

# EXISTENTIALLY CLOSED FIELDS WITH $G$ -DERIVATIONS

DANIEL HOFFMANN<sup>†</sup> AND PIOTR KOWALSKI<sup>♣</sup>

ABSTRACT. We prove that the theories of fields with Hasse-Schmidt derivations corresponding to actions of formal groups admit model companions. We also give geometric axiomatizations of these model companions.

## 1. INTRODUCTION

In this paper, we describe the model theory of fields with Hasse-Schmidt derivations (abbreviated as *HS-derivations* in the sequel) obeying iterativity conditions coming from the actions of formal groups. We consider “ $e$ -dimensional HS-derivations in a generalized sense” (see e.g. [10, Def. 2.12]). This approach includes the case of  $e$ -tuples of the usual HS-derivations. (Actually, both approaches are equivalent in the iterative case, see Remark 3.13.)

One could wonder why do the iterativity conditions help to understand the first-order theories of the fields with HS-derivations. The main reason is that the iterativity conditions enable us to characterize the étale extensions of fields in a first order fashion, see Lemma 3.22 (originating from [32, Cor. 2.2]). Such a characterization is crucial for the quantifier elimination results in Section 4.

We consider both truncated and full HS-derivations. The iterativity rules considered in this paper are governed by (finite in the truncated case) formal groups. We describe the model companions of the theories of fields with such HS-derivations mostly using the ideas from [32]. Then, we extend the results about the geometric axiomatizations [13] from the case of “additive” iterativity ( $F = \widehat{\mathbb{G}}_a^e$ ) to the case of an arbitrary  $F$ -iterative rule ( $F$  is a formal group). We address the question whether the theories we obtain are bi-interpretable with the theory of separably closed fields with a fixed imperfection invariant (it is the case in [32]). It turns out that we get such a bi-interpretability result for formal groups which are the formalizations of algebraic groups. It is not clear for us what happens for the other formal groups. We also discuss the notion of “canonical  $G$ -tuples” (see Definition 6.1), which generalizes Ziegler’s notion of canonical  $p$ -basis [32], and possible generalizations of our methods to the context of [21].

The paper is organized as follows. In Section 2, we introduce the notation and conventions which will be used in the paper. In Section 3, we develop an algebraic

---

2010 *Mathematics Subject Classification*. Primary 13N15, 03C60; Secondary 14L15.

*Key words and phrases*. Hasse-Schmidt derivations, group scheme actions, existentially closed structures.

<sup>♣</sup>Supported by Tübitak grant 2221 and NCN grant 2012/07/B/ST1/03513. Partially supported by ANR Modig (ANR-09-BLAN-0047).

theory of (iterative, truncated, multi-dimensional) HS-derivations. In Section 4, we apply the results from Section 3 to obtain a description of the model complete theories of fields with different types of HS-derivations. In Section 5, we give geometric axioms for the theories considered in Section 4. In Section 6, we speculate about possible extensions of the results of this paper to more general contexts.

**1.1. Formal group actions and model theory.** For convenience of a reader not familiar with commutative algebra around the theory of formal groups, we provide in this section an elementary argument (originating from an observation of Matsumura [19, Section 27]) explaining how formal group scheme actions can be understood as HS-derivations satisfying an iterativity rule.

For simplicity, we only consider the one-dimensional case. A sequence  $(D_i : R \rightarrow R)_{i \in \mathbb{N}}$  is an HS-derivation (over  $k$ ) if and only if the corresponding map

$$\mathbb{D} : R \rightarrow R[[X]], \quad \mathbb{D}(r) = \sum_{i=0}^{\infty} D_i(r) X^i$$

is a ring ( $k$ -algebra) homomorphism and a section of the projection map  $R[[X]] \rightarrow R$ . The standard iterativity condition may be expressed using the following diagram

$$\begin{array}{ccc} R & \xrightarrow{\mathbb{D}} & R[[X]] \\ \mathbb{D} \downarrow & & \downarrow \mathbb{D}[[X]] \\ R[[X]] & \xrightarrow{X \mapsto X+Y} & R[[X, Y]], \end{array}$$

