TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 360, Number 8, August 2008, Pages 4007–4027
S 0002-9947(08)04567-4
Article electronically published on March 20, 2008

SIMPLE DERIVATIONS OF DIFFERENTIABLY SIMPLE NOETHERIAN COMMUTATIVE RINGS IN PRIME CHARACTERISTIC

V. V. BAVULA

Abstract. Let R be a differentiably simple Noetherian commutative ring of characteristic $p > 0$ (then $(R, \mathfrak{m})$ is local with $n := \mathrm{emdim}(R) < \infty$). A short proof is given of the Theorem of Harper (1961) on classification of differentiably simple Noetherian commutative rings in prime characteristic. The main result of the paper is that there exists a nilpotent simple derivation δ of the ring R such that if $\delta^{p^i} \neq 0$, then $\delta^{p^i}(x_i) = 1$ for some $x_i \in \mathfrak{m}$. The derivation δ is given explicitly, and it is unique up to the action of the group $\mathrm{Aut}(R)$ of *ring* automorphisms of R. Let $\mathrm{nsder}(R)$ be the set of all such derivations. Then $\mathrm{nsder}(R) \simeq \mathrm{Aut}(R)/\mathrm{Aut}(R/\mathfrak{m})$. The proof is based on *existence* and *uniqueness* of an *iterative δ-descent* (for each $\delta \in \mathrm{nsder}(R)$), i.e., a sequence $\{y^{[i]}, 0 \leq i < p^n\}$ in R such that $y^{[0]} := 1$, $\delta(y^{[i]}) = y^{[i-1]}$ and $y^{[i]}y^{[j]} = \binom{i+j}{i} y^{[i+j]}$ for all $0 \leq i, j < p^n$. For each $\delta \in \mathrm{nsder}(R)$, $\mathrm{Der}_{k'}(R) = \bigoplus_{i=0}^{n-1} R\delta^{p^i}$ and $k' := \ker(\delta) \simeq R/\mathfrak{m}$.

1. Introduction

Throughout, ring means an associative ring with 1 and p is a *prime* number.

Let R be a commutative ring. An additive map $\delta : R \to R$ is called a *derivation* of R if $\delta(ab) = \delta(a)b + a\delta(b)$ for all $a, b \in R$. If, in addition, the ring R is an algebra over a field k, then a derivation δ is called a *k-derivation* provided $\delta(k) = 0$, i.e., provided δ is a k-linear map. Let $\mathrm{Der}(R)$ be the R-module of derivations of R. If, in addition, the ring R is an algebra over a field k, then $\mathrm{Der}_k(R)$ denotes the R-module of k-derivations of R.

An ideal I of the ring R is called a *differential ideal* if $\delta(I) \subseteq I$ for all $\delta \in \mathrm{Der}(R)$. The ring R is called *differentiably simple* if 0 and R are the only differential ideals of R.

Theorem 1.1 (Harper, [1]). *A Noetherian commutative ring R of characteristic $p > 0$ is differentiably simple iff it has the form $R = k[x_1, \ldots, x_n]/(x_1^p, \ldots, x_n^p)$ where k is a field of characteristic p.*

In his book H. Matsumura makes the following comment on the Theorem of Harper (p. 206, [4]): "The 'if' part is easy. The proof of the 'only if' part is not easy and we refer the reader to Harper [1] and Yuan [6]. Recently this theorem was

Received by the editors February 27, 2006.
2000 *Mathematics Subject Classification.* Primary 13N15, 13A35, 16W25.
Key words and phrases. Simple derivation, iterative δ-descent, differentiably simple ring, differential ideal, coefficient field.

used by Kimura-Niitsuma [2] to prove the following theorem which has been known as Kunz' conjecture." Later A. Maloo [3] gave a shorter proof of Theorem 1.1.

In this paper, apart from proving several statements equivalent to Theorem 1.1 (see Theorem 2.6) it is shown that essentially Theorem 1.1 follows from Theorem 27.3 in [4].

It is well known and easy to prove (Lemma 2.1) that each differentiably simple Noetherian ring R of characteristic $p > 0$ is a local $(R, \mathfrak{m})$ k-algebra for some subfield k of R such that $R = k + \mathfrak{m}$. We say that a subfield k' of R is a *coefficient field* or a *complement* subfield in R if $R = k' + \mathfrak{m}$. Clearly, each coefficient field is isomorphic to the residue field $R/\mathfrak{m}$ of R. Corollary 2.7 (together with Theorem 2.6.(3)-(6) and Proposition 2.5) gives *explicitly* all the coefficient fields of R (see also Theorem 4.2.(2)). It is well known that each differentiably simple Noetherian commutative ring R of characteristic $p > 0$ admits a simple derivation (see [6] and [5]). Let $\mathrm{nsder}(R)$ be the set of all *nilpotent simple* derivations δ of the ring R such that if $\delta^{p^i} \neq 0$, then $\delta^{p^i}(y_i) = 1$ for some element $y_i \in \mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal of R. The set $\mathrm{nsder}(R)$ is a nonempty set (Lemma 3.9, see also Theorem 4.2). An action of a group G on a set X is said to be fully faithful if for some/each $x \in X$ the map $G \to X$, $g \mapsto gx$, is a bijection.

For a prime number p, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a finite field that contains p elements. Given a derivation δ of an $\mathbb{F}_p$-algebra A, a sequence $\{y^{[i]}, 0 \leq i < p^n\}$ of elements in A (where $y^{[0]} := 1$) is called an **iterative δ-descent** if

$$\delta(y^{[i]}) = y^{[i-1]}, \quad y^{[i]}y^{[j]} = \binom{i+j}{i} y^{[i+j]}, \quad 0 \leq i, j \leq p^n - 1,$$

where $y^{[-1]} = y^{[k]} := 0$ for all $k \geq p^n$.

Let us give a list of the main results of the paper. *Let R be a differentiably simple Noetherian commutative ring of characteristic $p > 0$ which is not a field, $\mathfrak{m}$ be its maximal ideal, $k := R/\mathfrak{m}$, $n := \dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq 1$. Let $\delta \in \mathrm{nsder}(R)$ and $k' := \ker(\delta)$. Then*

- (Theorem 4.1) *k' is a coefficient field for R.*
- (Theorem 4.1.(1)) *$\delta^{p^n-1} \neq 0$ and $\delta^{p^n} = 0$.*
- (Proposition 4.4) $\mathrm{Der}_{k'}(R) = \bigoplus_{i=0}^{n-1} R\delta^{p^i}$.
- (Theorem 4.1.(2)) *There exists a* **unique** *iterative δ-descent $\{x^{[i]}, 0 \leq i < p^n\}$. Then $x^{[i]} \in \mathfrak{m}$, $1 \leq i < p^n$;*

$$R = \bigoplus_{i=0}^{p^n-1} k'x^{[i]} = k'\langle x_0, \ldots, x_{n-1}\rangle \simeq k'[x_0, \ldots, x_{n-1}]/(x_0^p, \ldots, x_{n-1}^p),$$

  where $x_j := x^{[p^j]}$ and $x^{[i]} := \prod_{k=0}^{t} \frac{x_k^{i_k}}{i_k!}$ where $i = \sum_{k=0}^{t} i_k p^k$, $0 \leq i_k < p$, and
- (Theorem 3.8) *the iterative δ-descent $\{x^{[i]}, 0 \leq i < p^n\}$ is given explicitly: choose elements $y_0, y_1, \ldots, y_{n-1} \in \mathfrak{m}$ such that $\delta^{p^k}(y_k) = 1$ for $k = 0, \ldots, n-1$; then $x_0 := y_0$,*

$$x_1 := (-1)^{p-1}\phi_0(y_1), \quad \phi_0(z) := \sum_{j=0}^{p-1} (-1)^j \frac{x_0^j}{j!} \delta^j(z),$$

and then recursively, for all $1 \leq k \leq n-2$,

$$x_{k+1} := (-1)^{p-1}\delta^{p^k-1}\Big(\prod_{l=0}^{k-1}\frac{x_l^{p-1}}{(p-1)!}\cdot\phi_k(y_{k+1})\Big),\ \ \phi_k(z) := \sum_{j=0}^{p-1}(-1)^j\frac{x_k^j}{j!}\delta^{p^k j}(z).$$

- (Lemma 3.1, Theorem 4.1) *The derivation* δ *has the unique presentation via its iterative* δ*-descent,* $\delta = \sum_{i=0}^{n-1} x^{[p^i-1]}\frac{\partial}{\partial x_i}$*, and* $\delta \in \mathrm{nsder}_{k'}(R) := \{\partial \in \mathrm{nsder}(R) \mid \partial(k') = 0\}$.
- (Theorem 4.1) $k' = \phi(R)$ *where* $\phi := \sum_{i=0}^{p^n-1}(-1)^i x^{[i]}\delta^i : R = k' \oplus \mathfrak{m} \to R = k' \oplus \mathfrak{m}$ *is the projection onto* k'.
- (Corollary 4.3.(1)) *For each coefficient field* l *of* R*, the action*

$$\mathrm{Aut}_l(R) \times \mathrm{nsder}_l(R) \to \mathrm{nsder}_l(R)$$

  defined by the rule $(\sigma, \partial) \mapsto \sigma\partial\sigma^{-1}$ *is fully faithful where* $\mathrm{Aut}_l(R)$ *is a the group of* l*-algebra automorphisms of* R *and* $\mathrm{nsder}_l(R) := \{\partial \in \mathrm{nsder}(R) \mid \partial(l) = 0\}$.
- (Corollary 4.3.(2)) *The action* $\mathrm{Aut}(R) \times \mathrm{nsder}(R) \to \mathrm{nsder}(R)$ *which is given by the rule* $(\sigma, \delta) \mapsto \sigma\delta\sigma^{-1}$ *has a single orbit and, for each* $\partial \in \mathrm{nsder}(R)$*,* $\mathrm{Fix}(\partial) \simeq \mathrm{Aut}(k)$*, and so* $\mathrm{nsder}(R) \simeq \mathrm{Aut}(R)/\mathrm{Aut}(k)$.

Note that the group $\mathrm{Aut}_{k'}(R)$ is easily described: any k'-automorphism of the algebra R is uniquely determined by n "polynomials" $\sigma(x_i) = \sum a_{ij}x_j + \cdots$, $0 \leq i \leq n-1$, $a_{ij} \in k'$, with $\det(a_{ij}) \neq 0$ where the three dots mean *any* linear combination of monomials of degree ≥ 2. So, the result above gives explicitly all the elements of $\mathrm{nsder}_{k'}(R)$.

In brief, almost all the results of the paper are consequences of two theorems on existence and uniqueness of an iterative δ-descent (Theorem 3.8 and Theorem 4.1) which is given explicitly for each $\delta \in \mathrm{nsder}(R)$. The importance of the iterative δ-descent lies in the facts that (i) the iterative δ-descent together with $\ker(\delta)$ determines uniquely and explicitly the derivation $\delta \in \mathrm{nsder}(R)$ (Lemma 3.1, Theorem 4.1), (ii) all the coefficient fields are precisely the kernels of derivations from $\mathrm{nsder}(R)$; and the iterative δ-descent $\{x^{[i]}\}$ describes explicitly the kernel of δ: $\ker(\delta) = (\sum_{i=0}^{p^n-1}(-1)^i x^{[i]}\delta^i)(R)$ (Theorem 4.1).

The paper is organized as follows: in Section 1, a short proof of the Theorem of Harper is given together with some equivalent statements (Theorem 2.6). Corollary 2.7 describes explicitly all the coefficient fields. An important technical result, Proposition 2.5, is proved which states roughly that having n derivations δ_i with $\delta_i(x_j) = \delta_{ij}$ one can produce n *commuting* derivations δ_i' such that $\delta_i'(x_i') = \delta_{ij}$ and $\delta_i'^p = 0$.

In Section 3, the concept of an iterative δ-descent is introduced. Theorem 3.8 (on existence and uniqueness of an iterative δ-descent) is proved.

In Section 4, the canonical form for each derivation $\delta \in \mathrm{nsder}(R)$ is given via the iterative δ-descent (Theorem 4.1, see also Lemma 3.1), and the coefficient fields are explicitly described (Theorem 4.1). An important bijection is established in Theorem 4.2 which is used in the proof of the canonical bijection $\mathrm{nsder}(R) \simeq \mathrm{Aut}(R)/\mathrm{Aut}(R/\mathfrak{m})$ (Corollary 4.3). Finally, it is proved that $\mathrm{Der}_{R^\delta}(R) = \bigoplus_{i=0}^{n-1} R\delta^{p^i}$ (Proposition 4.4).

2. Differentiably simple Noetherian commutative rings

In this section, a short proof of Theorem 1.1 is given and some equivalent statements to Theorem 1.1 are proved (Theorem 2.6). All coefficient fields of a differentiably simple Noetherian commutative ring of prime characteristic are found explicitly (see the remark at the end of this section).

