A. Tyc
Nagoya Math. J.
Vol. 115 (1989) 125–137

ON F-INTEGRABLE ACTIONS OF THE RESTRICTED LIE ALGEBRA OF A FORMAL GROUP F IN CHARACTERISTIC $p > 0$

ANDRZEJ TYC

§ 1. Introduction

Let k be an integral domain, let $F = (F_1(X, Y), \cdots, F_n(X, Y))$, $X = (X_1, \cdots, X_n)$, $Y = (Y_1, \cdots, Y_n)$, be an n-dimensional formal group over k, and let $L(F)$ be the Lie algebra of all F-invariant k-derivations of the ring of formal power series $k[\![X]\!]$ (cf. § 2). If A is a (commutative) k-algebra and $\mathrm{Der}_k(A)$ denotes the Lie algebra of all k-derivations $d: A \to A$, then by an action of $L(F)$ on A we mean a morphism of Lie algebras $\varphi: L(F) \to \mathrm{Der}_k(A)$ such that $\varphi(d^p) = \varphi(d)^p$, provided $\mathrm{char}(k) = p > 0$. An action of the formal group F on A is a morphism of k-algebras $D: A \to A[\![X]\!]$ such that $D(a) \equiv a \bmod (X)$ for $a \in A$, and $F_A \circ D = D_Y \circ D$, where $F_A: A[\![X]\!] \to A[\![X, Y]\!]$, $D_Y: A[\![X]\!] \to A[\![X, Y]\!]$ are morphisms of k-algebras given by $F_A(g(X)) = g(F)$, $D_Y(\sum_\alpha a_\alpha X^\alpha) = \sum_\alpha D(a_\alpha) Y^\alpha$, for a motivation of this notion, see [15]. Let $D: A \to A[\![X]\!]$ be such an action. Then, similarly as in the case of an algebraic group action, one proves that the map $\varphi_D: L(F) \to \mathrm{Der}_k(A)$ with $\varphi_D(d)(a) = \sum_\alpha a_\alpha d(X^\alpha)|_{X=0}$ for $d \in L(F)$, $a \in A$, and $D(a) = \sum_\alpha a_\alpha X^\alpha$, is an action of $L(F)$ on A.

Definition. An action $\varphi: L(F) \to \mathrm{Der}_k(A)$ of the Lie algebra $L(F)$ on a k-alegbra A is said to be F-integrable if there exists an action $D: A \to A[\![X]\!]$ of the formal group F on A such that $\varphi = \varphi_D$.

Observe that if $n = 1$, $F_a = X + Y$, and $F_m = X + Y + XY$, then an action of $L(F_a)$ (resp. $L(F_m)$) on a k-algebra A is nothing else than a k-derivation $d: A \to A$ with $d^p = 0$ (resp. $d^p = d$) whenever $\mathrm{char}(k) = p > 0$. Moreover, one readily checks that such d is F_a-integrable (resp. F_m-integrable) if there exists a differentiation (= higher derivation) $D = \{D_i: A \to A, i = 0, 1, \cdots\}$ such that $D_1 = d$ and $D_i \circ D_j = (i, j) D_{i+j}$ (resp.

Received September 14, 1987.

$D_i \circ D_j = \sum_r \binom{r}{i}\binom{i}{i+j-r} D_r$, where $\binom{u}{v} = 0$ for $v < 0$ or $v > u$) for all i, j. Thus we see that F_a-integrability amounts to strong integrability in the sense of [10].

If k is a field of characteristic 0, then from [15, Lemma 2.13] it follows that each action $\varphi: L(F) \to \mathrm{Der}_k(A)$ of F on an arbitrary k-algebra A is F-integrable. If k is not a field (being still of characteristic 0), then the above assertion is not true. For instance, if Z is the ring of rational integers and $A = Z[X]$, then the action of $L(F_a)$ on A given by the derivation $X \cdot \partial/\partial X$ is clearly not F_a-integrable. Nevertheless, also in this case there are some positive results, see [1, 12]. Now suppose that k is a field of characteristic $p > 0$. Then the situation is worse then that in characteristic 0. Namely, if $A = k[t]/(t^p)$ and $d: A \to A$ is the k-derivation induced by $\partial/\partial t$, then according to [10, Ex. 1] d is not integrable i.e., there does not exist a morphism of k-algebras $J: A \to A[\![X]\!]$ ($X = X_1$) such that $J(a) \equiv a + d(a)X \bmod (X^2)$ for all $a \in A$ (the existence of such J would imply: $0 \equiv J(t^p + (t^p)) = J(t + (t^p))^p \equiv X^p \bmod (X^{p+1})$). Hence the action of $L(F_a)$ on A defined by d is not F_a-integrable. However, Matsumura proved [10, Th. 7] that if A is a separable field extension of k, then every action of $L(F_a)$ on A is F_a-integrable. The goal of this paper is to extend Matsumura's result to a wider class of formal groups and to more general k-algebras. In particular, from our main result (cf. § 2) one derives the following.

THEOREM. *Let F be a one dimensional formal group over k, let $A = k[\![T_1, \cdots, T_m]\!]$, $m \geqslant 1$, and let $\varphi: L(F) \to \mathrm{Der}_k(A)$ be an action of $L(F)$ on A with $\varphi(y)(T_i) \notin (T_1, \cdots, T_m)$ for some $y \in L(F)$ and some i. Then φ is F-integrable, provided $F \simeq F_a$ or $F \simeq F_m$. Moreover, if the field k is algebraically closed, then φ is F-integrable for any F.*

Remark. If the field k is algebraically closed, then an action of F_a (resp, F_m) on a given k-algebra B is a differentiation $\{D_j: B \to B, j = 0, 1, \cdots\}$ such that $(D_{p^i})^p = 0$, $D_m = (D_{p^0})^{m_0} \circ \cdots \circ (D_{p^t})^{m_t}/(m_0! \cdots m_t!)$ (resp. $(D_{p^i})^p = D_{p^i}$, $D_m = (D_{p^0})_{m_0} \circ \cdots \circ (D_{p^t})_{m_t}$), $i, m = 0, 1, \cdots$, where $m = m_0 p^0 + \cdots + m_t p^t$ is the p-adic expansion of m and $(f)_j = f \circ (f-1) \circ \cdots \circ (f - j + 1)/j!$. The remark is well known for F_a (and is true for any field k of characteristic $p > 0$). As for the case of F_m, it may be deduced from [2, p. 127/128].