i.e.  $\mathbb{D}$  is iterative if and only if the diagram above is commutative. Clearly, the additive *formal group law*  $X + Y$  is crucial for the standard iterativity rule above. (A formal group law over  $k$ , see e.g. [28, Chapter IV.2], is a power series  $F$  over  $k$  in two variables satisfying formally the group axioms, e.g.  $F(F(X_1, X_2), X_3) = F(X_1, F(X_2, X_3))$ .) The diagram above may be interpreted as an action of the formal additive group scheme on the scheme  $\text{Spec}(R)$ . We explain it below in an easier case of *truncated* HS-derivations (see Section 3.1), which correspond to actions (in the category of schemes) of finite group schemes.

We start from the truncated iterativity diagram, which is just a truncation of the diagram above expressing the standard iterativity of HS-derivations

$$\begin{array}{ccc} R & \xrightarrow{\mathbb{D}} & R[v_m] \\ \mathbb{D} \downarrow & & \downarrow \mathbb{D}[v_m] \\ R[w_m] & \xrightarrow{c_R} & R[w_m, v_m]. \end{array}$$

Here  $c_R(w_m) = v_m + w_m$  gives a Hopf algebra structure over  $R$ . Using the tensor product over the base field  $k$ , we obtain the following diagram.

$$\begin{array}{ccc} R & \xrightarrow{\mathbb{D}} & k[v_m] \otimes R \\ \mathbb{D} \downarrow & & \downarrow \text{id}_{k[v_m]} \otimes \mathbb{D} \\ k[v_m] \otimes R & \xrightarrow{c \otimes \text{id}_R} & k[v_m] \otimes k[v_m] \otimes R \end{array}$$

Going to the opposite category (of  $k$ -schemes), we see that we get exactly the diagram expressing the mixed associativity of a group scheme action

$$\begin{array}{ccc} R & \xleftarrow{\tilde{\mathbb{D}}} & \mathfrak{g} \times X \\ \tilde{\mathbb{D}} \uparrow & & \uparrow \text{id}_{\mathfrak{g}} \times \tilde{\mathbb{D}} \\ \mathfrak{g} \times X & \xleftarrow{\mu \times \text{id}_X} & \mathfrak{g} \times \mathfrak{g} \times X, \end{array}$$

where  $X = \text{Spec}(R)$  and  $\mathfrak{g} = \ker(\text{Fr}_{\mathbb{G}_a}^m)$ .

The considerations above lead to an interesting conclusion that actions of groups with “no points” (i.e. finite local group schemes as above), which seem to be very far from any model-theoretic considerations, are actually amenable to model-theoretic treatment; it is the main point of this paper.

## 2. DEFINITIONS, NOTATION AND CONVENTIONS

In this section we introduce the notation and conventions which we are going to use throughout the paper. We also recall (or refer to) several standard notions.

In the entire paper,  $k$  will be a perfect field of characteristic  $p > 0$  (unless we clearly say that  $\text{char}(k) = 0$ ). The category of *affine group schemes* over  $k$  is the category opposite to the category of *Hopf algebras* over  $k$  [30, Section 1.4] (or it is the category of representable functors from  $k$ -algebras to groups, see [30, Section 1.2]). A *truncated group scheme* [3] over  $k$  is an affine group scheme whose universe is isomorphic to  $\text{Spec}(k[X_1, \dots, X_e]/(X_1^{p^m}, \dots, X_e^{p^m}))$ .

**Remark 2.1.** If  $\text{char}(k) = 0$ , then by a theorem of Cartier [30, Section 11.4] all Hopf algebras over  $k$  are reduced, so there are no truncated group schemes.

The category of *formal groups* over  $k$  is the category opposite to the category of *complete Hopf algebras* over  $k$  (or the category of representable functors from complete  $k$ -algebras to groups, see [5, Chapter VII]). There is a correspondence between smooth formal groups (the underlying complete algebra is the power series algebra in  $e$  variables) and formal group laws, where an  $e$ -dimensional formal group law over  $k$ , is a power series in  $2e$  variables formally satisfying the group axioms, see [5, Sect. 9.1]. Note that a truncated group scheme is both an affine group scheme and a formal group.

