INTEGRATING HASSE-SCHMIDT DERIVATIONS

DANIEL HOFFMANN[†] AND PIOTR KOWALSKI[♠]

Abstract. We study integrating (that is expanding to a Hasse-Schmidt derivation) derivations, and more generally truncated Hasse-Schmidt derivations, satisfying iterativity conditions given by formal group laws. Our results concern the cases of the additive and the multiplicative group laws. We generalize a theorem of Matsumura about integrating nilpotent derivations (such a generalization is implicit in work of Ziegler) and we also generalize a theorem of Tyc about integrating idempotent derivations.

1. Introduction

The algebraic theory of derivations is an important tool in commutative algebra. This theory works better in the characteristic 0 case due to the fact that any derivation vanishes on the set of p-th powers, if the characteristic is $p > 0$. To deal with this problem, Hasse and Schmidt introduced *higher differentiations* [19, p. 224] which we call *HS-derivations* in this paper. An HS-derivation (see Definition 2.1) is a sequence of maps having a usual derivation as its first element. In the case of a $\mathbb{Q}$-algebra, any derivation uniquely expands to an *iterative* HS-derivation (see Definition 2.2) and the two theories coincide.

Matsumura obtained several interesting results about expanding (called *integrating* in [14]) derivations to HS-derivations in the case of positive characteristic. The first result [14, Theorem 6 and Corollary] says that any derivation on a field is (non-uniquely) integrable. The second result [14, Theorem 7] says that a derivation D on a field can be integrated to an iterative HS-derivation (*strongly integrated* in Matsumura's terminology) if and only if composing D with itself p times gives the 0-map. In our paper we prove a version of the second Matsumura's result mentioned above.

Analyzing the definition of an iterative HS-derivation, one realizes [14, (1.9) and (1.10)] that the iterativity condition is given by the additive *formal group law* $\widehat{\mathbb{G}}_{\mathrm{a}} = X+Y$. It is natural to ask what happens if the additive formal group law is replaced with another formal group law F, e.g. the multiplicative one $\widehat{\mathbb{G}}_{\mathrm{m}} = X + Y + XY$. Such a replacement naturally leads to a definition of an *F-iterative* HS-derivation, see Definition 2.2. Such derivations were considered before in a number of contexts. In [21], they are defined as actions of a formal group law on an algebra (see also [1] and [2]). In a more general setting (i.e. on arbitrary schemes), they appear in [5, Def. 4.2] (for an even more general setting, see [16]).

2010 *Mathematics Subject Classification.* Primary 13N15; Secondary 14L15.
Key words and phrases. Hasse-Schmidt derivations, group scheme actions.
[†]AMDG.
[♠]Supported by NCN grant 2012/07/B/ST1/03513.

Any formal group (law) F can be considered as a direct limit of certain finite or truncated group laws $F[m]$. These truncated group laws give rise to the definition of $F[m]$-iterative truncated HS-derivations (see Definition 2.11) and we can ask whether such derivations are integrable. We prove the following.

Theorem 1.1. *Let F be a formal group law such that $F \cong \widehat{\mathbb{G}}_{\mathrm{a}}$ or $F \cong \widehat{\mathbb{G}}_{\mathrm{m}}$ and $m > 0$. Then any $F[m]$-iterative truncated HS-derivations on a field of positive characteristic can be integrated to an F-iterative HS-derivation.*

For $m = 1$ and $F \cong \widehat{\mathbb{G}}_{\mathrm{a}}$, the result above is [14, Theorem 7]. For $m = 1$ and $F \cong \widehat{\mathbb{G}}_{\mathrm{m}}$, the result above (formulated in terms of restricted Lie algebra actions) is contained in the main theorem of [21] (we were unaware of it while writing the first version of this paper). Similar results in the $m = 1$ case were also obtained in [1] and [2].

In the additive case (corresponding to the usual iterativity) such a generalization is implicit in the work of Ziegler ([23], [24]) and it was crucial to axiomatize the class of *existentially closed* (in the sense of logic, see [8]) iterative HS-fields [24]. The second author also used similar ideas to find *geometric* axioms of this class [12]. Our main motivation for considering this topic was to study other theories of existentially closed fields with HS-derivations, such issues are treated in [9].

Integrating HS-derivations is also related with singularity theory via Matsumura's positive characteristic version of the Zariski-Lipman conjecture (see [14, page 241]), but we do not pursue this direction here.

The paper is organized as follows. In Section 2, we set our notation and introduce iterative HS-derivations, where the iterativity notion comes from a truncated/formal group law. In Section 3, we prove some preparatory results about composing HS-derivations and their fields of constants. In section 4, we prove our theorems about integration of truncated HS-derivations. In Section 5, we comment on the "partial" (i.e. several HS-derivations) case.

We are grateful to the referee for a very useful report.

2. Definitions and Notation

Let us fix a field k and a k-algebra R. For any function $f : R \to R$, $r \in R$ and a positive integer n, $f^n(r) = f(r)^n$ and $f^{(n)}$ is the composition of f with itself n times.

2.1. Formal group laws and HS-derivations.

Definition 2.1. A sequence $\partial = (\partial_n : R \to R)_{n\in\mathbb{N}}$ of additive maps is called an *HS-derivation* if ∂_0 is the identity map, and for all $n \in \mathbb{N}$ and $x, y \in R$,

$$\partial_n(xy) = \sum_{i+j=n} \partial_i(x)\partial_j(y).$$

If moreover for all $n > 0$ and $x \in k$ we have $\partial_n(x) = 0$, then we call ∂ an *HS-derivation over k*.

For any sequence of maps $\partial = (\partial_n : R \to R)_{n\in\mathbb{N}}$ such that ∂_0 is the identity map and a variable X, we define a map

$$\partial_X : R \to R[\![X]\!], \quad \partial_X(r) = \sum_{n=0}^{\infty} \partial_n(r)X^n.$$

It is easy to see [15, p. 207] that ∂ is an HS-derivation if and only if ∂_X is a ring homomorphism and that ∂ is an HS-derivation over k if and only if ∂_X is a k-algebra homomorphism. It is also clear that for a ring homomorphism $\varphi : R \to R[\![X]\!]$, φ is of the form ∂_X for some derivation ∂ if and only if the composition of φ with the natural projection map $R[\![X]\!] \to R$ is the identity map.

Definition 2.2. An HS-derivation ∂ is called *iterative* if for all $i, j \in \mathbb{N}$ we have

$$\partial_i \circ \partial_j = \binom{i+j}{i} \partial_{i+j}.$$

Assume that S is a complete local R-algebra and $s_1, \ldots, s_k$ belong to the maximal ideal of S. There is a unique R-algebra homomorphism $R[\![X_1, \ldots, X_k]\!] \to S$ such that each X_i is mapped to s_i [4, Theorem 7.16]. We denote this homomorphism by $\mathrm{ev}_{(s_1,\ldots,s_k)}$ and for $F \in R[\![X_1, \ldots, X_k]\!]$ we often write $F(s_1, \ldots, s_k)$ instead of $\mathrm{ev}_{(s_1,\ldots,s_k)}(F)$.
It is again easy to see [15, p. 209] that an HS-derivation ∂ is iterative if and only if the following diagram is commutative

$$\begin{array}{ccc} R & \xrightarrow{\partial_Y} & R[\![Y]\!] \\ {\scriptstyle \partial_Z}\downarrow & & \downarrow{\scriptstyle \partial_{X}[\![Y]\!]} \\ R[\![Z]\!] & \xrightarrow{\mathrm{ev}_{X+Y}} & R[\![X,Y]\!]. \end{array}$$

One could replace the power series $X + Y$ in the definition above with an arbitrary power series in two variables. But it turns out that we get a meaningful definition only in the case when $F \in k[\![X, Y]\!]$ is a *formal group law* (over k) i.e. if it satisfies

$$F(X, 0) = X = F(0, X), \quad F(F(X, Y), Z) = F(X, F(Y, Z)).$$

Remark 2.3. The necessity of the first condition is clear. The necessity of the associativity condition comes from the associativity of the composition of functions together with some diagram chasing, similarly as in the proof of Proposition 3.9.

Example 2.4. We give examples of formal group laws.

- The additive formal group law $\widehat{\mathbb{G}}_{\mathrm{a}} = X + Y$.
- The multiplicative formal group law $\widehat{\mathbb{G}}_{\mathrm{m}} = X + Y + XY$.
- More generally, any one-dimensional algebraic group G over k gives (after choosing a local parameter at $1 \in G(k)$) a formal group law called the *formalization* of G (see [13, Section 2.2]) and denoted by $\widehat{G}$.
- For any $n > 0$, there is a formal group law $\bar{F}_{\Delta_n}$ (see [7, 3.2.3]) over $\mathbb{F}_p$. If $n > 2$, then this formal group law does not come from the formalization of an algebraic group.

Let us fix F, a formal group law over k.