Lemma 2.1. *Let R be a differentiably simple commutative ring of characteristic $p > 0$ (i.e., $p^k = 0$ in R for some $k \geq 1$). Then R is a local $\mathbb{F}_p$-algebra with maximal ideal $\mathfrak{m}$ such that $x^p = 0$ for all $x \in \mathfrak{m}$, and $\mathfrak{m}^\infty := \bigcap_{i\geq 1} \mathfrak{m}^i = 0$. If, in addition, R is a Noetherian ring, then $R = k + \mathfrak{m}$ for some subfield k of R necessarily isomorphic to the residue field $R/\mathfrak{m}$ of R.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of R. Then the ideal $I := \sum_{x\in\mathfrak{m}} Rx^p$ is differential (since $\delta(x^p) = px^{p-1}\delta(x) = 0$ for all $\delta \in \mathrm{Der}(R)$), and $I \subseteq \mathfrak{m}$; hence $I = 0$ (since R is a differentiably simple ring). Therefore, $\mathfrak{m} = \mathfrak{n}(R)$ is the only maximal ideal of R where $\mathfrak{n}(R)$ is the nil radical of R; that is, $(R, \mathfrak{m})$ is a local ring.

The ring of constants $C := \bigcap_{\delta\in\mathrm{Der}(R)} \ker \delta$ must be a field since R is a differentiably simple ring (for any $0 \neq c \in C$, cR is a differential ideal of the ring R; hence $cR = R$). Therefore, R is an $\mathbb{F}_p$-algebra. Note that $\mathfrak{m}^\infty$ is a differential ideal of R such that $\mathfrak{m}^\infty \subseteq \mathfrak{m}$. Hence $\mathfrak{m}^\infty = 0$.

If, in addition, R is a Noetherian ring, then $(R, \mathfrak{m})$ is a Noetherian local ring which is obviously equicharacteristic and complete in the $\mathfrak{m}$-adic topology since $\mathfrak{m}^i = 0$ for a large i. It is well known that *any equicharacteristic complete Noetherian local commutative ring contains a coefficient field* ([4], Theorem 28.3.(ii)), and so $R = k + \mathfrak{m}$ for some subfield k of R. □

So, in dealing with a differentiably simple commutative ring R of characteristic $p > 0$ there is no restriction in assuming that it is a local $\mathbb{F}_p$-algebra $(R, \mathfrak{m})$ with $x^p = 0$ for all $x \in \mathfrak{m}$. That explains why in many results of the present paper these conditions are present from the outset (aiming at a possible application to differentiably simple rings).

Let $\mathbb{F}_p[h]$ be a polynomial algebra in a variable h. The factor algebra $\Lambda := \mathbb{F}_p[h]/(h(h-1)\cdots(h-p+1))$ is isomorphic to the direct product of p copies of the field $\mathbb{F}_p$. In more detail, $\Lambda = \bigoplus_{i=0}^{p-1} \mathbb{F}_p\theta_i$ where $1 = \theta_0 + \theta_1 + \cdots + \theta_{p-1}$ is a sum of primitive orthogonal idempotents of the algebra Λ (i.e., $\theta_i\theta_j = \delta_{ij}\theta_i$ for all $i, j \in \mathbb{Z}/p\mathbb{Z}$ where δ_{ij} is the *Kronecker delta*) and

$$\theta_i \quad := \quad \frac{h(h-1)\cdots\widehat{(h-i)}\cdots(h-p+1)}{i(i-1)\cdots 1(-1)(-2)\cdots(i-p+1)},$$

where the hat over a symbol means that it is missed. Using the facts that $-i = p-i$ and $(-1)^{p-1} = 1$ in $\mathbb{F}_p$, it follows at once that

$$\theta_i = \frac{h(h-1)\cdots\widehat{(h-i)}\cdots(h-p+1)}{(p-1)!} = (-1)^{p-1}\frac{h(h-1)\cdots\widehat{(h-i)}\cdots(h-p+1)}{(p-1)!}.$$

These presentations of θ_i will be used later in calculations.

The $\mathbb{F}_p$-algebra automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}_p}(\Lambda)$, $h \mapsto h-1$, permutes cyclicly the idempotents θ_i: $\sigma(\theta_i) = \theta_{i+1}$. It is evident that

$$\prod_{i=0}^{p-1}(1-\theta_i) = 1 - \theta_0 - \theta_1 - \cdots - \theta_{p-1} = 1 - 1 = 0. \tag{1}$$

Note that if δ is a derivation of an $\mathbb{F}_p$-algebra A, then so are δ^{p^i}, $i \geq 0$. For $a \in A$, $(\operatorname{ad} a)(x) := ax - xa$ is an *inner derivation* of A. It is obvious that $\operatorname{Der}(A) = \operatorname{Der}_{\mathbb{F}_p}(A)$ for each $\mathbb{F}_p$-algebra A since $\delta(1) = \delta(1 \cdot 1) = 2\delta(1)$, i.e., $\delta(1) = 0$.

Lemma 2.2. *Let R be a commutative $\mathbb{F}_p$-algebra, $\delta \in \operatorname{Der}(R)$, $\delta(x) = 1$ for some $x \in R$ such that $x^p = 0$, $h := x\delta \in \operatorname{End}_{\mathbb{F}_p}(R)$ where x is identified with the $\mathbb{F}_p$-linear map $r \mapsto xr$.*

1. *The $\mathbb{F}_p$-subalgebra of the endomorphism algebra $\operatorname{End}_{\mathbb{F}_p}(R)$ generated by h is naturally isomorphic to the factor algebra $\Lambda := \mathbb{F}_p[h]/(h(h-1)\cdots(h-p+1)) = \bigoplus_{i=0}^{p-1} \mathbb{F}_p\theta_i$ (as above).*
2. *For each $i = 0, \ldots, p-1$, let $\delta_i := (1-\theta_i)\delta$. Then $\delta_i^p = 0$.*
3. *The map $\partial := \delta_{p-1} = (1-\theta_{p-1})\delta$ is, in fact, the derivation $\partial = \delta - (-1)^{p-1}\frac{x^{p-1}}{(p-1)!}\delta^p \in \operatorname{Der}(R)$ that satisfies the conditions $\partial(x) = 1$, $\partial^p = 0$, and $h = x\partial$.*

Proof. (1). In the algebra $\operatorname{End}_{\mathbb{F}_p}(R)$, we have $\delta x - x\delta = \delta(x) = 1$; hence $xh = (h-1)x$. Using this relation, we have

$$0 = x^p\delta^p = h(h-1)\cdots(h-p+1),$$

and so there is a natural $\mathbb{F}_p$-algebra epimorphism $\Lambda \to \mathbb{F}_p\langle h\rangle$. It is, in fact, an isomorphism. It suffices to show that the elements $1, h, \ldots, h^{p-1}$ are $\mathbb{F}_p$-linearly independent in $\mathbb{F}_p\langle h\rangle$. If $r := \lambda_0 + \lambda_1 h + \cdots + \lambda_m h^m = 0$ is a nontrivial relation (all $\lambda_i \in \mathbb{F}_p$ and $\lambda_m \neq 0$, $0 \leq m \leq p-1$), then applying $(-\operatorname{ad} x)^m$ to r we have $m!\lambda_m x^m = 0$ in $\operatorname{End}_{\mathbb{F}_p}(R)$. Evaluating this relation at 1, one has the relation $m!\lambda_m x^m = 0$ in the ring R, and so $0 = \delta^m(\lambda_m x^m) = m!\lambda_m \neq 0$, a contradiction.

Recall that the $\mathbb{F}_p$-algebra automorphism $\sigma \in \operatorname{Aut}_{\mathbb{F}_p}(\Lambda)$ is defined as follows: $\sigma(h) = h - 1$. Then $\sigma^{-1}(h) = h + 1$. In the algebra $\operatorname{End}_{\mathbb{F}_p}(R)$, $\delta x - x\delta = \delta(x) = 1$. For computational reasons, it is important to stress that this relation is equivalent to the following four relations:

$$xh = \sigma(h)x, \qquad x\delta = h,$$
$$\delta h = \sigma^{-1}(h)\delta, \qquad \delta x = \sigma^{-1}(h).$$

(2). Note that each $\theta_i \in \mathbb{F}_p[h]$ and $\delta\theta_i = \sigma^{-1}(\theta_i)\delta$. Then, by the equality (1),

$$\delta_i^p = \prod_{j=0}^{p-1} \sigma^j(1-\theta_i)\cdot\delta^p = \prod_{j=0}^{p-1}(1-\theta_{i+j})\cdot\delta^p = \prod_{k=0}^{p-1}(1-\theta_k)\cdot\delta^p = 0\cdot\delta^p = 0.$$

(3). Since $x^{p-1}\delta^{p-1} = x^{p-2}h\delta^{p-2} = (h-p+2)x^{p-2}\delta^{p-2} = \cdots = (h-p+2)\cdots(h-1)h$, we have

$$\begin{aligned}
\partial &= (1-\theta_{p-1})\delta = \delta - (-1)^{p-1}\frac{h(h-1)\cdots(h-p+2)}{(p-1)!}\delta \\
&= \delta - (-1)^{p-1}\frac{x^{p-1}\delta^{p-1}}{(p-1)!}\delta \\
&= \delta - (-1)^{p-1}\frac{x^{p-1}}{(p-1)!}\delta^p \in \operatorname{Der}(R).
\end{aligned}$$

Then it becomes obvious that $\partial(x) = \delta(x) = 1$ and $x\partial = x\delta - (-1)^{p-1}\frac{x^p}{(p-1)!}\delta^p = x\delta = h$. □

Theorem 2.3. *Let δ be a derivation of a commutative $\mathbb{F}_p$-algebra R such that $\delta^p = 0$ and $\delta(x) = 1$ for some element $x \in R$. Then*

1. *(Theorem 27.3, [4]) $R = \bigoplus_{i=0}^{p-1} R^\delta x^i$ where $R^\delta := \ker(\delta)$.*
2. *The map $\phi := \sum_{i=0}^{p-1} (-1)^i \frac{x^i}{i!}\delta^i : R = R^\delta \oplus (x) \to R = R^\delta \oplus (x)$ is a projection onto the subalgebra R^δ; that is, $\phi(a + bx) = a$ for all $a \in R^\delta$ and $b \in R$.*
3. *For any $a \in R$, $a = \sum_{i=0}^{p-1} \phi(\frac{\delta^i}{i!}(a))x^i$.*

Proof. (2). By the very definition, the map ϕ is a homomorphism of R^δ-modules. For each $n = 1, \dots, p-1$,

$$\phi(x^n) = \sum_{i=0}^{p-1} (-1)^i \binom{n}{i} x^i x^{n-i} = (1-1)^n x^n = 0 \cdot x^n = 0.$$

Therefore, $\phi(a + bx) = a$, which follows directly from statement (1).

(3). Given $a = \sum_{i=0}^{p-1} a_i x^i \in R$ where $a_i \in R^\delta$, by statement (2), $a_i = \phi(\frac{\delta^i}{i!}(a))$. □

Lemma 2.4. *Let $A = \bigoplus_{\alpha \in \mathbb{N}^n} A_\alpha = A_0 \oplus A_+$ be an $\mathbb{N}^n$-graded ring where $A_+ := \bigoplus_{0 \neq \alpha \in \mathbb{N}^n} A_\alpha$, and let δ be a derivation of the ring A. Then*

1. *for each $a \in A_0$, $\delta(a) = \delta_0(a) + \delta_+(a)$ where $\delta_0(a) \in A_0$, $\delta_+(a) \in A_+$, and δ_0 is a derivation of the ring A_0.*
2. *If $\delta(A_+) \subseteq A_+$ and $\delta(x) = 1$ for some element $x = x_0 + x_+$ where $x_0 \in A_0$ and $x_+ \in A_+$, then $\delta_0(x_0) = 1$.*

Proof. (1). Since $A = A_0 \oplus A_+$, both maps δ_0 and δ_+ are additive, by the very definition. For any $a, b \in A_0$, $\delta(ab) = \delta(a)b + a\delta(b) = \delta_0(a)b + a\delta_0(b) + c$ for some $c \in A_+$; hence $\delta_0(ab) = \delta_0(a)b + a\delta_0(b)$. This means that δ_0 is a derivation of the ring A_0.

