Atti dell'Accademia Peloritana dei Pericolanti
Classe I di Scienze Fis. Mat. e Nat.
Vol. LXXXI-LXXXII, C1A0401006 (2003-04)
Adunanza del 29 aprile 2004

A NOTE ON THE ZARISKI LEMMA FOR HOPF ALGEBRAS

GAETANA RESTUCCIA* AND ROSANNA UTANO

(*socio ordinario)

ABSTRACT. The formulation of the lemma of Zariski is given for coactions of a class of Hopf algebras of the additive group on algebras. Known formulations and consequences of the lemma of Zariski for derivations and differentiations are revised.

Introduction

The first formulation of the so-called lemma of Zariski is given for a derivation of a ring A containing the field of rational numbers $\mathbb{Q}$. Precisely the existence of an element y of A such that, if D is a derivation of A, then $D(y) = 1$ is postulated ([15], [3], [4]). This fact gives as a consequence information about the submodule $A^D = \{a \in A | D(a) = 0\}$ of the constants of A with respect to the derivation D and about properties of the element y, such as analytic independence on A^D, if A is (y)-adically complete. The generalization to a finite number of derivations is contained in [9]. In characteristic $p > 0$ the Zariski lemma is proved in [5] for a derivation D such that $D^p = 0$ under the form:

Let A be a ring of characteristic p and D be a derivation of A with $D^p = 0$. If $y \in A$ satisfies $Dy = 1$, then A is a free A^D-module with $1, y, y^2, \ldots, y^{p-1}$ as a basis.

This result is significant because such a derivation D is actually an iterative differentiation of A, in the sense of [4], such that it reduces to the derivation D on the element y.

Moreover a generalization of the lemma of Zariski, in characteristic $p > 0$, for a finite number of derivations is contained in [9].

Since in characteristic zero every differentiation is iterative, the previous formulations of the Zariski lemma are included in the following formulation ([9]):

Let A be a ring. Let $y \in A$ and suppose that there exists a differentiation $\underline{D} : A \longrightarrow A[[t]]$ such that $\underline{D}(y) = y + t$ and $\bigcap_{n=1}^{\infty} y^n A = (0)$.

Then y is not a zero divisor of A and, if $A^{\underline{D}}$ is the subring of invariants of A, $A^{\underline{D}} = \{a \in A | \underline{D}(a) = a\}$, then $A^{\underline{D}} \bigcap yA = (0)$.

We ask which is a sufficiently general context where it is possible to state a Zariski lemma.

We are able to formulate a Zariski lemma in the context of the finitely generated Hopf algebras on a field k and, precisely, for a special class of Hopf algebras. For such Hopf algebras, a coaction $\underline{D}$ on a k-algebra A gives, under certain conditions, the previous situations. Hence the generalization makes sense and becomes a starting point to study some problems of that sort in the context of the theory of derivations and differentiatons. The class of Hopf algebras that we consider is given as an algebra by $H_n = k[X]/(X^{p^n}) = k[x]$, $x^{p^n} = 0$, k field of characteristic $p > 0$. It depends on the positive integer number $n \geq 1$. If A is a k-algebra, a coaction of H_n on A is a k-algebra homomorphism $\underline{D} : A \to A \otimes_k H_n$ such that $(1 \otimes \varepsilon)\underline{D} = 1$ and $(1 \otimes \Delta)\underline{D} = (\underline{D} \otimes 1)\underline{D}$, where Δ and ε are respectively the comultiplication and the counit of the Hopf algebra H_n. Here the action is primitive, that is $\Delta(x) = x \otimes 1 + 1 \otimes x$. Such a Hopf algebra class has been intensively studied ([13], [8], [12], [11]). Besides being rather general (to know about its origin and motivation see [11] and [6]), it gives, for $n = 1$, the well known case considered in [9], where it is studied the case of the restricted Lie algebra case, for special actions of H_n. If H_n is cocommutative, the case of the iterative differentiations contained in [9] is obtained. The formulation of the Zariski lemma is the following:

Let A be a commutative ring, let $H_n = k[X]/(X^{p^n}] = k[x]$, $x^{p^n} = 0$, char $k = p > 0$ be the Hopf algebra with $\Delta(x) = x \otimes 1 + 1 \otimes x$ and $\underline{D} : A \longrightarrow A \otimes H_n$ a coaction of H_n on A. Let $y \in A$ be such that:

$$\underline{D}(y) = y \otimes 1 + 1 \otimes x.$$

Then

$$A^{\underline{D}} \bigcap yA = y^{p^n} A^{\underline{D}},$$

where $A^{\underline{D}}$ is the subring of invariants of A with respect to $\underline{D}$.

In general it should be

$$\underline{D}(y) = y \otimes 1 + D_1(y) \otimes x + \sum_{1 \leq i < p^n} D_i(y) \otimes x^i,$$

where D_1 is a derivation and $D_i : A \longrightarrow A$ are linear endomorphisms. Hence our coaction $\underline{D}$ is very special on the element y.

In the n-dimensional case the corresponding formulation is obtained considering the Hopf algebra $\underline{H} = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}})$, $n \geq 1$, $s_1, \ldots, s_n \geq 1$, with $\Delta(x_i) = x_i \otimes 1 + 1 \otimes x_i$, $i = 1, \ldots, n$ and n elements $y_1, \ldots, y_n \in A$, such that if $\underline{D} : A \to A \otimes_k \underline{H}$ is a coaction of $\underline{H}$ on A, then:

$$\begin{aligned} \underline{D}(y_1) &= y_1 \otimes 1 + 1 \otimes x_1 \\ &\vdots \\ \underline{D}(y_n) &= y_n \otimes 1 + 1 \otimes x_n \end{aligned}$$

If $\underline{D}$ is such a coaction, one of the most interesting consequences is that the elements $y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}}$ belong to $A^{\underline{D}}$. This fact is not always true (see [11]). It seems yet that rather interesting properties follow from the existence of elements of this type and simplifications in the proofs are obtained, without exploiting intrinsec properties of the Hopf

algebra ([11]).
In Section 1 known formulations of the Zariski lemma are given, in the contexts of derivations or differentiations, in both cases 1-dimensional and n-dimensional differentiations. Comments and some new formulations are considered.
In Section 2 the Zariski lemma is proved for Hopf algebras with underlying algebra respectively $H_n = k[X]/(X^{p^n})$ or $\underline{H} = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}})$, $n \geq 1$, $s_1 \geq \cdots \geq s_n \geq 1$, that correspond respectively to 1-dimensional and n-dimensional cases and coactions of H_n (respectively $\underline{H}$) on arbitrary commutative algebra A. The Hopf algebra is not necessarily cocommutative as in [7], then our coaction of H on A is general, except on the element $y \in A$.
In Section 3 some applications are given in order to obtain stronger properties of the algebras A and $A^{\underline{D}}$, when we have special elements of A in the direction of the validity of the Zariski lemma.

1. Preliminaries and known results

Let A be a ring.

A (1-dimensional) differentiation $\underline{D}$ of A is an infinite sequence $\underline{D} = (D_0, D_1, D_2, \ldots)$ of additive endomorphisms $D_i : A \longrightarrow A$ such that

$$D_0 = \text{identity},\ D_n(ab) = \sum_{i+j=n} D_i(a) D_j(b).$$

It follows that D_1 is a derivation. Let t be an indeterminate over A and put

$$E(a) = \sum_{n=0}^{\infty} t^n D_n(a) \in A[[t]] \qquad (a \in A).$$

Then E is a ring homomorphism from A into $A[[t]]$ such that $E(a) \equiv a \bmod t$. It can be uniquely extended to an endomorphism of $A[[t]]$ such that $E(t) = t$. Then, using

$$E(a) \equiv a \bmod t, \qquad a \in A, \qquad E(t) = t, \qquad (1)$$

we can easily see that E is an automorphism of $A[[t]]$. Conversely, any automorphism of $A[[t]]$ satisfying (1) comes from a differentiation. A differentiation $\underline{D}$ is said to be iterative if:

$$D_i \circ D_j = \binom{i+j}{i} D_{i+j} \qquad \text{for all } i, j.$$

If the ring A contains $\mathbb{Q}$, then every derivation D can be lifted to a unique iterative differentiation, namely $(1, D, (1/2!)D^2, \ldots, (1/n!)D^n, \ldots)$.