Definition 2.5. An HS-derivation ∂ over k is called *F-iterative* if the following diagram is commutative

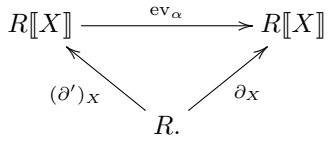
$$\begin{array}{ccc} R & \xrightarrow{\partial_Y} & R[\![Y]\!] \\ {\scriptstyle \partial_Z}\downarrow & & \downarrow{\scriptstyle \partial_{X}[\![Y]\!]} \\ R[\![Z]\!] & \xrightarrow{\mathrm{ev}_F} & R[\![X,Y]\!]. \end{array}$$

We shorten the long phrase "F-iterative HS-derivation over k" to *F-derivation*. For a one-dimensional algebraic group G over k we use the term *G-derivation* rather than $\widehat{G}$-derivation. In particular, a $\mathbb{G}_{\mathrm{a}}$-derivation is the same as an iterative HS-derivation.
If F' is also a formal group law and t is a variable, then $\alpha \in tk[\![t]\!]$ is called a homomorphism between F and F', denoted $\alpha : F \to F'$, if

$$\alpha(F(X,Y)) = F'(\alpha(X), \alpha(Y)).$$

The two statements below connect homomorphisms of formal group laws with iterative derivations. Note that homomorphisms on the formal group level go the *opposite* direction to k-algebra homomorphisms (since the category of complete Hopf algebras is opposite to the category of formal groups, see Section **??**).

Lemma 2.6. *Assume that $\alpha : F \to F'$ is a homomorphism of formal group laws over k and we have the following commutative diagram*



(1) *If ∂' is an F'-derivation, then ∂ is an F-derivation.*
(2) *If ∂ is an F-derivation and ev_α is one-to-one (equivalently, $\alpha \neq 0$), then ∂' is an F'-derivation.*

Proof. This is a relatively easy diagram chase which we leave to the reader. □

Remark 2.7. Assume that $\mathrm{char}(k) = 0$. Then any derivation D on R uniquely expands to a $\mathbb{G}_{\mathrm{a}}$-derivation $(D^{(n)}/n!)_{n\in\mathbb{N}}$. Therefore the theory of derivations coincides with the theory of iterative HS-derivations. Considering other formal group laws does not change this theory either, since by [7, Theorem 1.6.2] each formal group law F over k is isomorphic to $\widehat{\mathbb{G}}_{\mathrm{a}}$, and such an isomorphism gives a bijective correspondence (see Lemma 2.6) between $\mathbb{G}_{\mathrm{a}}$-derivations and F-derivations.

Therefore, from now on we assume that $\mathrm{char}(k) = p > 0$, but sometimes we will make comments regarding the characteristic 0 case.

2.2. **Truncated HS-derivations.** Let us fix a natural number $m > 0$.

Definition 2.8. A sequence $\partial = (\partial_n : R \to R)_{n<p^m}$ of additive maps is called an *m-truncated HS-derivation* if ∂_0 is the identity, and for all $n < p^m$ and $x, y \in R$,

$$\partial_n(xy) = \sum_{i+j=n} \partial_i(x)\partial_j(y).$$

If moreover for all $0 < n < p^m$ and $x \in k$ we have $\partial_n(x) = 0$, then we call ∂ an *m-truncated HS-derivation over k*.

Let v_m, w_m, u_m (or just v, w, u if m is clear from the context) denote the "m-truncated variables" e.g.

$$R[v_m] = R[X]/(X^{p^m}), \quad R[v_m, w_m, u_m] = R[X,Y,Z]/(X^{p^m}, Y^{p^m}, Z^{p^m}).$$

For any sequence of maps $\partial = (\partial_n : R \to R)_{n<p^m}$ such that ∂_0 is the identity map, we define a map

$$\partial_{v_m} : R \to R[v_m], \quad \partial_{v_m}(r) = \sum_{n=0}^{p^m-1} \partial_n(r) v_m^n.$$

It is easy to see again that ∂ is an m-truncated HS-derivation if and only if ∂_{v_m} is a ring homomorphism and that ∂ is an HS-derivation over k if and only if ∂_{v_m} is a k-algebra homomorphism.

Since for all $i, j < p^m$ if $i + j \geqslant p^m$ then $\binom{i+j}{i} = 0$, we can define *iterative m-truncated HS-derivations* exactly as in Definition 2.2.

Remark 2.9. If $\partial = (\partial_i)_{i<p^m}$ is an iterative m-truncated HS-derivation, then ∂_1 is a derivation such that $\partial_1^{(p)} = 0$ (see [15, page 209] or a more general Remark 3.10). Conversely, if D is a derivation such that $D^{(p)} = 0$, then $(D^{(i)}/i!)_{i<p}$ is an iterative 1-truncated HS-derivation. Thus there is a natural bijective correspondence between the set of derivations D such that $D^{(p)} = 0$ and the set of iterative 1-truncated HS-derivations.

The notion of iterativity in the truncated case can be explained again in terms of diagrams. Before this explanation we need some comments about the truncated evaluation maps. If S is any R algebra and $s \in S$ such that $s^{p^m} = 0$, then there is a unique R-algebra map $\mathrm{ev}_s : R[v_m] \to S$ such that $\mathrm{ev}_s(v_m) = s$. Again, for $f \in R[v_m]$ we sometimes write $f(s)$ for $\mathrm{ev}_s(f)$. Similarly in the case of several truncated variables. An m-truncated HS-derivation ∂ is iterative if and only if the following diagram is commutative

$$\begin{array}{ccc} R & \xrightarrow{\partial_w} & R[w] \\ {\scriptstyle \partial_u}\downarrow & & \downarrow{\scriptstyle \partial_v[w]} \\ R[u] & \xrightarrow{\mathrm{ev}_{v+w}} & R[v,w], \end{array}$$

where $v = v_m, w = w_m, u = u_m$ (note that $(v+w)^{p^m} = 0$).

Again, we can replace $v + w$ with any m-truncated polynomial $f \in k[v, w]$, but to get a meaningful definition (see Remark 2.3) we need f to be an *m-truncated group law* i.e. it should satisfy

$$f(v, 0) = v = f(0, v), \quad f(f(v, w), u) = f(v, f(w, u)).$$

Remark 2.10.
(1) Note that the condition $f(v, 0) = v = f(0, v)$ is equivalent to saying that f belongs to the maximal ideal of $k[v, w]$, which in turn is equivalent to the condition $f^{p^m} = 0$. Therefore, for a truncated group law f, the evaluation map ev_f makes sense.
(2) Truncated group laws correspond to *Hopf algebra* (see e.g. [22, Section 1.4]) structures on $k[v]$, where the comultiplication is the map ev_f (for a given truncated group law f). By a theorem of Cartier [22, Section 11.4], a Hopf algebra over a field of characteristic zero is reduced (i.e. has no non-zero nilpotent elements).

(3) There is a classical notion of a *(commutative) one dimensional formal group chunk of order n* (see [7, Def. 5.7.1]), which in our positive characteristic case coincides with the notion of an m-truncated group law for $n = p^m$ and, as in (2) above, a Hopf algebra structure on $k[v]$. However in the case of characteristic 0, these notions differ: there are plenty of formal group chunks, but (see (2) above) no Hopf algebra structures on the ring of the form $k[X]/(X^n)$ for $n > 1$.

Let us fix f, an m-truncated formal group law.

Definition 2.11. An m-iterative HS-derivation ∂ over k is called *f-iterative* if the following diagram is commutative

$$\begin{array}{ccc} R & \xrightarrow{\partial_w} & R[w] \\ {\scriptstyle \partial_u}\downarrow & & \downarrow{\scriptstyle \partial_v[w]} \\ R[u] & \xrightarrow{\mathrm{ev}_f} & R[v,w] \end{array}$$

where $v = v_m, w = w_m, u = u_m$.

We shorten the long phrase "f-iterative m-truncated HS-derivation over k" to *f-derivation*.

Let l be a positive integer and let us also take g, an l-truncated formal group law. We define a homomorphism between truncated group laws f and g, denoted by $\alpha : f \to g$, as an element $\alpha \in k[v_m]$ satisfying

$$\alpha^{p^l} = 0, \quad \alpha(f(v_m, w_m)) = g(\alpha(v_m), \alpha(w_m)).$$

Remark 2.12. Lemma 2.6 remains true if we replace formal group laws by truncated group laws (of course the injectivity is not equivalent anymore to being non-zero).

2.3. **Truncating HS-derivations and Frobenius.** We recall that F is a formal group law over k and $m > 0$. Let us define

$$F[m] := F(v_m, w_m) \in k[v_m, w_m].$$

It is clear that (see also [13, Lemma 1.1]) $F[m]$ is an m-truncated group law.

For any 1-dimensional algebraic group G over k, we use the term "$G[m]$-derivation" rather than "$\widehat{G}[m]$-derivation". In particular, we sometimes say $\mathbb{G}_{\mathrm{a}}[m]$-derivations for iterative m-truncated HS-derivations.

Assume that f is an m-truncated group law and take $1 \leqslant l \leqslant m$. We define

$$f[l] := f(v_l, w_l) \in k[v_l, w_l].$$

Then $f[l]$ is an l-truncated group law. Clearly this construction coincides with the previous one i.e.

$$F[m][l] = F[l].$$

We also have a natural homomorphism $v_l : f[l] \to f$ of truncated group laws. In particular we can understand F as the limit of the direct system of truncated group schemes $(F[l])_{l>0}$ (see [13, Lemma 1.1]).