(2). The equality $1 = \delta(x) = \delta_0(x_0) + \delta_+(x_0) + \delta(x_+)$ implies the equality $\delta_0(x_0) = 1$. □

Recall that for a local commutative ring $(R, \mathfrak{m})$, a subfield k' of R satisfying $R = k' + \mathfrak{m}$ is called a coefficient field for R. For a natural number $n \geq 1$, let

$$\mathcal{N}_n := \{\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n \mid 0 \leq \alpha_\nu < p\}.$$

Proposition 2.5. *Let $(R, \mathfrak{m})$ be a local Noetherian commutative $\mathbb{F}_p$-algebra such that $x^p = 0$ for all $x \in \mathfrak{m}$, $k := R/\mathfrak{m}$, $n := \dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq 1$. Let $\delta_1, \dots, \delta_n$ be derivations of the ring R such that $\delta_i(x_j) = \delta_{ij}$ for some elements $x_1, \dots, x_n \in \mathfrak{m}$. Then there exist commuting derivations $\delta_1', \dots, \delta_n'$ of the ring R and elements $x_1', \dots, x_n' \in \mathfrak{m}$ such that $\delta_i'(x_j') = \delta_{ij}$, $\delta_1'^p = \cdots = \delta_n'^p = 0$, and $(x_1', \dots, x_n') = \mathfrak{m}$. Then necessarily $k' := \bigcap_{i=1}^n \ker \delta_i'$ is a coefficient field of R and $R = \bigoplus_{\alpha \in \mathcal{N}_n} k' x^\alpha$ where $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. In particular, $R \simeq k'[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p)$.*

Remark. Necessarily, $\mathfrak{m} = (x_1, \dots, x_n)$ since $n = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ and $\delta_i(x_j) = \delta_{ij}$.

Proof. The idea of the proof is to use repeatedly Lemma 2.2(3), Theorem 2.3(1), and Lemma 2.4.

Since $x_1^p = 0$ and $\delta_1(x_1) = 1$, by Lemma 2.2(3), one can find a derivation δ_1' of the ring R such that $\delta_1'(x_1) = 1$ and $\delta_1'^p = 0$. Let $x_1' := x_1$. Then $(x_1') = (x_1)$. By Theorem 2.3.(1), $R = \bigoplus_{\alpha_1=0}^{p-1} R^{\delta_1'} x_1'^{\alpha_1}$ is a positively graded ring.

Suppose that using the derivations $\delta_1, \dots, \delta_s$ and the elements $x_1, \dots, x_s$ we have already found commuting derivations $\delta'_1, \dots, \delta'_s$ and elements $x'_1, \dots, x'_s \in \mathfrak{m}$ such that the following conditions hold: $\delta'^p_1 = \cdots = \delta'^p_s = 0$; $\delta'_i(x'_j) = \delta_{ij}$ for all $i, j = 1, \dots, s$; $(x'_1, \dots, x'_s) = (x_1, \dots, x_s)$ (the equality of ideals); and

$$R = \bigoplus_{\alpha \in \mathcal{N}_s} k'_s x^\alpha, \quad k'_s := \bigcap_{i=1}^{s} \ker \delta'_i.$$

The ring R is *naturally* $\mathbb{N}^s$-graded, and $R_+ := \bigoplus_{0 \neq \alpha \in \mathcal{N}_s} k'_s x^\alpha = (x'_1, \dots, x'_s)$. Then

$$\delta_{s+1}(R_+) = \delta_{s+1}((x'_1, \dots, x'_s)) = \delta_{s+1}((x_1, \dots, x_s)) \subseteq (x_1, \dots, x_s) = (x'_1, \dots, x'_s) = R_+.$$

Write $x_{s+1} = x'_{s+1} + x^+_{s+1}$ for some $x'_{s+1} \in k'_s \cap \mathfrak{m}$ and $x^+_{s+1} \in R_+ \subseteq \mathfrak{m}$. Then $(x'_1, \dots, x'_{s+1}) = (x_1, \dots, x_{s+1})$. Since $\delta_{s+1}(x_{s+1}) = 1$, by Lemma 2.4, $\delta'_{s+1}(x'_{s+1}) = 1$ for some derivation δ'_{s+1} of the ring k'_s. One can extend the derivation δ'_{s+1} to a derivation, say δ'_{s+1}, of the ring R by setting $\delta'_{s+1}(x'_1) = \cdots = \delta'_{s+1}(x'_s) = 0$. Changing (if necessary) the derivation δ'_{s+1} as in Lemma 2.2(3), one can assume additionally that $\delta'^p_{s+1} = 0$. Then the derivations $\delta'_1, \dots, \delta'_{s+1}$ commute, the elements $x'_1, \dots, x'_{s+1} \in \mathfrak{m}$, $\delta'^p_1 = \cdots = \delta'^p_{s+1} = 0$, $\delta'_i(x'_j) = \delta_{ij}$ for all $i, j = 1, \dots, s+1$, $(x'_1, \dots, x'_{s+1}) = (x_1, \dots, x_{s+1})$, and, by Theorem 2.3(3),

$$R = \bigoplus_{\alpha \in \mathcal{N}_{s+1}} k'_{s+1} x^\alpha, \quad k'_{s+1} := \bigcap_{i=1}^{s+1} \ker \delta'_i.$$

Now, by induction on s we have

$$R = \bigoplus_{\alpha \in \mathcal{N}_n} k' x^\alpha, \quad k' := \bigcap_{i=1}^{n} \ker \delta'_i,$$

$(x'_1, \dots, x'_n) = (x_1, \dots, x_n) = \mathfrak{m}$. Hence $k' \simeq k$, and so k' is a coefficient field for R. □

Let V and U be finite-dimensional vector spaces over a field k. A k-bilinear map $V \times U \to k$, $(v, u) \mapsto vu$, is called a pairing. It is a *perfect pairing* if $\operatorname{ann}(V) := \{u \in U \mid Vu = 0\} = 0$ and $\operatorname{ann}(U) := \{v \in V \mid vU = 0\} = 0$. A k-bilinear map $V \times U \to k$, $(v, u) \mapsto vu$, is a perfect pairing iff one of the equivalent conditions holds:

(i) $\dim_k(V) = \dim_k(U)$ and $\operatorname{ann}(V) = 0$;

(ii) the map $V \to U^* := \operatorname{Hom}_k(U, k)$, $v \mapsto (u \mapsto vu)$, is a bijection;

(iii) the map $V \otimes_k U \to \operatorname{End}_k(V)$, $v \otimes u \mapsto (v' \mapsto v(uv'))$, is a bijection.

Next, a short proof is given of the Theorem of Harper (Theorem 2.6, $(1 \Leftrightarrow 2)$), and some equivalent statements to the Theorem of Harper are added. Note that in the proof $(1 \Rightarrow 2)$ we use only Theorem 2.3 and Lemma 2.2.

Theorem 2.6. *Let $(R, \mathfrak{m})$ be a local Noetherian commutative $\mathbb{F}_p$-algebra such that $x^p = 0$ for all $x \in \mathfrak{m}$. Let $k := R/\mathfrak{m}$, $n := \dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq 1$, and $T := \operatorname{Der}(R)/\mathfrak{m}\operatorname{Der}(R)$. Then the following statements are equivalent:*

1. *R is a differentiably simple ring.*
2. *$R \simeq k[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p)$.*
3. *There exist derivations $\delta_1, \dots, \delta_n$ of the ring R and elements $x_1, \dots, x_n \in \mathfrak{m}$ such that $\det(\delta_i(x_j)) \notin \mathfrak{m}$.*

(4) *There exist commuting derivations* $\delta_1, \dots, \delta_n$ *of* R *and elements* $x_1, \dots, x_n \in \mathfrak{m}$ *such that* $\delta_1^p = \cdots = \delta_n^p = 0$ *and* $\delta_i(x_j) = \delta_{ij}$ *for all* $i, j = 1, \dots, n$.

(5) *The* k*-bilinear map* $T \times \mathfrak{m}/\mathfrak{m}^2 \to k$ *given by the rule* $(\overline{\delta}, \overline{x}) \mapsto \overline{\delta}(\overline{x}) := \delta(x) + \mathfrak{m}$ *has* $\operatorname{ann}(T) := \{u \in \mathfrak{m}/\mathfrak{m}^2 \mid Tu = 0\} = 0$ *and* $\dim_k(T) \geq n$ *where* $\overline{\delta} := \delta + \mathfrak{m}\mathrm{Der}(R) \in T$ *and* $\overline{x} := x + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$. *Equivalently, the* k*-bilinear map is a perfect pairing.*

(6) *The* k*-linear map* $\mathfrak{m}/\mathfrak{m}^2 \otimes_k T \to \operatorname{End}_k(\mathfrak{m}/\mathfrak{m}^2)$ *given by the rule* $\overline{x} \otimes \overline{\delta} \mapsto (\overline{y} \mapsto \overline{x}\overline{\delta}(\overline{y}))$ *is a surjection or, equivalently, is a bijection.*

(7) R *is a* $\operatorname{Der}_{k'}(R)$*-simple* k'*-algebra for some/any coefficient field* k' *of* R *(i.e.,* $R = k' \oplus \mathfrak{m}$*).*

Proof. The implications 7(some) $\Rightarrow$ 1 and 7(any) $\Rightarrow$ 7(some) are trivial.

(4 $\Rightarrow$ 3): Use the same δ_i and x_j and the fact that $\det(\delta_i(x_j)) = \det(E) = 1$ where E is the identity matrix.

(5 $\Rightarrow$ 6): Suppose that statement 5 holds. Let us prove first that the pairing of statement 5 is perfect; i.e., $\operatorname{ann}(T) = 0$ and $\dim_k(T) = n$. The first condition is given. To prove the second it suffices to show that $\dim_k(T) \leq n$ since $\dim_k(T) \geq n$, by the assumption. Since $\operatorname{ann}(T) = 0$, the k-linear map

$$T \to (\mathfrak{m}/\mathfrak{m}^2)^* := \operatorname{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k), \ \ \overline{\delta} \mapsto (\overline{y} \mapsto \overline{\delta}(\overline{y})),$$

is injective. Therefore, $\dim_k(T) \leq \dim_k((\mathfrak{m}/\mathfrak{m}^2)^*) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) = n$, as required. So, the pairing in statement 5 is perfect, i.e., the map in statement 6 is bijective. In particular, it is surjective.

(6 $\Rightarrow$ 5): Suppose that the first part of statement 6 holds; i.e., the map is surjective. First, we prove that statement 5 holds, which then gives the fact that the map in statement 6 is a bijection (see (5 $\Rightarrow$ 6) above). Since the map in statement 6 is surjective, this implies that the set $\operatorname{ann}(T)$ is annihilated by $\operatorname{End}_k(\mathfrak{m}/\mathfrak{m}^2)$, and so $\operatorname{ann}(T) = 0$. This gives the first condition of statement 5. On the other hand,

$$n^2 = \dim_k(\operatorname{End}_k(\mathfrak{m}/\mathfrak{m}^2)) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2 \otimes_k T) = n \cdot \dim_k(T);$$

hence $\dim_k(T) \geq n$. This gives the second condition of statement 5. So, statement 5 holds; hence the map in statement 6 is a bijection as was proved above in (5 $\Rightarrow$ 6). So, statements 5 and 6 are equivalent.

(2 $\Rightarrow$ 4): If $R = k[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p)$ (up to isomorphism), then the partial derivatives $\partial_1 := \frac{\partial}{\partial x_1}, \dots, \partial_n := \frac{\partial}{\partial x_n} \in \operatorname{Der}_k(R)$ and the elements $x_1, \dots, x_n$ satisfy the conditions of statement 4.

(2 $\Rightarrow$ 6): $\operatorname{End}_k(\mathfrak{m}/\mathfrak{m}^2) = \bigoplus_{i,j=1}^n k\overline{x}_i\overline{\partial}_j$ since $\dim_k(\operatorname{End}_k(\mathfrak{m}/\mathfrak{m}^2)) = n^2$ and $\overline{x}_i\overline{\partial}_j(\overline{x}_k) = \delta_{j,k}\overline{x}_i$ for all i, j, k (i.e., $\overline{x}_i\overline{\partial}_j$ play the role of the matrix units).

(2 $\Rightarrow$ 7(some)): Since $\operatorname{Der}_k(R) = \bigoplus_{i=1}^n R\partial_i$, the ring R is a simple $\operatorname{Der}_k(R)$-module.

(5 $\Rightarrow$ 3): The pairing $T \times \mathfrak{m}/\mathfrak{m}^2 \to k$ is perfect. Choose dual bases, say $\overline{\delta}_1, \dots, \overline{\delta}_n \in T$ and $\overline{x}_1, \dots, \overline{x}_n \in \mathfrak{m}/\mathfrak{m}^2$ (i.e., $\overline{\delta}_i(\overline{x}_j) = \delta_{i,j}$ for all i and j). Therefore, $\det(\delta_i(x_j)) \equiv 1 \mod \mathfrak{m}$, as required.

It remains to prove the implications 1 $\Rightarrow$ 2, 3 $\Rightarrow$ 2, and 7(some) $\Rightarrow$ 7(any).

