LE MATEMATICHE
Vol. XLIX (1994) – Fasc. I, pp. 35-51

SYSTEMS OF INTEGRABLE DERIVATIONS

VITTORIA BONANZINGA

Let A be a commutative k-algebra, with k a subring of A. We give the definition of n-dimensional differentiation of A over k which formally extends the known one of unidimensional differentiation and we study the group of all n-dimensional differentiations of A over k.

In the second part of the work we give some theorems of strong integrability for systems of derivations in terms of n-dimensional differentiation.

Introduction.

Let A be a commutative k-algebra and let $\mathrm{Der}_k(A)$ be the module of the k-derivations of A in itself.

If D is a derivation of A over k and $\mathrm{char}(k) = 0$, it is known that D is always strongly integrable over k, i.e. there exists an iterative unidimensional differentiation of A over k which lifts D ([4]).

If $\mathrm{char}(k) = p > 0$ and A is a separable field over k, $D^p = 0$ is a necessary and sufficient condition for the strong integrability ([4]), while if A is a ring separable over k, conditions for the integrability of D such that $D^p = 0$ are given in [1].

Now, considered a system of derivations $\underline{D} = \{D_1, \dots, D_n\}$ in the sense of [7], [1], non necessary independent, we say that $\underline{D}$ is integrable (strongly

Entrato in Redazione il 21 aprile 1994.

Work carried out with the funds of M.P.I. 60%, while Professor H. Matsumura had a contract in the University of Messina.

integrable) if there exists a n-dimensional (iterative) differentiation of A over k which lifts $\underline{D}$.

If $\mathrm{char}(k) = 0$, every commutative system of derivations is strongly integrable, while if $\mathrm{char}(k) = p > 0$, systems of strongly integrable derivations are considered in [7].

In this work we study the lifting problem for a system of derivations to a differentiation of dimension n, where n is the number of independent derivations of the system of derivations.
Precisely in n. 1 we define a n-dimensional differentiation and we study its main properties. After having defined a system of integrable and strongly integrable derivations we study the group $HS_k^n(A)$ of the n-dimensional differentiations of A over k.

In n. 2 we show that by the existence of a n-dimensional differentiation in the ring we can deduce theoretic properties of the ring (existence of an A-sequence formed by n elements, analytic independence of the same n elements, etc.).

We obtain theorems of structure for I-adically complete rings, I ideal of the ring, module the strong integrability of a system of independent derivations of the ring expressed by the existence of a differentiation of dimension n.

The author wishes to express her sincere thanks to Professor Matsumura, for his support to the present research and for his helpful advises.

1.- In this work, all rings are assumed to be commutative, noetherian, with a unit element.

Definition 1. *Let k be a ring and A be a k-algebra. A n-dimensional differentiation $\underline{D}$ (an infinite n-higher derivation in A) of A is a set of linear maps $\{D_\alpha : A \to A;\ \alpha \in N^n\}$ such that $D_0 = \mathrm{id}_A$ and*

$$(1) \qquad D_\gamma(a \cdot b) = \sum_{\alpha+\beta=\gamma} D_\alpha(a) \cdot D_\beta(b)$$

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

Such a definition is a formal extension of the definition of 1-dimensional differentiation $\underline{D}$ of A (in the sense of Hasse-Schmidt). The set of n-dimensional differentiations of A is denoted by $HS^n(A)$.

As for the 1-dimensional differentiations we can associate to a n-dimensional differentiation, a ring homomorphism E from A into $A[[X_1, X_2, \ldots, X_n]]$ such that $E(a) \equiv a \bmod (X_1, X_2, \ldots, X_n)$ and precisely

$$E(a) = \sum_\alpha D_\alpha(a) X^\alpha$$

with $\alpha \equiv (\alpha_1, \alpha_2, \ldots, \alpha_n) \in N^n$, $X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n}$.

Then E is a ring homomorphism of A into $A[[X_1, X_2, \ldots, X_n]]$, and conversely any such homomorphism E comes from a n-dimensional differentiation of A. Sometimes we identify E with $\underline{D}$.

Let k be a ring and A be a k-algebra. Given a k-algebra homomorphism:

$$\Phi_1 : A \to A[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^2$$

such that

$$\Phi_1(a) \equiv a \bmod (X_1, \ldots, X_n) \tag{2}$$

we can associate n derivations of A: $D_1, \ldots, D_n$ and condition (2) can be expressed in this way:

$$\Phi_1(a) = a + D_1(a)X_1 + \ldots + D_n(a)X_n\,.$$

Definition 2. *Let k a subring of A. A n-dimensional differentiation $\underline{D}$ of A is called a n-dimensional differentiation (or n-differentiation) of A over k if $D_\alpha(a) = 0$ for all $\alpha \neq 0$ and for all $\alpha \in k$.*

The set of such n-differentiations is denote by $HS_k^n(A)$.

Notation. If $\gamma = (\gamma_1, \ldots, \gamma_n)$ and $\alpha = (\alpha_1, \ldots, \alpha_n)$ then the symbol $\binom{\gamma}{\alpha}$ denotes the product of the binomial coefficients: $\binom{\gamma}{\alpha} = \binom{\gamma_1}{\alpha_1} \cdots \binom{\gamma_n}{\alpha_n}$.

Definition 3. *A n-differentiation $\underline{D}$ is said to be iterative if:*

$$D_\alpha \circ D_\beta = \binom{\alpha+\beta}{\alpha} D_{\alpha+\beta} \quad \textit{for all } \alpha, \beta \in N^n.$$

Remark 1. We note that, in characteristic 0, for any commutative set of n derivations $D_1, \ldots, D_n$, if we put $D_{(h_1,\ldots,h_n)} = \dfrac{1}{h_1! \ldots h_n!} D_1^{h_1} \ldots D_n^{h_n}$, we get a n-dimensional differentiation and we have $D_\alpha \circ D_\beta = \binom{\alpha+\beta}{\alpha} D_{\alpha+\beta}$.
(In substance, the Definition 3 is a generalization of that one given in [4]).