Remark 2.13. The situation is very different in the characteristic 0 case where a formal group law can not be approximated in a similar fashion (see Remark 2.10(3)).

Let $j := m - l$. Then $v_m^{p^j}$ need *not* be a homomorphism $f \to f[l]$ of truncated group laws unless f is defined over the prime field $\mathbb{F}_p$. For any field automorphism $\varphi : k \to k$ and $g = \sum_{n<p^m} c_n v_m^n \in k[v_m]$, we denote by g^φ the truncated polynomial $\sum_{n<p^m} \varphi(c_n) v_m^n$. Similarly for power series. Let Fr denote the Frobenius automorphism of k. Then g is a truncated group law if and only if g^φ is (similarly for formal group laws). Therefore $f^{\mathrm{Fr}^{-j}}$ is an m-truncated group law and $v_m^{p^j} : f^{\mathrm{Fr}^{-j}} \to f[l]$ (similarly for formal group laws).

3. Algebraic properties of F-derivations

We assume that k is a perfect field of positive characteristic p and R is a k-algebra. We also fix a formal group law F over k, a positive integer m and an m-truncated group law f.

3.1. **Morphisms of group laws and HS-derivations.** As any formal group law over a field is necessarily commutative [7, Theorem 1.6.7], an F-derivation $\partial = (\partial_i)_{i\in\mathbb{N}}$ satisfies $\partial_i \circ \partial_j = \partial_j \circ \partial_i$ for all $i, j \in \mathbb{N}$. We will use this fact often.

Remark 3.1. There are also consequences of the existence of the "inverse map" i.e. a power series W such that $F(X, W(X)) = 0$. There is a group operation on the set of HS-derivations on R over k defined as follows

$$(\partial * \partial')_n = \sum_{i+j=n} \partial_i \circ \partial'_j$$

(see [14, page 208]). For an F-derivation ∂, the inverse of ∂ (with respect to the group operation above) can be expressed in terms of W, e.g. if ∂ is a $\mathbb{G}_{\mathrm{a}}$-derivation, then the inverse of ∂ coincides with $((-1)^n \partial_n)_{n\in\mathbb{N}}$.

Lemma 3.2. *Assume that $0 < l \leqslant m$ and $j = m - l$.*

1. *If ∂ is an F-derivation on R, then $\partial' = (\partial_i)_{i<p^m}$ is an $F[m]$-derivation.*
2. *If ∂ is an f-derivation on R, then $\partial' = (\partial_i)_{i<p^l}$ is an $f[l]$-derivation.*
3. *Assume that ∂ is an F-derivation on R, such that for any $n \in \mathbb{N}$ nondivisible by p^m, we have $\partial_n = 0$. Let $F' = F^{\mathrm{Fr}^m}$ and $\partial' = (\partial_{ip^m})_{i\in\mathbb{N}}$. Then ∂' is an F'-derivation.*
4. *Assume that ∂ is an f-derivation on R, such that for any $n < p^m$ nondivisible by p^j, we have $\partial_n = 0$. Let $f' = f^{\mathrm{Fr}^j}$ and $\partial' = (\partial_{ip^j})_{i<p^l}$. Then ∂' is an $f'[l]$-derivation.*

Proof. The proofs of (1) and (2) are straightforward.
For the proof of (3) consider the following commutative diagram

$$\begin{array}{ccc} R[\![X]\!] & \xrightarrow{\mathrm{ev}_{X^{p^m}}} & R[\![X]\!] \\ & {\scriptstyle (\partial')_X} \nwarrow \quad \nearrow {\scriptstyle \partial_X} & \\ & R. & \end{array}$$

By the last paragraph of Section 2.3, $X^{p^m} : F \to F'$ is a homomorphism of formal group laws and clearly $\mathrm{ev}_{X^{p^m}}$ is one-to-one. By Lemma 2.6, ∂' is an F'-derivation. The proof of (4) is analogous to the proof of (3) (using Remark 2.12), since the homomorphism

$$\mathrm{ev}_{v_m^{p^j}} : k[v_l] \to k[v_m]$$

is injective. □

Remark 3.3. (1) This paper is concerned with the *opposite* operation to the one appearing in Lemma 3.2(1): we take an $F[m]$-derivation and we aim to integrate (i.e. expand) it to an F-derivation.
(2) One may ask whether any m-truncated group law f can be integrated i.e. whether there is a formal group law F such that $F[m] = f$. The answer is positive if and only if f is commutative [7, Corollary 5.7.4] (see [7, Example 5.7.8] for an example of a non-commutative f).
(3) We will see (Corollary 3.17) that the vanishing condition in Lemma 3.2(3) above is equivalent to the vanishing of ∂_{p^i} for $i = 0, \dots, m-1$. Similarly in Lemma 3.2(4).

3.2. **Canonical F-derivation.** One could wonder whether non-zero F-derivations exist at all. The next result provides a canonical example. Let t denote a variable which will play a somewhat different role than the variables X, Y, Z.

Proposition 3.4. *Consider the map*

$$\mathrm{ev}_{F(t,X)} : R[\![t]\!] \to R[\![t, X]\!].$$

There is an F-derivation ∂ on $R[\![t]\!]$ over R such that $\partial_X = \mathrm{ev}_{F(t,X)}$.

Proof. The composition of $\mathrm{ev}_{F(t,X)}$ with the projection map $R[\![t, X]\!] \to R[\![t]\!]$ is exactly the map $\mathrm{ev}_{F(t,0)}$. Since $F(t, 0) = t$, this composition is the identity map. Thus there is an HS-derivation ∂ over R on $R[\![t]\!]$ such that $\partial_X = \mathrm{ev}_{F(t,X)}$. It remains to check the F-iterativity condition, i.e. the commutativity of the following diagram (see Definition 2.5)

$$\begin{array}{ccc} R[\![t]\!] & \xrightarrow{\partial_Y} & R[\![t, Y]\!] \\ {\scriptstyle \partial_X}\downarrow & & \downarrow{\scriptstyle \partial_X[\![Y]\!]} \\ R[\![t, X]\!] & \xrightarrow{\mathrm{ev}_F} & R[\![t, X, Y]\!]. \end{array}$$

Note that ev_F is an $R[\![t]\!]$-algebra map. We will interpret all the maps in the diagram above as evaluation maps on power series R-algebras. We have:

$$\partial_X = \mathrm{ev}_{F(t,X)},\ \partial_Y = \mathrm{ev}_{F(t,Y)},\ \partial_X[\![Y]\!] = \mathrm{ev}_{(F(t,X),Y)},\ \mathrm{ev}_F = \mathrm{ev}_{(t,F(X,Y))}\,.$$

Therefore we obtain

$$\partial_X[\![Y]\!] \circ \partial_Y = \mathrm{ev}_{F(F(t,X),Y)},\quad \mathrm{ev}_F \circ \partial_X = \mathrm{ev}_{F(t,F(X,Y))}\,.$$

Hence the commutativity of the diagram above is equivalent to the associativity axiom for the formal group law F. □

Example 3.5. For $F = \widehat{\mathbb{G}}_{\mathrm{a}} = X + Y$ and ∂ the canonical F-derivation on $k[\![t]\!]$, we see that $\partial_1 = \frac{\mathrm{d}}{\mathrm{d}t}$ is the usual derivative with respect to the variable t and for any $n \in \mathbb{N}$ we have

$$\partial_n\Big(\sum_{i=0}^{\infty} a_i t^i\Big) = \sum_{i=0}^{\infty} a_{i+n}\binom{i+n}{n} t^i.$$

The formula above appears already in [6] (last line on p. 50). It is clear that ∂ restricts to the polynomial ring $k[t]$.

Example 3.6. For $F = \widehat{\mathbb{G}}_{\mathrm{m}} = X + Y + XY$ and ∂ the canonical F-derivation on $k[\![t]\!]$, one can compute (similarly as in Example 3.15) that

$$\partial_n\Big(\sum_{i=0}^{\infty} a_i t^i\Big) = \sum_{m=0}^{\infty} \sum_{j=0}^{\min(m,n)} \frac{(m+n-j)!}{(m-j)!(n-j)!j!} a_{m+n-j} t^m.$$

Clearly, this HS-derivation restricts to the polynomial ring $k[t]$ as well.

3.3. **Composing HS-derivations.** In this subsection we describe a passage from the diagram describing F-iterativity (Definition 2.5) to formulas for the actual composition of terms of an F-derivation. The p-th compositional power will play a special role.