(1 $\Rightarrow$ 2): Suppose that the algebra R is differentiably simple. Then $\mathfrak{m}$ is not a differential ideal of R; i.e., $\delta_1(\mathfrak{m}) \not\subseteq \mathfrak{m}$ for some derivation δ_1 of R. Then $\delta_1(x_1) \notin \mathfrak{m}$ for some $x_1 \in \mathfrak{m}$. Note that $x_1^p = 0$. Changing δ_1 for $\delta_1(x_1)^{-1}\delta_1 \in \operatorname{Der}(R)$, one can assume that $\delta_1(x_1) = 1$. Then, by Lemma 2.2.(3), one can assume that $\delta_1^p = 0$ (after possibly changing δ_1). By Theorem 2.3, $R = \bigoplus_{i=0}^{p-1} R^{\delta_1} x_1^i$. Note that R^{δ_1} is a

local ring with maximal ideal $R^{\delta_1} \cap \mathfrak{m}$. Let us prove that *if $\mathfrak{a}$ is a differential ideal of the ring R^{δ_1}, then $\mathfrak{a}' := \bigoplus_{i=0}^{p-1} \mathfrak{a} x_1^i$ is a differential ideal of R*: for any $\eta \in \mathrm{Der}(R)$ and $c \in R^{\delta_1}$ we have $\eta(c) = \sum_{i=0}^{p-1} \eta_i(c) x_1^i$ where $\eta_i \in \mathrm{Der}(R^{\delta_1})$, and the result follows. It implies that R^{δ_1} is a differentiably simple Noetherian ring. Applying the same argument several times (or use Proposition 2.5 and induction) we have $R = \bigoplus_{0 \le i_\nu \le p-1} R^{\delta_1,\dots,\delta_s} x_1^{i_1} \cdots x_s^{i_s}$ for some *commuting* derivations $\delta_1, \dots, \delta_s \in \mathrm{Der}(R)$ and elements $x_1, \dots, x_s \in \mathfrak{m}$ such that $\delta_i(x_j) = \delta_{ij}$ and $\delta_1^p = \cdots = \delta_s^p = 0$, where $R^{\delta_1,\dots,\delta_s} := \bigcap_{i=1}^{s-1} \ker \delta_i$ (note that any derivation δ of $R^{\delta_1,\dots,\delta_s}$ can be extended to a derivation of R by setting $\delta(x_1) = \cdots = \delta(x_s) = 0$). Let s be the largest number for which there exist derivations $\delta_1, \dots, \delta_s$ as above (the s exists since $\dim_k(\mathfrak{m}/\mathfrak{m}^2) < \infty$). Then necessarily $R^{\delta_1,\dots,\delta_s}$ is a *field* canonically isomorphic to k, and $R = R^{\delta_1,\dots,\delta_s} + \mathfrak{m}$. Clearly, the set of elements $x_1 + \mathfrak{m}^2, \dots, x_s + \mathfrak{m}^2$ is a k-basis for $\mathfrak{m}/\mathfrak{m}^2$; hence $n = s$.

$(3 \Rightarrow 2)$: The determinant $\Delta := \det(\delta_i(x_j))$ is a unit of R. For each $i = 1, \dots, n$, let us "drop" x_i in the determinant Δ and then multiply it by Δ^{-1}; as the result we have well-defined derivations of the ring R:

$$\partial_i(\cdot) := \Delta^{-1} \det \begin{pmatrix} \delta_1(x_1) & \cdots & \delta_n(x_1) \\ \vdots & \vdots & \vdots \\ \delta_1(\cdot) & \cdots & \delta_n(\cdot) \\ \vdots & \vdots & \vdots \\ \delta_1(x_n) & \cdots & \delta_n(x_n) \end{pmatrix}, \quad i = 1, \dots, n,$$

such that $\partial_i(x_j) = \delta_{ij}$ for all $i, j = 1, \dots, n$. Now, we finish the proof by applying Proposition 2.5.

7(some) $\Rightarrow$ 7(any): Clearly, statement 7(some) implies statement 1, and, as we have proved, statement 1 implies statement 2. We can assume that $R = k[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p)$ where $\mathfrak{m} = (x_1, \dots, x_n)$. Let l be a coefficient field of R. Then $R = l + \mathfrak{m} = k + \mathfrak{m}$ and $l \simeq R/\mathfrak{m} \simeq k$. Hence, for each $i \ge 0$, $\dim_k(\mathfrak{m}^i/\mathfrak{m}^{i+1}) = \dim_{R/\mathfrak{m}}(\mathfrak{m}^i/\mathfrak{m}^{i+1}) = \dim_l(\mathfrak{m}^i/\mathfrak{m}^{i+1})$. Therefore, $R \simeq l[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p)$. Now, it is obvious that R is a $\mathrm{Der}_l(R)$-simple l-algebra by using the partial l-derivatives. □

The next result gives *explicitly* a subfield k' of R such that $R = k' + \mathfrak{m}$.

Corollary 2.7. *Let R be a differentiably simple Noetherian $\mathbb{F}_p$-algebra, the derivations $\delta_1, \dots, \delta_n$ and the elements $x_1, \dots, x_n \in \mathfrak{m}$ be as in Theorem* 2.6(4) *(i.e., $\delta_i^p = 0$ and $\delta_i(x_j) = \delta_{ij}$ for all i, j). For each $i = 1, \dots, n$, let $\phi_i := \sum_{k=0}^{p-1} (-1)^k \frac{x_i^k}{k!} \delta_i^k : R \to R$ and $\mathcal{N}_n := \{\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n \mid 0 \le \alpha_i \le p-1$ for all $i\}$. Then $k' := \mathrm{im}\, \phi$ is a coefficient field for R where ϕ is equal to the composition of maps $\prod_{i=1}^n \phi_i = \sum_{\alpha \in \mathcal{N}_n} (-1)^\alpha x^{[\alpha]} \delta^\alpha$ where $x^{[\alpha]} := \prod_{i=1}^n \frac{x_i^{\alpha_i}}{\alpha_i!}$, $\delta^\alpha := \delta_1^{\alpha_1} \cdots \delta_n^{\alpha_n}$ and $(-1)^\alpha := (-1)^{\alpha_1} \cdots (-1)^{\alpha_n}$.*

Proof. We have proved already that $R = \bigoplus_{\alpha \in \mathcal{N}_n} k' x^{[\alpha]}$ (see the proof $(1 \Rightarrow 2)$ of Theorem 2.6) where $k' := \bigcap_{i=1}^n \ker \delta_i$ is a subfield of R such that $R = k' + \mathfrak{m}$. By Theorem 2.3, the map ϕ is a projection onto k'. □

Remark. In view of Theorem 2.6(3)-(6), Corollary 2.7, in fact, gives all the coefficient fields for R when combined with Proposition 2.5 provided one knows explicitly generators for the R-module $\mathrm{Der}(R)$. In more detail, one can find derivations

$\delta_1, \dots, \delta_n$ satisfying Theorem 2.6(3); then applying Proposition 2.5 one obtains derivations satisfying Corollary 2.7 which produce the coefficient field k'. Varying the derivations $\delta_1, \dots, \delta_n$ one obtains all the coefficient fields for R as follows from Theorem 4.2.

3. Existence and uniqueness of an iterative δ-descent

The main result of this section is Theorem 3.8 on *existence* and *uniqueness* of an *iterative δ-descent*. This is the key (and the most difficult) result of the paper.

Let δ be a derivation of a ring R. A finite sequence of elements in R, $\mathbf{y}$: $y^{[-1]} := 0, y^{[0]} := 1, y^{[1]}, \dots, y^{[m]}$ $(m \geq 1)$ is called a δ-**descent** if $\delta(y^{[i]}) = y^{[i-1]}$ for all $i \geq 0$. If R is an $\mathbb{F}_p$-algebra, $m = p^n - 1$, then a sequence in R, $\{y^{[i]}, 0 \leq i < p^n\}$, is called an *iterative sequence*, if

$$y^{[i]}y^{[j]} = \binom{i+j}{i} y^{[i+j]}, \quad \text{for all } \ 0 \leq i, j \leq p^n - 1.$$

Note that $y^{[i]}y^{[j]} = 0$ if $i + j \geq p^n$ since $\binom{i+j}{i} = 0$ in $\mathbb{F}_p$.

Definition. An iterative sequence $\{y^{[i]}, 0 \leq i < p^n\}$ which is a δ-descent is called an **iterative δ-descent** of *exponent* n. Note that any truncation $\{y^{[i]}, 0 \leq i < p^m\}$, $1 \leq m < n$, of the iterative δ-descent $\{y^{[i]}, 0 \leq i < p^n\}$ is an iterative δ-descent of exponent m.

The following lemma establishes relations between iterative descents and simple derivations.

Lemma 3.1. *Let δ be a derivation of an $\mathbb{F}_p$-algebra R, $K := \ker \delta$, and $\mathbf{x} = \{x^{[i]}, 0 \leq i < p^n\}$ be an iterative δ-descent, elements of which commute with K. Then*

(1) *the K-algebra $K\langle \mathbf{x} \rangle$ generated over K by all the elements $x^{[i]}$ is equal to*

$$K\langle x_0, \dots, x_{n-1} \rangle = \bigoplus_{i=0}^{p^n-1} Kx^{[i]} \simeq K[x_0, \dots, x_{n-1}]/(x_0^p, \dots, x_{n-1}^p)$$

where $x_k := x^{[p^k]}$ and $x^{[i]} = \prod_{k=0}^{t} \frac{x_k^{i_k}}{i_k!}$ where $i = \sum_{k=0}^{t} i_k p^k$, $0 \leq i_k < p$, the p-adic presentation of the integer i.

(2) $\delta' := \delta|_{K\langle \mathbf{x} \rangle} = \sum_{k=0}^{n-1} x^{[p^k-1]} \frac{\partial}{\partial x_k} \in \mathrm{Der}_K(K\langle \mathbf{x} \rangle)$.

(3) *If K is a field, then δ' is a simple K-derivation of the algebra $K\langle \mathbf{x} \rangle$.*

Proof. (1). Clearly, the equality $K\langle \mathbf{x} \rangle = \sum_{i=0}^{p^n-1} Kx^{[i]}$ holds since $\mathbf{x}$ is an iterative sequence. Since the sequence $\mathbf{x}$ is a δ-descent, it follows easily that the sum is a direct one, i.e., $K\langle \mathbf{x} \rangle = \bigoplus_{i=0}^{p^n-1} Kx^{[i]}$. The $\mathbf{x}$ is an iterative sequence; hence $x_0^p = \cdots = x_{n-1}^p = 0$ and $x^{[i]} = \prod_{k=0}^{t} \frac{x_k^{i_k}}{i_k!}$ where $i = \sum_{k=0}^{t} i_k p^k$, $0 \leq i_k < p$. So, there is a natural K-algebra isomorphism $K[x_0, \dots, x_{n-1}]/(x_0^p, \dots, x_{n-1}^p) \simeq K\langle \mathbf{x} \rangle$.

(2). This is obvious.

(3). If $a = a_0 + a_1 x^{[1]} + \cdots + a_s x^{[s]}$ is a nonzero element of the algebra $K\langle \mathbf{x} \rangle$ where $a_i \in K$ and $a_s \neq 0$, then $\delta^s(a_s^{-1} a) = 1$. Therefore, δ' is a simple K-derivation of the algebra $K\langle \mathbf{x} \rangle$. □

An algebra S over a field K is a positively filtered algebra if S is a union of its subspaces, $S = \bigcup_{i \geq 0} S_i$, such that $K \subseteq S_0 \subseteq S_1 \subseteq \cdots$ and $S_i S_j \subseteq S_{i+j}$ for all $i, j \geq 0$. Let A be an algebra over a field K and let δ be a K-derivation of the

algebra A. For any elements $a, b \in A$ and a natural number n, an easy induction argument yields

$$\delta^n(ab) = \sum_{i=0}^{n} \binom{n}{i} \delta^i(a)\delta^{n-i}(b).$$

It follows that the union of the vector spaces $N := N(\delta, A) = \bigcup_{i\geq 0} N_i$, $N_i := \ker \delta^{i+1}$, is a positively *filtered* algebra ($N_iN_j \subseteq N_{i+j}$ for all $i, j \geq 0$), so-called, the *nil algebra* of δ. Clearly, $N_0 = A^\delta := \ker \delta$ is a subalgebra (of *constants* for δ) of A, and $N = \{a \in A \mid \delta^n(a) = 0 \text{ for some natural } n = n(a)\}$.