Definition 3′. *We say that a n-differentiation $\underline{D}$ is iterative if the following diagram:*

$$\begin{array}{ccc} A & \xrightarrow{E_X} & A[[X]] \\ {\scriptstyle E_{X+Y}}\downarrow & & \downarrow{\scriptstyle E_Y} \\ A[[X+Y]] & \xrightarrow{i} & A[[X,Y]] \end{array}$$

is commutative, where $X = (X_1, X_2, \ldots, X_n)$, $Y = (Y_1, Y_2, \ldots, Y_n)$, i is the inclusion map and $E_Y(X) = X$.

Definitions 3 and 3′ are equivalent because the usual check in the classic case holds this case too; more generally, the equivalence follows by the relation

$$(X+Y)^{\alpha} = \sum \binom{\alpha}{\beta} X^{\beta} Y^{\alpha-\beta},$$

even if X, Y, α, β are n-tuples.

Definition 4. *Given n independent derivations $D_1, \ldots, D_n \in \mathrm{Der}(A)$ we say that they form a n-integrable set if there exists a ring homomorphism $E : A \to A[[X_1, X_2, \ldots, X_n]]$ such that*

$$E(a) = a + D_1(a)X_1 + \ldots + D_n(a)X_n + \ldots$$

Such an homomorphism E is called n-dimensional integral of $D_1, \ldots, D_n$.

Definition 5. *Given n independent derivations $D_1, \ldots, D_n \in \mathrm{Der}(A)$ we say that they form a n-integrable set over k if there exists a differentiation $\underline{D} = \{D_\alpha : A \to A; \alpha \in N^n\} \in HS_k^n(A)$ with $D_{(0,\ldots,\underset{i}{1},\ldots 0)} = D_i$.*

Definition 6. *We say that differentiations $\underline{D} = \{D_\alpha : A \to A;\ \alpha \in N^n\}$ and $\underline{D'} = \{D'_\beta : A \to A;\ \beta \in N^n\}$ commute if D_α and D'_β commute for every pair (α, β).*

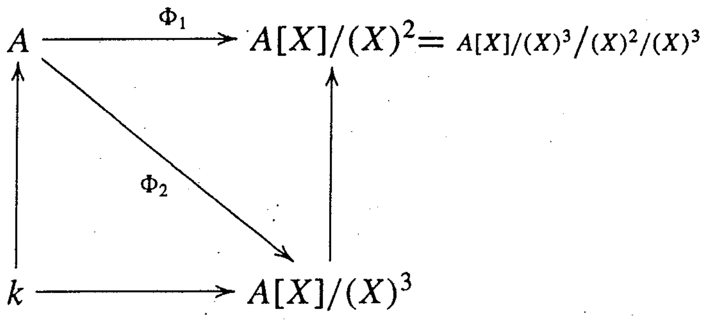
Proposition 1. *Let k be a ring. If A is a smooth k-algebra then every set of n independent derivations of A can be lifted to a n-differentiation.*

Proof. If $D_1, \ldots, D_n$ is a set of independent derivations of A over k there exists a k-algebra homomorphism:

$$\Phi_1 : A \to A[X]/(X)^2$$

(where $X = (X_1, X_2, \ldots, X_n)$), such that $\Phi_1(a) \equiv a \mod (X)$.

Since A is a smooth k-algebra, we have the following commutative diagram:



For the formal smoothness there exists $\Phi_2 : A \to A[X]/(X)^3$ and so, for $\Phi_n : A \to A[X]/(X)^{n+1}$ such that $\Phi_{n-1}(a) \equiv \Phi_n(a) \mod (X)^n$; for all n.

Since $A[[X]] = \varprojlim A[X]/(X)^n$, Φ_1 can be lifted to a k-algebra homomorphism $E : A \to A[[X]]$ such that

$$E(a) = a + \sum_{i=1}^{n} D_i(a)X_i + \ldots = \sum_{\alpha} D_\alpha(a)X^\alpha ,$$

and so the proof is complete. □

Remark 2. In characteristic 0, every set commutative of n derivations D_1, $D_2, \ldots, D_n$ is n-integrable and its integral is:

$$E(a) = \sum_{\alpha} \frac{1}{\alpha_1! \ldots \alpha_n!} D_1^{\alpha_1} \ldots D_n^{\alpha_n}(a) X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n} ,$$

with $\alpha \equiv (\alpha_1, \ldots, \alpha_n) \in N^n$, by Remark 1.

Remark 3. If $\alpha = (\alpha_1, \ldots, \alpha_n) \in N^n$, then $|\alpha|$ stands for $\alpha_1 + \ldots + \alpha_n$.

Let $E : A \to A[[X_1, \ldots, X_n]]$ be a k-algebra morphism so defined:

$$E(a) = \sum_{\alpha} D_\alpha(a)X^\alpha,$$

with $D_0 = \mathrm{id}_A$, then $D_\alpha : A \to A$ is a k-derivations $\forall \alpha \in N^n$ with $|\alpha| = 1$.

Remark 4. If $\underline{D} = \{D_\alpha : A \to A;\ \alpha \in N^n\}$ is a differentiation and $E : A \to A[[X_1, \ldots, X_n]] = A[X]$ is the corresponding ring homomorphism $(E(a) = \sum_\alpha D_\alpha(a)X^\alpha)$ then E can be extended to a map $A[[X]] \to A[[X]]$, by:

$$E\left(\sum_\alpha a_\alpha X^\alpha\right) = \sum_\alpha E(a_\alpha)X^\alpha . \tag{3}$$

It is easy to see that this is an endomorphism of the ring $A[[X]]$.