Let $\partial = (\partial_0, \partial_1, \ldots)$ be an HS-derivation on R. Till Proposition 3.9, we do not assume that ∂ obeys any iterativity law, although we still assume that the maps ∂_i, ∂_j commute with each other (see the beginning of Section 3.1). For each $i \geqslant 1$, let

$$E_i : R[\![X_1, \ldots, X_{i-1}]\!] \to R[\![X_1, \ldots, X_i]\!], \quad E_i = \partial_{X_i}[\![X_1, \ldots, X_{i-1}]\!].$$

In particular $E_1 = \partial_{X_1}$. For any $m \geqslant 1$, let $E_{(m)}$ denote the composition of the maps below:

$$R \xrightarrow{E_1} R[\![X_1]\!] \xrightarrow{E_2} R[\![X_1, X_2]\!] \xrightarrow{E_3} \ldots \xrightarrow{E_m} R[\![X_1, \ldots, X_m]\!] \xrightarrow{\mathrm{ev}_{(X,\ldots,X)}} R[\![X]\!].$$

Then the map $E_{(m)} : R \to R[\![X]\!]$ coincides with $(\partial^{*m})_X$, where $\partial^{*m} = \partial * \ldots * \partial$ (m times) for the group operation $*$ on the set of HS-derivations on R from Remark 3.1.

Lemma 3.7. *For any $r \in R$ we have:*

$$E_{(p)}(r) = \sum_{i=0}^{\infty} \partial_i^{(p)}(r) X^{pi}.$$

Proof. We have

$$E_{(p)}(r) = \sum_{n=0}^{\infty} \sum_{i_1+\ldots+i_p=n} (\partial_{i_1} \circ \ldots \circ \partial_{i_p})(r) X^i.$$

Since all the maps ∂_i commute with each other, the lemma follows from the fact that the number of different permutations of the sequence $(i_1, \ldots, i_p)$ is one if $i_1 = \ldots = i_p$ and divisible by p otherwise. □

Corollary 3.8. *Under the assumptions above, $\partial^{(p)} := (\partial_i^{(p)})_i$ is an HS-derivation.*

Proof. Let $\iota : R[\![X^p]\!] \to R[\![X]\!]$ denote the inclusion map. By Lemma 3.7, we have

$$\iota \circ (\partial^{(p)})_{X^p} = E_{(p)}.$$

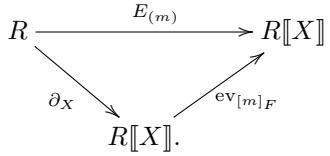
Since $E_{(p)}$ is a ring homomorphism, $(\partial^{(p)})_{X^p}$ is a ring homomorphism as well, so $\partial^{(p)}$ is an HS-derivation. □

For an F-derivation ∂, we aim to express $\partial^{(p)}$ in terms of F and ∂. For any positive integer m, let

$$[m+1]_F(X) = F(X, [m]_F(X))$$

be the "multiplication by m map" ($[1]_F = X$).

Proposition 3.9. *If ∂ is an F-derivation, then the following diagram commutes:*



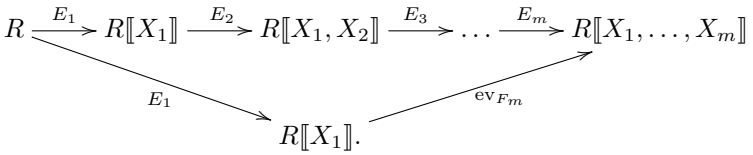
Proof. Let F_2 denote $F(X_1, X_2)$ and for $m \geqslant 2$ let

$$F_{m+1} = F_m(X_1, \ldots, X_{m-1}, F(X_m, X_{m+1})).$$

By the definitions of $E_{(m)}$ and $[m]_F$, it is enough to prove the following.

Claim

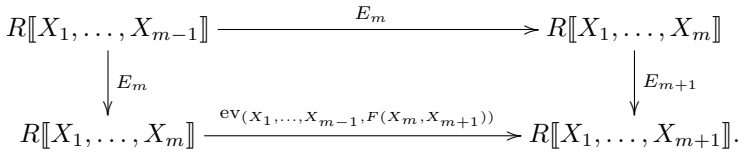
For each $m \geqslant 2$, the following diagram is commutative



Proof of Claim. Induction on m. For $m = 2$ the diagram above is the F-iterativity diagram (Definition 2.5). Assume that $m \geqslant 2$ and that the diagram above is commutative. Since

$$\mathrm{ev}_{(X_1,\ldots,X_{m-1},F(X_m,X_{m+1}))} \circ \mathrm{ev}_{F_m} = \mathrm{ev}_{F_{m+1}},$$

the commutativity of the corresponding diagram for $m + 1$ follows from the commutativity of the following diagram



The commutativity of this last diagram diagram follows from the application of the functor

$$S \mapsto S[\![X_1, \ldots, X_{m-1}]\!]$$

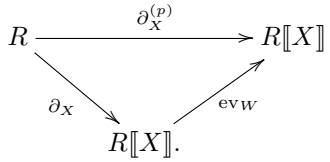
to the F-iterativity diagram after setting $X = X_{m+1}$ and $Y = Z = X_m$. □

Remark 3.10.

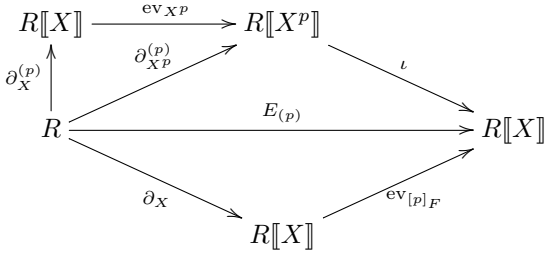
(1) Note that for a $\mathbb{G}_{\mathrm{a}}$-derivation ∂, Proposition 3.9 immediately implies that $\partial^{(p)} = (\mathrm{id}, 0, 0, \ldots)$.

(2) If ∂' is an HS-derivation such that $(\partial')_X = E_{(m)}$, then by Remark 2.12 and Proposition 3.9, ∂' is F-iterative as well (since $[m]_F$ is an endomorphism of the formal group law F).

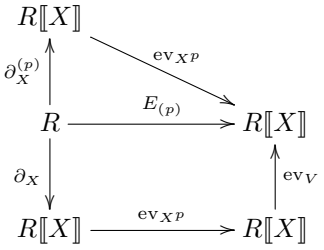
Proposition 3.11. *If ∂ is an F-derivation, then there is $W \in Xk[\![X]\!]$ such that the following diagram commutes*



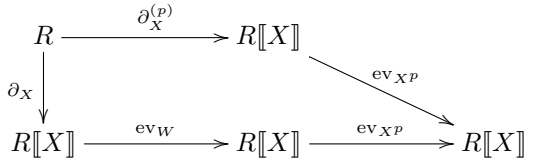
Proof. From the displayed formula in the proof of Corollary 3.8 and from Proposition 3.9 we get the following commutative diagram.



By [20, Example IV.7.1] (or Proposition on page 29 of [3]), there is $V \in Xk[\![X]\!]$ such that $[p]_F(X) = V(X^p)$. Thus we have the second commutative diagram (understanding now ev_{X^p} as a function from $R[\![X]\!]$ to itself).



We define the power series W as $V^{\mathrm{Fr}^{-1}}$. We clearly have $V(X^p) = W^p$ and we get the third commutative diagram.



Since ev_{X^p} is a monomorphism, the result follows. □

Remark 3.12.

(1) The power series W from the statement of Proposition 3.11 coincides with $(V_F)^{\mathrm{Fr}^{-1}}$, where V_F is the power series corresponding to the *Verschiebung morphism* (see e.g. page 28 of [3]).
(2) Note that for $F = X_1 + X_2 + X_1X_2$, the proposition above immediately implies that $\partial^{(p)} = \partial$, since in this case $W = V = X$ (it also follows from the description of the restricted Lie algebra action in [21, page 129]).
(3) For (additively) iterative HS-derivations if $i, j < p^m$ and $i + j \geqslant p^m$ then $\partial_i \circ \partial_j = 0$. It is not true for other types of iterativity, e.g. $\partial_1 \circ \partial_1 = \partial_1$ for $p = 2$ and a multiplicatively iterative HS-derivation $\partial = (\partial_i)_{i\in\mathbb{N}}$.
(4) Proposition 3.11 remains true if we replace F-derivations with f-derivations for an m-truncated group law f, just by replacing the ring $R[\![X]\!]$ with $R[X]/(X^{p^m})$ and using [13, Proposition 1.4] instead of [20, Example IV.7.1].

Let us fix $q = p^m$. If $\partial = (\partial)_{i<q}$ is an f-derivation, then in general it is difficult to give formulas for $\partial_j \circ \partial_i$. We show below that the general f-iterativity rule resembles the standard (additive) one up to the lower order terms.

Lemma 3.13. *Let ∂ be an f-derivation on R. For every positive integers i, j such that $i + j < q$ we have*

$$\partial_j \circ \partial_i = \binom{i+j}{i} \partial_{i+j} + \mathcal{O}(\partial_{<i+j}),$$

where $\mathcal{O}(\partial_{<i+j})$ is a k-linear combination of the maps $\partial_1, \ldots, \partial_{i+j-1}$.