Some interesting theorems in the classic case prove the existence of analytically independent elements of a ring A, under the hypothesis that a derivation of A or a differentiation of A, that satisfy certain conditions, exist.

We have to introduce two subrings of A: A^D = subring of constants with respect to the derivation D and $A^{\underline{D}}$ = subring of invariants with respect to the differentiation $\underline{D}$. In general $A^D \subseteq A^{\underline{D}}$. In the same way, if $E : A \longrightarrow A[[t]]$ is the ring homomorphism such that $E(a) \equiv a \bmod t$, then we call $F = \{a \in A | E(a) = a\}$, $F \subseteq A$, is the subring of invariants of A with respect to E. In [15] it is proved the following:

Lemma 1.1. *(Zariski, 1965) Let (A, m) be a complete semilocal ring of characteristic zero (with m denoting the intersection of the maximal ideals of A) and let D be a derivation of A with values in A. Assume that there exists an element $y \in m$ such that Dy is a unit in A. Then A contains a ring A^D of representatives of the complete local ring A/Ay having the following properties:*

a) *D is zero on A^D;*
b) *y is analytically independent on A^D;*
c) *A is the power series ring $A^D[[y]]$.*

It follows that y is not a zero divisor of A and hence $\dim A^D = \dim A - 1$.

In [3] a sufficient condition is given for an I-adically complete ring A to be a power series ring over a subring.

Theorem 1.2. ([3], Theorem 1) *Let A be a ring and let I be a proper ideal in A such that $\cap_{i=0}^{\infty} I^i = 0$ and A is complete with respect to the I-adic topology. Assume that there exists a differentiation $\underline{D} = \{D_i\}_{i=0}^{\infty}$ of A such that $D_1(y) = 1$ for some $y \in I$. Let $E = D_0 - yD_1 + \cdots + (-1)^n y^n D_n + \cdots$. If $E(y) = 0$, then there exists a subring $A^{\underline{D}}$ of A such that $A = A^{\underline{D}}[[y]]$ and y is analytically independent over $A^{\underline{D}}$ (i.e. if $\sum_{i=0}^{\infty} a_i y^i = 0$ where $a_i \in A^{\underline{D}}$ then $a_i = 0$ for all $i = 1, 2, \ldots$).*

Corollary 1.3. ([3], Corollary 1) *Let A be a ring containing the field of rational numbers as a subring. Let I be an ideal in A such that A is a complete Hausdorff space with respect to the I-adic topology. Assume that there exists a derivation D of A such that $D(y) = 1$ for some $y \in A$. Then there exists a subring A^D of A such that*

(1) *D is zero on A^D;*
(2) *$A \cong A^D[[y]]$;*
(3) *y is analytically independent over A^D.*

Proof. $E = e^{-yD} = \sum (-1)^n y^n \frac{D^n}{n!}$, $\underline{D} = \{(-1)^n y^n \frac{D^n}{n!}\}$, $A^{\underline{D}} = A^D$ and $y \in A$ is such that $Dy = 1$. □

Corollary 1.4. ([3], Corollary 3) *Let (A, m) be a complete local ring of characteristic zero. Let $y \in m$ and let $D = \{D_i\}_{i=0}^{\infty}$ be a differentiation of A such that $D_1(y)$ is a unit in A and $D_i(y) = 0$ for $i > 1$. Then there exists a subring A^D of A such that:*

i) *A^D is a complete local ring;*
ii) *y is analytically independent over A^D;*
iii) *$A = A^D[[y]]$.*

Remark 1.5. The previous corollary is important because the differentiation D acts on the element y in this way: $D(y) = y + ut$, $u \in U(A)$.

Remark 1.6. The Corollary **1.4** is a first formulation of the Zariski lemma in the form as in [9].

The following theorem is called Zariski lemma, too. If we consider rings of characteristic $p > 0$:

Theorem 1.7. *Let A be a ring of characteristic p and D be a derivation of A with $D^p = 0$. Put $A^D = \{a \in A | Da = 0\}$. If $y \in A$ satisfies $Dy = 1$, then A is a free A^D-module with $1, y, y^2, \ldots, y^{p-1}$ as a basis.*

Proof. Cf. [4], Lemma 4. □

We observe that Theorem **1.7** can be reformulated in the same way as the Zariski lemma. Precisely:

Theorem 1.8. *Let A be a ring of characteristic $p > 0$ and let $y \in A$ be such that there exists an iterative differentiation $\underline{D}$ of A that satisfies $D_1(y) = 1$, and $D_i(y) = 0$ for $i > 1$.*
Then

i) $A = A^{\underline{D}}[[y]]$;
ii) *y is a p-basis of A on $A^D = A^{\underline{D}}$.*

Proof. Since $\underline{D}$ is iterative and $\underline{D}(y) = y + t$, then the theorem follows from Theorem **1.7.** □

In 1992 Restuccia and Matsumura ([9]) proved:

Theorem 1.9. *Let A be a commutative ring and $E : A \longrightarrow A[[t]]$ is a differentiation. Put $F = \{a \in A | E(a) = a\}$. Let $y \in A$ be such that*

$$E(y) = y + t \qquad \text{and} \qquad \bigcap_{n=1}^{\infty} y^n A = (0).$$

Then:

i) *y is not a zerodivisor;*
ii) $F \cap (y) = (0)$.

Proof. See [9], Theorem 1. □

Remark 1.10. The Theorem **1.9** is true in any characteristic and for a differentiation that is not necessarily iterative.

An easy extension is:

Theorem 1.11. *Let A be a commutative noetherian ring and let $y_1, \ldots, y_r$ be elements of the Jacobson radical $Rad(A)$ of A. Put $I = Ay_1 + \cdots + Ay_n$. Suppose either:*

(i) *A contains $\mathbb{Q}$ and there exist $D^{(1)}, \ldots, D^{(n)} \in Der(A)$ such that $det(D^{(i)}(y_j)) =$ a unit of A; or*
(ii) *there exist differentiations $E^{(1)}, \ldots, E^{(n)} : A \longrightarrow A[[t]]$ such that $E^{(i)}(y_j) = y_j + t\delta_{ij} (i, j = 1, \ldots, r)$.*

Put $F = \{a \in A | D^{(1)}(a) = \cdots = D^{(n)}(a) = 0\}$ in case (i) and $F = \{a \in A | E^{(1)}(a) = \cdots = E^{(n)}(a) = a\}$ in case (ii). Then

a) *F is a subring of A;*
b) $F \cap I = (0)$.

Proof. See [9], Theorem 2. □

Remark 1.12. Theorem **1.11** gives the formulation of hypothesis of the Zariski lemma for a finite number of elements and a finite number of differentiations.

The following theorem completes the information given by Theorem **1.11** under strong hypotheses.

Theorem 1.13. *Let (A, m) be a noetherian local ring of dimension n, containing $\mathbb{Q}$ and let $y_1, \dots, y_n \in m$. Put $I = (y_1, \dots, y_n)$. Suppose that:*

(1) *A is I-adically complete and*
(2) *there exist $D_1, \dots, D_n \in Der(A)$ such that $[D_i, D_j] \in \sum AD_\nu$ and $\det(D_i x_j) \notin m$.*

Then the subring $F = \{a \in A | D_1(a) = \cdots = D_n(a) = 0\}$ is a coefficient ring of A modulo I in the sense that $A = F + I$, $F \cap I = (0)$. Moreover the elements $y_1, \dots, y_n$ are analytically independent over F and $A = F[[x_1, \dots, x_n]]$. We have $\sum AD_i = \sum A(\partial/\partial y_i)$ where $\partial/\partial y_i$ denotes the partial derivation in $F[[y_1, \dots, y_r]]$.