Lemma 3.2. *Let δ be a derivation of a ring A and $\{x^{[i]}, 0 \leq i \leq m\}$ be a δ-descent. Then $N(\delta, A)_i = \bigoplus_{j=0}^{i} A^\delta x^{[j]} = \bigoplus_{j=0}^{i} x^{[j]}A^\delta$, $0 \leq i \leq m$.*

Proof. For each $i \geq 0$, let $N_i' := \bigoplus_{j=0}^{i} A^\delta x^{[j]}$ and $N_i := N(\delta, A)_i$. Then $N_i' \subseteq N_i$, $i \geq 0$. Clearly, $N_0' = A^\delta = N_0$. We use induction on i to prove that $N_i' = N_i$. Let $i \geq 1$ and $N_{i-1}' = N_{i-1}$ (by the induction hypothesis). Let $u \in N_i$. Then $c := \delta^i(u) \in A^\delta$; hence $\delta^i(u) = \delta^i(cx^{[i]})$, and so $u - cx^{[i]} \in N_{i-1} = N_{i-1}'$. Therefore, $u \in N_i'$, and so $N_i' = N_i$. Since δ is a derivation of the opposite algebra A^{op}, the equalities $N_i = \bigoplus_{j=0}^{i} x^{[j]}A^\delta$, $i \geq 0$, follow from the just proved equalities. □

Lemma 3.3. *Let δ be a derivation of a ring A and $\{x^{[i]}, 0 \leq i \leq m\}$ be a δ-descent. Then $\{x^{[i]'}, 0 \leq i \leq m\}$ is a δ-descent iff $x^{[0]'} := 1$ and $x^{[i]'} = x^{[i]} + \sum_{j=1}^{i} \lambda_j x^{[i-j]}$, $1 \leq i \leq m$, where all $\lambda_j \in A^\delta$.*

Proof. ($\Leftarrow$) Obvious.

($\Rightarrow$) We prove this implication by induction on $i \geq 1$. Let $i = 1$. Then $\delta(x^{[1]'}) = 1 = \delta(x^{[1]})$ implies $x^{[1]'} = x^{[1]} + \lambda_1$ for some element $\lambda_1 \in A^\delta$. Suppose that $i \geq 2$, and, by the induction hypothesis, $x^{[i-1]'} = x^{[i-1]} + \sum_{j=1}^{i-1} \lambda_j x^{[i-1-j]}$ for some $\lambda_j \in A^\delta$. Then $\delta(x^{[i]'}) = x^{[i-1]'} = \delta(x^{[i]} + \sum_{j=1}^{i-1} \lambda_j x^{[i-j]})$ implies $\lambda_i := x^{[i]'} - x^{[i]} - \sum_{j=1}^{i-1} \lambda_j x^{[i-j]} \in A^\delta$, as required. □

Lemma 3.4. *Let δ be a derivation of a ring A such that $\delta^i(y^{[i]}) = 1$, $0 \leq i \leq m$, for some elements $y^{[i]}$ of A. Note that $y^{[0]} = 1$. Then there exists a* **unique** *δ-descent $\{x^{[i]}, 0 \leq i \leq m\}$ such that $x^{[1]} = y^{[1]}$ and $x^{[i]} = y^{[i]} + \sum_{j=1}^{i-1} c_{ij}y^{[j]}$, $2 \leq i \leq m$, for some $c_{ij} \in A^\delta$.*

Proof. One can easily prove that $N_i := N(\delta, A)_i = \bigoplus_{j=0}^{i} A^\delta y^{[j]}$, $0 \leq i \leq m$ (repeat the argument of the proof of Lemma 3.2). Let, for a moment, a sequence $\{x^{[i]'}, 0 \leq i \leq m\}$ be an arbitrary δ-descent. Then, by Lemma 3.2, $x^{[i]'} \in N_i$, i.e., $x^{[i]'} = y^{[i]} + \sum_{j=0}^{i-1} c'_{ij}y^{[j]}$, $1 \leq i \leq m$, for some elements $c'_{ij} \in A^\delta$ (note that one can easily find a δ-descent, e.g. $\{z^{[i]} := \delta^{m-i}(y^{[m]}), 0 \leq i \leq m\}$). Let $\{x^{[i]}, 0 \leq i \leq m\}$ be another δ-descent, and so $x^{[i]} = y^{[i]} + \sum_{j=0}^{i-1} c_{ij}y^{[j]}$, $1 \leq i \leq m$, for some elements $c_{ij} \in A^\delta$. By Lemma 3.3,

$$x^{[i]} = x^{[i]'} + \sum_{j=1}^{i} \lambda_j x^{[i-j]'}, \quad 1 \leq i \leq m,$$

for some elements $\lambda_j \in A^\delta$. We have to prove that the defining conditions

$$c_{1,0} = c_{2,0} = \cdots = c_{m,0} = 0$$

of the δ-descent from Lemma 3.4 *uniquely* determine the elements $\lambda_1, \lambda_2, \dots, \lambda_m$. The equality $c_{1,0} = 0$ yields the equalities $y^{[1]} = x^{[1]} = x^{[1]'} + \lambda_1 = y^{[1]} + c'_{1,0} + \lambda_1$; hence $\lambda_1 = -c'_{1,0}$. Suppose that, using the equalities $c_{1,0} = \cdots = c_{i-1,0} = 0$, we have already found unique elements $\lambda_1, \lambda_2, \dots, \lambda_{i-1}$. Then the element λ_i can be found uniquely from the equality $x^{[i]} = x^{[i]'} + \lambda_1 x^{[i-1]'} + \cdots + \lambda_{i-1} x^{[1]'} + \lambda_i$. We have to equate to zero the coefficient $c_{i,0}$ of $y^{[0]} := 1$ after we substitute the sum for each $x^{[i]'}$ above (via $y^{[k]}$):

$$x^{[i]} = y^{[i]} + \sum_{j=1}^{i-1} c_{ij} y^{[j]} + c'_{i,0} + \lambda_1 c'_{i-1,0} + \cdots + \lambda_{i-1} c'_{1,0} + \lambda_i;$$

that is, $\lambda_i := -c'_{i,0} - \lambda_1 c'_{i-1,0} - \cdots - \lambda_{i-1} c'_{1,0}$. Therefore, for this unique choice of $\{\lambda_i\}$, we have $c_{1,0} = c_{2,0} = \cdots = c_{m,0} = 0$ for the δ-descent $\{x^{[i]}\}$ in Lemma 3.4. □

Binomial coefficients modulo p. For any two nonnegative integers i and j written in the p-adic form as $i = \sum_k i_k p^k$, $0 \le i_k < p$, and $j = \sum_k j_k p^k$, $0 \le j_k < p$, in the field $\mathbb{F}_p$ there is the equality

$$\binom{i}{j} = \prod_k \binom{i_k}{j_k}. \tag{2}$$

The equality is obvious if $i < j$ since both sides of the equality are equal to zero. If $i \ge j$, this equality can be proved by comparing the coefficients of x^j of the polynomials in $\mathbb{F}_p[x]$ at both ends of the equality

$$\sum_{j=0}^{i} \binom{i}{j} x^j = (1+x)^i = \prod_k (1+x^{p^k})^{i_k} = \prod_k \Big(\sum_{j_k=0}^{i_k} \binom{i_k}{j_k} x^{j_k p^k}\Big) = \sum_{j=0}^{i} \prod_k \binom{i_k}{j_k} x^j.$$

It follows that in $\mathbb{F}_p$,

$$\binom{i}{j} \neq 0 \ \text{ iff } \ j_k \le i_k \ \text{ for all } k, \tag{3}$$

$$\binom{i+j}{j} \neq 0 \ \text{ iff } \ i_k + j_k < p \ \text{ for all } \ k, \ \text{ and} \tag{4}$$

$$\binom{ip^s}{jp^s} = \binom{i}{j}, \ \ s \ge 1. \tag{5}$$

Let A be an $\mathbb{F}_p$-algebra. Recall that a sequence $\{x^{[i]}, 0 \le i < p^n\}$ in A is called an *iterative sequence* iff $x^{[i]} x^{[j]} = \binom{i+j}{j} x^{[i+j]}$ for all $0 \le i, j < p^n$ where $x^{[k]} := 0$ for $k \ge p^n$. Note that if $i + j \ge p^n$, then $x^{[i]} x^{[j]} = \binom{i+j}{j} x^{[i+j]} = 0 \cdot x^{[i+j]} = 0$.

Proposition 3.5 (Structure of iterative sequence)**.** *Let A be an $\mathbb{F}_p$-algebra and $\{x^{[i]}, 0 \le i < p^n\}$ be an iterative sequence. Then*

1. *for each $i = 1, \dots, p^n - 1$, written p-adically as $i = \sum_k i_k p^k$, $x^{[i]} = \prod_k \frac{x^{[p^k]^{i_k}}}{i_k!}$. This means that the iterative sequence is determined by the elements $\{x^{[0]}, x^{[p^j]} \mid j = 0, 1, \dots, n-1\}$.*
2. *For each $j = 0, 1, \dots, n-1$, $x^{[p^j]p} = 0$ (hence $x^{[i]p} = 0$ for all $i = 1, \dots, p^n - 1$, by statement 1).*
3. *$x^{[0]} x^{[p^j]} = x^{[p^j]}$, $j = 0, 1, \dots, n-1$, and $x^{[0]} x^{[0]} = x^{[0]}$.*

Conversely, given commuting elements $\{x^{[0]}, x^{[p^j]} \mid j = 0, 1, \ldots, n-1\}$*, in* A *that satisfy the conditions of statements (2) and (3) above, then the elements* $\{x^{[i]}, 0 \leq i < p^n\}$ *defined as in statement (1) form an iterative sequence.*

Remark. To make formulae more readable we often use the notation $x^{[p^k]j}$ for $(x^{[p^k]})^j$.

Proof. (1). We have to prove that $\prod_k \frac{x^{[p^k]i_k}}{i_k!} = x^{[\sum_k i_k p^k]}$. Consider first a special case using (5),

$$\frac{x^{[p^k]i_k}}{i_k!} = \frac{\binom{2p^k}{p^k}\binom{3p^k}{p^k}\cdots\binom{i_kp^k}{p^k}}{i_k!}x^{[i_kp^k]} = \frac{\binom{2}{1}\binom{3}{1}\cdots\binom{i_k}{1}}{i_k!}x^{[i_kp^k]} = \frac{i_k!}{i_k!}x^{[i_kp^k]} = x^{[i_kp^k]}.$$

Now, the general case follows from the special case and (2) by simply multiplying the elements below and using the fact that each multiplication yields a binomial which is 1 in $\mathbb{F}_p$, by (2):

$$\prod_{k=0}^{s} \frac{x^{[p^k]i_k}}{i_k!} = \prod_{k=0}^{s} x^{[i_kp^k]}$$
$$= \cdots = x^{[\sum_{k=0}^{t-1} i_kp^k]}x^{[i_tp^t]}\cdots x^{[i_sp^s]} = \cdots = x^{[\sum_{k=0}^{s} i_kp^k]} = x^{[i]}.$$

(2). For each $i = 1, \ldots, p^n - 1$,

$$(x^{[i]})^p = x^{[i]}x^{[i]}\cdots x^{[i]} = \binom{2i}{i}\binom{3i}{i}\cdots\binom{pi}{i}x^{[pi]} = 0 \cdot x^{[pi]} = 0,$$

since $\binom{pi}{i} = 0$ in $\mathbb{F}_p$.

(3). This is obvious.

Conversely, suppose that elements $\{x^{[0]}, x^{[p^j]} \mid j = 0, 1, \ldots, n-1\}$ satisfy the conditions of statements (2) and (3), and that the elements $\{x^{[i]}, 0 \leq i < p^n\}$ are defined as in statement (1). To prove that the sequence $\{x^{[i]}, 0 \leq i < p^n\}$ is iterative it suffices to show that $x^{[i]}x^{[j]} = \binom{i+j}{j}x^{[i+j]}$ for all $1 \leq i, j < p^n$. Let $i = \sum i_kp^k$ and $j = \sum j_kp^k$ be the p-adic forms of i and j. Suppose that $i_k + j_k \geq p$ for some k. Then, on the one hand, $\binom{i+j}{j} = 0$ (by (4)), and so $x^{[i]}x^{[j]} = 0 = \binom{i+j}{j}x^{[i+j]}$. Suppose that $i_k + j_k < p$ for all k. Then

$$\begin{aligned} x^{[i]}x^{[j]} &= \prod_k \frac{(x^{[p^k]})^{i_k}}{i_k!}\frac{(x^{[p^k]})^{j_k}}{j_k!} = \prod_k \binom{i_k + j_k}{i_k}\frac{(x^{[p^k]})^{i_k+j_k}}{(i_k+j_k)!} \\ &= \prod_k \binom{i_k + j_k}{i_k} \cdot \prod_l \frac{(x^{[p^l]})^{i_l+j_l}}{(i_l+j_l)!} = \binom{i+j}{i}x^{[i+j]}. \end{aligned}$$

This means that $\{x^{[i]}, 0 \leq i < p^n\}$ is an iterative sequence. □

The following corollary gives necessary and sufficient conditions for an iterative sequence to be a δ-descent.