Proof. It follows from the f-iterativity diagram (Definition 2.11) that for any $r \in R$ we have:

$$\sum_{i,j<q} \partial_j(\partial_i(r)) v^i w^j = \sum_{n<q} \partial_n(r) f(v,w)^n.$$

Since f is a truncated group law, $f = v + w + s$ for some $s \in k[v, w]$ divisible by vw. Therefore we get

$$\partial_j(\partial_i(x)) = \binom{i+j}{i} \partial_{i+j}(x) + \mathcal{O}(\partial_{<i+j})(x)$$

proving the required equality. □

Remark 3.14.

(1) Since for a formal group law F, $F[m]$ is an m-truncated group law, the above lemma is also true for F-derivations (with no restrictions for i, j).

(2) Let ∂ be an f-derivation on R. Using Lemma 3.13, we can find $\alpha \in k$ such that

$$\partial_1 \circ \partial_1 = \partial_2 + \alpha \partial_1.$$

For each $0 < n < p - 1$, we inductively obtain that ∂_n is a k-linear combination of non-zero compositional powers of ∂_1. Therefore we have

$$\ker(\partial_1) = \ker(\partial_1) \cap \ldots \cap \ker(\partial_{p-1}).$$

Example 3.15. Assume that ∂ is a $\mathbb{G}_{\mathrm{m}}$-derivation and $k, l \in \mathbb{N}$. For any $r \in R$ we have

$$\begin{aligned}
\sum_{i,j} \partial_j(\partial_i(r)) X^i Y^j &= \sum_n \partial_n(r)(X + Y + XY)^n \\
&= \sum_n \partial_n(r) \sum_{a+b \leqslant n} \frac{n!}{a!b!(n-a-b)!} X^a Y^b (XY)^{n-a-b} \\
&= \sum_{i,j} \left(\sum_{l=0}^{\min(i,j)} \frac{(i+j-l)!}{(j-l)!l!(i-l)!} \partial_{i+j-l}(r) \right) X^i Y^j.
\end{aligned}$$

Therefore we get the following multiplicative iterativity rule

$$\partial_j \circ \partial_i = \sum_{n=\max(i,j)}^{i+j} \frac{n!}{(n-i)!(n-j)!(i+j-n)!} \partial_n,$$

which recovers the formula from [1, Def. 11].

The following lemma will help to find "canonical elements" for certain HS-derivations.

Lemma 3.16. *Let ∂, ∂' be f-iterative derivations on R. If for every $k < m$ we have $\partial_{p^k} = \partial'_{p^k}$, then for any $n < q$ we have $\partial_n = \partial'_n$.*

Proof. Induction on n. Take $n < q$ and assume that for all $k < n$ we have $\partial_k = \partial'_k$. Let $k < m$ be biggest such that $p^k \leqslant n$. By the assumption we can assume that $n = p^k + l$ for some positive integer l. Then p does not divide $\binom{n}{l}$. Take any $r \in R$, by Lemma 3.13, we have

$$\partial_{p^k}(\partial_l(r)) = \binom{n}{l}\partial_n(r) + \mathcal{O}(\partial_{<n})(r),$$

$$\partial'_{p^k}(\partial'_l(r)) = \binom{n}{l}\partial'_n(r) + \mathcal{O}(\partial'_{<n})(r).$$

By the induction assumption we get $\partial_n(r) = \partial'_n(r)$. □

Corollary 3.17. *Let ∂ be an f-iterative derivation on R and $r \in R$. If for every $k < m$ we have $\partial_{p^k}(r) = 0$, then for any $n < q$ we have $\partial_n(r) = 0$.*

Remark 3.18.
(1) Similarly as before, the appropriate versions of 3.16 and 3.17 for F-derivations are also true.
(2) Similar formulas to the ones appearing in the proof of Lemma 3.16 (in the case of the additive iterativity rule) can be found at the top of page 175 of [18].

3.4. **Fields of constants.** In this subsection we generalize a result of Matsumura [15, Theorem 27.3] saying that the field of constants C of a non-zero derivation ∂ on a field K such that $\partial^{(p)} = 0$ is largest possible i.e. $[K : C] = p$. If ∂ is a truncated HS-derivation or an HS-derivation, then we define its *field of constants* as the intersection of $\ker(\partial_i)$ for all $i \neq 0$. By Remark 2.9, having a derivation ∂ such that $\partial^{(p)} = 0$ is equivalent to having a $\mathbb{G}_{\mathrm{a}}[1]$-derivation $(\partial_i)_{i<p}$ and by Remark 3.14(2), both fields of constants coincide. In Proposition 3.24, we generalize Matsumura's result from $\mathbb{G}_{\mathrm{a}}[1]$-derivations to f-derivations, where f is an arbitrary truncated group law. Such a generalization will be necessary for integrating truncated HS-derivations.

We will need a slight generalization of a result from [15] (recall that $q = p^m$).

Lemma 3.19. *Let ∂ be a non-zero derivation on a field K of characteristic p. Then the functions $\mathrm{id}_K^q, \partial^q, \ldots, (\partial^{(p-1)})^q$ are linearly independent over K.*

Proof. The case of $m = 0$ is exactly [15, Theorem 25.4]. For the general case it is enough to notice that the K-linear independence of $\mathrm{id}_K, \partial, \ldots, \partial^{(p-1)}$ implies the $K^{q^{-1}}$-linear independence of $\iota, \iota \circ \partial, \ldots, \iota \circ \partial^{(p-1)}$, where $\iota : K \to K^{q^{-1}}$ is the inclusion map. Applying the m-th power of the Frobenius map we get the independence of $\mathrm{id}_K^q, \partial^q, \ldots, (\partial^{(p-1)})^q$ over K. □

The result below is a multiplicative version of a part of [15, Theorem 27.3(ii)].

Lemma 3.20. *Let ∂ be a non-zero derivation on a field K such that $\partial^{(p)} = \partial$. Then there is a non-zero $x \in K$ such that $\partial(x) = x$.*

Proof. We argue by contradiction. Suppose that $\partial(x) \neq x$ for all non-zero $x \in K$. It means that the map $\partial - \mathrm{id}_K$ is one-to-one. Notice that

$$(\partial - \mathrm{id}_K) \circ (\mathrm{id}_K + \partial + \partial^{(2)} + \ldots + \partial^{(p-1)}) = \partial^{(p)} - \mathrm{id}_K = \partial - \mathrm{id}_K .$$

From the injectivity of $\partial - \mathrm{id}_K$, we obtain

$$\mathrm{id}_K + \partial + \partial^{(2)} + \ldots + \partial^{(p-1)} = \mathrm{id}_K,$$

which contradicts [15, Theorem 25.4] (see Lemma 3.19 above for $q = 1$). □

Remark 3.21. Such an element x is also given by [21, Lemma 3.5(3)].

Before the next result, we need a very general lemma, which is not particularly related to derivations.

Lemma 3.22. *Let $\partial : R \to R$ be a function.*

(1) *We have*
$$\partial^{(p-1)} + \sum_{l=1}^{p-1}\sum_{i=1}^{p-1} l^{p-1-i}\partial^{(i)} = 0.$$

(2) *Let $l \in \mathbb{N}$ and assume that ∂ is additive and $\partial^{(p)} = \partial$. Then*
$$\partial\Big(\sum_{i=1}^{p-1} l^{p-1-i}\partial^{(i)}\Big) = l\Big(\sum_{i=1}^{p-1} l^{p-1-i}\partial^{(i)}\Big).$$

Proof. Note that for any $\alpha \in \mathbb{F}_p$, since $\alpha^p = \alpha$, we get

$$(*) \qquad \sum_{r=1}^{p-1} \alpha^r = \alpha(\sum_{r=1}^{p-1} \alpha^r).$$

Let ξ be a generator of $\mathbb{F}_p^*$ and $i \in \{1, \dots, p-2\}$. Then we have

$$(**) \qquad \sum_{l=1}^{p-1} l^i = \sum_{r=1}^{p-1} (\xi^r)^i = \sum_{r=1}^{p-1} (\xi^i)^r = 0,$$

where the last equality follows from $(*)$ (for $\alpha = \xi^i$), since $\xi^i \neq 1$.
Using $(**)$ we get

$$\begin{aligned}\partial^{(p-1)} + \sum_{l=1}^{p-1}\sum_{i=1}^{p-1} l^{p-1-i}\partial^{(i)} &= \partial^{(p-1)} + \sum_{i=1}^{p-1}(\sum_{l=1}^{p-1} l^{p-1-i})\partial^{(i)} \\ &= \partial^{(p-1)} + \sum_{l=1}^{p-1} l^0\partial^{(p-1)} \\ &= 0.\end{aligned}$$

The proof of (2) is an easy computation which is similar to the one needed to obtain the equality $(*)$ above. □

We prove now the main result of this subsection. Recall that f is a fixed m-truncated group law.

