that the integral $\Lambda := x_1^{p^{s_1}-1} \dots x_n^{p^{s_n}-1}$ is in the image of the canonical map can : $A \otimes_R A \to A \otimes H$.

For all $1 \le l \le n$, using (2.2) and (2) we compute:

$$\begin{aligned}\mathrm{can}(\sum_j a_{jl} \otimes y_j) &= \sum_j a_{jl} y_j \otimes 1 + \sum_{j,i} a_{jl} D_i(y_j) \otimes x_i \\ &\quad + \sum_{j,|\alpha|\ge 2} a_{jl} D_\alpha(y_j) \otimes x^\alpha \\ &= \sum_j a_{jl} y_j \otimes 1 + 1 \otimes x_l + \sum_{j,|\alpha|\ge 2} a_{jl} D_\alpha(y_j) \otimes x^\alpha.\end{aligned}$$

Defining $z_l = \sum_j a_{jl} \otimes y_j - \sum_j a_{jl} y_j \otimes 1$, and $a_l^\alpha = \sum_j a_{jl} D_\alpha(y_j)$ for all $1 \le l \le n$ and $\alpha \in \mathbb{A}, |\alpha| \ge 2$, we obtain

$$\mathrm{can}(z_l) = 1 \otimes x_l + \sum_{|\alpha|\ge 2} a_l^\alpha \otimes x^\alpha, 1 \le l \le n.$$

We claim that

$$\mathrm{can}(z_1^{p^{s_1}-1} \cdots z_n^{p^{s_n}-1}) = 1 \otimes \Lambda.$$

Since the canonical map is an algebra map, we have

$$\begin{aligned}\mathrm{can}(z_1^{p^{s_1}-1} \cdots z_n^{p^{s_n}-1}) &= \mathrm{can}(z_1)^{p^{s_1}-1} \cdots \mathrm{can}(z_n)^{p^{s_n}-1} \\ &= \prod_{1\le l\le n} \Big(1 \otimes x_l + \sum_{|\alpha|\ge 2} a_l^\alpha \otimes x^\alpha\Big)^{p^{s_l}-1}.\end{aligned}$$

We see that this product is a sum of terms of the form

$$\prod_{1\le l\le n} (1 \otimes x_l)^{c_l} \Big(\sum_{|\alpha|\ge 2} a_l^\alpha \otimes x^\alpha\Big)^{d_l}, c_l + d_l = p^{s_l} - 1, \text{ for all } 1 \le l \le n.$$

The general term of this sum can be written as

$$a \otimes x^\gamma, a \in A, \gamma \in \mathbb{N}^n, |\gamma| \ge \sum_{1\le l\le n} (c_l + 2d_l) = \sum_{1\le l\le n} (p^{s_l} - 1) + \sum_{1\le l\le n} d_l.$$

Only the terms $a \otimes x^\gamma$ with $\gamma = (\gamma_1, \dots, \gamma_n)$ and $\gamma_l \le p^{s_l} - 1, 1 \le l \le n$, can be non-zero. Therefore we only have to consider $a \otimes x^\gamma$ with $|\gamma| \le \sum_{1 \le l \le n}(p^{s_l} - 1)$, that is with $d_l = 0$ for all l. This proves our claim.

(2) $\Rightarrow$ (3) follows from the next Lemma.

□

Lemma 4.2. *Let A be a commutative local ring, $1 \le n, N \in \mathbb{N}$ and $d_{ij} \in A, 1 \le i \le n, 1 \le j \le N$. Assume that there are $a_{jl} \in A, 1 \le l \le n, 1 \le j \le N$ with $\sum_{1 \le j \le N} d_{ij} a_{jl} = \delta_{il}$, for all $1 \le i, l \le n$.*

Then there are $1 \le j_1 < \cdots < j_n \le N$ and a permutation $\sigma \in S_n$ such that for all $1 \le m \le n$, the $m \times m$ matrix $(d_{ij_{\sigma(l)}})_{1 \le i,l \le m}$ is invertible.

Proof. Since a square matrix over A is invertible if and only if its determinant is $\not\equiv 0 \mod \mathfrak{m}$, $\mathfrak{m}$ the maximal ideal of A, we may assume that A is a field.