For the rest of the paper we fix the following.

- Let  $m$  and  $e$  be positive integers.
- Let  $\mathbf{X}$  denote the tuple of variables  $(X_1, \dots, X_e)$ . For a tuple  $\mathbf{n} = (n_1, \dots, n_e)$  of natural numbers, we denote  $X_1^{n_1} \dots X_e^{n_e}$  by  $\mathbf{X}^{\mathbf{n}}$ .
- Let  $k[\mathbf{v}_m]$  denote the ring  $k[\mathbf{X}]/(X_1^{p^m}, \dots, X_e^{p^m})$ .
- For a positive integer  $l$ , let  $[l]$  denote the set  $\{0, \dots, l-1\}$ .
- Let  $\mathfrak{g}$  be a group scheme over  $k$  whose underlying scheme is  $\text{Spec}(k[\mathbf{v}_m])$ .
- Let  $R$  and  $S$  be  $k$ -algebras.
- Let  $G$  be an algebraic group over  $k$ .
- Let  $V$  be a scheme over  $k$ .
- Let  $F$  be an  $e$ -dimensional formal group law over  $k$ .

**2.1. Truncations of group schemes.** Let  $\mathfrak{G}$  be an affine group scheme over  $k$ ,  $H$  the corresponding Hopf algebra and  $\mathfrak{m}$  be the kernel of the counit map  $H \rightarrow k$  (the *augmentation ideal*). Using the base-change given by the automorphism  $\text{Fr}^m : k \rightarrow k$  we get the affine group scheme  $\mathfrak{G}^{\text{Fr}^m}$  over  $k$  and a group scheme morphism  $\text{Fr}_{\mathfrak{G}}^m : \mathfrak{G} \rightarrow \mathfrak{G}^{\text{Fr}^m}$ . Let  $\mathfrak{G}[m]$  be the kernel of  $\text{Fr}_{\mathfrak{G}}^m$  which is a truncated  $k$ -group scheme. (In the case of a commutative group scheme  $A$ ,  $A[m]$  often denotes the kernel of multiplication by  $m$  and “our”  $A[m]$  is often denoted by  $A[\text{Fr}^m]$ . Since we do not consider the kernel of multiplication by  $m$  in this paper, we prefer our simplified notation.)

It corresponds to the quotient Hopf algebra

$$H[m] := H / \text{Fr}^m(\mathfrak{m})H.$$

We get a direct system of truncated  $k$ -group schemes  $(\mathfrak{G}[n])_{n \in \mathbb{N}}$ . If  $\mathfrak{G} = G$ , then  $\varinjlim (G[n])$  coincides with  $\widehat{G}$ , the formal group which is the formalization of  $G$  (see [16, Lemma 1.1]).

Similarly, for a complete Hopf algebra  $\mathcal{H}$ , we have the analogous quotient  $\mathcal{H}[m]$  which is a Hopf algebra and also a complete Hopf algebra. Hence for a formal group  $F$ , we have a direct system of truncated group schemes  $F[m]$  and in this case we get that  $F = \varinjlim F[m]$ , see [16, Lemma 1.1] again.

**Remark 2.2.** One may ask whether any truncated group scheme  $\mathfrak{g}$  can be integrated i.e. whether there is a formal group law  $F$  such that  $F[m] = \mathfrak{g}$ . For  $e = 1$ , the answer is positive if and only if  $\mathfrak{g}$  is commutative [5, Corollary 5.7.4] (see [5, Example 5.7.8] for an example of a non-commutative  $\mathfrak{g}$ ).