Proposition 3.23. *Let K be a field and ∂ be an f-derivation on K such that ∂_1 is non-zero. Let C be the constant field of ∂. Then $[K : C] = p^m$.*

Proof. First we show inductively that without loss of generality we can assume that $m = 1$. Assume that $m > 1$ and let $C' = \ker(\partial_1)$. By Lemma 3.2(4) and Corollary 3.17, $\partial' = (\partial_{pi}|_{C'})_{i<p^{m-1}}$ is an $f'[m-1]$-derivation on C', where $f' = f^{\mathrm{Fr}}$.
By Lemma 3.13 and Corollary 3.17, the constant field of ∂' coincides with C, so we are done by the inductive assumption and by the $m = 1$ case. Assume that $m = 1$. By Remark 3.14(2), we have $C = \ker(\partial_1)$. By Remark 3.12(4), there is $t \in vk[v]$ such that
$$\partial_v^{(p)} = \mathrm{ev}_t \circ \partial_v.$$

Hence we have $\partial_1^{(p)} = c\partial_1$ for $c \in k$ such that $t - cv \in v^2 k[v]$ (i.e. $t = cv + \ldots$). The case $\partial_1^{(p)} = 0$ is treated in [15, Theorem 27.3], so we can assume that $c \neq 0$. We assume first that $c = 1$ (which corresponds to the multiplicative case) and will treat the general case at the end of the proof.
Let us take an arbitrary $a \in K$ and let $x \in K \setminus \{0\}$ be such that $\partial(x) = x$ (see Lemma 3.21). By Lemma 3.23(2), we have

$$a = a - \partial^{(p-1)}(a) - \sum_{k=1}^{p-1} \frac{\alpha_k}{x^k} x^k,$$

where $\alpha_k = \sum_{i=1}^{p-1} k^{p-1-i} \partial^{(i)}(a)$. By Lemma 3.23(1), we have $\partial(\alpha_k) = k\alpha_k$. Since $\partial(x) = x$, it is easy to see that

$$\partial\left(\frac{\alpha_k}{x^k}\right) = 0.$$

Therefore K is spanned over C by $\{1, x, \ldots, x^{p-1}\}$, so $[K : C] = p$.
Let us come back now to the general case when $\partial_1^{(p)} = c\partial_1$ for an arbitrary $c \in k \setminus \{0\}$. Note that for any $d \in C$ and $\partial_d := d\partial$ we have

$$\partial_d^{(p)} = d^p \partial^{(p)} = d^p c\partial = d^{p-1} c\partial_d.$$

(The first equality is easy to see, it is also a special case of the Hochschild formula, see [15, Theorem 25.5].) If $d \neq 0$, then the constants of ∂_d coincide with the constants of ∂, so we can replace ∂ with ∂_d. Therefore we are done if there is $d \in C$ such that $d^{p-1} = c^{-1}$. Let K' denote the separable closure of K. The derivation ∂ uniquely extends to a derivation ∂' on K'. Let C' denote the field of constants of ∂'. From the uniqueness of extensions of derivations, we get $(\partial')^{(p)} = c\partial'$. Clearly, there is $d \in K'$ such that $d^{p-1} = c^{-1}$. Therefore $[K' : C'] = p$. Since C' is linearly disjoint from K over C (see [11, Corollary 1 p. 87]), we get $[K : C] = p$. □

4. Expanding HS-derivations

In this section we generalize the result of Matsumura [14, Theorem 7] about strong integrability of certain derivations. Throughout this section $k \subseteq M \subseteq K$ is a tower of fields such that k is perfect (of characteristic $p > 0$) and the extension $M \subseteq K$ is separable (not necessarily algebraic). We fix $m > 0$ and set $q := p^m$.

Our generalization is two-fold:

(1) From an M-derivation D on K such that $D^{(p)} = 0$ (equivalent to a $\mathbb{G}_{\mathrm{a}}[1]$-derivation, see Remark 2.9) to any $\mathbb{G}_{\mathrm{a}}[m]$-derivation (Theorem 4.7).
(2) Analogue of (1) for $\mathbb{G}_{\mathrm{m}}[m]$-derivations (Theorem 4.11).

It should be mentioned that Proposition 4.5, which is the main technical point needed for (1) above, was essentially obtained by Ziegler in [23, Theorem 1].

It is natural to ask whether similar results can be obtained for any formal group law.

Question 4.1. Let F be a formal group law over k and ∂ be an $F[m]$-derivation on K. Does ∂ expand to an F-derivation?

Unfortunately, we do not know the answer to this question. In [10], we give some evidence why the answer may be negative.

For the notion of a p-basis of an extension of fields of characteristic $p > 0$, the reader may consult [15, p. 202]. The proof of [15, Theorem 27.3(ii)] gives the following.

Lemma 4.2. *Let $M \subseteq L \subseteq K$ be a tower of fields ($M \subseteq K$ separable), $[K : L] = p$, $L \subseteq K$ is purely inseparable and $a \in K \setminus L$. Then we have:*

1. *There is $B_0 \subseteq L$ such that $B_0 \cup \{a^p\}$ is a p-basis of L over M.*
2. *For any $B_0 \subseteq L$ such that $B_0 \cup \{a^p\}$ is a p-basis of L over M, the set $B_0 \cup \{a\}$ is a p-basis of K over M.*

We will need a generalization of the second part of the lemma above.

Lemma 4.3. *Let $m \in \mathbb{N}$ and $M \subseteq K_{m-1} \subseteq \ldots K_0 \subseteq K$ be a tower of fields ($M \subseteq K$ separable) such that $K_{m-1} \subseteq K$ is purely inseparable and*

$$[K : K_0] = [K_0 : K_1] = \ldots = [K_{m-2} : K_{m-1}] = p.$$

Let $x \in K$ be such that for all $i \in \{0, \ldots, m-1\}$, we have $x^{p^i} \notin K_i$. Then there is $B_0 \subseteq K_{m-1}$ such that $B_0 \cup \{x\}$ is a p-basis of K over M.

Proof. Clearly, for all $i \in \{0, \ldots, m-1\}$, the extension $M \subseteq K_i$ is separable. Using Lemma 4.2(1) for $a = x^{p^{m-1}}$ and $M \subseteq K_{m-1} \subseteq K_{m-2}$, we get $B_0 \subseteq K_{m-1}$ such that $B_0 \cup \{x^{p^m}\}$ is a p-basis of K over M. Using Lemma 4.2(2) and the downward induction on i, we get that $B_0 \cup \{x\}$ is a p-basis of K over M. □

For the remainder of this section we consider only the additive and the multiplicative laws, so we can assume that k is the prime field $\mathbb{F}_p$.

4.1. **Additive case.** We will need one fact about derivations.

Lemma 4.4. *Assume that ∂ is a non-zero derivation on K such that $\partial^{(p)} = 0$. Then*

$$\operatorname{im}(\partial) = \ker(\partial^{(p-1)}).$$

Proof. Let $C = \ker(\partial)$. By [15, Theorem 27.3], (see also Proposition 3.24) $[K : C] = p$. Clearly $\operatorname{im}(\partial) \subseteq \ker(\partial^{(p-1)})$. It is enough to show that

$$\dim_C \operatorname{im}(\partial) \geqslant \dim_C \ker(\partial^{(p-1)}).$$

By [15, Theorem 25.4] (see also Lemma 3.19), $\partial^{(p-1)} \neq 0$, so $\dim_C \ker(\partial^{(p-1)}) \leqslant p - 1$.
By [15, Theorem 27.3(ii)], there is $x \in K$ such that $\partial(x) = 1$ (namely, $x = \partial^{(i-1)}(z)/\partial^{(i)}(z)$ for $z \in K \setminus C$ and $i > 0$ such that $\partial^{(i)}(z) \neq 0$ and $\partial^{(i+1)}(z) = 0$). Therefore, $\partial(x^n) = nx^{n-1}$ for $n = 0, \ldots, p-1$ and $1, x, x^2, \ldots, x^{p-2}$ are linearly independent over C. Hence $\dim_C(\operatorname{im}(\partial)) \geqslant p - 1$. □

We show now that any $\mathbb{G}_{\mathrm{a}}[m]$-derivation has something in common with the canonical one.

Proposition 4.5. *Let ∂ be a $\mathbb{G}_{\mathrm{a}}[m]$-derivation on K such that ∂_1 is non-zero. Then there is $x \in K$ such that*

$$\partial_1(x) = 1, \quad \partial_2(x) = 0, \quad \ldots, \quad \partial_{q-1}(x) = 0.$$

Proof. Induction on m. The case of $m = 1$ is [15, Theorem 27.3(ii)]. Assume that the proposition is true for m and take a $\mathbb{G}_{\mathrm{a}}[m+1]$-derivation ∂ on K over k such that ∂_1 is non-zero. Let $\partial' = (\partial_i)_{i<p^m}$. By Lemma 3.2(2), ∂' is a $\mathbb{G}_{\mathrm{a}}[m]$-derivation. By the inductive assumption, there is $x \in K$ such that

$$(*) \qquad \partial_1(x) = 1, \quad \partial_2(x) = 0, \ \dots \ , \partial_{p^m-1}(x) = 0.$$

Let C be the field of constants of ∂ and C' the field of constants of ∂'. By higher Leibniz rules, ∂_{p^m} is a C-derivation on C'. It is easy to see that ∂_{p^m} is non-zero on C', since $x^{p^m} \in C'$ and

$$\partial_{p^m}(x^{p^m}) = \partial_1(x)^{p^m} \neq 0.$$

By Remark 3.10(1), $\partial_{p^m}^{(p)} = 0$, so by Lemma 4.4 we have

$$(**) \qquad \partial_{p^m}(C') = \ker(\partial_{p^m}^{(p-1)}) \cap C'.$$

Since $\partial_{p^m}^{(p)} = 0$, we have $\partial_{p^m}(x) \in \ker(\partial_{p^m}^{(p-1)})$. Since ∂_{p^m} commutes with $\partial_1, \ \dots \ , \partial_{p^{m-1}}$, we get by $(*)$ that $\partial_{p^m}(x) \in C'$. By $(**)$, there is $y \in C'$ such that

$$\partial_{p^m}(y) = \partial_{p^m}(x).$$

Let $z := y - x$. It is clear that

$$\partial_1(z) = 1, \quad \partial_2(z) = 0, \ \dots \ , \partial_{p^m}(z) = 0.$$

By the iterativity rule, for any $i < (p-1)p^m$ we also have $\partial_{p^m+i}(z) = 0$. □

We will call an element $x \in K$ satisfying the conclusion of Proposition 4.5, a *canonical* element for a $\mathbb{G}_{\mathrm{a}}[m]$-derivation ∂.