Any element ξ of $A[[X]] = A[[X_1, \ldots, X_n]]$ can be written

$$\xi = \xi_r + \xi_{r+1} + \ldots,$$

where ξ_i is a homogeneous polynomial of degree i in $X_1, \ldots, X_n$ with coefficients in A. If $\xi_r \neq 0$ then ξ_r is called the *initial form* and is denoted by $\mathrm{In}(\xi)$. Its degree r is called the *initial degree* and is denoted by $v(\xi)(\in N)$.

Then, for $\xi \in A[[X]]$ we have

$$\mathrm{In}(E(\xi)) = \mathrm{In}(\xi) \tag{4}$$

or equivalently

$$v(E(\xi) - \xi) > v(\xi). \tag{5}$$

Formula (4) shows that $E(\xi) \neq 0$ if $\xi \neq 0$, i.e. that E is injective. We claim that E is also surjective (hence an automorphism of $A[[X]]$). To prove this, take $\eta = \eta_0 + \eta_1 + \ldots \in A[[X]]$, and construct $\xi = \xi_0 + \xi_1 + \xi_2 + \ldots$ (where ξ_i is a form of degree i) such that $E(\xi) = \eta$ inductively by

$$\xi_0 = \eta_0,$$

$$\xi_i = \text{the homogeneous part of degree } i \text{ of } \eta - \sum_{j=0}^{i-1} E(\xi_j).$$

Then $v\left(\eta - \sum_{j=0}^{i} E(\xi_j)\right) > i$, and so $E\left(\sum_{i=0}^{\infty} \xi_i\right) = \eta$.

The set G of all such automorphisms of $A[[X]]$ is characterised by formula (4). Therefore it is easy to see that

1) $E, E' \in G \Rightarrow E \cdot E' \in G$

2) $E \in G \Rightarrow E^{-1} \in G$.

Therefore G is a subgroup of Aut $(A[[X]])$.

Explicitly, if $E(a) = \sum_\alpha D_\alpha(a)X^\alpha$, $E'(a) = \sum_\beta D'_\beta(a)X^\beta$, $(EE')(a) = \sum_\gamma D''_\gamma(a)X^\gamma$, then

$$(EE')(a) = E(E'(a)) = \sum_\beta X^\beta E(D'_\beta(a)) = \sum_{\alpha,\beta} X^{\alpha+\beta}(D_\alpha(D'_\beta(a)))$$

hence

$$D''_\gamma = \sum_{\alpha+\beta=\gamma} D_\alpha D'_\beta = \sum_{\alpha\leq\gamma} D_\alpha D'_{\gamma-\alpha}$$

(where if $\alpha, \beta \in N^n$, $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n)$, then we write $\alpha \leq \beta$ if $\alpha_i \leq \beta_i \ \forall i$, and $\alpha < \beta$ if $\alpha \leq \beta$ and $\alpha \neq \beta$).

Let us write D_i for $D_{(0,\dots,\underset{i}{1},\dots0)}$. Then we have $D''_i = D_i + D'_i$.

The explicit form of E^{-1} can be obtained as follows. Set $E^{-1} = E^*$, $E^*(a) = \sum_\alpha D^*_\alpha(a)X^\alpha$ $(a \in A)$. Then D^*_α' s are obtained by solving the equations

$$\sum_{\alpha\leq\gamma} D_\alpha D^*_{\gamma-\alpha} = 0 \quad (\gamma \neq 0).$$

Hence inductively

$$D^*_0 = \text{id}, \quad D^*_\gamma = -\sum_{0<\alpha\leq\gamma} D_\alpha D^*_{\gamma-\alpha}.$$

For instance

$$D^*_i = -D_i \qquad (i = 1, 2, \dots, n),$$

$$D^*_{(2,0,\dots,0)} = -D_{(2,0,\dots,0)} - D_1 D^*_1 = D_1^2 - D_{(2,0,\dots,0)},$$

$$D^*_{(1,1,0,\dots,0)} = -D_1 D^*_2 - D^*_2 D_1 - D_{(1,1,0,\dots,0)} = D_1 D_2 + D_2 D_1 - D_{(1,1,0,\dots,0)}.$$

Definition 7. *Let $\underline{D} = \{D_\alpha : A \to A;\ \alpha \in N^n\}$ and $\underline{D}' = \{D'_\alpha : A \to A;\ \alpha \in N^n\}$ be n-dimensional differentiations. If E and E' are their corresponding homomorphisms, we define $\underline{D} \cdot \underline{D}'$ as the n-dimensional differentiations corresponding to $E \circ E'$. As a consequence of Remark 4, we have: $(D \circ D')_\gamma = \sum_{0<\alpha\leq\gamma} D_\alpha D'_{\gamma-\alpha}$.*

Moreover, the set of all n-dimensional differentiations is a group.

Example. Let $A = k[T_1, \dots, T_r] = k[\underline{T}]$ and let $\Psi_1(\underline{X}), \Psi_2(\underline{X}), \dots, \Psi_r(\underline{X}) \in A[[X]] = A[[X_1, \dots, X_n]]$ be such that $\Psi_i(0) = T_i$, $(1 \le i \le r)$. Then there exists one and only one homomorphism of k-algebras $E : A \to A[[X]]$ such that:

$$E(T_i) = \Psi_i = T_i + \sum_{j=1}^{n} f_{ij} X_j + \sum_{j,k=1}^{n} f_{ijk} X_j X_k + \dots .$$

This is the n-dimensional differentiation which lifts $D_1, D_2, \dots, D_n \in \mathrm{Der}_k(A)$, where $D_j = \sum_{i=1}^{r} f_{ij} \frac{\partial}{\partial T_i}$.

This differentiation is not iterative because it doesn't check the diagram of Definition 3′.

2.- We extend, some results relative to unidimensional differentiations and contained in [7] to the n-dimensional differentiations.

From now on, if $E(a) = \sum_{\alpha} D_\alpha(a) X^\alpha$ is a n-dimensional differentiation, we always denote $D_{(0,\dots,\underset{i}{1},\dots0)}$ by D_i.