Since the rows of (d_{ij}) are linearly independent, there is a sequence $1 \le j_1 < \cdots < j_n \le N$ such that $(d_{ij_l})_{1 \le i,l \le n}$ is invertible.

Hence it suffices to show that for any invertible square matrix $B = (b_{ij})_{1 \le i,j \le n}$ over a field there is a permutation $\sigma \in S_n$ such that each submatrix $(b_{ij})_{1 \le i,j \le m}$, $1 \le m \le n$, is invertible. We prove this result by induction on n. Since the first $n-1$ rows of B are linearly independent, there are column indices $1 \le j_1 < \cdots < j_{n-1} \le n$ such that $(b_{ij_l})_{1 \le i,l \le n-1}$ is invertible. By induction there is a permutation $\tau \in S_{n-1}$ such that all submatrices $(b_{ij_{\tau(l)}})_{1 \le i,l \le m}$, $1 \le m \le n-1$, are invertible. Let j_n be the column index not contained in $\{j_1, \dots, j_{n-1}\}$. Then $(j_{\tau(1)}, \dots, j_{\tau(n-1)}, j_n)$ is the permutation of the columns we want. □

Theorem 4.3. *Let H, $\delta : A \to A \otimes H$ and R be as in Theorem 4.1 and assume $y_1, \dots, y_n \in A$ such that for all $1 \le m \le n$, $(D_i(y_j))_{1 \le i,j \le m}$ is invertible.*

Then the elements

$$y^\alpha := y_1^{\alpha_1} \cdots y_n^{\alpha_n}, \alpha = (\alpha_1 \dots \alpha_n) \in \mathbb{A},$$

form an R-basis of A.

Proof. We proceed by induction on the biggest exponent s_1.

If $s_1 = 1$, we are in the Lie algebra case, and the claim follows by Lemma 3.4. For the induction step suppose

$$s_1 \ge s_2 \cdots \ge s_m > 1, s_{m+1} = \cdots = s_1, \text{ for some } 1 \le m \le n.$$

Recall from Section 2 that $H^{[1]} = k[H^p]$ is a Hopf subalgebra of H with quotient Hopf algebra $\overline{H}_{(1)} = H/(x^p \mid x \in H^+)$. Then

$$k[X_1, \dots, X_m]/(X_1^{p^{s_1-1}}, \dots, X_m^{p^{s_m-1}}) \to H^{[1]}, \overline{X_i} \mapsto x_i^p, 1 \le i \le m,$$

and

$$k[X_1, \dots, X_n]/(X_1^p, \dots, X_n^p) \to \overline{H}_{(1)}, \overline{X_i} \mapsto \overline{x_i}, 1 \le i \le n,$$

are isomorphisms.

Let $B = A^{co\overline{H}_{(1)}}$. By Theorem 4.1, $R \subset A$ is an H-Galois extension. Hence by Theorem 2.3, $R \subset B$ is an $H^{[1]}$-Galois and $B \subset A$ an $\overline{H}_{(1)}$-Galois extension. The coaction of B is the restriction of δ. Therefore we obtain from the formula (2.2) for the coaction for all $b \in B$,

$$\delta(b) = b \otimes 1 + \sum_{p\alpha \in \mathbb{A}} D_{p\alpha}(b) \otimes x^{p\alpha}.$$

Here we use the notation $p\alpha = (p\alpha_1, \ldots, p\alpha_n)$ for all $\alpha = (\alpha_1, \ldots, \alpha_n)$.

On the other hand, by taking p-th powers it follows from (2.2) that for all $a \in A$,

$$\delta(a^p) = a^p \otimes 1 + \sum_{1 \leq i \leq n} D_i(a)^p \otimes x_i^p + \sum_{\substack{\alpha \in \mathbb{A} \\ |\alpha| \geq 2}} D_\alpha(a)^p \otimes x_{p\alpha}.$$

In particular, $D_i(a)^p = D_{p\delta_i}(a^p)$.

By assumption, the matrix $(D_i(y_j))_{1 \leq i,j \leq t}$ is invertible for all $1 \leq t \leq m$. Hence also $(D_i(y_j)^p)_{1 \leq i,j \leq t} = (D_{p\delta_i}(y_j^p))_{1 \leq i,j \leq t}$ is invertible for all $1 \leq t \leq m$. Therefore it follows by induction that

$$y_1^{p\alpha_1} \cdots y_m^{p\alpha_m}, 0 \leq \alpha_i < p^{s_i - 1}, 1 \leq i \leq m,$$

is an R-basis of B.