Proof. See [9], Theorem 3. □

Remark 1.14. Theorem **1.13** is said Frobenius integrability theorem because it is the algebraic version of the classical Frobenius integrability theorem ([9]).

We shall call Theorem **1.13** the Lie algebra case of Theorem **1.2**. We do not require the existence of a differentiation E of A, but we need the hypotheses A local, containing the rational field $\mathbb{Q}$.

We observe that this is not the exact formulation of the Zariski lemma. In the context of the n-dimensional differentiations we can substitute a finite number of derivations with only one n-dimensional differentiation.

Definition 1.15. Let A be a k-algebra, k a ring. A n-dimensional differentiation $\underline{D}$ of A is a set of maps $\{D_\alpha : A \longrightarrow A | \alpha \in \mathbb{N}^n\}$ such that:

$$D_0 = id_A \qquad \text{and} \qquad D_\gamma(ab) = \sum_{\alpha+\beta=\gamma} D_\alpha(a) D_\beta(b)$$

for all $a, b \in A$ and $\alpha, \beta, \gamma \in \mathbb{N}^n$.

Let $X_1, \dots, X_n$ be indeterminates over A, put

$$\underline{\mathrm{E}}(a) = \sum_\alpha D_\alpha(a) \underline{\mathrm{X}}^\alpha \in A[[X_1, \dots, X_n]] \qquad (a \in A),$$

with $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, $\underline{\mathrm{X}}^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n}$, $D_0 = id_A$. Then $\underline{\mathrm{E}}$ is a ring homomorphism from A into $A[[X_1, \dots, X_n]]$ such that

$$\underline{\mathrm{E}}(a) \equiv a \operatorname{mod}(X_1, \dots, X_n) \tag{1}$$

Conversely, any homomorphism $\underline{\mathrm{E}} : A \longrightarrow A[[X_1, \dots, X_n]]$ satisfying (1) comes from a differentiation.

Theorem 1.16. *Let A be a commutative noetherian ring and let $y_1, \dots, y_n$ be elements of the Jacobson radical Rad(A) of A. Put $I = Ay_1 + \cdots + Ay_n$. Suppose that A contains $\mathbb{Q}$ and there exists a n-dimensional differentiation of A on k such that $\underline{E} : A \longrightarrow A[[X_1, \dots, X_n]]$ such that $\underline{E}(y_j) = y_j + t\delta_{ij}(i, j = 1, \dots, n)$. Put $F = \{a \in A | \underline{E}(a) = a\}$ Then*

i) *F is a subring of A;*

ii) $F \cap I = (0)$.

Proof. It is indeed a reformulation of the Theorem **1.13.** □

Theorem 1.17. *Let (A, m) be a local noetherian ring and let $I = (y_1, \ldots, y_n) \subseteq m$. Suppose that:*

(1) *A is I-adically complete;*
(2) *there exists a n-dimensional iterative differentiation $\underline{E} : A \longrightarrow A[[X_1, \ldots, X_n]]$ such that $\underline{E}(y_j) = y_j + t\delta_{ij}$.*

Then

i) *the subring $F = \{a \in A | \underline{E}(a) = a\}$ is a coefficient ring of A mod I;*
ii) *$A = F[[y_1, \ldots, y_r]]$, with $y_1, \ldots, y_r$ analytically independent over F.*

Proof. See [9], Theorem 4. □

In all theorems we consider very particular elements or we consider rings of characteristic zero. We want to extend the Zariski lemma in the form of Theorem **1.8** for Hopf algebras.

2. The Zariski lemma for Hopf algebras

Let k be a field of characteristic $p > 0$.
We recall the following:

Definition 2.1. *(Hopf Algebra over a field k)* We say that $(H, \mu, \eta; \Delta, \varepsilon; S)$, where μ = multiplication, η = unit map, Δ= comultiplication, ε = counit map, $S : H \to H$ = antipode,

$$\begin{array}{llll} \mu & : H \otimes_k H \to H & \eta & : k \hookrightarrow H \\ \Delta & : H \to H \otimes_k H & \varepsilon & : H \to k \end{array}$$

is a Hopf algebra if

1) μ, η are coalgebra maps and Δ, ε are algebra maps;
2) the following diagrams are commutative:

$$\begin{array}{ccc} H \otimes_k H \otimes_k H & \xrightarrow{\mu \otimes 1_H} & H \otimes_k H \\ \downarrow 1_H \otimes \mu & & \downarrow \mu \\ H \otimes_k H & \xrightarrow{\mu} & H \end{array} \qquad \begin{array}{ccc} H & \xrightarrow{\Delta} & H \otimes_k H \\ \downarrow \Delta & & \downarrow \Delta \otimes 1_H \\ H \otimes_k H & \xrightarrow{1_H \otimes \Delta} & H \otimes_k H \otimes_k H \end{array}$$

$$\begin{array}{ccccccc} H \otimes_k H & \xleftarrow{\Delta} & H & \xrightarrow{\Delta} & H \otimes_k H \\ 1_H \otimes S \downarrow & & \eta\varepsilon \downarrow & & \downarrow S \otimes 1_H \\ H \otimes_k H & \xrightarrow{\mu} & H & \xleftarrow{\mu} & H \otimes_k H \end{array}$$

Definition 2.2. Let A be a k-algebra and H an Hopf algebra. A right coaction D of H on A is a k-algebra homomorphism $\underline{D} : A \longrightarrow A \otimes H$ such that

$$(1_A \otimes \Delta)\underline{D} = (\underline{D} \otimes 1_H)\underline{D} \qquad \text{and} \qquad (1_A \otimes \varepsilon)\underline{D} = 1_A.$$

1-dimensional case

Let H_n be the Hopf algebra $k[X]/(X^{p^n})$, with counit $\varepsilon(x) = 0$, antipode $S(x) = -x$, $\Delta(x) \in k[X,Y]/\left(X^{p^n}, Y^{p^n}\right)$ (for details on H_n see [8]). A coaction of H_n on a commutative k-algebra A is a higher derivation $\underline{D} = \{D_i\}_{i\in\mathbb{N}}, D_i : A \longrightarrow A$, of order p^n, satisfying certain conditions on the D_i's which depend on the algebra structure of H_n and

$$A^{\underline{D}} = \{a \in A | \underline{D}(a) = a \otimes 1\} = \{a \in A | D_i(a) = 0, 0 \leq i \leq p^n - 1\}$$

is the subring of invariants of A with respect to $\underline{D}$.

If comultiplication in H_n is given by $\Delta(x) = x \otimes 1 + 1 \otimes x$, then we call H_n the Hopf algebra of the additive group and we denote it by H_a.
The following proposition shows that the formulation of the Zariski Lemma in the classic form contained in the introduction necessarily involves that H_n is the Hopf algebra of the additive group. In fact:

Proposition 2.3. *Let A be a commutative ring, let $H_n = k[X]/(X^{p^n}] = k[x]$, $x^{p^n} = 0$, be the Hopf algebra and $\underline{D} : A \longrightarrow A \otimes H_n$ a coaction of H_n on A. Let $y \in A$ be such that*

$$\underline{D}(y) = y \otimes 1 + 1 \otimes x.$$

Then

$$H_n = H_a.$$

Proof. It follows from the special form of the coaction on the element y and from the equality $(1_A \otimes \Delta)\underline{D} = (\underline{D} \otimes 1_H)\underline{D}$. In fact the equality

$$(\underline{D} \otimes 1_H)\underline{D}(y) = (1_A \otimes \Delta)\underline{D}(y)$$

implies

$$\Delta(x) = x \otimes 1 + 1 \otimes x.$$

□

The same situation will occur in the n-dimensional case, as we will point out in the next section. This fact is rather restrictive, hence a weaker formulation of the Zariski Lemma could be given. In this paper we confine ourselves to the case of the Hopf algebra of the additive group, that we always call H_a.