Proposition 2. *Let A be a commutative ring and $E : A \to A[[X_1, \dots, X_n]]$ a n-dimensional differentiation. Put $A_0 = \{a \in A \mid E(a) = a\}$. Let $x \in A$ such that*

$$E(x) = x + \sum_{i=1}^{n} a_i X_i$$

with some a_i invertible and $\bigcap_{n=1}^{\infty} x^n A = (0)$.

Then, if $z \in A$ and $xz \in A_0$, we have $z = 0$. Consequently x is not a zero-divisor of A and $A_0 \cap xA = (0)$.

Proof.

$$xz = E(xz) = E(x)E(z) = \left(x + \sum_{i=1}^{n} a_i X_i\right)\left(z + \sum_{i=1}^{n} D_i(z) X_i + \dots\right) =$$

$$= xz + \sum_{i=1}^{n} X_i (a_i z + x D_i(z)) + \sum_{i=1}^{n} X_i^2 \left(a_i D_i(z) + x D_{(0,\dots,\underset{i}{2},\dots,0)}\right) + \dots$$

Therefore, we have:

$$a_i z + x D_i(z) = 0\,,$$
$$a_i D_i(z) + x D_{(0,\dots,\underset{i}{2},\dots 0)}(z) = 0\,,$$
$$\dots\dots\dots\dots\dots\dots$$
$$a_i D_{(0,\dots,\underset{i}{n},\dots 0)}(z) + x D_{(0,\dots,\underset{i}{n+1},\dots 0)}(z) = 0$$

and so on. It follows that, if a_i is invertible, $z \in x^n A$ for all $n > 0$. Therefore $z = 0$. □

Proposition 3. *Let A be a noetherian ring and let $x_1, x_2, \dots, x_r$ be elements of the Jacobson radical* $\mathrm{Rad}(A)$ *of A. We put $I = Ax_1 + \dots + Ax_r$. Suppose either:*
(α) A contains Q, and there exist r derivations $D^{(1)}, \dots, D^{(r)} \in \mathrm{Der}(A)$ such that $\det(D^{(i)}(x_j)) \in U(A) = \{$*units of* $A\}$ *and* $[D^{(i)}, D^{(j)}] = 0$*; or*
(β) there exists a r-dimensional differentiation $E : A \to A[[Y_1, \dots, Y_r]]$ such that

$$E(x_j) = x_j + \sum_{i=1}^{r} D^{(i)}(x_j) Y_i$$

$j = 1, \dots, r$, and $\det(D^{(i)}(x_j)) \in U(A)$. *Put $F = \{a \in A \mid D^{(1)}a = \dots = D^{(r)}a = 0\}$ in case α, and $F = \{a \in A \mid E(a) = a\}$ in case β. Then F is a subring of A and $F \cap I = (0)$.*

Proof. In case α, replacing $D^{(i)}$ by suitable linear combinations we may assume that $D^{(i)}(x_i) = \delta_{ij}$. Then the iterative differentiation:

$$E(a) = \sum_{\alpha} \frac{1}{\alpha_1! \dots \alpha_r!} D^{(1)^{\alpha_1}} D^{(2)^{\alpha_2}} \dots D^{(r)^{\alpha_r}}(a) Y_1^{\alpha_1} Y_2^{\alpha_2} \dots Y_r^{\alpha_r}$$

satisfies condition (β). Since the condition (α) implies (β), it suffices to prove the proposition by hypothesis (β). We proceed by induction on r. When $r = 1$ the assertion is true by [7] Theorem 2.

We consider the differentiation E^* constructed by $D^{(2)}, \dots, D^{(r)}$. Since $D^{(2)}(x_1) = \dots = D^{(r)}(x_1) = 0$, $\overline{D}^{(2)}, \dots, \overline{D}^{(r)}$ are derivations of the quotient. Thus E^* passes to the quotient $\mathrm{mod} x_1 A$. $E^*(x_1) = x_1 \in x_1 A$ and we have

$$\overline{E}^*(x_j) = x_j + \overline{D}^{(2)} x_j Y_2 + \dots + \overline{D}^{(r)} x_j Y_r\,.$$

Now let $y \in F \cap I$, $y \in F$. It results then $\overline{E}^*(\overline{y}) = \overline{y}$ and $\overline{y} \in (\overline{x}_2, \dots, \overline{x}_r)$. Therefore $\overline{y} = 0$ by the induction hypothesis. Thus $y = x_1 z$ with some $z \in A$. Since

$$E(x_1) = x_1 + D^{(1)}(x_1) Y_1 + \dots + D^{(r)}(x_1) Y_r$$

and since $x_1 \in \mathrm{Rad}(A)$, we can apply Proposition 2 to conclude $z = 0$, $y = 0$. □

Proposition 4. *Let A be a noetherian ring, let $x_1, x_2, \dots, x_n \in \mathrm{Rad}(A)$ and let $E : A \to A[[X_1, \dots, X_n]]$ be a n-dimensional differentiation such that $\det(D_i(x_j)) \in U(A)$, where D_i $i = 1, \dots, n$ are the derivations associated to E. Then $(x_1, x_2, \dots, x_n)$ is a regular sequence.*

Proof. Replacing D_i with $\sum c_{ij} D_j$, where c_{ij} are elements of the inverse matrix of $(D_i(x_j))$, we may assume that $D_j(x_j) = \delta_{ij}$. In particular we have $D_1(x_1) = 1$, $D_2(x_1) = \dots = D_n(x_1) = 0$. We consider the homomorphism $E : A \to A[[X_1, \dots, X_n]]$ such that

$$E(x_j) = x_j + \sum_{i=1}^{n} D_i(x_j) X_i ;$$

it results $E(x_1) = x_1 + X_1$, then by Proposition 2, x_1 is regular. In the ring $A/(x_1)$ we can consider the derivations of the quotient $\overline{D}_2, \dots, \overline{D}_n$ and the differentiation

$$\overline{E}(\overline{x}_j) = \overline{x}_j + \overline{D}_2 \overline{x}_j X_2 + \dots + \overline{D}_n \overline{x}_j X_n .$$