Corollary 3.6. *Let* A *be an* $\mathbb{F}_p$*-algebra,* δ *be a derivation of* A*, and* $\{x^{[i]}, 0 \leq i < p^n\}$ *be an iterative sequence in* A *with* $x^{[0]} = 1$*. Then the iterative sequence* $\{x^{[i]}, 0 \leq i < p^n\}$ *is a* δ*-descent iff* $\delta(x^{[p^j]}) = x^{[p^j-1]}$*,* $0 \leq j \leq n-1$.

Proof. ($\Rightarrow$) Trivial.

($\Leftarrow$) We have to show that $\delta(x^{[i]}) = x^{[i-1]}$, $1 \leq i < p^n$. Observe that, for each $k \geq 1$, $p^k - 1 = \sum_{l=0}^{k-1}(p-1)p^l$. Then, by (4), $\binom{p^j-1+p^s}{p^s} = 0$, $0 \leq s < j$, and so

$$x^{[p^s]} \cdot \delta(x^{[p^j]}) = x^{[p^s]}x^{[p^j-1]} = \binom{p^j-1+p^s}{p^s} x^{[p^s+p^j-1]} = 0.$$

These equalities imply that, for any integer i ($1 \leq i < p^n$) written p-adically as $i = i_s p^s + i_{s+1}p^{s+1} + \cdots + i_t p^t$ with $i_s \neq 0$, $s \leq t$, and $i = i_s p^s + j$, $j := i_{s+1}p^{s+1} + \cdots + i_t p^t$,

$$\begin{aligned} \delta(x^{[i]}) &= \delta(x^{[i_s p^s]}x^{[j]}) = \delta(\frac{x^{[p^s]i_s}}{i_s!}x^{[j]}) = \delta(\frac{x^{[p^s]i_s}}{i_s!})x^{[j]} = x^{[p^s-1]}\frac{x^{[p^s](i_s-1)}}{(i_s-1)!}x^{[j]} \\ &= x^{[p^s-1]}x^{[p^s(i_s-1)]}x^{[j]} = x^{[p^s i_s-1]}x^{[j]} = x^{[p^s i_s-1+j]} = x^{[i-1]}. \quad \square \end{aligned}$$

Combining Proposition 3.5 and Corollary 3.6, one obtains necessary and sufficient conditions for a sequence to be an iterative δ-descent.

Corollary 3.7. *Let A be an $\mathbb{F}_p$-algebra, δ be a derivation of A, and $x^{[1]}, x^{[p]}, \ldots, x^{[p^{n-1}]}$ be commuting elements of A. Let $x^{[i]} := \prod_k \frac{x^{[p^k]i_k}}{i_k!}$ for each $i = \sum_k i_k p^k$, $0 \leq i_k < p$, such that $0 \leq i < p^n$. Then the sequence $\{x^{[i]}, 0 \leq i < p^n\}$ is an iterative δ-descent iff $\delta(x^{[p^j]}) = x^{[p^j-1]}$ and $x^{[p^j]p} = 0$ for $0 \leq j \leq n-1$.*

Proof. ($\Rightarrow$) Trivial.

($\Leftarrow$) The conditions $x^{[p^j]p} = 0$, $0 \leq j \leq n-1$, mean that $\{x^{[i]}, 0 \leq i < p^n\}$ is an iterative sequence, by Proposition 3.5. Then, the conditions $\delta(x^{[p^j]}) = x^{[p^j-1]}$, $0 \leq j \leq n-1$, imply that $\{x^{[i]}, 0 \leq i < p^n\}$ is a δ-descent, by Corollary 3.6. $\square$

Let A be a commutative $\mathbb{F}_p$-algebra and δ be a derivation of A. Let $\mathrm{ID}(\delta, n)$ be the set of all iterative δ-descents $\{x^{[i]}, 0 \leq i < p^n\}$ of exponent n in A. Let $C(\delta, n)$ be the set of all n-tuples $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ such that $\lambda_j \in A^\delta$ and $\lambda_j^p = 0$ for $0 \leq j \leq n-1$. Note that if A^δ is a *reduced* ring, then $C(\delta, n) = \{(0, \ldots, 0)\}$; i.e., $C(\delta, n)$ contains a single element. By Lemma 3.2 and Proposition 3.5, for each iterative δ-descent, say $\{x^{[i]}, 0 \leq i < p^n\}$,

(6)
$$N(\delta, A)_{p^n-1} = \bigoplus_{i=0}^{p^n-1} A^\delta x^{[i]} \simeq A^\delta[x^{[1]}, x^{[p]}, \ldots, x^{[p^{n-1}]}]/(x^{[1]p}, x^{[p]p}, \ldots, x^{[p^{n-1}]p}).$$

So, $N(\delta, A)_{p^n-1}$ is a *subring* of A that contains A^δ, and the decomposition (6) holds for *all* iterative δ-descents in A of exponent n. In particular, all iterative δ-descents in A of exponent n belong to $N(\delta, A)_{p^n-1}$. Then

$$N(\delta, A)_{p^n-1} = A^\delta \oplus \mathfrak{m}, \quad \mathfrak{m} := (x^{[1]}, x^{[p]}, \ldots, x^{[p^{n-1}]}). \tag{7}$$

If $\{y^{[i]}, 0 \leq i < p^n\}$ is an iterative δ-descent in A, then $\{y^{[i]}, 0 \leq i < p^n\} \subseteq N(\delta, A)_{p^n-1}$. Therefore, the following map is well defined:

$$r = r_n : \mathrm{ID}(\delta, n) \to C(\delta, n), \quad \{y^{[i]}, 0 \leq i < p^n\} \mapsto (\lambda_0, \lambda_1, \ldots, \lambda_{n-1}), \tag{8}$$

where $\lambda_j \equiv y^{[p^j]} \mod \mathfrak{m}$, $j = 0, 1, \ldots, n-1$. Note that the map r depends on the choice of the iterative δ-descent $\{x^{[i]}, 0 \leq i < p^n\}$ since the decomposition (7) does.

Theorem 3.8 (Existence and uniqueness of an iterative δ-descent)**.** *Let A be a commutative algebra over a field K of characteristic $p > 0$ and δ be a K-derivation of the algebra A such that there exists a finite sequence of elements $y_0, y_1, \dots, y_{n-1}$ of A such that $y_k^p = 0$ and $\delta^{p^k}(y_k) = 1$ for all $0 \leq k \leq n-1$. Then*

(1) *(Existence) The following sequence $\{x^{[i]}, 0 \leq i < p^n\}$ is an iterative δ-descent where $x^{[0]} := 1$, $x^{[1]} := y_0$, and, for $i \geq 2$ written p-adically as $i = \sum_{k=0}^{t} i_k p^k$ $(0 \leq i_k \leq p-1)$ the element $x^{[i]}$ is defined as $x^{[i]} := \prod_{k=0}^{t} \frac{(x^{[p^k]})^{i_k}}{i_k!}$, where*

$$x^{[p]} := (-1)^{p-1}\phi_0(y_1), \;\; \phi_0(z) := \sum_{j=0}^{p-1}(-1)^j \frac{(x^{[1]})^j}{j!}\delta^j(z),$$

and then recursively, for each k such that $1 \leq k \leq n-2$, the element $x^{[p^{k+1}]}$ is defined by the rule

$$x^{[p^{k+1}]} := (-1)^{p-1}\delta^{p^k-1}\Big(\prod_{l=0}^{k-1} \frac{(x^{[p^l]})^{p-1}}{(p-1)!} \cdot \phi_k(y_{k+1})\Big),$$

$$\phi_k(z) := \sum_{j=0}^{p-1}(-1)^j \frac{(x^{[p^k]})^j}{j!}\delta^{p^k j}(z).$$

(2) *(Almost uniqueness) Let $\{x^{[i]}, 0 \leq i < p^n\}$ be an arbitrary iterative δ-descent (not necessarily as in statement (1), and n here is not necessarily as in statement (1) either). Then the map (8) is a bijection.*

(3) *(Uniqueness). If, in addition, the ring A^δ is reduced, then $\{x^{[i]}, 0 \leq i < p^n\}$ from statement (1) is the only iterative δ-descent.*

Proof. (1). By Corollary 3.7, it suffices to prove two statements: $\delta(x^{[p^j]}) = x^{[p^j-1]}$ and $(x^{[p^j]})^p = 0$ for all $0 \leq j \leq n-1$. For $j = 0$, we have $\delta(x^{[1]}) = \delta(y_0) = 1 = x^{[0]}$ and $(x^{[1]})^p = y_0^p = 0$. A direct calculation shows that $\delta\phi_0(z) = (-1)^{p-1}\frac{y_0^{p-1}}{(p-1)!}\delta^p(z)$. If $j = 1$, then $\delta(x^{[p]}) = (-1)^{p-1}\delta\phi_0(y_1) = (-1)^{p-1}(-1)^{p-1}\frac{y_0^{p-1}}{(p-1)!}\delta^p(y_1) = x^{[p-1]}$ and

$$(x^{[p]})^p = (-1)^{(p-1)p}\Big(\sum_{k=0}^{p-1}(-1)^k\frac{y_0^k}{k!}\delta^k(y_1)\Big)^p = \sum_{k=0}^{p-1}(-1)^{kp}\Big(\frac{y_0^k}{k!}\Big)^p(\delta^k(y_1))^p = y_1^p = 0.$$

Let $j \geq 2$. We use induction on j. By the induction hypothesis, for all $k < j$, $\delta(x^{[p^k]}) = x^{[p^k-1]}$ and $(x^{[p^k]})^p = 0$. This means that $\{x^{[i]}, 0 \leq i < p^j\}$ is an iterative δ-descent, by Corollary 3.7. In particular, $\delta(x^{[l]}) = x^{[l-1]}$ for all $l < p^j$, which implies that

$$x^{[p^j-1]} = x^{[\sum_{l=0}^{j-1}(p-1)p^l]} = \prod_{l=0}^{j-1}\frac{(x^{[p^l]})^{p-1}}{(p-1)!} \in \ker\delta^{p^j}. \tag{9}$$

For each k such that $2 \leq k < j$, a direct calculation shows that

$$\delta^{p^k}\phi_k(z) = (-1)^{p-1}\frac{(x^{[p^k]})^{p-1}}{(p-1)!}\delta^{p^{k+1}}(z). \tag{10}$$

Now, using the two equalities above we have

$$\begin{aligned}
\delta(x^{[p^j]}) &= (-1)^{p-1}\delta^{p^{j-1}}\Big(\prod_{l=0}^{j-2}\frac{(x^{[p^l]})^{p-1}}{(p-1)!}\phi_{j-1}(y_j)\Big)\\
&= (-1)^{p-1}\delta^{p^{j-1}}(x^{[p^{j-1}-1]}\phi_{j-1}(y_j))\\
&= (-1)^{p-1}x^{[p^{j-1}-1]}\delta^{p^{j-1}}\phi_{j-1}(y_j) \qquad \text{(by (9))}\\
&= (-1)^{p-1}x^{[p^{j-1}-1]}(-1)^{p-1}\frac{(x^{[p^{j-1}]})^{p-1}}{(p-1)!}\delta^{p^j}(y_j) \qquad \text{(by (10))}\\
&= \prod_{l=0}^{j-1}\frac{(x^{[p^l]})^{p-1}}{(p-1)!} = x^{[p^j-1]}.
\end{aligned}$$

Finally, letting $t := p^{j-1}-1$,

$$\begin{aligned}
x^{[p^j]} &= (-1)^{p-1}\delta^t(x^{[t]}\phi_{j-1}(y_j)) = (-1)^{p-1}\sum_{s=0}^{t}\binom{t}{s}\delta^s(x^{[t]})\delta^{t-s}\phi_{j-1}(y_j)\\
&= (-1)^{p-1}\sum_{s=0}^{t}\binom{t}{s}x^{[t-s]}\delta^{t-s}\phi_{j-1}(y_j).
\end{aligned}$$

Since $(x^{[1]})^p = \cdots = (x^{[t]})^p = 0$, it follows from the equality above that $(x^{[p^j]})^p = 0$ iff $\phi_{j-1}(y_j)^p = 0$. Since $\phi_{j-1}(y_j) = \sum_{k=0}^{p-1}(-1)^k\frac{(x^{[p^{j-1}]})^k}{k!}\delta^{kp^{j-1}}(y_j)$ and $y_j^p = 0 = (x^{[p^{j-1}]})^p$, we have $\phi_{j-1}(y_j)^p = 0$. This proves that $(x^{[p^j]})^p = 0$, as required.