**Remark 2.3.** For the truncated group scheme  $\mathfrak{g}$ , we get a finite direct system of truncated group schemes

$$0 = \mathfrak{g}[0] < \mathfrak{g}[1] < \dots < \mathfrak{g}[m-1] < \mathfrak{g}[m] = \mathfrak{g}.$$

The group schemes in this direct system may be described as follows. Let  $i \in [m+1]$  and  $\mathfrak{g}^{\text{Fr}^i}$  be the group scheme  $\mathfrak{g}$  twisted by the  $i$ -th power of the Frobenius map. Then we have a group scheme morphism  $\text{Fr}_{\mathfrak{g}}^i : \mathfrak{g} \rightarrow \mathfrak{g}^{\text{Fr}^i}$  such that

$$\ker(\text{Fr}_{\mathfrak{g}}^i) = \mathfrak{g}[i], \quad \text{Fr}_{\mathfrak{g}}^i(\mathfrak{g}) = \mathfrak{g}^{\text{Fr}^i}[m-i].$$

### 3. FINITE GROUP SCHEMES AND ITERATIVE HS-DERIVATIONS

In this section, we develop an algebraic theory of (iterative, truncated) multi-dimensional HS-derivations.

**3.1. Multi-dimensional truncated HS-derivations.** We are going to use the following definition.

**Definition 3.1.** (1) An  $e$ -dimensional HS-derivation on  $R$  over  $k$  is a  $k$ -algebra homomorphism

$$\mathbb{D} : R \rightarrow R[[\mathbf{X}]]$$

which is a section of the projection map

$$R[[\mathbf{X}]] \rightarrow R, \quad H \mapsto H(\mathbf{0}).$$

- (2) An  $m$ -truncated  $e$ -dimensional HS-derivation on  $R$  over  $k$  is a  $k$ -algebra homomorphism

$$\mathbb{D} : R \rightarrow R[\mathbf{v}_m]$$

which is a section of the projection map  $R[\mathbf{v}_m] \rightarrow R$ .

**Remark 3.2.** (1) From any  $e$ -dimensional HS-derivation  $\mathbb{D}$  on  $R$  over  $k$  and any positive integer  $n$ , we get in an obvious way (i.e. by post-composing with the quotient map  $R[\mathbf{X}] \rightarrow R[\mathbf{v}_n]$ ) an  $n$ -truncated  $e$ -dimensional HS-derivation on  $R$  which we denote by  $\mathbb{D}[n]$ .

- (2) Let us denote  $\mathbb{D}(r)$  by  $\sum_{\mathbf{i}} D_{\mathbf{i}}(r)\mathbf{X}^{\mathbf{i}}$ . Using such a notation, an  $e$ -dimensional HS-derivation on  $R$  over  $k$  is a sequence

$$\mathbb{D} = (D_{\mathbf{i}} : R \rightarrow R)_{\mathbf{i} \in \mathbb{N}^e}$$

satisfying the following properties:

- $D_{\mathbf{0}} = \text{id}_R$ ,
- each  $D_{\mathbf{i}}$  is  $k$ -linear,
- for any  $x, y \in R$  we have

$$D_{\mathbf{i}}(xy) = \sum_{\mathbf{j}+\mathbf{k}=\mathbf{i}} D_{\mathbf{j}}(x)D_{\mathbf{k}}(y).$$

- (3) Each  $e$ -dimensional HS-derivation  $\mathbb{D}$  on  $R$  gives the following tuple of (1-dimensional) HS-derivations on  $R$ :

$$\mathbb{D}_1 := (D_{(i,0,\dots,0)})_{i \in \mathbb{N}}, \dots, \mathbb{D}_e := (D_{(0,\dots,0,i)})_{i \in \mathbb{N}}.$$

On the level of  $k$ -algebra maps, the above  $m$ -truncated HS-derivations correspond to the composition of  $\mathbb{D} : R \rightarrow R[\mathbf{X}]$  with the appropriate projection map  $R[\mathbf{X}] \rightarrow R[X]$ .