Since $\overline{D}_2 \overline{x}_2 = 1$, by the same reasoning, we can find that $\overline{x}_2$ is regular in $A/(x_1)$ and $\overline{D}_3 \overline{x}_2 = \dots = \overline{D}_n \overline{x}_2 = 0$. Proceeding by induction, we deduce that $\forall i$, x_i is regular in $A/(x_1, \dots, x_{i-1})$, i.e. $(x_1, \dots, x_n)$ is an A-regular sequence. □

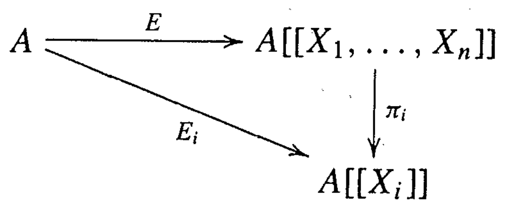
Proposition 5. *Given n 1-dimensional differentiations*

$$E_i : A \to A[[X_i]] , \quad i = 1, \dots, n ,$$

there exists a n-dimensional differentiation

$$E : A \to A[[X_1, \dots, X_n]]$$

such that the following diagram



(where π_i is the projection of $A[[X_1, \dots, X_n]]$ into the residue class ring

$$A[[X_1, \dots, X_n]]/(X_1, \dots, \widehat{X}_1, \dots, X_n) \cong A[[X_i]])$$

is commutative for all i, $i = 1, \dots, n$.

Moreover, if the homomorphisms E_i are iterative and commute then E is iterative too.

Proof. Using the n unidimensional differentiations E_i defined by $E_i(a) = \sum_{n=0}^{\infty} X_i^n D_n(a)$, we set $E(a) = \sum_{\alpha} D_\alpha(a) X^\alpha$, $\alpha = (\alpha_1, \ldots, \alpha_n)$, where $D_\alpha = D^{(1)}_{\alpha_1} \circ D^{(2)}_{\alpha_2} \circ \ldots \circ D^{(n)}_{\alpha_n}$. Obviously, $E \equiv E_i \mod (X_1, \ldots, \widehat{X_i}, \ldots, X_n)$. Let us prove that E is an n-dimensional differentiation. The only non trivial fact is the equality $E(ab) = E(a)E(b)$. Let us use induction on n. For $n = 1$, there is nothing to prove; so, let us suppose the equality true for $n-1$. This means that $E^*(a) = \sum D^{(2)}_{\alpha_2} \ldots D^{(n)}_{\alpha_n}(a) X^{(\alpha_2,\ldots,\alpha_n)}$ satisfies $E^*(ab) = E^*(a)E^*(b)$.

But, put $X_i^{\alpha_i} = X^{\alpha_i}$,

$$E(a) = \sum_{\alpha_1} D'_{\alpha_1}\left(\sum_{(\alpha_2,\ldots,\alpha_n)} D^{(2)}_{\alpha_2} \ldots D^{(n)}_{\alpha_n}(a) X^{\alpha_2} \ldots X^{\alpha_n}\right) X^{\alpha_1} =$$
$$= \sum_{\alpha_1} D'_{\alpha_1}(E^*(a)) X^{\alpha_1}$$

so that

$$E(ab) = \sum_{\alpha_1} D'_{\alpha_1}\left(E^*(ab)\right) X_1^\alpha = \sum_{\alpha_1} D'_{\alpha_1}\left(E^*(a)E^*(b)\right) X_1^\alpha =$$
$$= \sum_{\alpha_1} \sum_{\gamma_1+\delta_1=\alpha_1} D'_{\gamma_1}(E^*(a)) D'_{\delta_1}(E^*(b)) X^{\alpha_1}$$
$$E(a)E(b) = \sum_{\gamma_1} D'_{\gamma_1} E^*(a) X^{\gamma_1} \sum_{\delta_1} D'_{\delta_1} E^*(b) X^{\delta_1} =$$
$$= \sum_{\alpha_1} \sum_{\gamma_1+\delta_1=\alpha_1} D'_{\gamma_1}(E^*(a)) D'_{\delta_1}(E^*(b)) X^{\alpha_1}.$$

If the homomorphisms E_i are iterative and commute then the differentiation constructed above is iterative too. In fact:

$$D_\alpha \circ D_\beta(a) = D_\alpha(D_\beta(a)) = D_\alpha(D^{(1)}_{\beta_1} D^{(2)}_{\beta_2} \ldots D^{(n)}_{\beta_n}(a)) =$$
$$= D^{(1)}_{\alpha_1} D^{(2)}_{\alpha_2} \ldots D^{(n)}_{\alpha_n}(D^{(1)}_{\beta_1} D^{(2)}_{\beta_2} \ldots D^{(n)}_{\beta_n}(a)) =$$
$$= D^{(1)}_{\alpha_1} \circ D^{(1)}_{\beta_1} \circ \ldots \circ D^{(n)}_{\alpha_n} \circ D^{(n)}_{\beta_n}(a) =$$
$$= \frac{(\alpha_1+\beta_1)!}{\alpha_1!\beta_1!} \cdots \frac{(\alpha_n+\beta_n)!}{\alpha_n!\beta_n!} D^{(1)}_{(\alpha_1+\beta_1)} \cdots D^{(n)}_{(\alpha_n+\beta_n)}(a).$$

$$D_{\alpha+\beta}(a) = D_{(\alpha_1+\beta_1,\ldots,\alpha_n+\beta_n)}(a) = D^{(1)}_{(\alpha_1+\beta_1)} D^{(2)}_{(\alpha_2+\beta_2)} \cdots D^{(n)}_{(\alpha_n+\beta_n)}(a). \quad \square$$

Remark 5. We can reformulate Lipman's theorem using differentiations instead of derivations.