(2). In order to prove statement (2), we use induction on $n \geq 1$. The case $n = 1$ is almost obvious. If $\{y^{[i]}, 0 \leq i < p\} \in \mathrm{ID}(\delta, 1)$, then $\delta(y^{[1]}) = 1 = \delta(x^{[1]})$, and so $y^{[1]} = x^{[1]} + \lambda_0$ for some element $\lambda_0 \in A^\delta$; necessarily $\lambda_0^p = 0$ since $y^{[1]p} = x^{[1]p} = 0$, and $y^{[1]} \equiv \lambda_0 \mod \mathfrak{m}$. By Corollary 3.7, the sequence $\{y^{[i]}, 0 \leq i < p\}$ is uniquely determined by the element $y^{[1]}$, and so the map r is injective. It remains to show that r is surjective. For each element, say $\lambda_0 \in A^\delta$, such that $\lambda_0^p = 0$, the element $y^{[1]} = x^{[1]} + \lambda_0$ satisfies the following conditions: $y^{[1]} \equiv \lambda_0 \mod \mathfrak{m}$, $\delta(y^{[1]}) = 1$, and $y^{[1]p} = x^{[1]p} + \lambda_0^p = 0$. Hence, by Corollary 3.7, the element $y^{[1]}$ determines an iterative δ-descent. Therefore, r is a surjection, as required.

Now, let $n \geq 2$. Suppose that the result is true for all $n' < n$. First, let us prove that the map $r := r_n$ is injective. Let $y := \{y^{[i]}, 0 \leq i < p^n\}$ and $z := \{z^{[i]}, 0 \leq i < p^n\}$ be two iterative δ-descents such that $r(y) = r(z) = (\lambda_0, \ldots, \lambda_{n-1})$. We have to show that $y = z$. By induction, $y^{[i]} = z^{[i]}$, $0 \leq i < p^{n-1}$. It follows from the equalities

$$\delta(y^{[p^{n-1}]}) = y^{[p^{n-1}-1]} = z^{[p^{n-1}-1]} = \delta(z^{[p^{n-1}]})$$

that $y^{[p^{n-1}]} - z^{[p^{n-1}]} \in A^\delta$. Since $y^{[p^{n-1}]} \equiv \lambda_{n-1} \equiv z^{[p^{n-1}]} \mod \mathfrak{m}$ and $N(\delta, A)_{p^n-1} = A^\delta \oplus \mathfrak{m}$ (by (7)), we must have $y^{[p^{n-1}]} = z^{[p^{n-1}]}$. By Corollary 3.7, $y = z$, i.e., r is an injection.

It remains to show that r is a surjection. Let $\lambda := (\lambda_0, \ldots, \lambda_{n-1}) \in C(\delta, n)$. We have to show that there exists an element $y := \{y^{[i]}, 0 \leq i < p^n\} \in \mathrm{ID}(\delta, n)$ such that $r(y) = \lambda$. By induction, there exists a unique element $y' := \{y^{[i]}, 0 \leq i < p^{n-1}\} \in \mathrm{ID}(\delta, n-1)$ such that $r_{n-1}(y') = (\lambda_0, \ldots, \lambda_{n-2})$. By Corollary 3.7, it suffices to find an element $y^{[p^{n-1}]}$ such that $y^{[p^{n-1}]p} = 0$, $\delta(y^{[p^{n-1}]}) = y^{[p^{n-1}-1]}$, and

$y^{[p^{n-1}]} \equiv \lambda_{n-1} \mod \mathfrak{m}$. By Lemma 3.2,

$$N(A,\delta)_{p^{n-1}-1} = \bigoplus_{i=0}^{p^{n-1}-1} A^\delta x^{[i]} = \bigoplus_{i=0}^{p^{n-1}-1} A^\delta y^{[i]},$$
$$N(A,\delta)_{p^{n-1}} = N(A,\delta)_{p^{n-1}-1} \oplus A^\delta x^{[p^{n-1}]}.$$

Since the map $\delta : N(A,\delta)_{p^{n-1}} \to N(A,\delta)_{p^{n-1}-1}$ is *surjective* and $y^{[p^{n-1}-1]} \in N(A,\delta)_{p^{n-1}-1}$, one can find an element $y^{[p^{n-1}]} \in N(A,\delta)_{p^{n-1}}$ such that $\delta(y^{[p^{n-1}]}) = y^{[p^{n-1}-1]}$. The element $y^{[p^{n-1}]}$ is unique up to adding an element of A^δ. By adding a well-chosen element of A^δ to $y^{[p^{n-1}]}$, we can assume that $y^{[p^{n-1}]} \equiv \lambda_{n-1} \mod \mathfrak{m}$; i.e., $y^{[p^{n-1}]} = \lambda_{n-1} + v$ for some element $v \in \mathfrak{m}$. Since $\lambda_{n-1}^p = 0$ and $v^p = 0$ (since $v \in \mathfrak{m}$), $y^{[p^{n-1}]p} = 0$. Now, by Corollary 3.7, the elements $y^{[p^j]}$, $0 \le j \le n-1$, determine an element, say y, of $\mathrm{ID}(A,n)$ such that, obviously, $r(y) = \lambda$. This proves that r is a surjection. By induction, statement (2) holds.

(3). Since A^δ is a reduced ring, the set $C(\delta,n)$ contains the single element $(0,\dots,0)$, and so the result follows from statement (2). □

The next lemma shows that the set $\mathrm{nsder}(R)$ is nonempty where R is a differentiably simple Noetherian commutative ring.

Lemma 3.9. *Let k be a field of characteristic $p > 0$ and $R := k[x_0,\dots,x_{n-1}]/(x_0^p,\dots,x_{n-1}^p)$ (by Theorem 4.1.(2), R is a differentiably simple Noetherian commutative ring). Then*

$$\delta := \sum_{i=0}^{n-1} x^{[p^i-1]} \frac{\partial}{\partial x_i} \in \mathrm{nsder}(R)$$

where $x^{[p^i-1]} := \prod_{\nu=0}^{i-1} \frac{x_\nu^{p-1}}{(p-1)!}$, $1 \le i \le n-1$, and $x^{[0]} := 1$.

Proof. For each natural number $j = 0,1,\dots,p^n-1$, written p-adically, $j = \sum_\nu j_\nu p^\nu$, let $x^{[j]} := \prod_\nu \frac{x_\nu^{j_\nu}}{j_\nu!}$. By Proposition 3.5, $\{x^{[j]}, 0 \le j < p^n\}$ is the iterative sequence with $x^{[0]} := 1$. By Corollary 3.6, this iterative sequence is a δ-descent. Since $R = \bigoplus_{j=0}^{p^n-1} k x^{[j]}$ and $\delta(x^{[j]}) = x^{[j-1]}$ for all $j = 0,1,\dots,p^n-1$, the derivation δ is simple and nilpotent with $\delta^{p^n} = 0$. For each $i = 0,1,\dots,n-1$, $\delta^{p^i}(x^{[p^i]}) = 1$, and so $\delta \in \mathrm{nsder}(R)$. □

4. Simple derivations of differentiably simple Noetherian commutative rings

In this section, we will see that for a differentially simple Noetherian commutative ring $(R,\mathfrak{m})$ there are strong connections between simple nilpotent derivations $\mathrm{nsder}(R)$, coefficient fields for R, iterative descents, and the group $\mathrm{Aut}(R)$ of ring automorphisms of R. Namely, there is a canonical bijection $\mathrm{nsder}(R) \simeq \mathrm{Aut}(R)/\mathrm{Aut}(R/\mathfrak{m})$ (Corollary 4.3).

Recall that for a local commutative ring $(R,\mathfrak{m})$, a subfield k' of R is called a coefficient field of R if $R = k' + \mathfrak{m}$. Let $\mathcal{F}(R)$ be the set of all the coefficient fields of R. If k' is a coefficient field of R, then $k' \simeq (k'+\mathfrak{m})/\mathfrak{m} \simeq R/\mathfrak{m} = k$, the residue field of R.

Let k be a field of characteristic $p > 0$. For a differentiably simple Noetherian commutative ring $(R, \mathfrak{m})$ of characteristic $p > 0$ with $n := \dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq 1$ where $k := R/\mathfrak{m}$ (i.e., $R \simeq T_n := k[x_0, \dots, x_{n-1}]/(x_0^p, \dots, x_{n-1}^p)$), a subset $\{x'_0, \dots, x'_{n-1}\} \subseteq \mathfrak{m}$ is called a *canonical set of generators* for R if there exists a coefficient field k' of R such that

$$R = k'\langle x'_0, \dots, x'_{n-1}\rangle \simeq k'[x'_0, \dots, x'_{n-1}]/(x_0'^p, \dots, x_{n-1}'^p).$$

Let $\mathcal{C} = \mathcal{C}(R)$ be the set of all such $(k'; x'_0, \dots, x'_{n-1})$. Then $\mathcal{C} = \bigcup_{k' \in \mathcal{F}(R)} \mathcal{C}(R, k')$ is a disjoint union of its subsets

$$\mathcal{C}(R, k') = \{(k'; x'_0, \dots, x'_{n-1}) \mid (k'; x'_0, \dots, x'_{n-1}) \in \mathcal{C}(R)\}.$$

Let $\operatorname{sder}(R)$ be the set of all *simple* derivations of the ring R. For a local commutative ring $(R, \mathfrak{m})$, let $\operatorname{nsder}(R)$ be the set of all *nilpotent simple* derivations δ of the ring R such that if $\delta^{p^i} \neq 0$, then $\delta^{p^i}(y_i) = 1$ for some $y_i \in \mathfrak{m}$.

The next theorem gives (i) another description of all the coefficient fields for a differentiably simple Noetherian commutative $\mathbb{F}_p$-algebra, (ii) the canonical form of each derivation $\delta \in \operatorname{nsder}(R)$ (Theorem 4.1(2)) via the unique iterative δ-descent. Recall that the set $\operatorname{nsder}(R)$ is a nonempty set (Lemma 3.9).

Theorem 4.1. *Let $(R, \mathfrak{m})$ be a differentiably simple Noetherian commutative $\mathbb{F}_p$-algebra with residue field $k = R/\mathfrak{m}$, $n := \dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq 1$, and $\delta \in \operatorname{nsder}(R)$. Then*

(1) *$\delta^{p^{n-1}} \neq 0$ and $\delta^{p^n} = 0$.*

(2) *There exists a* **unique** *iterative δ-descent $\{x^{[i]}, 0 \leq i < p^n\}$. Then $x^{[i]} \in \mathfrak{m}$ for all $i = 1, \dots, p^n - 1$; $R^\delta \in \mathcal{F}(R)$;*

$$R = \bigoplus_{i=0}^{p^n-1} R^\delta x^{[i]} = R^\delta\langle x_0, \dots, x_{n-1}\rangle \simeq R^\delta[x_0, \dots, x_{n-1}]/(x_0^p, \dots, x_{n-1}^p),$$

where $x_j := x^{[p^j]}$, $x^{[i]} = \prod_{\nu=0}^t \frac{x_\nu^{i_\nu}}{i_\nu!}$, $i = \sum_{\nu=0}^t i_\nu p^\nu$, $0 \leq i_\nu < p$, and

$$\delta = \sum_{i=0}^{n-1} x^{[p^i-1]} \frac{\partial}{\partial x_i} \in \operatorname{Der}_{R^\delta}(R).$$

(3) *The map $\phi := \sum_{i=0}^{p^n-1} (-1)^i x^{[i]} \delta^i : R \to R$ is a* **projection** *onto the direct summand R^δ of R. In particular, $R^\delta = \phi(R)$.*

Proof. Let s be the natural number such that $\delta^{p^{s-1}} \neq 0$ but $\delta^{p^s} = 0$. For each $j = 0, \dots, s-1$, let $\delta_j := \delta^{p^j}$ and fix an element $y_j \in \mathfrak{m}$ such that $\delta_j(y_j) = 1$ (we can do this since $\delta \in \operatorname{nsder}(R)$). Clearly, $y_j^p = 0$ for all j (Lemma 2.1). Let $\{x^{[i]}, 0 \leq i < p^s\}$ be an iterative δ-descent (Theorem 3.8), and let $x_j := x^{[p^j]}$, for $j = 0, \dots, s-1$. Note that $R = N(\delta, R)_{p^s-1}$ since $\delta^{p^s} = 0$. By (6),

$$R = \bigoplus_{i=0}^{p^s-1} R^\delta x^{[i]} \simeq R^\delta[x_0, \dots, x_{s-1}]/(x_0^p, \dots, x_{s-1}^p). \tag{11}$$

Since the derivation δ is simple, R^δ is a field (if $\mathfrak{a}$ is an ideal of R^δ, then $\mathfrak{b} := \bigoplus_{i=0}^{p^s-1} \mathfrak{a}x^{[i]}$ is an ideal of R such that $\delta(\mathfrak{b}) \subseteq \mathfrak{b}$). Then, by Theorem 3.8.(3), the iterative δ-descent $\{x^{[i]}, 0 \leq i < p^s\}$ is unique. By (11), $\mathfrak{m} = (x_0, \dots, x_{s-1})$; hence $s = n$. Now, statements (1) and (2) follows from (11).