All rings in this paper are assumed to be commutative. A local ring is assumed to be Noetherian. A ring R is called reduced if it has no non-zero nilpotent elements.

§ 2. Preliminaries and formulation of the main result

Throughout this paper k denotes a fixed field of characteristic $p > 0$ and N stands for the set of non-negative rational integers.

Let S' be a subalgebra of a k-algebra S. A subset Γ of S is called a p-basis of S over S' if S is a free $S'[S^p]$-module ($S^p = \{s^p,\ s \in S\}$) and the set of all monomials $y_1^{i_1} \cdots y_t^{i_t}$, where $y_1, \cdots, y_t$ are distinct elements in Γ and $0 \leqslant i_r < p$, $r = 1, \cdots, t$, is a basis of S over $S'[S^p]$. As usual, $\Omega_{S'}(S)$ will denote the S-module of Kähler differentials over S' and $\delta\colon S \to \Omega_{S'}(S)$ will denote the canonical S'-derivation. It is not difficult to verify that if Γ is a p-basis of S over S', then $\Omega_{S'}(S)$ is a free A-module with $\{\delta y,\ y \in \Gamma\}$ as a basis. Given a k-algebra A, $\mathrm{Der}_k(A)$ will denote the restricted Lie algebra over k of all k-derivations $d\colon A \to A$ with $[d, d'] = d \circ d' - d' \circ d$ and $d^{[p]} = d^p$. If $d \in \mathrm{Der}_k(A)$ and $a \in A$, then ad is the k-derivation $x \to ad(x)$, $x \in A$.

By a formal group over a ring R we shall mean a one dimensional commutative formal group over R i.e., a formal power series $F(X, Y) \in R[\![X, Y]\!]$ such that $F(X, 0) = X$, $F(0, Y) = Y$, $F(F(X, Y), Z) = F(X, F(Y, Z))$, $F(X, Y) = F(Y, X)$, see [6]. Two important examples are the additive formal group $F_a = X + Y$ and the multiplicative one $F_m = X + Y + XY$. If F and G are formal groups over R, then a homomorphism $f\colon F \to G$ is a power series $f(X) \in R[\![X]\!]$ such that $f(0) = 0$ and $f(F(X, Y)) = G(f(X), f(Y))$. A homomorphism f is said to be an isomorphism if $f'(0)$ is an invertible element in R ($f'(X) = \partial f/\partial X$). Let $F = F(X, Y)$ be a formal group over the field k and let $d_i\colon k[\![X]\!] \to k[\![X]\!]$, $i \in N$, be the maps given by the equality

$$(1) \qquad g(F(X, Y)) = \sum_{i \geqslant 0} d_i(g(X)) Y^i, \qquad g \in k[\![X]\!].$$

We say that a function $t\colon k[\![X]\!] \to k[\![X]\!]$ is F-invariant if $t \circ d_j = d_j \circ t$ for all $j \in N$. It is clear that if $a, b \in k$ and $t, t'\colon k[\![X]\!] \to k[\![X]\!]$ are F-invariant functions, then $at + bt'$ and $t \circ t'$ are also F-invariant functions. Hence it follows that the set of all F-invariant k-derivations $d\colon k[\![X]\!] \to k[\![X]\!]$ is a restricted Lie subalgebra of the restricted Lie algebra $\mathrm{Der}_k(k[\![X]\!])$. This subalgebra is called the restricted Lie algebra of the formal group F and it is denoted by $L(F)$. Let $d_F\colon k[\![X]\!] \to k[\![X]\!]$ denote the k-derivation determined by $d_F(X) = \partial F(0, X)/\partial Z$ $(= \partial F(Z, X)\partial Z|_{Z=0})$. Then, similarly as in the case of algebraic groups, we have the following.

2.1 Lemma. *Let $f\colon F \to G$ be an isomorphism of formal groups over k and let $\tilde{f}\colon k[\![X]\!] \to k[\![X]\!]$ be the isomorphism of k-algebras induced by f (i.e., $\tilde{f}(g(X)) = g(f(X))$). Then $L(f)\colon L(F) \to L(G)$ with $L(f)(d) = \tilde{f}^{-1} \circ d \circ \tilde{f}$, is an isomorphism of restricted Lie algebras. Moreover, $L(F)$ is a one dimensional vector space over k spanned by d_F.*

Proof. Given an $H(X, Y) \in k[\![X, Y]\!]$ with $H(0, 0) = 0$ we denote by $\tilde{H}\colon k[\![X]\!] \to k[\![X, Y]\!]$ the homomorphism of k-algebras given by $\tilde{H}(g(X)) = g(H(X, Y))$. If $u, v\colon k[\![X]\!] \to k[\![X]\!]$ are k-linear maps, then $u \hat{\otimes} v\colon k[\![X, Y]\!] \to k[\![X, Y]\!]$ will denote the map taking $\sum a_{ij}X^iY^j$ into $\sum a_{ij}u(X^i)v(Y^j)$. It is easy to see that if $d \in \mathrm{Der}_k(k[\![X]\!])$, then $d \hat{\otimes} \mathrm{id} \in \mathrm{Der}_k(k[\![X, Y]\!])$. Moreover, a k-derivation d of $k[\![X]\!]$ is in $L(F)$ if and only if $\tilde{F} \circ d = (d \hat{\otimes} \mathrm{id}) \circ \tilde{F}$. Observe also that $(\tilde{f} \hat{\otimes} \tilde{f}) \circ \tilde{G} = \tilde{F} \circ \tilde{f}$, because $f(F(X, Y)) = G(f(X), f(Y))$. Similarly, $(\tilde{f}^{-1} \hat{\otimes} \tilde{f}^{-1}) \circ \tilde{F} = \tilde{G} \circ \tilde{f}^{-1}$, because $\tilde{f}^{-1} = \widetilde{f^{-1}}$, where $f(f^{-1}(X)) = X$.