Moreover we know from the Lie algebra case that

$$y_1^{\beta_1} \cdots y_n^{\beta_n}, 0 \leq \beta_l < p, 1 \leq l \leq n,$$

is a B-basis of A.

Hence

$$y_1^{p\alpha_1} \cdots y_m^{p\alpha_m} y_1^{\beta_1} \cdots y_n^{\beta_n},$$
$$0 \leq \alpha_i < p^{s_i - 1}, 1 \leq i \leq m, 0 \leq \beta_l < p, 1 \leq l \leq n,$$

is an R-basis of A, and we are done. □

Note that any H-Galois extension of commutative algebras $R \subset A$, H a finite-dimensional Hopf algebra, is finite by Theorem 2.2. In particular, if A is local, then also R is local.

Corollary 4.4. *Let H, $\delta : A \to A \otimes H$ and R be as in Theorem 4.1, and assume that A is local with maximal ideal $\mathfrak{m}_A$. Then the following are equivalent:*

1. *$R \subset A$ is an H-Galois extension, and $R + \mathfrak{m}_A = A$, that is A and R have the same residue field.*
2. *There are $y_1, \ldots, y_n \in \mathfrak{m}_A$ such that the matrix $(D_i(y_j))_{1 \leq i,j \leq n}$ is invertible.*

Proof. (1) $\Rightarrow$ (2): By Theorem 4.1 there are $y_1, \ldots, y_n \in A$ such that $(D_i(y_j))_{1 \leq i,j \leq n}$ is invertible. By assumption we can write $y_i = r_i + \widetilde{y}_i$, where $r_i \in R$ and $\widetilde{y}_i \in \mathfrak{m}_A$ for all $1 \leq i \leq n$. Then $D_i(r_j) = 0$ for all $1 \leq i, j \leq n$ since $R = A^{coH}$. Thus $(D_i(\widetilde{y}_j))_{1 \leq i,j \leq n} = (D_i(y_j))_{1 \leq i,j \leq n}$ is invertible.

(2) $\Rightarrow$ (1): By Theorem 4.1, $R \subset A$ is H-Galois, and by Lemma 4.2 we can choose the y_i in $\mathfrak{m}_A$ such that condition (3) in Theorem 4.1 is satisfied. Then the equality $R + \mathfrak{m}_A = A$ follows from Theorem 4.3. $\square$

Corollary 4.5. *Let H, $\delta : A \to A \otimes H$ and R be as in Theorem 4.1 and assume $y_1, \ldots, y_n \in A$ such that for all $1 \le m \le n$, $(D_i(y_j))_{1 \le i,j \le m}$ is invertible.*

(1) *If $s_1 = \cdots = s_n =: s$, then $y_i^{p^s} \in R$ for all $1 \le i \le n$.*
(2) *If $y_i^{p^{s_i}} \in R$ for all $1 \le i \le n$, then the algebra map*

$$R[T_1, \ldots, T_n]/(T_1^{p^{s_1}} - y_1^{p^{s_1}}, \ldots, T_n^{p^{s_n}} - y_n^{p^{s_n}}) \to A, \overline{T_i} \mapsto y_i, 1 \le i \le n,$$

where $R[T_1, \ldots, T_n]$ is the polynomial ring in n variables, and the canonical map

$$R/(y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}}) \to A/(y_1, \ldots, y_n)$$

are bijective.

Proof. (1) follows by raising (2.2) to the p^s-th power, and (2) follows from 4.3. $\square$

The examples below show that Theorem 4.3 does not hold if we just assume that the matrix $(D_i(y_j))_{1 \le i,j \le n}$ is invertible; also in the situation of Corollary 4.5 it is not always true that $y_i^{p^{s_i}} \in R$ for all $1 \le i \le n$.

Example 4.6. We consider the Hopf algebra

$$H = H_a = k[X_1, X_2]/(X_1^{p^2}, X_2^p) = k[x_1, x_2]$$

of the additive group with $n = 2$ and $s_1 = 2, s_2 = 1$, and the polynomial algebra in two variables $A = k[T_1, T_2]$.