Let (A, m) be a noetherian local ring containing the rational number field Q and let $x_1, \dots, x_r \in m$, $I = (x_1, \dots, x_r)$.

Suppose that

(1) A is I-adically complete,

(2) there exists a r-dimensional differentiation

$$E : A \to A[[Y_1, \dots, Y_r]] = A[[Y]],$$

associated to a commutative set of independent derivations, such that

$$E(x_j) = x_j + \sum_{i=1}^{r} D_i(x_j)Y_i$$

and $\det(D_i(x_j)) \notin m$.

Then $A_0 = \{a \in A \mid E(a) = a\}$ is a subring of A such that $A = A_0[[x_1, \dots, x_r]]$, with $x_1, \dots, x_r$ analytically independent over A_0.

Since we are in characteristic 0, every commutative set of r derivations $D_1, \dots, D_r$, associated to a r-dimensional E, is r-integrable and its integral is

$$E(a) = \sum_{\alpha} \frac{1}{\alpha_1! \dots \alpha_r!} D_1^{\alpha_1} D_2^{\alpha_2} \dots D_r^{\alpha_r}(a) Y_1^{\alpha_1} Y_2^{\alpha_2} \dots Y_r^{\alpha_r}.$$

Proposition 6. *Let K be a separable extension field of a field k of characteristic $p > 0$. Let $D_1, \dots, D_n \in$* $\mathrm{Der}_k(K)$ *and $x_1, \dots, x_n \in K$ such that* $\det(D_i(x_j)) \neq 0$.

Then there exists an iterative n-dimensional $E : K \to K[[X_1, \dots, X_n]]$ associated to the system of derivations $\{D_1, D_2, \dots D_n\} \Leftrightarrow$

$$[D_i, D_j] \in \sum_{\alpha=1}^{n} K D_\alpha, \quad 1 \le i, j \le n \qquad D_i^p \in \sum_{\alpha=1}^{n} K D_\alpha \quad 1 \le i \le n.$$

Proof. It follows by Theorem 1 of [1] and by Proposition 4. □

Definition 8. *Let S be a ring of characteristic p and S^p denote the subring $\{x^p \mid x \in S\}$. Let S' be a subring of S. A subset Γ of S is said to be p-independent over S', if the monomials $b_1^{e_1} \dots b_n^{e_n}$, where $b_1, \dots, b_n$ are distinct elements of Γ and $0 \le e_i \le p - 1$, are linearly independent over $S^p[S']$. Γ is called a p-basis of S over S' if it is p-independent over S' and $S^p[S', \Gamma] = S$.*

Let B be a subring of A. We denote the differential module of A over B by $\Omega_B(A)$ and the canonical B-derivation by $d : A \to \Omega_B(A)$. For the definition and elementary properties we refer to [5], par. 25. It is not difficult to verify that if Γ is a p-basis of A over B then $\Omega_B(A)$ is a free A-module with $\{dy,\ y \in \Gamma\}$ as a basis. Not every rings have a p-basis and there are sets p-independent which cannot be extended to a p-basis.

Theorem 1. *Let (A, m) be a local ring containing a field k of characteristic $p > 0$. Let A be separable over k. Let $D_1, \ldots, D_n \in \mathrm{Der}_k(A)$. Set $A_0 = \{a \in A \mid D_i(a) = 0,\ i = 1, \ldots, n\}$. Suppose that*

1) there exist $x_1, \ldots, x_n \in A / \det(D_i(x_j)) \notin m$,
2) $\Omega_k(A_0)$ is a free A_0-module and A_0 is finite over $k[A_0^p]$,
3) there exists a p-basis B_0 of A_0 over k containing $x_1^p, \ldots, x_n^p$.
4) $$[D_i, D_j] \in \sum_{\alpha=1}^{n} AD_\alpha, \quad 1 \le i, j \le n \qquad D_i^p \in \sum_{\alpha=1}^{n} AD_\alpha, \quad 1 \le i \le n.$$

Then the system of derivations $\{D_1, D_2, \ldots D_n\}$ can be prolonged to an iterative n-dimensional differentiation.

Proof. Let (c_{ij}) be the inverse matrix of $(D_i x_j)$ and put $\partial_i = \sum_j c_{ij} D_j$.

Then $\partial_i x_j = \delta_{ij}$, and $\sum_{i=1}^{n} AD_i = \sum_{i=1}^{n} A\partial_i$, $[\partial_i, \partial_j] \in \sum A\partial_i$, $\partial_i^p \in \sum A\partial_j$ (this last follows from the Hochschild formula $(aD)^p = a^p D^p + (aD)^{p-1}(a)D$, [5], p. 197). But if $[\partial_i, \partial_j] = \sum_k b_{ijk}\partial_k$ then $b_{ijk} = [\partial_i, \partial_j]x_k = 0$ for all k, therefore $[\partial_i, \partial_j] = 0$. Similarly $\partial_i^p = 0$.

By Theorem 1 of [2], $x_1, x_2, \ldots, x_n$ is a p-basis of A over A_0. Thus $x_1, x_2, \ldots x_n$ are *p-independent* over A_0.

Moreover, with the same process that is found in theorem 7 of [4], for the separability of A over k, we can obtain that $x_i^p \notin A_0^p k$, and x_i^p can belong to a p-basis B_0 of A_0 over k.

Let $B_0^* = B_0 \setminus \{x_1^p, \ldots, x_n^p\}$.

Put $B = B_0^* \cup \{x_1, x_2, \ldots x_n\}$.

It results $A = A_0[x_1, x_2, \ldots x_n]$ (since $x_1, x_2 \ldots x_n$ is a p-basis of A over A_0).