Now we may prove that $L(f)$ is an isomorphism of restricted Lie algebras. First notice that if $d \in L(F)$, then $L(f)(d) = \tilde{f}^{-1} \circ d \circ \tilde{f} \in L(G)$. Indeed, $\tilde{G} \circ \tilde{f}^{-1} \circ d \circ \tilde{f} = (\tilde{f}^{-1} \hat{\otimes} \tilde{f}^{-1}) \circ \tilde{F} \circ d \circ \tilde{f} = (\tilde{f}^{-1} \hat{\otimes} \tilde{f}^{-1})(d \hat{\otimes} \mathrm{id}) \circ \tilde{F} \circ \tilde{f} = (\tilde{f}^{-1} \circ d \hat{\otimes} \tilde{f}^{-1}) \circ (\tilde{f} \hat{\otimes} \tilde{f}) \circ \tilde{G} = (\tilde{f}^{-1} \circ d \circ \tilde{f} \hat{\otimes} \mathrm{id}) \circ \tilde{G}$, which implies $L(f)(d) \in L(G)$. Further, for d, $t \in L(F)$ we have:

$$L(f)(d)^{[p]} = (\tilde{f}^{-1} \circ d \circ \tilde{f})^p = \tilde{f}^{-1} \circ d^p \circ \tilde{f} = L(f)(d^{[p]}),$$

and

$$\begin{aligned}[L(f)(d), L(f)(t)] &= \tilde{f}^{-1} \circ d \circ \tilde{f} \circ \tilde{f}^{-1} \circ t \circ \tilde{f} - \tilde{f}^{-1} \circ t \circ \tilde{f} \circ \tilde{f}^{-1} \circ d \circ f \\ &= \tilde{f}^{-1} \circ (d \circ t - t \circ d) \circ \tilde{f} \\ &= L(f)([d, t]).\end{aligned}$$

Since clearly $L(f^{-1}) = L(f)^{-1}$ we are done. It remains to verify that $L(F) = kd_F$. Let $g(X)$ be in $k[\![X]\!]$. Then

$$\begin{aligned}\tilde{F} \circ d_F(g(X)) &= \tilde{F}(g'(X) \cdot \partial F(0, X)/\partial Z)) \\ &= g'(F(X, Y)) \cdot \partial F(0, F(X, Y))/\partial Z \\ &= g'(F(X, Y))(\partial/\partial Z(F(F(Z, X), Y))|_{Z=0} \\ &= g'(F(X, Y))((\partial F(T, Y)/\partial T)|_{T=F(Z,X)} \cdot \partial F(Z, X)/\partial Z)|_{Z=0}\end{aligned}$$

$$= g'(F(X, Y))\partial F(X, Y)/\partial X)(\partial F(0, X)/\partial Z)$$
$$= (d_F \hat{\otimes} \mathrm{id})\tilde{F}(g(X)),$$

whence $d_F \in L(F)$. Further, if $d \in L(F)$ and $h(X) = d(X)$, then $h(F(X, Y)) = \tilde{F} \circ d(X) = (d \hat{\otimes} \mathrm{id}) \circ \tilde{F}(X) = (\partial F(X, Y)/\partial X)h(X)$. Hence, putting $X = 0$, $Y = X$, we get $d(X) = h(X) = (\partial F(0, X)/\partial Z)h(0) = h(0)d_F(X)$, which means that $d = h(0)d_F$. Consequently $L(F) = kd_F$, and the lemma is proved.

Remark. The equality $L(F) = kd_F$ may be deduced from Proposition 1 in [T. Honda, Formal Groups and Zeta Functions, Osaka J. Math. v. 5 (1968)].

From the above lemma it follows that $d_F^p = c_F \cdot d_F$ for some uniquely determined constant $c_F \in k$. Notice that $c_F = 0$ for $F = F_a$ and $c_F = 1$ for $F = F_m$. By an action of $L(F)$ on a k-algebra A we mean a morphism of restricted Lie algebras φ: $L(F) \to \mathrm{Der}_k(A)$. It is obvious that such an action is nothing else than a k-derivation d of A with $d^p = c_F d$.

Now recall [15] that an action of the formal group F on a k-algebra A is a morphism of k-algebras D: $A \to A[\![X]\!]$ such that if $D(a) = \sum_i D_i(a)X^i$, $a \in A$, then $D_0 = \mathrm{id}_A$ and $\sum_{i,j} D_i \circ D_j(a)X^iY^j = \sum_s D_s(a)F(X, Y)^s$ for all $a \in A$. If D: $A \to A[\![X]\!]$ is such an action and t: $k[\![X]\!] \to k[\![X]\!]$ is any k-linear map, then we define the k-linear map $\varphi_D(t)$: $A \to A$ by formula $\varphi_D(t)(a) = \sum_i D_i(a)t(X^i)|_{X=0}$. A straightforward calculation proves that $\varphi_D(d) \in \mathrm{Der}_k(A)$ and $\varphi_D(d \circ d') = \varphi_D(d) \circ \varphi_D(d')$ for $d \in L(F)$ and $d' \in \mathrm{Der}_k(k[\![X]\!])$. Hence it results that φ_D: $L(F) \to \mathrm{Der}_k(A)$ is an action of $L(F)$ on the k-algebra A. Since $\varphi_D(d_F) = D_1$, this means that $D_1^p = c_F D_1$.