Proposition 2.4. *Let A be a commutative ring, let $H_a = k[X]/(X^{p^n}] = k[x]$, $x^{p^n} = 0$, be the Hopf algebra of the additive group and $\underline{D} : A \longrightarrow A \otimes H_a$ a coaction of H_a on A. Let $y \in A$ be such that*

$$\underline{D}(y) = y \otimes 1 + 1 \otimes x.$$

Then

1 $A^{\underline{D}} \bigcap yA = y^{p^n} A^{\underline{D}}$;
2) $y^0 = 1, y, \ldots, y^{p^n-1}$ *is a linear basis of A on $A^{\underline{D}}$.*

Proof. Before we observe that:

$$\begin{aligned} \underline{D}(y^{p^n}) &= \textstyle\sum_{0\leq i<p^n} D_i(y^{p^n}) \otimes x^i = \sum_{0\leq i<p^n} (D_i(y^{p^n}) \otimes x^i)^{p^n} \\ &= y^{p^n} \otimes 1 + \textstyle\sum_{1\leq i<p^n} D_{ip^n}(y^{p^n}) \otimes x^{ip^n} \\ &= y^{p^n} \otimes 1. \end{aligned}$$

Then $y^{p^n} \in A^{\underline{D}}$.
1) Let $z \in A$ and $yz \in A^{\underline{D}} \cap yA$. Since $yz \in A^{\underline{D}}$, we have:

$$\underline{D}(yz) = yz \otimes 1 = \underline{D}(y)\underline{D}(z) = (y \otimes 1 + 1 \otimes x)\left(z \otimes 1 + \sum_{i=1}^{p^n-1} D_i(z) \otimes x^i\right).$$

Hence we have

$$\begin{aligned} yz \otimes 1 \quad = \quad & yz \otimes 1 + (yD_1(z) + zD_1(y)) \otimes x + (yD_2(z) + D_1(z)) \otimes x^2 + \dots \\ & (yD_{p^n-1}(z) + D_{p^n-2}(z)) \otimes x^{p^n-1} + D_{p^n-1}(z) \otimes x^{p^n}. \end{aligned}$$

Since $x^{p^n} = 0$ and $x, x^2, \dots, x^{p^n-1}$ are linearly independent, we have:

$$\begin{aligned} & yD_1(z) + z = 0, \\ & yD_2(z) + D_1(z) = 0, \\ & \vdots \\ & yD_{p^n-1}(z) + D_{p^n-2}(z) = 0. \end{aligned}$$

$$\begin{aligned} z &= -yD_1(z) \\ &= D_2(z)y^2 \\ &= -D_3(z)y^3 \\ &= \dots \\ &= (-1)^{p^n-1} D_{p^n-1}(z) y^{p^n-1}. \end{aligned}$$

Then $z \in y^{p^n-1}A$ and $yz \in y^{p^n}A$, hence $A^{\underline{D}} \bigcap yA \subseteq y^{p^n} A^{\underline{D}}$.
The inverse inclusion is clear.
2) The proof can be found in [11], Theorem 3.1. □

Remark 2.5. The linear independence of $y^0, y, \dots, y^{p^n-1}$ follows directly from the form of the coaction. In fact, let $a_0 + a_1 y + a_2 y^2 + \dots + a_{p^n-1} y^{p^n-1} = 0$, $a_i \in A^{\underline{D}}$. We have:

$$\begin{aligned} 0 &= \underline{D}(a_0 + a_1 y + a_2 y^2 + \dots + a_{p^n-1} y^{p^n-1}) \\ &= a_0 \otimes 1 + (a_1 \otimes 1)(y \otimes 1 + 1 \otimes x) + (a_2 \otimes 1)(y \otimes 1 + 1 \otimes x)^2 + \dots \\ &\quad + (a_{p^n-1} \otimes 1)(y \otimes 1 + 1 \otimes x)^{p^n-1} \\ &= a_0 \otimes 1 + a_1 y \otimes 1 + a_2 y^2 \otimes 1 + \dots + a_{p^n-1} y^{p^n-1} \otimes 1 \\ &\quad + a_1 \otimes x + a_2 \otimes x^2 + \dots + a_{p^n-1} \otimes x^{p^n-1} \end{aligned}$$

Since $1 \otimes x, 1 \otimes x^2, \dots, 1 \otimes x^{p^n-1}$ are linearly independent, then the linear independence of $y^0, y, \dots, y^{p^n-1}$ follows.
The special form of the coaction will surely condition the property of $y^0, y, \dots, y^{p^n-1}$ to be a system of generators. In fact we are persuaded that the assertion 2) can follow from the form of the coaction. However we already have the proof of this fact for a more general coaction, satisfying only the condition $D_1(y) \in U(A)$ as in [11], Theorem **3.1**.

Remark 2.6. i) Proposition **2.4** is a corollary of Theorem 2.11 that we will prove later, but we want to prove it separately, to compare it with the previous results of section 1, regarding the 1-dimensional case. For $n = 1$ we obtain Theorem **1.7**, then the Lie algebra case of the additive group H_a.
The subring A^p is contained in the subring of constants $A^{\underline{D}}$, then y is a p-basis of A on $A^{\underline{D}}[A^p] = A^{\underline{D}}$.

ii) The case of Theorem **1.9** cannot be found starting from the Hopf algebra H_n. We need to consider complete Hopf algebras, in particular if we reduce to the case of a formal group, that is a special complete Hopf algebra ([14], 11.8).

Now we consider the **n-dimensional case**.

Now let $\underline{H}$ be a commutative Hopf algebra with underlying algebra

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

In the following we may suppose, without loss of generality, that $s_1 \geq \cdots \geq s_n \geq 1$. Let $\mathbb{A}$ be the set of all multiindices $\alpha = (\alpha_1, \dots, \alpha_n)$ with $0 \leq \alpha_i < p^{s_i}, 1 \leq i \leq n$.

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

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

For all i, we denote the residue class of X_i in $\underline{H}$ by x_i. Then

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

is a k-basis of $\underline{H}$. Note that $\varepsilon(x_i) = 0$ for all i, where $\varepsilon : \underline{H} \to k$ is the counit of $\underline{H}$, since $\underline{H}$ is local with maximal ideal $(x_1, \dots, x_n)$.

Let A be an algebra, $\underline{D} : A \to A \otimes H$ an algebra map and a right H-comodule algebra structure on A. Then $(A, \underline{D})$ is called a right H-comodule algebra and

$$A^{\underline{D}} = \{a \in A | \underline{D}(a) = a \otimes 1\}$$

is the subalgebra of $\underline{H}$-coinvariant elements.

We will always write

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

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

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

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

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

Moreover we want to consider the Lie algebra case of the additive group , because this case is the classic situation in many theorems of Matsumura, Restuccia, Utano, etc ([9], [10], [12].

Remark 2.7. The Hopf algebra $\underline{H}_a$ with underlying algebra

(4) $$\underline{H}_a = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}}), \qquad n \geq 1,\ s_1 \geq \cdots \geq s_n \geq 1,$$

and comultiplication given by

(5) $$\Delta(x_i) = x_i \otimes 1 + 1 \otimes x_i, \qquad 1 \leq i \leq n,$$

where x_i is the residue class of X_i in $\underline{H}_a$, is called the Hopf algebra of the additive group. If $s_1 = \cdots = s_n = 1$, $\underline{H}_a$ is called the Lie algebra of the additive group and is denoted by H_a.
In this case the coactions of H_a are given by derivations $D_1, \ldots, D_n \in Der(A, A)$ with

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

and

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

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

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

In the n-dimensional case we have a similar proposition to **2.3**. It concerns the strong formulation of the Zariski Lemma in the n-dimensional case, that forces $\underline{H}$ to be additive:

Proposition 2.8. *Let A be a noetherian commutative ring. Let*

$$\underline{H} = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}}) = k[x_1, \ldots, x_n], \qquad x_1^{p^{s_1}} = \cdots = x_n^{p^{s_n}} = 0,$$

$s_1 \geq \cdots \geq s_n \geq 1$, be the Hopf algebra and let $\underline{D} : A \longrightarrow A \otimes \underline{H}$ a coaction of $\underline{H}$ on A. Let $A^{\underline{D}}$ be the subring of coinvariants of $\underline{D}$ ($A^{\underline{D}} = \{a \in A : \underline{D}(a) = a \otimes 1\}$).