- (4) On the other hand, each  $e$ -tuple of (1-dimensional) HS-derivations on  $R$  gives an  $e$ -dimensional HS-derivation on  $R$ , e.g. for  $e = 2$  and  $\mathbb{D}_1, \mathbb{D}_2 : R \rightarrow R[X]$  we get the 2-dimensional HS-derivation on  $R$  given by the composition below

$$R \xrightarrow{\mathbb{D}_1} R[X] \xrightarrow{\mathbb{D}_2[X]} R[X, Y].$$

However, not all  $e$ -dimensional HS-derivations on  $R$  can be obtained in such a way. In fact an  $e$ -dimensional HS-derivation  $\mathbb{D}$  is not necessarily determined by the  $e$ -tuple  $\mathbb{D}_1, \dots, \mathbb{D}_e$  from (3). For example consider the (truncated) case when  $p = 2$  and  $m = 1$ . If  $\partial$  is a non-zero derivation on  $R$ , then the map

$$\mathbb{D}(r) = r + \partial(r)(X + (X^2))(Y + (Y^2))$$

is a non-zero 1-truncated 2-dimensional HS-derivation, but the corresponding 1-truncated 1-dimensional HS-derivations from (3) are the zero maps.

- (5) All the above (for  $n \leq m$ ) applies to  $m$ -truncated  $e$ -dimensional HS-derivations (after replacing “ $\mathbb{N}$ ” with “ $[p^m]$ ” and “ $[\mathbf{X}]$ ” with “ $[\mathbf{v}_m]$ ”).
- (6) We can extend Definition 3.1 to define  $m$ -truncated  $e$ -dimensional HS-derivations from  $R$  to  $S$  (we do not require anything about the sections here).
- (7) Our  $m$ -truncated 1-dimensional HS-derivations correspond to the *higher derivations of length  $p^m - 1$*  from [19].

For the definition of an étale map/algebra, the reader is advised to consult [19, p. 193] (called “0-étale” there). It is easy to see that the condition “ $N^2 = 0$ ” from [19, p. 193] may be replaced with the condition “ $N$  is nilpotent” (see e.g. Remark on page 199 of [17]).

**Proposition 3.3.** *Assume that  $R \rightarrow S$  is an étale  $k$ -algebra map. Then any ( $m$ -truncated)  $e$ -dimensional HS-derivation  $\mathbb{D}$  on  $R$  uniquely extends to an ( $m$ -truncated)  $e$ -dimensional HS-derivation  $\mathbb{D}'$  on  $S$ .*

*Proof.* The proof goes almost exactly as in [19, theorem 27.2], so we will just sketch the main inductive step which makes clear how the étale assumption is used. We apply the induction on the truncation degree. Assume that for  $l \in \mathbb{N}$  (resp.  $l < m$ ) we have extended  $\mathbb{D}[l]$  to an  $l$ -truncated  $e$ -dimensional HS-derivation  $\mathbb{D}' := (D'_i)_{i < [p^l]^e}$  on  $S$ . Consider the following diagram

$$\begin{array}{ccc}
 & S[\mathbf{X}]/(X_1^{p^l}, \dots, X_e^{p^l}) & \\
 \mathbb{D}' \nearrow & & \nwarrow \pi \\
 S & \dashrightarrow & S[\mathbf{X}]/(X_1^{p^{l+1}}, \dots, X_e^{p^{l+1}}) \\
 \searrow f & & \nearrow \mathbb{D}[l+1] \\
 & R &
 \end{array}$$

where  $\pi$  is the quotient map. Then  $(\ker \pi)^{e+1} = 0$ , so  $\ker(\pi)$  is nilpotent. Since the map  $R \rightarrow S$  is étale, we get a unique  $k$ -algebra map

$$S \rightarrow S[\mathbf{X}]/(X_1^{p^{l+1}}, \dots, X_e^{p^{l+1}})$$

completing the diagram above.  $\square$

**Remark 3.4.** Proposition 3.3 enables us to generalize Definition 3.1 in the following way.

- (1) Since the localization maps are étale (see [19, p. 193]), any ( $m$ -truncated)  $e$ -dimensional HS-derivation on  $R$  uniquely extends to an ( $m$ -truncated)  $e$ -dimensional HS-derivation on a localization of  $R$ .
- (2) By (1), we get a notion of an ( $m$ -truncated)  $e$ -dimensional HS-derivation on any scheme over  $k$ .
- (3) Proposition 3.3 generalizes to schemes over  $k$ .
- (4) The notion of an ( $m$ -truncated)  $e$ -dimensional HS-derivation on a scheme  $V$  is a special case of the notion of a  $\underline{\mathcal{D}}$ -structure on a scheme  $V$ , see [21]. We will discuss possible generalizations of the results of this paper to the context of [21] in Section 6.
- (5) It is easy to generalize the assumptions of Proposition 3.3 to include the case of ( $m$ -truncated)  $e$ -dimensional HS-derivations *from  $R$  to  $S$* .