DEFINITION. An action φ of the restricted Lie algebra $L(F)$ on a k-algebra A is called F-integrable if there exists an action D of the formal group F on A such that $\varphi_D = \varphi$.

The main result of this paper is the following.

THEOREM. *Let F be a formal group over k and let φ: $L(F) \to \mathrm{Der}_k(A)$ be an action of $L(F)$ on a local k-algebra A with the unique maximal ideal m satisfying the conditions* (i) *and* (ii) *below*:

(i) *the ring $A \otimes_k k^{p^{-1}}$ is reduced,*

(ii) *if $m \neq 0$, then $\Omega_k(A)$ is a free A-module of finite rank and $\varphi(d_F)(m) \not\subset m$.*

Then φ is F-integrable in each of the following two cases.

Case 1) *F is isomorphic to F_a or to F_m,*

Case 2) *the field k is separably closed and A is a complete local ring with $m \neq 0$.*

The idea of the proof of this theorem comes in part from [10, proof of Theorem 7] and relies on the construction of a special p-basis Γ of A over k and an element $x \in \Gamma$ such that $x \in m$ (if $m \neq 0$), $d(\Gamma - \{x\}) = 0$, and $d(x) = \partial F(x, 0)/\partial Y$, where $d = \varphi(d_F)$. Having such a pair (Γ, x), one shows that the function $D\colon \Gamma \to A[\![X]\!]$ given by $D(x) = F(x, X)$, $D(y) = y$, $y \neq x$, extends to an action $D\colon A \to A[\![X]\!]$ of the formal group F on A with $\varphi_D = \varphi$. We start with

§ 3. Auxiliary Lemmas

In what follows, given a k-algebra A, a subset $\Gamma \subset A$, and a function $f\colon \Gamma \to A[\![X_1, \cdots, X_m]\!]$, $f_\alpha\colon \Gamma \to A$, $\alpha \in N^m$, will denote the functions determined by the equality $\sum_\alpha f_\alpha(y)X^\alpha = f(y)$, $y \in \Gamma$, where $X^\alpha = X_1^{\alpha_1} \cdots X_m^{\alpha_m}$ for $\alpha = (\alpha_1, \cdots, \alpha_m)$. If $\alpha = (\alpha_1, \cdots, \alpha_m) \in N^m$, then $|\alpha|$ and $p\alpha$ stand for $\alpha_1 + \cdots + \alpha_m$ and $(p\alpha_1, \cdots, p\alpha_m)$, respectively. Note that if $D\colon A \to A[\![X_1, \cdots, X_m]\!]$ is a morphism of k-algebras with $D_0 = \mathrm{id}_A$, then $D_\alpha\colon A \to A$ is a k-derivation for any $\alpha \in N^m$ with $|\alpha| = 1$.

3.1 Lemma. *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. Then for any $m \geqslant 1$ and any function $s\colon \Gamma \to A[\![X]\!] = A[\![X_1, \cdots, X_m]\!]$ with $s_0(y) = y$ for $y \in \Gamma$ there exists a unique morphism of k-algebras $D\colon A \to A[\![X]\!]$ such that $D_0 = \mathrm{id}_A$ and $D|_\Gamma = s$.*

The lemma is a simple generalization of Heerema's Theorem 1 in [7] (see also, [5, Theorem 3]), where the case $m = 1$, $k = F_p$, and A being a field was considered. For the sake of completeness we sketch its proof.

By induction on $|\alpha|$ we define k-linear maps $D_\alpha\colon A \to A$, $\alpha \in N^m$, in such a way that $D\colon A \to A[\![X]\!]$ with $D(a) = \sum_\alpha D_\alpha(a)X^\alpha$, $a \in A$, will be the desired morphism of k-algebras. If $\alpha = 0$, one has to put $D_\alpha = \mathrm{id}_A$. Suppose that D_γ's have been already defined for all $\gamma \in N^m$ with $|\gamma| < r$, and take $\alpha \in N^m$ with $|\alpha| = r$. In order to define D_α we first define its restriction to $k[A^p]$. Let $y = \sum_i t_i a_i^p$, where $t_i \in k$ and $a_i \in A$. Then by definition

$$D_\alpha(y) = \begin{cases} \sum t_i D_\gamma(a_i)^p, & \text{when } \alpha = p\gamma \text{ for some } \gamma \\ 0, & \text{otherwise}. \end{cases}$$

Since $A \otimes_k k^{p^{-1}}$ is a reduced ring, one easily verifies that D_α: $k[A^p] \to A$ is a well-defined k-linear map. If $y_1, \cdots, y_q$ are distinct elements in Γ, $\mu_1, \cdots, \mu_q \in N$ are smaller than p, and $y^\mu = y_1^{\mu_1} \cdots y_q^{\mu_q}$, then $D_\alpha(y^\mu)$ is defined to be the coefficient at X^α in $s(y_1)^{\mu_1} \cdots s(y_q)^{\mu_q} \in A[\![X]\!]$. Finally, for $z \in k[A^p]$ and y^μ as above we set

$$(2) \qquad D_\alpha(zy^\mu) = \sum_{\omega+\gamma=\alpha} D_\omega(z) D_\gamma(y^\mu).$$