Let $y_1, \ldots, y_n \in A$ be such that

(6) $$\begin{aligned} \underline{D}(y_1) &= y_1 \otimes 1 + 1 \otimes x_1 \\ &\vdots \\ \underline{D}(y_n) &= y_n \otimes 1 + 1 \otimes x_n \end{aligned}$$

Then

$$\underline{H} = \underline{H}_a.$$

Proof. It follows easily from (6) and the connnection between the coaction $\underline{D}$ and Δ.

Proposition 2.9. *Let A be a noetherian commutative ring. Let*

$$\underline{H}_a = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}}) = k[x_1, \ldots, x_n], \qquad x_1^{p^{s_1}} = \cdots = x_n^{p^{s_n}} = 0,$$

$s_1 \geq \cdots \geq s_n \geq 1$, be the Hopf algebra and let $\underline{D} : A \longrightarrow A \otimes \underline{H}_a$ a coaction of $\underline{H}_a$ on A. Let $A^{\underline{D}}$ be the subring of coinvariants of $\underline{D}$.

Let $y_1, \ldots, y_n \in A$ be such that (6) holds. Then

$$y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}} \in A^{\underline{D}}.$$

Proof. We have, for $i = 1, \dots, n$:

$$\begin{aligned} \underline{D}(y_i^{p^{s_i}}) &= (\underline{D}(y_i))^{p^{s_i}} = (y_i \otimes 1 + 1 \otimes x_i)^{p^{s_i}} \\ &= y_i^{p^{s_i}} \otimes 1 + 1 \otimes x_i^{p^{s_i}} = y_i^{p^{s_i}} \otimes 1, \end{aligned}$$

hence $y_i^{p^i} \in A^{\underline{D}}$, $i = 1, \dots, n$.

□

Remark 2.10. Throughout the last part of the paper the Hopf algebra $\underline{H}$ will be the Hopf algebra $\underline{H}_a$ of the additive group.

Theorem 2.11. (Zariski Lemma) *Let A be a noetherian commutative ring. Let*

$$\underline{H} = k[X_1, \dots, X_n]/(X_1^{p^{s_1}}, \dots, X_n^{p^{s_n}}) = k[x_1, \dots, x_n], \qquad x_1^{p^{s_1}} = \dots = x_n^{p^{s_n}} = 0,$$

$s_1 \geq \dots \geq s_n \geq 1$, *be the Hopf algebra and let $\underline{D} : A \longrightarrow A \otimes \underline{H}$ a coaction of $\underline{H}$ on A. Let $A^{\underline{D}}$ be the subring of coinvariants of $\underline{D}$.*

Let $y_1, \dots, y_n \in A$ be such that

$$\begin{aligned} \underline{D}(y_1) &= y_1 \otimes 1 + 1 \otimes x_1 \\ &\vdots \\ \underline{D}(y_n) &= y_n \otimes 1 + 1 \otimes x_n \end{aligned} \tag{7}$$

Then

i) *the elements $y^\alpha := y_1^{\alpha_1} \cdots y_n^{\alpha_n}$, $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{A}$, $0 \leq \alpha_i < p^{s_i}$, $i = 1, \dots, n$, form an $A^{\underline{D}}$- basis of A;*

ii) $A^{\underline{D}} \bigcap (y_1, \dots, y_n)A = \left(y_1^{p^{s_1}}, \dots, y_n^{p^{s_n}}\right)$.

Proof. We have the following facts:

1) The elements $y_1^{\alpha_1} \cdots y_n^{\alpha_n}$, $1 \leq \alpha_i \leq p^{s_i} - 1$, are a basis of A over $A^{\underline{D}}$, A is a $A^{\underline{D}}$–free module ([11], Theorem 4.3). Then $A^{\underline{D}} + \sum_{1 \leq i \leq n} Ay_i = A$.
2) If $s_1 = \dots = s_n = s$, the elements $y_1^{p^{s_1}}, \dots, y_n^{p^{s_n}} \in A^{\underline{D}}$ ([11], Corollary 4.5).

We have only to prove that $A^{\underline{D}} \cap I = (y_1^{p^{s_1}}, \dots, y_n^{p^{s_n}})$. The inclusion $(y_1^{p^{s_1}}, \dots, y_n^{p^{s_n}}) \subset A^{\underline{D}} \cap I$ is true. By Theorem 4.3, [11], any element $a \in A^{\underline{D}} \cap \sum_{i=1}^n Ay_i$ has the form

$$a = \sum_{i=1}^n \left(\sum_{\alpha \in \mathbb{A}} c_{i,\alpha} \underline{y}^\alpha \right) y_i,$$

for some $c_{i,\alpha} \in A^{\underline{D}}$, otherwise $a \in A \setminus A^{\underline{D}}$. Since $a \in A^{\underline{D}}$ and $\underline{y}^\alpha$ are linearly independent on $A^{\underline{D}}$,

$$a = \sum_{i=1}^n \sum_{\alpha_i = p^{s_i} - 1} c_{i,\alpha} y_1^{\alpha_1} \dots y_i^{\alpha_i + 1} \dots y_n^{\alpha_n} \in A^{\underline{D}}.$$

Then, by the same argument,

$$a = \sum_{0 \leq i \leq n} c_{i,(p^{s_i}-1)\alpha_i} y_i^{p^{s_i}} \in \sum_{0 \leq i \leq n} A^{\underline{D}} y_i^{p^{s_i}},$$

$\alpha_{i+1} = p^{s_i}, \alpha_j = 0$ for $j \neq i$. The result follows. □

The next example shows that Theorem **2.11** does not hold without the hypotheses on $\underline{D}(y_i), i = 1, \ldots, n$.

Example 2.12. We consider the Hopf algebra

$$\underline{H} = k[X, Y]/(X^{p^2}, Y^p) = k[x, y], \qquad x^{p^2} = 0, y^p = 0$$

of the additive group and the polynomial algebra $A = k[T_1, T_2]$.

The algebra map $\underline{D} : A \longrightarrow A \otimes \underline{H}$, defined by

$$\begin{array}{rcl} \underline{D}(T_1) & = & T_1 \otimes 1 + 1 \otimes x_1 \\ \underline{D}(T_2) & = & T_1 \otimes 1 + 1 \otimes x_1 + 1 \otimes x_2 \end{array}$$

is an $\underline{H}$-comodule algebra structure on A. Put $y_i := T_i$, $i = 1, 2$. Then the element $y_2^p \notin A^{\underline{D}}$.

A little variation of Theorem **2.11** is given now. It involves only one element of the algebra A, then the result is not in the direction of the Zariski lemma, however it can be interesting, when we study a coaction of $\underline{H}$, that always involves n derivations.

Theorem 2.13. *Let A be a noetherian, commutative ring. Let*

$$\underline{H} = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}}) = k[x_1, \ldots, x_n], \qquad x_1^{p^{s_1}} = \cdots = x_n^{p^{s_n}} = 0$$

be the Hopf algebra and let $\underline{D} : A \longrightarrow A \otimes \underline{H}$ a coaction of $\underline{H}$ on A. Let $A^{\underline{D}}$ be the subring of invariants of A with respect to $\underline{D}$.