Remark 4.6. Ziegler in [23] and [24] defines the notion of a *canonical p-basis* which in our "ordinary" (i.e. one HS-derivation) case reduces to the notion of a canonical element. For the sake of clarity we restrain ourselves from considering the case of several HS-derivations, see Section 5.

We can prove now our additive integrability theorem. This theorem is implicit in work of Ziegler, see [23] and [24]. Let us recall that $M \subseteq K$ is a separable (not necessarily algebraic) extension of fields.

Theorem 4.7. *Let $\partial = (\partial_i)_{i<p^m}$ be a $\mathbb{G}_{\mathrm{a}}[m]$-derivation on K over M. Then ∂ can be expanded to a $\mathbb{G}_{\mathrm{a}}$-derivation on K over M.*

Proof. Let us assume first that ∂_1 is non-zero. The proof in this case is similar to the proof of [14, Theorem 7]. Take a canonical element $x \in K$ from Proposition 4.5. For $i \in \{0, \dots, m-1\}$ let us define

$$K_i := \bigcap_{j<p^{i+1}} \ker(\partial_i).$$

By Proposition 3.24, for each $i \in \{0, \dots, m-1\}$, we have $[K : K_i] = p^{i+1}$ and

$$\partial_{p^i}(x^{p^i}) = \partial_1(x)^{p^i} = 1 \neq 0,$$

so $x^{p^i} \notin K_i$. Hence $M, K_{m-1}, \dots, K_0, K, x$ satisfy the assumptions of Lemma 4.3, therefore there is $B_0 \subset K_{m-1}$ such that $B := B_0 \cup \{x\}$ is a p-basis of K over M. By [15, Theorem 26.8] x is transcendental over $M(B_0)$, so we can define a canonical $\mathbb{G}_{\mathrm{a}}$-derivation on $M(B)$ over $M(B_0)$ (see Example 3.5). By [15, Theorem 26.8] again, $M(B) \subseteq K$ is étale, so by [15, Theorem 27.2] our canonical $\mathbb{G}_{\mathrm{a}}$-derivations

uniquely extends to a $\mathbb{G}_{\mathrm{a}}$-derivation D on K over M. Since for any $i < q$, ∂_i coincides with D_i on B (therefore on $M(B)$ as well), it is easy to see that they coincide on K.

Let us now consider the case $\partial_1 = 0$. Obviously, we can assume that ∂_i is non-zero for some $0 < i < p^m$. By Lemma 3.13 and Corollary 3.17, there is $j < m$ such that $\partial_1 = \ldots = \partial_{p^j-1} = 0$ but ∂_{p^j} is non-zero. Let $l := m - j$ and $\partial' = (\partial_{ip^j})_{i<p^l}$. By Lemma 3.2(4), ∂' is a $\mathbb{G}_{\mathrm{a}}[l]$-derivation (since $(X+Y)^{\mathrm{Fr}^{-j}}$ clearly coincides with $X+Y$). Since ∂'_1 is non-zero, by the first part of the proof ∂' expands to a $\mathbb{G}_{\mathrm{a}}$-derivation $D' = (D'_i)_{i\in\mathbb{N}}$. Define $D = (D_i)_{i\in\mathbb{N}}$, where $D_i = D'_{i/p^j}$ for i divisible by p^j and $D_i = 0$ otherwise. Using the map

$$\mathrm{ev}_{X^{p^l}} : K[\![X]\!] \to K[\![X]\!],$$

which gives a morphism from $\mathbb{G}_{\mathrm{a}}$ to $\mathbb{G}_{\mathrm{a}}$ and Lemma 2.6, we see that D is a $\mathbb{G}_{\mathrm{a}}$-derivation. By the construction, D expands ∂. □

4.2. **Multiplicative case.** In this subsection we prove an analogue of Theorem 4.7 for multiplicatively iterative derivations. The general scheme of the proof is the same as in the additive case: the main point is to find a canonical element (in the appropriate, multiplicative sense) for a truncated multiplicatively iterative HS-derivation, this is done in Proposition 4.10.

The lemma below does not require any iterativity assumption.

Lemma 4.8. *Let ∂ be an m-truncated HS-derivation on a ring R. For any $i < m$, $j \in \mathbb{N}$, $x \in R$ and $y \in R$ we have*

$$(*) \qquad \partial^{(j)}_{p^i}(xy^{p^i}) = \sum_{l=0}^{j} \binom{j}{l} \partial^{(j-l)}_{p^i}(x) \cdot \partial^{(l)}_1(y)^{p^i}.$$

Proof. We prove $(*)$ by induction on j. The case of $j = 0$ is clear. Let us assume that $(*)$ above holds. Then we have

$$\begin{aligned}
\partial^{(j+1)}_{p^i}(xy^{p^i}) &= \sum_{l=0}^{j} \binom{j}{l} \partial_{p^i}\Big(\partial^{(j-l)}_{p^i}(x) \cdot \partial^{(l)}_1(y)^{p^i}\Big) \\
&= \sum_{l=0}^{j} \binom{j}{l} \Big(\partial_{p^i}(\partial^{(j-l)}_{p^i}(x)) \cdot \partial^{(l)}_1(y)^{p^i} + \partial^{(j-l)}_{p^i}(x) \cdot \partial_{p^i}(\partial^{(l)}_1(y)^{p^i})\Big) \\
&= \sum_{l=0}^{j} \binom{j}{l} \Big(\partial^{(j+1-l)}_{p^i}(x) \cdot \partial^{(l)}_1(y)^{p^i} + \partial^{(j-l)}_{p^i}(x) \cdot \partial^{(l+1)}_1(y)^{p^i}\Big) \\
&= \sum_{l=0}^{j+1} \binom{j+1}{l} \partial^{(j+1-l)}_{p^i}(x) \cdot \partial^{(l)}_1(y)^{p^i},
\end{aligned}$$

where the second equality holds, since for every $0 < s < p^i$ and $a \in R$ we have $\partial_s(a^{p^i}) = 0$. □

Lemma 4.9. *Let ∂ be a $\mathbb{G}_{\mathrm{m}}[m]$-derivation on a ring R and $i \in \{0, \ldots, m-2\}$. Assume that $x \in R$ satisfies*

$$\partial_1(x) = x, \quad \partial_p(x) = 0, \ \ldots \ , \partial_{p^i}(x) = 0.$$

Take any $y \in R$ and let $x' := y^{p^{i+1}}x - \partial^{(p-1)}_{p^{i+1}}(y^{p^{i+1}}x)$. Then we have:

$$\partial_1(x') = x', \quad \partial_p(x') = 0, \ \dots \ , \partial_{p^{i+1}}(x') = 0.$$

Proof. We compute

$$\begin{aligned}\partial_1(x') &= y^{p^{i+1}}\partial_1(x) - \partial^{(p-1)}_{p^{i+1}}(y^{p^{i+1}}\partial_1(x)) \\ &= y^{p^{i+1}}x - \partial^{(p-1)}_{p^{i+1}}(y^{p^{i+1}}x) \\ &= x';\end{aligned}$$

$$\partial_{p^{i+1}}(x') = \partial_{p^{i+1}}(y^{p^{i+1}}x) - \partial^{(p)}_{p^{i+1}}(y^{p^{i+1}}x) = 0.$$

Take any $j \in \{1, \dots, i\}$. We have

$$(*) \qquad \partial_{p^j}(x') = \partial_{p^j}(y^{p^{i+1}}x) - \partial_{p^j}(\partial^{(p-1)}_{p^{i+1}}(y^{p^{i+1}}x)).$$

By the choice of j we have $\partial_{p^j}(y^{p^{i+1}}) = 0$ and $\partial_{p^j}(x) = 0$, hence the first term in $(*)$ vanishes. The second one vanishes for the same reason, since ∂_{p^j} commutes with $\partial_{p^{i+1}}$. □

We show below that canonical elements for $\mathbb{G}_{\mathrm{m}}[m]$-derivations exist as well.