Since Γ is a p-basis of A over k, formula (2) determines a k-linear map D_α: $A \to A$. Thus the inductive procedure gives us a set of k-linear maps D_α: $A \to A$, $\alpha \in N^m$, such that $D_0 = \mathrm{id}_A$ and $D_\alpha|_\Gamma = s_\alpha$: $\Gamma \to A$. This means that D: $A \to A[\![X]\!]$ with $D(a) = \sum_\alpha D_\alpha(a) X^\alpha$, $a \in A$, is a k-linear map with $D_0 = \mathrm{id}_A$ and $D|_\Gamma = s$. The fact that D preserves multiplication may be shown similarly as in [7]. As for the uniqueness of D, if D': $A \to A[\![X]\!]$ is another morphism of k-algebras such that $D'_0 = \mathrm{id}_A$ and $D'|_\Gamma = s$, then one easily proves, using induction on $|\alpha|$, that $D'_\alpha = D_\alpha$ for all $\alpha \in N^m$. Hence $D' = D$, and consequently the lemma follows.

3.2 COROLLARY. *Under the assumptions of the lemma we have:*

1) *if D', D: $A \to A[\![X]\!]$ are morphisms of k-algebras with $D'_0 = D_0 = \mathrm{id}_A$ and $D'|_\Gamma = D|_\Gamma$, then $D' = D$,*

2) *for any k-derivations $d_1, \cdots, d_m$: $A \to A$ there is a morphism of k-algebras D: $A \to A[\![X]\!]$ such that $D_0 = \mathrm{id}_A$ and $D_{(i)} = d_i$, $i = 1, \cdots, m$, where $(i) = (0, \cdots, 0, 1, 0, \cdots, 0) \in N^m$ with 1 on the i-th positions.*

Proof. Part 1) results immediately by Lemma 3.1 (to $s = D'|_\Gamma = D|_\Gamma$). To prove part 2) let us define the function s: $\Gamma \to A[\![X]\!]$ by $s(y) = y + \sum_{i=0}^m d_i(y) X_i$, $y \in \Gamma$. Then according to Lemma 3.1 there exists a morphism of k-algebras D: $A \to A[\![X]\!]$ such that $D_0 = \mathrm{id}_A$ and $D|_\Gamma = s$. Hence $D_{(i)}(y) = d_i(y)$ for $y \in \Gamma$, which clearly implies that $D_{(i)} = d_i$, $i = 1, \cdots, m$. The corollary is proved.

3.3 LEMMA. *Let A be a local algebra with the unique maximal ideal m such that $\Omega_k(A)$ is a free A-module of finite rank, and let Γ be a subset of A such that $\{\delta y \otimes \bar{1}, y \in \Gamma\}$ is a basis of the A/m-vector space $\Omega_k(A) \otimes_A A/m$. Then Γ is a p-basis of A over k. In particular, A possesses a p-basis over k.*

Proof. Since $\Omega_k(A)$ is a finite A-module, A is a finite $k[A^p]$-module, by [3, Proposition 1]. Moreover, it is easy to see that $\{\delta y, y \in \Gamma\}$ is a basis of $\Omega_k(A)$ over A. The conclusion now follows from [9, Proposition 38. G].

3.4 LEMMA (Hochschild Lemma, [14, § 6, Lemma 1]). *If R is any ring of characteristic p and d: $R \to R$ is a derivation, then*

$$d^{p-1}(u^{p-1}d(u)) = -d(u)^p + u^{p-1}d^p(u)$$

for all $u \in R$.

Below, for a given ring R, $U(R)$ denotes the set of all units in R. Moreover, for any derivation d: $R \to R$, R^d stands for the subring $\{a \in R, d(a) = 0\} \subset R$.

3.5 LEMMA. *Let A be a k-algebra and let d: $A \to A$ be a non-zero k-derivation such that $d^p = ad$ for some $a \in A$. Then we have:*

1) *if $d(z) \in U(A)$ for some $z \in A$, then A is a free A^d-module with $1, z, \cdots, z^{p-1}$ as a basis,*

2) *if $c \in A^d$ is such that $c^{p-1} = a$ and A is an integral domain, then there is a $y \in A - \{0\}$ with $d(y) = cy$,*

3) *if $d(z) \in U(A)$ and $c^{p-1} = a$ for some $z \in A$ and $c \in A^d$, then there is an $x \in Az$ such that $d(x) = cx + 1$.*

Proof. Suppose that $d(z) \in U(A)$ and set $u = d(z)^{-1}$. Thanks to [8, Lemma 1] we know that $(ud)^p = c_1 d$ for some $c_1 \in A$. Since $c_1 = uc_1 d(z) = u(ud)^p(z) = u(ud)^{p-1}(1) = 0$, we see that $(ud)^p = 0$. Applying now Lemma 4 in [10] to the derivation ud: $A \to A$ and $z \in A$, one gets part 1) of the lemma. To prove 2) assume that $c^{p-1} = a$ for some $c \in A^d$ and denote by L_c: $A \to A$ the map taking b into cb for $b \in A$. Then $d \circ L_c = L_c \circ d$ and $0 = d^p - ad = d^p - c^{p-1}d = d^p - L_c^{p-1} \circ d = (d^{p-1} - L_c^{p-1}) \circ d = (d - L_c) \circ F(d)$, where $F(Z)$ is a polynomial of degree $p-1$ from the ring $A^d[Z]$. What we must show is that $\operatorname{Ker}(d - L_c) \neq 0$. But the equality $\operatorname{Ker}(d - L_c) = 0$ would imply $F(d) = 0$, which is impossible by [11, Theorem 3.1]. So, it remains to prove part 3). Suppose $z \in A$, $c \in A^d$ are such that $d(z) \in U(A)$, $c^{p-1} = a$, and set $x_1 = z^{p-1}d(z)$. Then from the Hochschild Lemma and the equality $d^p = ad$ it follows that $d^{p-1}(x_1) = ax_1 - d(z)^p$. Hence if we put then $x \in Az$ and

$$d(x) - cx = -d(z)^{-p}\left[(d - L_c) \circ \sum_{i=0}^{p-2} L_c^i d^{p-2-i}(x_1)\right] = -d(z)^{-p}(d^{p-1} - L_c^{p-1})(x_1)$$
$$= -d(z)^{-p}(d^{p-1}(x_1) - c^{p-1}x_1) = -d(z)^{-p}(d^{p-1}(x_1) - ax_1) = 1\,.$$

This means that $d(x) = cx + 1$, as was to be shown. The lemma is proved.