Let $y \in A$ be such that

$$\underline{D}(y) = y \otimes 1 + \sum_{i=1}^{n} D_i(y) \otimes x_i$$

$(D_i = D_{\delta(i)} = D_{(0,\ldots,0,1,\ldots,0)})$ with $D_i(y) = 1$ for some $i \in \{1, \ldots, n\}$.

Then $A^{\underline{D}} \bigcap (y) = \left(y^{p^s}\right)$, $s = min\ \{s_1, \ldots, s_n\}$.

Proof. Let $z \in A$ and $yz \in A^{\underline{D}} \cap (y)$. Since $yz \in A^{\underline{D}}$, we have:

$$\begin{array}{rcl} yz \otimes 1 & = & \underline{D}(yz) = \underline{D}(y)\underline{D}(z) \\ & = & (y \otimes 1 + D_1(y) \otimes x_1 + D_2(y) \otimes x_2 + \cdots + D_n(y) \otimes x_n) \\ & & \left(z \otimes 1 + D_1(z) \otimes x_1 + \cdots + D_n(z) \otimes x_n + \sum_{|\alpha| \geq 2} D_\alpha(z) x^\alpha\right). \end{array}$$

Hence we have

$$\begin{array}{rcl} yz \otimes 1 & = & yz \otimes 1 + (yD_1(z) + zD_1(y)) \otimes x_1 + \ldots \\ & & + (yD_n(z) + zD_n(y)) \otimes x_n + \left(D_1(y)D_1(z) + yD_{(2,0,\ldots,0)}(z)\right) \otimes x_1^2 \\ & & + \left(D_1(y)D_2(z) + D_2(y)D_1(z) + yD_{(110\ldots0)}(z)\right) \otimes x_1x_2 + \ldots \\ & & + \left(D_1(y)D_n(z) + D_n(y)D_1(z) + yD_{(100\ldots01)}(z)\right) \otimes x_1x_n \\ & & + \left(D_2(y)D_2(z) + yD_{(020\ldots0)}(z)\right) \otimes x_2^2 + \ldots \end{array}$$

Hence:

$$\sum_{i=1}^{n}(D_i(z)y+D_i(y)z)\otimes x_i+\sum_{i=1}^{n}\left(D_i(y)D_i(z)+yD_{(00\ldots\underset{i}{2},0,\ldots,0)}(z)\right)\otimes x_i^2$$
$$+\sum_{i,j=1\ i\neq j}^{n}(D_i(y)D_j(z)+D_j(y)D_i(z))\otimes x_ix_j+\ldots$$
$$+\sum_{i=1}^{n}\left(D_i(y)D_{(0,0,\ldots,\underset{i}{2},0,\ldots,0)}(z)+yD_{(0,0,\ldots,\underset{i}{3},0,\ldots,0)}(z)\right)\otimes x_i^3$$
$$+\sum_{i,j=1\ i\neq j}^{n}\left(D_i(y)D_{(0,0,\ldots,\underset{i}{1},0,\ldots,0)}(z)+D_j(y)D_{(0,0,\ldots,\underset{i}{2},0,\ldots,0)}(z)\right)\otimes x_i^2x_j+\ldots$$

For all $i,j=1,\ldots,n,$

$$\begin{array}{l}
D_i(z)y+D_i(y)z=0\\
D_i(y)D_i(z)+yD_{(0,0,\ldots,\underset{i}{2},0,\ldots,0)}(z)=0,\\
D_i(y)D_j(z)+D_j(y)D_i(z)=0,\\
\ldots\ldots\ldots\\
D_i(y)D_{(0,0,\ldots,\underset{i}{2},0,\ldots,0)}(z)+yD_{(0,0,\ldots,\underset{i}{3},0,\ldots,0)}(z)=0,\\
D_i(y)D_{(0,0,\ldots,\underset{i}{1},0,\ldots,\underset{j}{1},0,\ldots,0)}(z)+D_j(y)D_{(0,0,\ldots,\underset{i}{2},0,\ldots,0)}(z)=0\\
\ldots\ldots\ldots\ldots
\end{array}$$

Let k be such that $D_k(y)=1$.
Then:

$$\begin{aligned}
z &= -D_k(z)y=D_{(0,0,\ldots,\underset{k}{2},0,\ldots,0)}(z)y^2\\
&= -D_{(0,0,\ldots,\underset{k}{3},0,\ldots,0)}(z)y^3=\ldots\\
&= (-1)^{p^s-1}D_{(0,0,\ldots,\underset{k}{p^s-1},0,\ldots,0)}(z)y^{p^s-1}.
\end{aligned}$$

Then

$$yz=(-1)^{p^s-1}D_{(0,0,\ldots,\underset{k}{p^s-1},0,\ldots,0)}(z)y^{p^s}\in\left(y^{p^s}\right).$$

$\square$

Theorem 2.14. *(Lie algebra case of the additive group) Let H_a be a commutative Hopf algebra with underlying algebra $H_a=k[X_1,\ldots,X_n]/(X_1^p,\ldots,X_n^p)$, $n\geq 1$. Let A be an algebra and $\underline{D}:A\longrightarrow A\otimes H$ be a coaction. Define the derivations $D_1,\ldots,D_n$ by*

(3) and let $A^{\underline{D}}$ be the subalgebra of H-coinvariant elements. Suppose there exist elements $y_1, \ldots, y_n \in A$ such that:

$$\begin{aligned} &\underline{D}(y_1) = y_1 \otimes 1 + D_1(y_1) \otimes x_1 + \cdots + D_n(y_1) \otimes x_n \\ &\vdots \\ &\underline{D}(y_n) = y_n \otimes 1 + D_1(y_n) \otimes x_1 + \cdots + D_n(y_n) \otimes x_n \end{aligned} \tag{8}$$

with det $(D_i(y_j))_{1 \le i,j \le n} \in U(A)$. Then, put $I = (y_1, \ldots, y_n)$,

1) *There exists a coaction $\underline{D}' : A \longrightarrow A \otimes H_a$ such that*

$$\begin{aligned} &\underline{D}'(y_1) = y_1 \otimes 1 + 1 \otimes x_1 \\ &\vdots \\ &\underline{D}'(y_n) = y_n \otimes 1 + 1 \otimes x_n \end{aligned} \tag{9}$$

2) $A^{\underline{D}} = A^{\underline{D}'}$*;*
3) $A^{\underline{D}} \cap I = (y_1^p, \ldots, y_n^p)$*;*
4) $y_1^{\alpha_1} \cdots y_n^{\alpha_n}$*, $0 \le \alpha_i < p$, $1 \le i \le n$ form a basis of A on $A^{\underline{D}}$.*

Proof. Consider the derivations $D_1, \ldots, D_n$ defined by (3). They are such that

$$[D_i, D_j] = \sum AD_i \qquad \text{e} \qquad D_i^p = \sum AD_i.$$

Consider the matrix (a_{ji}) = the inverse of the matrix $(D_i(y_j))$. Then there are derivations $\partial_1, \ldots, \partial_n$ such that $\partial_i(y_j) = \delta_{ij}$, $\partial_i^p = 0$ ([9], Theorem 3).
Then these derivations come from a coaction $\underline{D}'$ of the Hopf algebra of the additive group H_a and for this $\underline{D}'$ we have

$$\begin{aligned} &\underline{D}'(y_1) = y_1 \otimes 1 + 1 \otimes x_1 \\ &\vdots \\ &\underline{D}'(y_n) = y_n \otimes 1 + 1 \otimes x_n. \end{aligned}$$

By Lemma 3.4 in [11], $y_1^{\alpha_1} \cdots y_n^{\alpha_n}$, $0 \le \alpha_i \le p-1$, $1 \le i \le n$ form a basis of A over $A^{\{D_1, \ldots, D_n\}}$ and $y_i^p \in A^{\{D_1, \ldots, D_n\}}$. Finally we have the assertion. □

The previous theorem shows that if $H = H_a$ and $s_1 = \cdots = s_n = 1$, a coaction of H of the form (8) can always be reduced to the form (9), that is we always can have the hypotheses of the Zariski lemma.