Proposition 4.10. *Assume that ∂ is a $\mathbb{G}_{\mathrm{m}}[m]$-derivation such that ∂_1 is non-zero. Then there is $x \in K$ such that*

$$\partial_1(x) = x + 1 \neq 0, \quad \partial_2(x) = 0, \ \dots \ , \partial_{q-1}(x) = 0.$$

Proof. First, we inductively construct a sequence $x_0, \dots, x_{m-1} \in K \setminus \{0\}$ such that for all $i \in \{0, \dots, m-1\}$ we have

$$(*_i) \qquad \partial_1(x_i) = x_i, \quad \partial_p(x_i) = 0, \ \dots \ , \partial_{p^i}(x_i) = 0.$$

Using Lemma 3.21, we get a non-zero $x_0 \in K$ such that $\partial_1(x_0) = x_0$. Assume that $i < m-1$ and that we have a non-zero $x_i \in K$ satisfying $(*_i)$.
By Lemma 4.8 for all $y \in K$ we have (setting $q := p^{i+1}$),

$$\begin{aligned}y^{p^{i+1}}x_i - \partial^{(p-1)}_{p^{i+1}}(y^{p^{i+1}}x_i) &= y^{p^{i+1}}x_i - \sum_{l=0}^{p-1}\binom{p-1}{l}\partial^{(p-1-l)}_{p^{i+1}}(x_i)\cdot\partial^{(l)}_1(y)^{p^{i+1}} \\ &= \Big(\sum_{l=0}^{p-2}\alpha_i\cdot\partial^{(l)}_1(y)^q\Big) + x_i\partial^{(p-1)}_1(y)^q,\end{aligned}$$

for some $\alpha_0, \dots, \alpha_{p-2} \in K$. Since $x_i \neq 0$, by Lemma 3.19 there is $y_0 \in K$ such that

$$x_{i+1} := y_0^{p^{i+1}}x_i - \partial^{(p-1)}_{p^{i+1}}(y_0^{p^{i+1}}x_i)$$

is non-zero. By Lemma 4.9, the element x_{i+1} satisfies $(*_{i+1})$.
Let $x := x_{m-1} - 1$. Then we have

$$\partial_1(x) = \partial_1(x_{m-1}) = x_{m-1} = x + 1 \neq 0.$$

Clearly $\partial_{p^i}(x) = 0$ for $i = 1, \dots, m-1$. Since $\partial_1(x) \neq 0$, x is necessarily transcendental over $\mathbb{F}_p$. By Example 3.6, there is a canonical $\mathbb{G}_{\mathrm{m}}$-derivation ∂' on $\mathbb{F}_p[x]$. By the definition of the canonical $\mathbb{G}_{\mathrm{m}}$-derivation, we have $\partial'_1(x) = x+1$ and $\partial'_j(x) = 0$ for $j > 0$ (since the multiplicative formal group law is given by the following power series $X + (X+1)Y$). Hence $\partial_{p^i}(x) = \partial'_{p^i}(x)$ for $i = 1, \dots, m-1$. By Lemma 3.16, $\partial_n(x) = \partial'_n(x)$ for $n < p^m - 1$, hence $\partial_n(x) = 0$ for $n \in \{2, \dots, p^m - 1\}$. □

We have now all the ingredients to prove a multiplicative version of Theorem 4.7. Since the proof is exactly the same as the proof of Theorem 4.7, we will skip it.

Theorem 4.11. *Let $M \subseteq K$ be a separable field extension and ∂ a $\mathbb{G}_{\mathrm{m}}[m]$-derivation on K over M. Then ∂ can be expanded to a $\mathbb{G}_{\mathrm{m}}$-derivation on K over M.*

Remark 4.12. The case of $m = 1$ is contained in the main theorem of [21].

4.3. **Mixed case.** For an arbitrary $c \in k$, one can consider the formal group law $F_c := X + Y + cXY$ and F_c-iterative derivations (as in [21]). Clearly, F_c specializes to the additive law (for $c = 0$) and to the multiplicative law (for $c = 1$). However, it is easy to see that for $c \neq 0$, we have $F_c \cong F_1$. Thus by Lemma 2.6, considering F_c-iterative derivations reduces to considering additively iterative ones (Section 4.1) and multiplicatively iterative ones (Section 4.2).
For the sake of completeness, we notice that if $\partial = (\partial_i)_i$ is an F_c-iterative derivation, then $\partial_1^{(p)} = c^{p-1}\partial_1$.

5. Several HS-derivations

We could have extended the results of Section 4 to the case of several iterative HS-derivations. For example, the crucial notion of a canonical element would be replaced with the notion of a *canonical p-basis* as in [24]. However, we feel that such a generalization would not be a satisfactory one. For example, a tuple of e commuting $\mathbb{G}_{\mathrm{a}}$-derivations is the same as a "$\mathbb{G}_{\mathrm{a}}^e$-derivation", see [16, Prop. 2.20]. Therefore one should consider G-derivations for an arbitrary (not necessarily commutative!) algebraic group or even a formal group. Such sequences of HS-derivations are studied in [9].

It may be also interesting to compare Pierce's theory of several derivations in arbitrary characteristic [17] where the composition of derivations is governed by a Lie algebra $\mathfrak{g}$ with the theory of G-derivations for $\mathrm{Lie}(G) = \mathfrak{g}$.

References

[1] G Crupi, M.; Restuccia. Integrable derivations and formal groups in unequal characteristic. *Rend. Circ. Mat. Palermo*, 47(2):169–190, 1998.
[2] G Crupi, M.; Restuccia. Iterative differentiations in rings of unequal characteristic. *Boll. Unione Mat. Ital. Sez. B Artic. Ric. Mat.*, 4(3):635–646, 2001.
[3] M. Demazure. *Lectures on p-divisible groups*, volume 302 of *Lecture Notes in Mathematics*. Springer-Verlag, 1972.
[4] D. Eisenbud. *Commutative Algebra with a View Towards Algebraic Geometry*. Springer, 1996.
[5] H. Gillet. Differential algebra: A scheme theory approach. In *Differential Algebra and Related Topics*, pages 95–123. World Sci., River Edge, N.J., Newark, N.J., 2002.
[6] D. Hasse. Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik. *J. reine und angew. Math.*, 175:50–54, 1936.
[7] Michiel Hazewinkel. *Formal Groups and Applications*. Academic Press, 1978.
[8] Wilfrid Hodges. *A shorter model theory*. Cambridge University Press, Cambridge, 1997.
[9] Daniel Hoffmann and Piotr Kowalski. Existentially closed fields with G-derivations. In preparation.
[10] Daniel Hoffmann and Piotr Kowalski. A note on integrating group scheme actions. Available on `http://www.math.uni.wroc.pl/~pkowa/mojeprace/integnote.pdf`.
[11] E.R. Kolchin. *Differential Algebra and Algebraic Groups*. Pure and applied mathematics. Academic Press, 1973.

[12] Piotr Kowalski. Geometric axioms for existentially closed Hasse fields. *Annals of Pure and Applied Logic*, 135:286–302, 2005.
[13] Yu I. Manin. The theory of commutative formal groups over fields of finite characteristic. *Russ. Math. Surv.*, 18(6):1–83, 1963.
[14] Hideyuki Matsumura. Integrable derivations. *Nagoya Math. J.*, 87:227–245, 1982.
[15] Hideyuki Matsumura. *Commutative ring theory*. Cambridge University Press, 1986.
[16] Rahim Moosa and Thomas Scanlon. Generalized Hasse-Schmidt varieties and their jet spaces. *Proc. Lond. Math. Soc.*, 103(2):197–234, 2011.
[17] D. Pierce. Fields with several commuting derivations, to appear in the Journal of Symbolic Logic. Available on `http://mat.msgsu.edu.tr/~dpierce/Mathematics/Derivations/Revisited/`.
[18] H. Restuccia, G.; Matsumura. Integrable derivations in rings of unequal characteristic. *Nagoya Math. J.*, 93:173–178, 1984.
[19] F.K. Schmidt and D. Hasse. Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten. *J. reine und angew. Math.*, 177:215–237, 1937.
[20] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer-Verlag, 1986.
[21] A. Tyc. On F-integrable actions of the restricted Lie algebra of a formal group F in characteristic $p > 0$. *Nagoya Math. J.*, 115:125–137, 1989.
[22] William C. Waterhouse. *Introduction to Affine Group Schemes*. Springer-Verlag, 1979.
[23] M. Ziegler. Canonical p-bases, preprint. Available on `http://home.mathematik.uni-freiburg.de/ziegler/preprints/canonical-p-bases.pdf`.
[24] M. Ziegler. Separably closed fields with Hasse derivations. *Journal of Symbolic Logic*, 68:311–318, 2003.

†Instytut Matematyczny, Uniwersytet Wrocławski, Wrocław, Poland
E-mail address: `daniel.max.hoffmann@gmail.com`

♠Instytut Matematyczny, Uniwersytet Wrocławski, Wrocław, Poland
E-mail address: `pkowa@math.uni.wroc.pl`
URL: `http://www.math.uni.wroc.pl/~pkowa/`