Set $y_i = x_i^p$, $1 \le i \le n$, we have

$$A = A_0[X_1, \ldots, X_n]/(X_1^p - y_1, \ldots, X_n^p - y_n).$$

Set $I = (X_1^p - y_1, \ldots, X_n^p - y_n)$ and $(\underline{X}) = (X_1, X_2, \ldots, X_n)$.

Since

$$\Omega_k(A_0[\underline{X}]) \cong (\Omega_k(A_0) \otimes_{A_0} A_0[\underline{X}]) \oplus A_0[\underline{X}]dX_1 \oplus \ldots \oplus A_0[\underline{X}]dX_n,$$

$\Omega_k(A_0)$ is a free module with basis dB_0 and the following sequence

$$I/I^2 \to \Omega_k(A_0[\underline{X}]) \otimes A \to \Omega_k(A) \to 0,$$

is exact, we have

$$\Omega_k(A) \cong (\Omega_k(A_0) \otimes_{A_0} A)/(Ady_1 \oplus Ady_2 \oplus \ldots \oplus Ady_n) \oplus Adx_1 \oplus \ldots \oplus Adx_n,$$

i.e. $\Omega_k(A)$ is free with differential basis $B = B_0^* \cup \{x_1, x_2, \ldots, x_n\}$, i.e. B is a p-basis of A over k.

Since A is separable over k, $A \otimes_k k^{p^{-1}}$ is reduced and we can settle on the grounds of the theorem of [8].

The homomorphism $E : A \to A[[X_1, X_2, \ldots, X_n]]$ defined by $E(x_j) = x_j + \sum_{i=1}^{n} D_i(x_j)X_i$, $1 \leq j \leq n$ is the iterative differentiation sought.

The following results concern the case of a set of derivations $\mathscr{D} = \{D_1, D_2, \ldots, D_n\}$ which aren't necessarily independent.

In such ambit we have the following result:

Corollary 1. ([8] Corollary 3.2). *Let A be a k-algebra such that the ring $A \otimes_k k^{p^{-1}}$ is reduced and let Γ be a p-basis of A over k. For any set of k-derivations $d_1, \ldots, d_m : A \to A$ there exists a m-dimensional differentiation $\underline{D} : A \to A[[X_1, \ldots, X_m]]$*

$$\underline{D}(a) = \sum_{\alpha} D_\alpha(a) X^\alpha$$

with $\alpha \equiv (\alpha_1, \alpha_2, \ldots, \alpha_m) \in N^m$, $X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_m^{\alpha_m}$, such that $D_0 = \mathrm{id}_A$ and $D_{(0,\ldots,0,\underset{i}{1},0,\ldots,0)} = d_i$, $i = 1, \ldots, m$, with 1 on the i-th position.

Remark 5. We notice that the $d_1, \ldots, d_m$ of Corollary 1 are ordinary derivations and they can be dependent or independent. If A is a field K, k doesn't necessarily coincides with the subfield of the constants K_0. In general $k \subseteq K_0$. The hypothesis K has a p-basis (also infinite over k) is too strong. In fact we can deduce that K has a finite p-basis over K_0. (Theorem 7 [4]).

If $d_1, \ldots, d_m$ are dependent derivations of which are independent $s < m$, by renaming and reordering we can suppose that the first s derivations are independent. If $\Gamma = \{x_1, \ldots, x_s\}$ is a p-basis of K over K_0, we can define $d_i(x_j) = \delta_{ij} 1 \leq i, j \leq s$. If $d_1, \ldots, d_m$ are not linearly independent we can't suppose that $d_i(x_j) = \delta_{ij}$ $1 \leq i, j \leq m$.

We reformulate Proposition 6 and Theorem 1 in the case of a set of derivations not necessarily independent.

Theorem 2. *Let K be a separable extension field of a field k of characteristic $p > 0$. Let $\mathscr{D} = \{D_1, D_2, \dots D_n\}$ be a set of derivations of K over k such that $D_1, D_2 \dots D_r$ with $r < n$ are independent. Let $x_1, x_2, \dots x_r \in K$ such that*

$$\det(D_i(x_j)) \neq 0\,, \quad 1 \leq i, j \leq r.$$

We suppose that $\left[D_i, D_j\right] = 0$ and $D_i^p = 0$, $1 \leq i, j \leq r$, $1 \leq i \leq r$.

Then we have the following facts:

1) $D_1, D_2, \dots D_r$ are strongly integrable.

2) We can find integrals of $E^{(1)}, \dots, E^{(r)}$ of $D_1, D_2, \dots D_r$ such that $E^{(i)}$ and $E^{(j)}$ commute, for any i, j.

3) There exist integrals of $D_{r+1}, \dots, D_n$ of the form $E^{(1)}_{\lambda_1} \circ \cdots \circ E^{(r)}_{\lambda_r}$ where $\lambda_1, \dots, \lambda_r \in K$ and $E^{(i)}_{\lambda_i}$ is the homomorphism associated to the differentiation

$$\underline{D}_{\lambda_i} = \{1, \lambda_i D_j^{(1)}, \lambda_i^2 D_j^{(2)}, \dots, \lambda_i^n D_j^{(n)}, \dots\}\,, \quad 1 \leq i, j \leq r\,.$$

Proof. To integrate $\mathscr{D} = \{D_1, D_2, \dots D_n\}$ we find n ring homomorphisms $E^{(i)}, \dots, E^{(n)}$ that lift $D_1, D_2 \dots D_n$ respectively. We observe that $E^{(1)}, \dots, E^{(r)}$ don't have ties because $D_1, D_2, \dots D_r$ are independent. Given two differentiations $\underline{D}_i = \{1, D_{i_1}, D_{i_2}, \dots\}$ with $D_{i_1} = D_i$ and $\underline{D}_j = \{1, D_{j1}, D_{j2}, \dots\}$ with $D_{j1} = D_j$, we can define the product $\underline{D}_i \cdot \underline{D}_j$ by the automorphisms $E^{(i)}$ and $E^{(j)}$ associated to $\underline{D}_i$ and $\underline{D}_j$ respectively. The differentiation obtained

$$\underline{D}_i \cdot \underline{D}_j = \{1, D_{i_1} + D_{j_1}, \dots\}$$

is an unidimensional differentiation that lifts the sum $D_{i_1} + D_{j_1}$.