3. Some applications

In this section we want to prove some further properties under the hypotheses of the Zariski lemma. It may be that such properties can be proved for a more general coaction, that is under the usual hypothesis det$(D_i(y_j)) \in U(A)$, but actually such properties are not known.

Theorem 3.1. *Let k be a perfect field of characteristic $p > 0$, let*

$$\underline{H} = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}}) = k[x_1, \ldots, x_n], \qquad x_1^{p^{s_1}} = \cdots = x_n^{p^{s_n}} = 0$$

be the Hopf algebra and A an integral domain. Let us suppose there exist $y_1, \ldots, y_n \in A$ and a coaction $\underline{D}$ of $\underline{H}$ on A, such that:

$$\begin{aligned} \underline{D}(y_1) &= y_1 \otimes 1 + 1 \otimes x_1 \\ &\vdots \\ \underline{D}(y_n) &= y_n \otimes 1 + 1 \otimes x_n \end{aligned}$$

and such that $y_1^{\alpha_1} \cdots y_n^{\alpha_n}$, $0 \le \alpha_i \le p^{s_i} - 1$ are linearly independent on $k[y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}}]$.

Then the set $\{y_1, \ldots, y_n\} \subset A$ is algebraically independent over k.

Proof. Let us suppose that there exists an algebraic relation among the y_i's and let

$$f(y_1, \ldots, y_n) = 0$$

be such a relation in the lowest possible degree. It is possible to suppose that f has the following form:

$$f(y_1, \ldots, y_n) = g(y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}}),$$

where $g(Y_1, \ldots, Y_n) \in k[Y_1, \ldots, Y_n]$ has the lowest degree. Put: $g_i := \frac{\partial g}{\partial Y_i}$, then $g_i \neq 0$ for some i. By suitable renumbering of the elements x_i we may assume that $g_1 \neq 0$. Since k is a perfect field, we get the relation $g(y_1^{p^{s_1}-1}, \ldots, y_n^{p^{s_n}-1}) = 0$.
We obtain

$$\begin{aligned} 0 &= \underline{D}\left(g\left(y_1^{p^{s_1}-1}, \ldots, y_n^{p^{s_n}-1}\right)\right) \\ &= g\left((y_1 \otimes 1 + 1 \otimes x_1)^{p^{s_1}-1}, \ldots, (y_n \otimes 1 + 1 \otimes x_n)^{p^{s_n}-1}\right) \\ &= g\left(y_1^{p^{s_1}-1}, \ldots, y_n^{p^{s_n}-1}\right) \otimes 1 + g_1\left(y_1^{p^{s_1}-1}, \ldots, y_n^{p^{s_n}-1}\right) \otimes x_1^{p^{s_1}-1} + \ldots \\ &\quad + g_n\left(y_1^{p^{s_1}-1}, \ldots, y_n^{p^{s_n}-1}\right) \otimes x_n^{p^{s_n}-1} \end{aligned}$$

Since $g_1(Y_1, \ldots, Y_n) \neq 0$, $g_1\left(y_1^{p^{s_1}-1}, \ldots, y_n^{p^{s_n}-1}\right) = 0$, hence we have a relation of lower degree than $f(X_1, \ldots, X_n)$, a contradiction. □

Theorem 3.2. *Let k be a perfect field of characteristic $p > 0$, let*

$$\underline{H} = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}}) = k[x_1, \ldots, x_n], \qquad x_1^{p^{s_1}} = \cdots = x_n^{p^{s_n}} = 0$$

be the Hopf algebra and A an integral domain. Let us suppose there exist $y_1, \ldots, y_n \in A$ and a coaction $\underline{D}$ of $\underline{H}$ on A, such that:

$$\begin{aligned} \underline{D}(y_1) &= y_1 \otimes 1 + 1 \otimes x_1 \\ &\vdots \\ \underline{D}(y_n) &= y_n \otimes 1 + 1 \otimes x_n \end{aligned}$$

and such that $y_1^{\alpha_1} \cdots y_n^{\alpha_n}$, $0 \le \alpha_i \le p^{s_i} - 1$ are linearly independent on $k[y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}}]$.

Then, put $z_i = y_i^{p^{s_i}} \in A^{\underline{D}}$, if $A^{\underline{D}}$ has a linear basis on $(k[A^{\underline{D}}])^{p^s}$, then the monomials $z_1^{\alpha_1} \ldots z_n^{\alpha_n}$, $0 \le \alpha_i \le p^s - 1$ can belong to a linear basis of $A^{\underline{D}}$ on $\left(A^{\underline{D}}\right)^{p^s}$, where $s =$ max $\{s_1, \ldots, s_n\}$.

Proof. **Claim.** For all i, $z_i \notin \left(k[A^{\underline{D}}]\right)^{p^{s_i}}$.
In fact, if we suppose $z_i \in \left(k[A^{\underline{D}}]\right)^{p^{s_i}}$,

$$z_i = y_i^{p^{s_i}} = \sum_j t_j^{p^{s_j}} c_j, \qquad c_j \in k, \qquad t_j \in A^{\underline{D}}.$$

Then we have $y_i^{p^{s_i-1}} = \sum_j t_j^{p^{s_j-1}} c'_j$, $c'_j \in k$ and $\underline{D}(y_i^{p^{s_i-1}}) = \sum_j t_j^{p^{s_j-1}} c'_j \otimes 1$, that is:

$$(y_i \otimes 1 + 1 \otimes x_i)^{p^{s_i-1}} = \sum_j t_j^{p^{s_j-1}} c'_j \otimes 1.$$

$$y_i^{p^{s_i-1}} \otimes 1 + 1 \otimes x_i^{p^{s_i-1}} = \sum_j t_j^{p^{s_j-1}} c'_j \otimes 1,$$

hence $x_i^{p^{s_i-1}} = 0$, a contradiction.
Now we prove the linear independence of the z_i's. Let us consider the relation:

$$\lambda_1 z_1^{\alpha_{11}} \dots z_n^{\alpha_{1n}} + \dots + \lambda_s z_1^{\alpha_{s1}} \dots z_n^{\alpha_{sn}} = 0,$$

$\lambda_i \in \left(k[A^{\underline{D}}]\right)^{p^s}$, $0 \le \alpha_{ij} \le p^s$, $i = 1, \dots, s$. We consider the p-th root:

$$\lambda'_1 y_1^{\alpha_{11} p^{s-1}} \cdots y_n^{\alpha_{1n} p^{s-1}} + \dots \lambda'_s y_1^{\alpha_{s1} p^{s-1}} \cdots y_n^{\alpha_{s1} p^{s-1}} = 0,$$

$\lambda'_i \in \left(k[A^{\underline{D}}]\right)^{p^{s-1}}$.

$$\begin{aligned} 0 &= \underline{D}\left(\lambda'_1 y_1^{\alpha_{11} p^{s-1}} \cdots y_n^{\alpha_{1n} p^{s-1}} + \dots + \lambda'_s y_1^{\alpha_{s1} p^{s-1}} \cdots y_n^{\alpha_{s1} p^{s-1}}\right) \\ &= \lambda'_1 (y_1 \otimes 1 + 1 \otimes x_1)^{\alpha_{s1} p^{s-1}} \cdots (y_n \otimes 1 + 1 \otimes x_n)^{\alpha_{1n} p^{s-1}} + \dots \\ &\quad + \lambda'_s (y_1 \otimes 1 + 1 \otimes x_1)^{\alpha_{s1} p^{s-1}} \cdots (y_n \otimes 1 + 1 \otimes x_n)^{\alpha_{sn} p^{s-1}} \end{aligned}$$

By a suitable choice of α_{ij} we obtain $\lambda'_i \otimes x_1^{p^{s-1}} \cdots x_n^{p^{s-1}} = 0$. Then $\lambda'_i = 0$, for $i = 1, \dots, n$, hence $\lambda_i = 0$, for $i = 1, \dots, n$. □

Remark 3.3. Since k is perfect, $k = k^p$, but the hypothesis $k = k^{p^s}$, for which

$$(k[A^{\underline{D}}])^{p^s} = \left(A^{\underline{D}}\right)^{p^s},$$

can be also examined. Moreover the hypothesis: k perfect field can be replaced from some weaker condition but, at present, we are not interested to this problem.