3.6 COROLLARY. *Let (A, m) be a local k-algebra and let $d\colon A \to A$ be a k-derivation with $d^p = ed$ for some $e \in \{0, 1\}$ and with $d(m) \not\subset m$, whenever $m \neq 0$. Then there exists an $x \in A$ such that $d(x) = ex + 1 \in U(A)$ and A is a free A^d-module with $1, x, \cdots, x^{p-1}$ as a basis. Moreover, if $m \neq 0$, then one may assume that $x \in m$.*

Proof. Let $m \neq 0$. Then from the assumption we know that $d(z) \in U(A)$ for some $z \in m$. Hence, by Lemma 3.5, 3), there exists an $x \in Az$ with $d(x) = ex + 1$. Since $ex + 1 \in U(A)$, by applying Lemma 3.5, 1), one gets that A is a free A^d-module with $1, x, \cdots, x^{p-1}$ as a basis. Now suppose that $m = 0$, that is, A is a field. If $e = 0$, then again by Lemma 3.5, 3) there is an $x \in A$ with $d(x) = 1$. If $e = 1$, then in view of Lemma 3.5, 2) we may find $0 \neq y \in A$ such that $d(y) = y$. Set $x = y - 1$. Then $d(x) = d(y) = y = x + 1$ and $x + 1 \in U(A)$, because $y \neq 0$. In both cases ($e = 0$ or $e = 1$) A is a free A^d-module, by part 1) of the above lemma. The corollary follows.

Now, for later use, let us recall the notion of height of a formal group. Let $G(X, Y)$ be a formal group over a ring R. As $G(X, Y) = G(Y, X)$, the induction formula: $[1]_G(X) = X$, $[m]_G(X) = G([m-1]_G(X), X)$, $m \in N$, determine a sequence of endomorphisms of the group G. If $pR = 0$, then according to [4, Chap. III, § 3, Theorem 2] each homomorphism $f\colon G \to G'$ of formal groups over R can be uniquely written in the form $f(X) = f_1(X^{p^h})$, where $f_1(X) \in R[\![X]\!]$, $f_1'(0) \neq 0$, and $h \in N \cup \{\infty\}$ ($h = \infty$, if $f = 0$). The number h is called the height of f. Now the height $\mathrm{Ht}(F)$ of a formal group F over the field k is defined to be the height of the endomorphism $[p]_F(X)$. It is easily seen that $\mathrm{Ht}(F) \geqslant 1$ for any F and that $\mathrm{Ht}(F_a) = \infty$, $\mathrm{Ht}(F_m) = 1$. Observe also that $\mathrm{Ht}(F) = \mathrm{Ht}(F')$, provided $F \simeq F'$.

3.7 LEMMA. *Let F be a formal group over k and let as before $c_F \in k$ be the constant determined by the equality $d_F^p = c_F d_F$. Then $c_F = 0$ if and only if $\mathrm{Ht}(F) \neq 1$.*

Proof. Thanks to [4, Chap. III, § 1,. Theorem 2] we know that $F \simeq F_a$ if and only if $\mathrm{Ht}(F) = \infty$. So, let $\mathrm{Ht}(F) < \infty$, and let $D\colon A \to A[\![Y]\!]$ be an action of F on a k-algebra A. For the proof of the lemma it suffices to show that $D_1^p = 0$, when $\mathrm{Ht}(F) \geqslant 2$, and that $D_1^p = cD_1$ for some $c \in k - \{0\}$, when $\mathrm{Ht}(F) = 1$. Indeed, for $A = k[\![X]\!]$ and D given by $D(g(X)) = g(F(X, Y))$ we have $D_1 = d_F$, whence (under the above assumption) $c_F = 0$ if and only if $\mathrm{Ht}(F) \geqslant 2$. From the definition of an action of F on A it follows that $D_i \circ D_j = \sum_m C_{ijm} D_m$, $i, j \in N$, where C_{ijm}'s are constants in k determined by the equality $F(X, Y)^m = \sum_{i,j} C_{ijm} X^i Y^j$. In view of Lemma 2 in [4, Chap. III, § 2] we may assume that

$$F(X, Y) \equiv X + Y + w \cdot \sum_{i=1}^{p^h-1} \left(\binom{p^h}{i} \Big/ p\right) X^i Y^{p^h-i} \bmod \deg p^h + 1$$

for $h = \mathrm{Ht}(F)$ and some $0 \neq w \in k$. Hence

$$D_i \circ D_j = (i, j) D_{p^h} + w \binom{p^h}{i} \Big/ p \cdot D_1 \qquad \text{for } i + j = p^h,$$

and

$$D_i \circ D_j = (i, j) D_{i+j} \qquad \text{for } i + j < p^h.$$

The first equality implies that $D_1 \circ D_{p-1} = wD_1$ if $h = 1$, while the second one that $D_1 \circ D_{p-1} = pD_p = 0$ for $h \geqslant 2$ and that$D_i = D_1^i/i!$ for $0 \leqslant i < p$ and any h. Therefore, if $h = 1$, then $D_1 = w^{-1} D_1 \circ D_{p-1} = w^{-1} D_1 \circ D_1^{p-1}/(p-1)! = D_1^p/w(p-1)!$, i.e., $D_1^p = cD_1$ with $c = w(p-1)!\,1_k \neq 0$.