1) The algebra map $\delta : A \to A \otimes H$, defined by

$$\delta(T_1) = T_1 \otimes 1 + 1 \otimes x_2, \delta(T_2) = T_2 \otimes 1 + 1 \otimes x_1 + 1 \otimes x_2,$$

is an H-comodule algebra structure on A. Let $y_i := T_i, 1 \le i \le 2$. Then the matrix $(D_i(y_j))_{1 \le i,j \le 2}$ is invertible, but the elements

$$y_1^{i_1} y_2^{i_2}, 0 \le i_1 < p^2, 0 \le i_2 < p,$$

do not form a basis of A over $R = A^{coH}$.

2) The algebra map $\delta : A \to A \otimes H$, defined by

$$\delta(T_1) = T_1 \otimes 1 + 1 \otimes x_1, \delta(T_2) = T_2 \otimes 1 + 1 \otimes x_1 + 1 \otimes x_2,$$

is an H-comodule algebra structure on A. Let $y_i := T_i, 1 \le i \le 2$. Then the matrices $(D_i(y_j))_{1 \le i,j \le m}$ are invertible for $1 \le m \le 2$, and $y_i^p \notin R = A^{coH}, 1 \le i \le 2$.

3) In both examples 1) and 2), δ induces an H-comodule algebra structure on the localization $A_{\mathfrak{m}}, \mathfrak{m} := (T_1, T_2)$.

Proof. 1) It is easy to check that δ is coassociativ. By definition, $D_1(T_1) = 0, D_1(T_2) = 1, D_2(T_1) = 1, D_2(T_2) = 1$. Hence the elements

$$T_2^{i_1} T_1^{i_2}, 0 \leq i_1 < p^2, 0 \leq i_2 < p,$$

are an R-basis of A by Theorem 4.3. In particular, A is free over R of rank p^3. Therefore the elements

$$T_1^{i_1} T_2^{i_2}, 0 \leq i_1 < p^2, 0 \leq i_2 < p,$$

do not generate the R-module A, since $T_1^p \in R$, although the 2×2 matrix $(D_i(T_j))_{1 \leq i,j \leq 2}$ is invertible.

2) is easy to check. To prove 3) note that for any commutative H-comodule algebra structure $\delta : A \to A \otimes H$, H commutative and local with $(\mathfrak{m}_H)^{p^s} = 0$, and for all $a \in A$, $\delta(a) \in a \otimes 1 + A \otimes \mathfrak{m}_H$, hence $(\delta(a))^{p^s} = a^{p^s} \otimes 1$. Thus δ induces an H-comodule algebra structure on each localization of A.

□

5. An application

We finally apply the previous results to the case when A is regular local or regular local and complete.

Theorem 5.1. *Let H be a Hopf algebra satisfying* (2.1)*, and A a commutative right H-comodule algebra with structure map $\delta : A \to A \otimes H$. Define the derivations $D_1, \ldots, D_n$ by* (2.2) *and let $R = A^{coH}$.*

Assume that A is a regular local ring of dimension d with maximal ideal $\mathfrak{m}_A$ and there are $y_1, \ldots, y_n \in \mathfrak{m}_A$ such that for all $1 \leq m \leq n$, $(D_i(y_j))_{1 \leq i,j \leq n}$ is invertible.

Then R is regular local.

(1) Assume moreover that $s_1 = \cdots = s_n$, or more generally that for all $1 \leq i \leq n, y^{p^{s_i}} \in R$.

Then there are $z_{n+1}, \ldots, z_d \in R$ such that

$$y_1, \ldots, y_n, z_{n+1}, \ldots, z_d \text{ is a regular system of parameters of } A, \text{ and}$$

$$y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}}, z_{n+1}, \ldots, z_d \text{ is a regular system of parameters of } R.$$