It is possible now to give a corollary to Theorem 5.1 in [11]. For the sake of completeness, we recall it.

Theorem 3.4. ([11], Theorem 5.1) *Let*

$$\underline{H} = k[X_1, \dots, X_n]/(X_1^{p^{s_1}}, \dots, X_n^{p^{s_n}}) = k[x_1, \dots, x_n], \qquad x_1^{p^{s_1}} = \dots = x_n^{p^{s_n}} = 0,$$

$s_1 \ge \dots \ge s_n \ge 1$ *be a Hopf algebra with structure map* $\underline{D} : A \longrightarrow A \otimes \underline{H}$. *Define the derivations* $D_1, \dots, D_n$ *by (3). Assume that* A *is a regular local ring of dimension* d *with maximal ideal* m_A *and there are* $y_1, \dots, y_n \in m_A$ *such that for all* $1 \le m \le n$, $(D_i(y_j))_{1 \le i,j \le m}$ *is invertible.*
Then $A^{\underline{D}}$ *is regular local, too.*

(1) *Assume moreover that* $s_1 = \cdots = s_n$ *or, more generally, that for all* $1 \leq i \leq n$, $y^{p^{s_i}} \in A^{\underline{D}}$. *Then there are* $z_{n+1}, \ldots, z_d \in A^{\underline{D}}$ *such that*
- $y_1, \ldots, y_n, z_{n+1}, \ldots, z_d$ *is a regular system of parameters of* A, *and*
- $y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}}, z_{n+1}, \ldots, z_n$ *is a regular system of parameters of* $A^{\underline{D}}$.

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

$$F \xrightarrow{\simeq} A^{\underline{D}}/m_{A^{\underline{D}}} \xrightarrow{\simeq} A/m_A,$$

and an algebra isomorphism

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

inducing an algebra isomorphism

$$F[[Y_1^{p^{s_1}}, \ldots, Y_n^{p^{s_n}}, Z_{n+1}, \ldots, Z_d]] \xrightarrow{\simeq} A^{\underline{D}}.$$

Corollary 3.5. *Let* k *be a perfect field,*

$$\underline{H} = k[X_1, \ldots, X_n]/(X_1^{p^{s_1}}, \ldots, X_n^{p^{s_n}}) = k[x_1, \ldots, x_n], \qquad x_1^{p^{s_1}} = \cdots = x_n^{p^{s_n}} = 0,$$

$s_1 \geq \cdots \geq s_n \geq 1$ *be a Hopf algebra with structure map* $\underline{D} : A \longrightarrow A \otimes \underline{H}$. *Define the derivations* $D_1, \ldots, D_n$ *by (3). Assume that* A *is a local regular complete ring of dimension* d *with maximal ideal* m_A, $k \subset A/m_A$ *and there are* $y_1, \ldots, y_n \in m_A$ *such that:*

$$\begin{array}{rcl} \underline{D}(y_1) & = & y_1 \otimes 1 + 1 \otimes x_1 \\ \vdots & & \\ \underline{D}(y_n) & = & y_n \otimes 1 + 1 \otimes x_n \end{array}.$$

Then

(1) $y_1, \ldots, y_n$ *are algebraically independent on* k.

(2) *The elements* $z_1^{\alpha_1} \cdots z_n^{\alpha_n}$, $z_i = y_i^{p^{s_i}}$, $i = 1, \ldots, n$, $0 \leq \alpha_i \leq p^s - 1$, *can belong to a linear basis of* $A^{\underline{D}}$ *on* $(A^{\underline{D}})^{p^s}$, $s = s_1 = \max\{s_1, \ldots, s_n\}$.

Proof. Since k is a perfect field and $k \subset A/m_A$, $A/m_A \cong F$ is separable on k.
1) By (2) of Theorem **3.4**, $A \cong F[[y_1, \ldots, y_n, z_{n+1}, \ldots, z_d]]$ is a local regular complete ring, then $y_1, \ldots, y_n$ are algebraically independent on k.
2) Moreover, $y^{p^{s_i}} \in A^{\underline{D}}$, for all i, by Proposition **2.9** and the elements $y^\alpha = y_1^{\alpha_1} \cdots y_n^{\alpha_n}$ form an $A^{\underline{D}}$-basis (Theorem **2.11**, i). But $A^{\underline{D}} = F[[y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}}, z_{n+1}, \ldots, z_n]]$, then the elements y^α are linarly independent on $k[y_1^{p^{s_1}}, \ldots, y_n^{p^{s_n}}] \subset A^{\underline{D}}$. From Theorem **3.2**, it follows that $z_1^{\alpha_1} \cdots z_n^{\alpha_n}$, $z_i = y_i^{p^{s_i}}$, $i = 1, \ldots, n$, can belong to a linear basis of $A^{\underline{D}}$ on $(A^{\underline{D}})^{p^s}$, $s = s_1 = \max\{s_1, \ldots, s_n\}$. ☐

References

[1] V. Bonanzinga, "Systems of integrable derivations " Le Matematiche **XLIX** (1994), Fasc. I, 35–51.
[2] A. Frölich, "Formal groups ", Lecture Notes in Math. **74** (1968).
[3] W. Kuan, "A note on a lemma of Zariski and higher derivations ", Proceed. Am. Math. Soc. **42** No. 2 (1974).
[4] H. Matsumura, " Commutative algebra", Ben. Inc. New York, (1980).
[5] H. Matsumura, "Integrable derivations " Nagoya Math. J. **87** (1982), 227–245.

[6] S. Montgomery, " Hopf algebras and their actions on rings", CBMS Lecture Notes **82** Amer. Math. Soc., (1993).

[7] F. Oort, D. Mumford, "Deformations and liftings of finite, cocommutative group schemes" Invent. Math. **5** (1968), 317–334

[8] G. Restuccia, A. Tyc, " Regularity of the ring of invariants under certain actions of finite abelian Hopf algebras in characteristic p " J. Algebra **159**, No. 2, (1993), 347–357.

[9] G. Restuccia, H. Matsumura, "Integrable derivations II " Atti Accademia Peloritana dei Pericolanti, Classe Sc. Fis., Mat. e Nat. **LXX** (1992), 153–172.

[10] G. Restuccia, H. Matsumura, "Integrable derivations III " Atti Accademia Peloritana dei Pericolanti, Classe Sc. Fis., Mat. e Nat. **LXXIII** (1995), 227–238.

[11] G. Restuccia, H.J. Schneider, "On actions of infinitesimal group schemes" J. Algebra, **261** (2003), 229-244.

[12] G. Restuccia, R. Utano, "n-dimensional actions of finite abelian Hopf algebras in characteristic $p > 0$ " Revue Roumaine, Tome **XLIII**, Vol. 9-10 (1998), 881–895.

[13] A. Tyc, "On F-integrable actions of the restricted Lie algebra of a formal group F in characteristic $p > 0$ " Nagoya Math. J. , **115** (1989), 125–137.

[14] W.C. Waterhouse, " Introduction to Affine Group Schemes", Springer-Verlag New York Inc., (1979).

[15] O. Zariski, "Studies in equisingularity, I - Equivalent singularities of plane algebroid curves " Amer. J. Math. **87** (1965), 507–536.

Gaetana Restuccia
e-mail: grest@dipmat.unime.it
Dipartimento di Matematica
Università di Messina
Contrada Papardo, salita Sperone, 31
98166 Messina

Rosanna Utano
e-mail: utano@dipmat.unime.it
Dipartimento di Matematica
Università di Messina
Contrada Papardo, salita Sperone, 31
98166 Messina