In the case where $h \geqslant 2$ we have $0 = D_1 \circ D_{p-1} = D_1^p/(p-1)!$, whence $D_1^p = 0$. Thus the lemma is established.

§ 4. Proof of the theorem

Below, $\boldsymbol{Z}$ and $\boldsymbol{Q}$ denote the ring of rational integers and the field of rationals, respectively. Moreover, N^+ denotes the set $N - \{0\}$. It is easy to see that if F and G are isomorphic formal groups over k and the theorem is true for G, then it is also true for F. Therefore, in case 1) of the theorem we may (and will) assume that $F = X + Y + eXY$, $e \in \{0, 1\}$. In case 2) of the theorem we replace quite general F by a certain (isomorphic to F) formal group $\bar{F}_h$, which is much easier to deal with. To this end set $h = \mathrm{Ht}(F)$ and consider the following formal power series from $\boldsymbol{Q}[\![X, Y]\!]$

$$(3) \qquad \begin{aligned} f_h(X) &= X + \sum_{j=1}^{\infty} p^{-j} X^{p^{jh}} \quad (f_\infty(X) = X), \\ F_h(X, Y) &= f_h^{-1}(f_h(X) + f_h(Y)). \end{aligned}$$

Thanks to [6, Chap. I, § 3.2] one knows that $F_h = F_h(X, Y)$ is a formal group over Z and that $[p]_{F_h}(X) \equiv X^{p^h} \bmod pZ[\![X]\!]$ $(X^{p^\infty} = 0)$. Now $\bar{F}_h$ is defined to be the formal group over $k \supset Z/pZ$ obtained by reducing all the coefficients of F_h modulo p. Certainly, $\mathrm{Ht}(\bar{F}_h) = h = \mathrm{Ht}(F)$. It results that $F \simeq \bar{F}_h$, because by [4, Chap. III, § 2, Theorem 2] the height classifies (up to isomorphism) formal groups over a separably closed field. In the sequel, when dealing with case 2) we will assume that $F = \bar{F}_h$, where $h = \mathrm{Ht}(F)$. Moreover, it will be assumed that $h \geqslant 2$, since otherwise, i.e., when $h = 1$, F is isomorphic to F_m (by the already mentioned Theorem 2 in [4, Chap. III, § 2]), and case 1) can be applied.

Now let $d = \varphi(d_F)$. Then $d\colon A \to A$ is a k-derivation with $d^p = c_F d$ and with $d(m) \not\subset m$, if $m \neq 0$. The second important ingredient of the proof is the construction of a special p-basis Γ of A over k and an element $x \in \Gamma$ satisfying the following conditions

a) $x \in m$, whenever $m \neq 0$,

b) $d(x) = \partial F(x, 0)/\partial Y$,

c) $d(y) = 0$ for $y \in \Gamma$, $y \neq x$.

First we show such a pair (Γ, x) exists in case 1) of the theorem i.e., when $F = X + Y + eXY$, $e \in \{0, 1\}$. Then $c_F = e$, and therefore $d^p = ed$. If A is a field, then by Corollary 3.6, there is an $x \in A$ such that $d(x) = ex + 1$ and $1, x, \cdots, x^{p-1}$ is a basis of A as an A^d-module. Since, by the assumption (i) of the theorem, A is a separable field extension of k, the latter permits to find a p-basis Γ of A over k with $x \in \Gamma$ and $\Gamma - \{x\} \subset A^d$, see [10, proof of Theorem 7]. It is clear that the pair (Γ, x) has properties a)–c) above. Now suppose that A is not a field, that is, $m \neq 0$. Then again making use of Corollary 3.6 one may find an $x \in m$ such that $d(x) = ex + 1 \in U(A)$ and $A = \sum_{i \geqslant 0} A^d x^i$. Hence $\delta(x) \notin m \cdot \Omega_k(A)$, because $d = q \circ \delta$ for some homomorphism of A-modules $q\colon \Omega_k(A) \to A$. In view of Lemma 3.3 this implies that there exists a p-basis Γ' of A over k containing x. We "improve Γ'". Since $A = \sum A^d x^i$, each $y' \in \Gamma'$ can be written in the form $y' = y + s_{y'} x$, for suitable $y \in A^d$ and $s_{y'} \in A$. Let $\Gamma = \{y, y' \in \Gamma' - \{x\}\} \cup \{x\}$. Then from the equalities $\delta(y') = \delta(y) + s_{y'}\delta(x) + x\delta(s_{y'})$, $y' \in \Gamma - \{x\}$, and Lemma 3.3 it follows that Γ is a p-basis of A over k ($x \in m$!). The p-basis Γ and $x \in \Gamma$ satisfy conditions a)–c), and thus the existence of the required pair (Γ, x) has been shown in case 1). In case 2) of the theorem we have $d^p = 0$, by Lemma 3.7, and $d(m) \not\subset m$. Hence, again by Corollary 3.6, there is an $x \in m$ with $d(x) = 1$ and $A = \sum_{i \geqslant 0} A^d x^i$. Similarly as above this makes it possible to find a p-basis Γ such that $x \in \Gamma$ and $\Gamma - \{x\} \subset A^d$. It remains to verify that $d(x) = 1 = \partial \bar{F}_h(x, 0)/\partial Y$. From the equality $f_h(F_h(X, Y)) = f_h(X) + f_h(Y)$ (see (3)) it results that $f'_h(X)\partial F_h(X, 0)/\partial Y = 1$. This implies $\bar{f}'_h(X)\partial \bar{F}_h(X, 0)/\partial Y = 1$, where $\bar{f}'_h(X)$ is obtained by reducing all the coefficients of $f'_h(X)$ modulo p. But $f'_h(X) = 1 + \sum_{j=1}^{\infty} p^{j(h-1)} X^{p^{jh}-1}$ (see (3)), whence $\bar{f}'_h(X) = 1$, as $h \geqslant 2$. Consequently $\partial \bar{F}_h(x, 0)/\partial Y = 1$ $(= d(x))$, which means that also in case 2) there exist a p-basis Γ and an element $x \in \Gamma$ satisfying conditions a)–c).