(2) Assume in addition to (1) that the regular local ring $(A, \mathfrak{m}_A)$ is complete, and $k \subset A/\mathfrak{m}_A$ is a separable field extension. Then there is a subfield $k \subset F \subset R$ of R such that

$$F \xrightarrow{\cong} R/\mathfrak{m}_R \xrightarrow{\cong} A/\mathfrak{m}_A,$$

and an algebra isomorphism

$$F[[Y_1, \ldots Y_n, Z_{n+1}, \ldots, Z_d]] \xrightarrow{\cong} A,$$

inducing an algebra isomorphism

$$F[[Y_1^{p^{s_1}}, \ldots Y_n^{p^{s_n}}, Z_{n+1}, \ldots, Z_d]] \xrightarrow{\cong} R.$$

Proof. By Theorem 4.1, $R \subset A$ is H-Galois, in particular A is a finitely generated free R-module. Hence R is local, noetherian and regular (see [Ma, 23.7]).

Assume (1). Following the argument in [RM, Theorem 5], we first note that the residue classes of $y_1, \dots, y_n$ in $\mathfrak{m}_A/\mathfrak{m}_A^2$ are linearly independent over $A/\mathfrak{m}_A$. Suppose $\sum_{1 \le j \le n} a_j y_j \in \mathfrak{m}_A^2$ for some $a_j \in A$. By applying the derivations ∂_i of the proof of Lemma 3.4 we see that $a_i \in \mathfrak{m}_A$ for all i.

Thus by 4.5 $R/(y_1^{p^{s_1}}, \dots, y_n^{p^{s_n}}) \xrightarrow{\cong} A/(y_1, \dots, y_n)$ is regular, and we can extend the $y_i^{p^{s_i}}$ by $z_{n+1}, \dots, z_d$ to a regular system of parameters of R. Then $y_1, \dots, y_n, z_{n+1}, \dots, z_d$ is a regular system of parameters of A since A and R have the same residue field by 4.4.

To prove (2), we note that R is also complete local since A is finitely generated and free over A (The $\mathfrak{m}_R$-adic topology of A is the $\mathfrak{m}_A$-adic topology, since $A/\mathfrak{m}_R A$ is artinian. Hence $R \subset \widehat{R} \subset A$, and A is free over R and $\widehat{R}$ of the same rank. Thus $R = \widehat{R}$ by Nakayama).

Since $R/\mathfrak{m}_R \xrightarrow{\cong} A/\mathfrak{m}_A$ is separable over k there is a coefficient field $k \subset F \subset R$ by [Ma, 28.3]. The claim follows from (1) and [Ma, 29.7]. □

References

[DG] M. Demazure, P. Gabriel, Groupes Algébriques I, North-Holland, 1970.

[L] J. Lipman, Free derivations modules on algebraic varieties, *Amer. J. Math.* **87** (1965), 874–898.

[Ma] H. Matsumura, Commutative Ring Theory, Cambridge studies in advanced mathematics 8, Cambridge University Press, 1986.

[M] S. Montgomery, Hopf algebras and their actions on rings, CBMS Lecture Notes 82, Amer. Math. Soc., 1993.

[MS] S. Montgomery and H.-J. Schneider, Prime ideals in Hopf Galois extensions, *Israel J. Math.* **112** (1999), 187–235.

[RM] G. Restuccia and H. Matsumura, Integrable derivations II, Atti Accademia Peloritana dei Pericolanti Classe Sc, Fis. Mat. Natur. LXX (1992), 153–172.

[RU] G. Restuccia and R. Utano, n-dimensional actions of finite abelian Hopf algebras in characteristic $p > 0$, *Rev. Roumaine Math. Pures Appl.* **43** (1998), 881–895.

[RT] G. Restuccia and A. Tyc, Regularity of the ring of invariants under certain actions of finite abelian Hopf algebras in characteristic p, *J. Algebra* **159** (1993), 347–357.

[S] H.-J. Schneider, Principal homogeneous spaces for arbitrary Hopf algebras, *Israel J. Math.* **72** (1990), 167–195.

[W] W. C. Waterhouse, Introduction to affine group schemes, Graduate Texts in Mathematics 66, Springer, 1979.

Università di Messina, Dipartimento di Matematica,, Contrada Papardo, salita Sperone 31,, 98166 Sant'Agata (ME), Italy

E-mail address: `grest@dipmat.unime.it`

Mathematisches Institut, Universität München, Theresienstrasse 39, D-80333 München, Germany

E-mail address: hanssch@rz.mathematik.uni-muenchen.de