The map ϕ is an endomorphism of the R^δ-module R. For each $j = 1, \dots, p^n - 1$,

$$\phi(x^{[j]}) = \sum_{i=0}^{j} (-1)^i x^{[i]} x^{[j-i]} = \sum_{i=0}^{j} (-1)^i \binom{j}{i} \cdot x^{[j]} = (1-1)^j \cdot x^{[j]} = 0 \cdot x^{[j]} = 0.$$

Hence ϕ is the projection onto R^δ in view of the decomposition $R = \bigoplus_{i=0}^{p^n-1} R^\delta x^{[i]}$; see (11). This proves statement (3). □

Theorem 4.2. *Let $(R, \mathfrak{m})$ be a differentiably simple Noetherian commutative $\mathbb{F}_p$-algebra with residue field $k = R/\mathfrak{m}$ and $n := \dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq 1$.*

(1) *Then the map*

$$g : \operatorname{nsder}(R) \to \mathcal{C}(R), \quad \delta \mapsto (\ker \delta; x^{[p^0]}, x^{[p^1]}, \dots, x^{[p^{n-1}]}),$$

is a bijection (where $\{x^{[i]}, 0 \leq i < p^n\}$ is the iterative δ-descent as in Theorem 4.1) with the inverse map given by the rule

$$g^{-1} : \mathcal{C}(R) \to \operatorname{nsder}(R), \quad (k'; x_0, \dots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} x^{[p^i-1]} \frac{\partial}{\partial x_i} \in \operatorname{Der}_{k'}(R),$$

where $x^{[0]} := 1$ and $x^{[p^i-1]} := \prod_{j=0}^{i-1} \frac{x_j^{p-1}}{(p-1)!}$ (see Theorem 4.1).

(2) *For each coefficient field k' in R, the restriction $g_{k'}$ of the map g to the subset $\operatorname{nsder}_{k'}(R) := \{\delta \in \operatorname{nsder}(R) \mid \delta(k') = 0\}$ of $\operatorname{nsder}(R)$ yields an isomorphism $g_{k'} : \operatorname{nsder}_{k'}(R) \to \mathcal{C}(R, k')$.*

Proof. (1). The map g is well defined due to Theorem 4.1(1,3), and, by Theorem 4.1(2), for each derivation $\delta \in \operatorname{nsder}(R)$, $\delta = \sum_{i=0}^{n-1} x^{[p^i-1]} \frac{\partial}{\partial x_i} \in \operatorname{Der}_{R^\delta}(R)$, where $\{x^{[j]}, 0 \leq j < p^n\}$ is the iterative δ-descent, $x_i := x^{[p^i]}$ and $x^{[p^i-1]} = \prod_{j=0}^{i-1} \frac{(x^{[p^j]})^{p-1}}{(p-1)!} = \prod_{j=0}^{i-1} \frac{x_j^{p-1}}{(p-1)!}$.

Conversely, for each $(k'; x_0, \dots, x_{n-1}) \in \mathcal{C}(R)$, let $x := \{x^{[i]}, 0 \leq i < p^n\}$ be the corresponding iterative sequence which exists, by Proposition 3.5, since $x_0^p = \dots = x_{n-1}^p = 0$. The derivation $\delta := \sum_{i=0}^{n-1} x^{[p^i-1]} \frac{\partial}{\partial x_i} \in \operatorname{Der}_{k'}(R)$ is nilpotent (by the very definition of δ), and $\delta(x^{[p^i]}) = \delta(x_i) = x^{[p^i-1]}$, $0 \leq i \leq n-1$ (by the very definition of δ). By Corollary 3.7 and Theorem 3.8(3), x is the iterative δ-descent. Hence R is a δ-simple ring with $\ker(\delta) = k'$ (Lemma 3.1(3)).

(2). If k' is a coefficient field of $R = k[x_0, \dots, x_{n-1}]/(x_0^p, \dots, x_{n-1}^p)$, then the fields k' and k are isomorphic. Let us fix an isomorphism, say $\sigma : k \to k'$. Then σ can be extended to an automorphism of the ring R by setting $\sigma(x_i) = x_i$ for all i (since $R = k' + \mathfrak{m} = k'\langle x_0, \dots, x_{n-1}\rangle \simeq k'[x_0, \dots, x_{n-1}]/(x_0^p, \dots, x_{n-1}^p)$). This implies that the set $\operatorname{nsder}_{k'}(R) \neq \emptyset$ since $\operatorname{nsder}_k(R) \neq \emptyset$. Now, statement (2) follows from statement (1). □

For the ring R and its coefficient field $k' \in \mathcal{F}(R)$, let $\operatorname{Aut}(R)$ (resp. $\operatorname{Aut}_{k'}(R)$) be the group of all ring (resp. k'-algebra) automorphisms of R. For the residue field $k := R/\mathfrak{m}$, $\operatorname{Aut}(k)$ is the group of its automorphisms.

Recall that an action of a group G on a set X is said to be *fully faithful* if for some/each $x \in X$ the map $G \to X$, $g \mapsto gx$, is a bijection.

Corollary 4.3. *Let $(R, \mathfrak{m})$ be as in Theorem 4.2. Then*

(1) *for each coefficient field $k' \in \mathcal{F}(R)$, the action $\mathrm{Aut}_{k'}(R) \times \mathrm{nsder}_{k'}(R) \to \mathrm{nsder}_{k'}(R)$ which is given by the rule $(\sigma, \delta) \mapsto \sigma\delta\sigma^{-1}$ is fully faithful.*
(2) *The action $\mathrm{Aut}(R) \times \mathrm{nsder}(R) \to \mathrm{nsder}(R)$, $(\sigma, \delta) \mapsto \sigma\delta\sigma^{-1}$, has a single orbit and, for each $\delta \in \mathrm{nsder}(R)$, $\mathrm{Fix}(\delta) \simeq \mathrm{Aut}(k)$, and so $\mathrm{nsder}(R) \simeq \mathrm{Aut}(R)/\mathrm{Aut}(k)$ where $\mathrm{Fix}(\delta) := \{\sigma \in \mathrm{Aut}(R) \,|\, \sigma\delta\sigma^{-1} = \delta\}$.*

Proof. (1). By the Theorem of Harper (Theorem 2.6(2)), one can assume that $R = k'[x_0, \dots, x_{n-1}]/(x_0^p, \dots, x_{n-1}^p)$. The natural action of the group $\mathrm{Aut}_{k'}(R)$ on the set $\mathcal{C}(R, k')$ is fully faithful where $\sigma \cdot (k'; x_0, \dots, x_{n-1}) := (k'; \sigma(x_0), \dots, \sigma(x_{n-1}))$. The bijection $g_{k'} : \mathrm{nsder}_{k'}(R) \to \mathcal{C}(R, k')$ *commutes* with the action of the group $\mathrm{Aut}_{k'}(R)$. Therefore, the action of $\mathrm{Aut}_{k'}(R)$ on $\mathrm{nsder}_{k'}(R)$ is fully faithful.

(2). The action of $\mathrm{Aut}(R)$ on $\mathcal{C}(R)$, $\sigma \cdot (k; x_0, \dots, x_{n-1})) := (\sigma(k); \sigma(x_0), \dots, \sigma(x_{n-1}))$, has a single orbit. The bijection g from Theorem 4.2(1) commutes with the action of the group $\mathrm{Aut}(R)$. Therefore, $\mathrm{nsder}(R)$ is an orbit of $\mathrm{Aut}(R)$.

One can assume that $R = k[x_0, \dots, x_{n-1}]/(x_0^p, \dots, x_{n-1}^p)$ and that $\delta = \sum_{i=0}^{n-1} x^{[p^i-1]} \frac{\partial}{\partial x_i} \in \mathrm{Der}_k(R)$ where $k = \ker \delta$ (see Theorem 4.1). Consider the group monomorphism $\mathrm{Aut}(k) \to \mathrm{Aut}(R)$, $\tau \mapsto \tau$, given by the rule $\tau(x_i) = x_i$ for all i. It remains to show that $\mathrm{Fix}(\delta) = \mathrm{Aut}(k)$. The inclusion $\mathrm{Aut}(k) \subseteq \mathrm{Fix}(\delta)$ is obvious. To prove the reverse inclusion we must show that if an automorphism σ commutes with δ, then $\sigma(x_i) = x_i$ for all i. Note that each $x_i' := \sigma(x_i) \in \mathfrak{m}$ for all i. Since $\delta(x_0') = \delta\sigma(x_0) = \sigma\delta(x_0) = \sigma(1) = 1$, we have $x_0' = x_0 + \lambda$ for some scalar $\lambda \in k$. The scalar λ must be zero since $x_0' \in \mathfrak{m}$, and so $x_0' = x_0$. Suppose that $x_0' = x_0, \dots, x_{i-1}' = x_{i-1}$ for some $i \geq 1$. Then $x^{[p^i-1]} = \prod_{k=0}^{i-1} \frac{x_k^{p-1}}{(p-1)!}$ and so $\sigma(x^{[p^i-1]}) = x^{[p^i-1]}$. Now, $\delta(x_i') = \sigma\delta(x^{[p^i]}) = \sigma(x^{[p^i-1]}) = x^{[p^i-1]} = \delta(x_i)$. This yields the equality $x_i' = x_i + \lambda$ for some scalar $\lambda \in k$. The scalar λ is forced to be zero since $x_i', x_i \in \mathfrak{m}$. By induction, we have $x_j' = x_j$ for all j. □

Proposition 4.4. *Let $(R, \mathfrak{m})$ be a differentiably simple Noetherian commutative $\mathbb{F}_p$-algebra, $k := R/\mathfrak{m}$, $n := \dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq 1$. Then, for each $\delta \in \mathrm{nsder}(R)$, $R^\delta \in \mathcal{F}(R)$ and $\mathrm{Der}_{R^\delta}(R) = \bigoplus_{i=0}^{n-1} R\delta^{p^i}$.*

Proof. Let $\{x^{[i]}, 0 \leq i < p^n\}$ be the iterative δ-descent and $k' := R^\delta$ (see Theorem 4.1(2)). By Theorem 4.1, $R \simeq k'[x_0, \dots, x_{n-1}]/(x_0^p, \dots, x_{n-1}^p)$ where $x_i := x^{[p^i]}$, $\mathfrak{m} = (x_0, \dots, x_{n-1})$, and $k' \in \mathcal{F}(R)$. It is obvious that $\mathrm{Der}_{k'}(R) = \bigoplus_{i=0}^{n-1} R\partial_i$ where $\partial_i := \frac{\partial}{\partial x_i} \in \mathrm{Der}_{k'}(R)$ (since for each $\delta \in \mathrm{Der}_{k'}(R)$, $\delta = \sum_{i=0}^{n-1} \delta(x_i)\partial_i$), and that

$$\delta^{p^i}(x_j) \equiv \delta_{ij} \equiv \partial_i(x_j) \mod \mathfrak{m} \text{ for all } i, j = 0, \dots, n-1.$$

Hence $\mathrm{Der}_{k'}(R) = \sum_{i=0}^{n-1} R\delta^{p^i} + \mathfrak{m}\mathrm{Der}_{k'}(R)$. By the Nakayama Lemma, $\mathrm{Der}_{k'}(R) = \sum_{i=0}^{n-1} R\delta^{p^i}$. It is obvious that this sum is a direct one (if $\partial := \lambda_s\delta^{p^s} + \cdots + \lambda_t\delta^{p^t} = 0$ is a nontrivial relation, i.e., $\lambda_s \neq 0$, then $0 = \partial(x_s) = \lambda_s$, a contradiction). □

Acknowledgements

The author would like to thank the referee of this paper for a careful reading of the manuscript and valuable comments.

References

[1] L. Harper, On differentiably simple algebras, *Trans. Amer. Math. Soc.* **100** (1961), 63–72. MR0130250 (24:A116)

[2] T. Kimura and H. Niitsuma, On Kunz's conjecture, *J. Math. Soc. Japan* **34** (1982), 371–378. MR651278 (83h:13030)

[3] A. K. Maloo, Generators for a maximally differential ideal in positive characteristic, *Nagoya Math. J.* **132** (1993), 37–41. MR1253693 (94m:13009)

[4] H. Matsumura, *Commutative ring theory*, Cambridge Univ. Press, 1986. MR879273 (88h:13001)

[5] C. Maxson and K. Retert, Simple derivations of graded affine algebras in positive characteristic, *Comm. Algebra* **32** (2004), no. 3, 1151–1181. MR2099344 (2005h:13042)

[6] S. Yuan, Differentiably simple rings of prime characteristic, *Duke Math. J.* **31** (1964), 623–630. MR0167499 (29:4772)

Department of Pure Mathematics, University of Sheffield, Hicks Building, Sheffield S3 7RH, United Kingdom

E-mail address: v.bavula@sheffield.ac.uk