We are now in position to prove the theorem. Choose a p-basis Γ of A over k and an $x \in \Gamma$ satisfying the conditions a)–c), and then define the function $s\colon \Gamma \to A[\![X]\!]$ by the formula: $s(x) = F(x, X)$, $s(y) = y$, $y \in \Gamma - \{x\}$. In view of Lemma 3.1 the function s (uniquely) extends to a morphism of k-algebras $D\colon A \to A[\![X]\!]$ with $D_0 = \mathrm{id}_A$. We show that D is an action of the formal group F on the k-algebra A such that $\varphi_D = \varphi$. The latter amounts to $D_1 = d$ and it is a consequence of the fact that the k-derivations D_1 and d coincide on the p-basis Γ of A over k. So, all that remains to be proved is that $F_A \circ D = D_Y \circ D$, where as before $F_A\colon A[\![X]\!] \to A[\![X, Y]\!]$, $D_Y\colon A[\![X]\!] \to A[\![X, Y]\!]$ are the morphisms of k-algebras defined as follows: $F_A(g(X)) = g(F(X, Y))$, $D_Y(\sum a_i X^i) = \sum D(a_i) Y^i$. By Corollary 3.2, it suffices to check that $F_A \circ D(y) = D_Y \circ D(y)$ for all $y \in \Gamma$. If $y \neq x$, then both sides are equal to y. Write $F(X, Y) = \sum_j F_j(X) Y^j$, where $F_j \in k[\![X]\!]$. Then

$$F_A \circ D(x) = F(x, F(X, Y)) = F(F(x, X), Y) = \sum F_j(F(x, X)) Y^j .$$

On the other hand

$$D_Y \circ D(x) = D_Y(\textstyle\sum F_j(x) Y^j) = \sum D(F_j(x)) Y^j = \sum F_j(F(x, X)) Y^j .$$

Hence $F_A \circ D(x) = D_Y \circ D(x)$, and thus the theorem has been established.

4.1 COROLLARY (from the proof). *Under the assumptions of the theorem there exist a p-basis Γ of the k-algebra A over k and an element $x \in \Gamma$ such that $d(x) = \partial F(x, 0)/\partial Y$, $\Gamma - \{x\} \subset A^d$, and $x \in m$, if $m \neq 0$.*

4.2 *Remark.* Let (A, m) be a local k-algebra satisfying the conditions (i), (ii) of the theorem. Then A turns out to be a regular local ring.

This is a consequence of [16, Lemma 1].

4.3 *Remark.* If the field k is algebraically closed, $F = F_a$, and A is the completion of the local ring of a regular point on some algebraic variety over k, then Corollary 4.1 may be easily deduced from [13, proof of Theorem 1].

REFERENCES

[1] V. Carfi, Integrable derivations in rings of analytic type over a DVR, Atti Sem. Mat. Fis. Università di Modena, **32** (1983), No. 1, 1–10.

[2] R. M. Fossum, Invariants and Formal Group Law Actions, in Contemporary Mathematics, vol. 43, 1985.

[3] J. Fogarty, Kähler differentials and Hilbert's fourteenth problem for finite groups, Amer. J. Math., **102** (1980), 1159–1174.

[4] A. Fröhlich, Formal Groups, in Lecture Notes in Math., **74**, Springer-Verlag, New York/Berlin, 1968.

[5] M. Furuya, Note on local rings with integrable derivations, TRU Math., **17** (1981), No. 1, 39–45.

[6] M. Hazewinkel, Formal Groups and Applications, Academic Press, New York/San Francisco, 1978.

[7] N. Heerema, Derivations and embeddings of a field in its power series ring, II, Michigan Math. J., **8** (1961), 129–134.

[8] G. Hochschild, Simple algebras with purely inseparable splitting fields of exponent 1, Trans. Amer. Math. Soc., **79** (1955), 477–489.

[9] H. Matsumura, Commutative Algebra, 2nd. ed., Benjamin, 1980.

[10] H. Matsumura, Integrable derivations, Nagoya Math. J., **87** (1982), 227–245.

[11] A. Nowicki, Stiff derivations of commutative rings, Colloquium Math., **47** (1984), Fasc. 1, 7–16.

[12] G. Restuccia, H. Matsumura, Integrable derivations in rings of unequal characteristic, Nagoya Math. J., **93** (1984), 173–178.

[13] A. Rudakov, I. Shafarevich, Inseparable morphisms of algebraic surfaces, Izv. AN SSSR, Ser. mat., **40** (1976), 1269–1307 in Russian, Engl. transl.: Math. USSR Izv., **10** (1976), 1205–1237.

[14] C. S. Sheshadri, L'operation de Cartier. Application, in Seminaire C. Chevalley, 3e, année, 1958/59.

[15] A. Tyc, Invariants of linearly reductive formal group actions, J. Algebra, **101** (1986), no. 1, 166–187.

[16] A. Tyc, Differential basis, p-basis, and smoothness in characteristic $p > 0$, to appear in Proc. Amer. Math. Soc.

Institute of Mathematics
Polish Academy of Sciences
ul. Chopina 12/18, 87-100 Toruń
Poland