If $\underline{D}_i = \{1, D_{i_1}, D_{i_2}, \dots\}$ is an unidimensional differentiation of A and $\lambda_i \in A$ then the differentiation $\underline{D}_{i_{\lambda_i}} = \{1, \lambda_i D_{i_1}, \lambda_i^2 D_{i_2}, \dots\}$ is a differentiation that lifts $\lambda_i D_{i_1}$. Then there exists an unidimensional differentiation that lifts $\lambda_1 D_1 + \lambda_2 D_2 + \dots + \lambda_r D_r$, that one which we obtain putting in order $E^{(1)}_{\lambda_1}, \dots, E^{(r)}_{\lambda_r}$ and thus there exist integrals of $D_{r+1}, \dots, D_n$ of the form $E^{(1)}_{\lambda_1} \circ \cdots \circ E^{(r)}_{\lambda_r}$. □

Definition 9. *We say that a set $\mathscr{D} = \{D_1, D_2, \dots D_n\}$ of derivations of a field K is integrable if there are s unidimensional differentiations $E^{(1)}, \dots, E^{(s)}$ that commute and integrate $D_1, D_2, \dots D_s$ if $s < n$ are independent derivations and $D_{s+1}, \dots, D_n$ have each one an integral unidimensional that we can obtain from $E^{(1)}, \dots, E^{(s)}$.*

Theorem 3. *Let (A, m) be a local ring containing a field k of characteristic $p > 0$. Let A be separable over k. Let $D_1, \ldots, D_n$ be a set of derivations of A over k, such that $D_1, \ldots, D_r$ with $r < n$ are independent. Set $A_0 = \{a \in A \mid D_i(a) = 0,\ i = 1, \ldots, n\}$. We suppose that*

1) there exist $x_1, \ldots, x_r \in A / \det(D_i(x_j)) \notin m$ $1 \leq i, j \leq r$,
2) $\Omega_k(A_0)$ is a free A_0-module and A_0 is finite over $k[A_0^p]$,
3) there exists a p-basis B_0 of A_0 over k containing $x_1^p, \ldots, x_n^p$,
4) $[D_i, D_j] = 0$ $\quad 1 \leq i, j \leq r$ $\qquad D_i^p = 0$ $\quad 1 \leq i \leq r$.
Then

1) There exists an iterative r-dimensional integral $\underline{E}^{(r)}$ for $D_1, D_2, \ldots D_r$.

2) For any $D_{r+1}, \ldots, D_n$ there exists an iterative unidimensional integral of the form $E^{(1)}_{\lambda_1} \circ \cdots \circ E^{(r)}_{\lambda_r}$ where $E^{(i)}$ $1 \leq i \leq r$ is obtained by $\underline{E}^{(r)}$ putting $X_1 = \ldots = \widehat{X}_i = \ldots = X_r = 0$.

Proof. Let $\underline{E}^{(r)}$ be the integral relative to $D_1, D_2, \ldots D_r$ (see Theorem 2). Let $E^{(1)}, \ldots E^{(r)}$ be unidimensional integrals obtained by $\underline{E}^{(r)}$ putting $X_1 = \ldots = \widehat{X}_i = \ldots = X_r = 0$.

$E^{(1)}$ integrates $D_1, \ldots, E^{(r)}$ integrates D_r.

Let $D_i, r + 1 \leq i \leq n . D_i = \lambda_1 D_1 + \lambda_2 D_2 + \ldots + \lambda_r D_r$.

We consider $E^{(1)}_{\lambda_1}, \ldots, E^{(r)}_{\lambda_r}$, it is clear that we can get $E^{(1)}_{\lambda_1} \circ \cdots \circ E^{(r)}_{\lambda_r}$ integral of $D_i, r + 1 \leq i \leq n$. □

It is allowed to give the following:

Definition 10. *Let $\mathcal{D} = \{D_1, D_2, \ldots D_n\}$ a set of derivations of a ring A with $s < n$ independent derivations. To integrate $\mathcal{D}$ means to give an integral $\underline{E}$ of dimension r for the independent derivations and $n - r$ integrals of dimension 1 that we can always construct by $\underline{E}$.*

REFERENCES

[1] V. Bonanzinga, *Integrable derivations in rings of characteristic $p > 0$,* Atti Acc. Peloritana dei Pericolanti, 70 (1992), pp. 101 - 116.

[2] M. Crupi, *Subring of constants of a ring of characteristic $p > 0$,* Le Matematiche, 48 (1993), pp. 203 - 212.

[3] J. Lipman, *Free derivation modules on algebraic varieties,* Amer. J. Math., 87 (1965), pp. 874 - 898.

[4] H. Matsumura, *Integrable derivations,* Nagoya Math. J., 87 (1982), pp. 227 - 245.

[5] H. Matsumura, *Commutative ring theory,* Cambridge University Press, 1986.

[6] H. Matsumura, *Criteri Jacobiani,* Quaderni dei Gruppi di Ricerca Matem. del C.N.R., Istit. Matem. del Politecnico di Torino, 1975.

[7] H. Matsumura - G. Restuccia, *Integrable derivations II,* Acc. Peloritana dei Pericolanti, 70 (1992), pp. 153 - 172.

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

[9] A. Tyc, *Invariants of linearly reductive formal group actions,* J. Algebra, 101 (1986), pp. 166 - 187 .

Dipartimento di Matematica,
Università di Messina,
Contrada Papardo, Salita Sperone 31,
98166 Sant'Agata (Me), (ITALIA)