**Definition 3.5.** If  $\mathbb{D}$  is an ( $m$ -truncated)  $e$ -dimensional HS-derivation on  $R$  over  $k$ , then we define the following.

- (1) The *ring of constants* of  $(R, \mathbb{D})$  is

$$\ker(D_{(1,0,\dots,0)}) \cap \dots \cap \ker(D_{(0,\dots,0,1)}).$$

Clearly,  $R^p$  is contained in the ring of constants of  $(R, \mathbb{D})$ .

- (2) We call  $(R, \mathbb{D})$  *strict*, if the ring of constants of  $\mathbb{D}$  coincides with  $R^p$ .

(3) The *ring of absolute constants* of  $(R, \mathbb{D})$  is

$$\bigcap_{i \neq 0} \ker(D_i).$$

**Remark 3.6.** If  $\mathbb{D}$  is an (resp.  $m$ -truncated)  $e$ -dimensional HS-derivation on  $R$  over  $k$ , then  $R^{p^\infty}$  (resp.  $R^{p^m}$ ) is contained in the ring of absolute constants. It is easy to see (e.g. in the  $m$ -truncated case) considering  $\mathbb{D} : R \rightarrow R[\mathbf{v}_m]$  as a ring homomorphism and taking the  $p^m$ -th power.

**Notation 3.7.** The couple  $(R, \mathbb{D})$  will be usually denoted by  $\mathbf{R}$  and called an ( $m$ -truncated  $e$ -dimensional) *HS-ring*. Similarly, we get the notions of *HS-fields*, *HS-extension*, etc.

**3.2. Group scheme actions.** We introduce a notion which generalizes the notion of an  $m$ -truncated iterative HS-derivation from [13].

**Definition 3.8.** (1) A  $\mathfrak{g}$ -*derivation on  $V$*  is a  $k$ -group scheme action of  $\mathfrak{g}$  on  $V$  (see Section 12 in [23]).  
 (2) A  $\mathfrak{g}$ -*derivation on  $R$*  is a  $\mathfrak{g}$ -derivation on  $\text{Spec}(R)$ .  
 (3) We naturally get the notions of a  $\mathfrak{g}$ -*ring*, a  $\mathfrak{g}$ -*field* and a  $\mathfrak{g}$ -*extension*.

**Remark 3.9.** A  $\mathfrak{g}$ -derivation on  $R$  is the same as an  $m$ -truncated  $e$ -dimensional HS-derivation on  $R$  over  $k$  satisfying a “ $\mathfrak{g}$ -iterativity” rule. It is easy to see that the trivial action of the unit morphism corresponds to the condition  $D_{\mathbf{0}} = \text{id}_R$  and the diagram expressing the mixed associativity of the  $k$ -group scheme action  $d$  is the following “ $\mathfrak{g}$ -iterativity” diagram

$$\begin{array}{ccc} R & \xrightarrow{d} & R[\mathbf{v}_m] \\ d \downarrow & & \downarrow d[\mathbf{v}_m] \\ R[\mathbf{w}_m] & \xrightarrow{c} & R[\mathbf{w}_m, \mathbf{v}_m] \end{array}$$

where  $\mathbf{w}_m$  is another “ $m$ -truncated  $e$ -tuple of variables” and  $c$  is the Hopf algebra comultiplication given by  $\mathfrak{g}$ . Therefore for an arbitrary  $k$ -scheme  $V$ , any  $\mathfrak{g}$ -derivation on  $V$  is also an  $m$ -truncated  $e$ -dimensional HS-derivation on  $V$  over  $k$  in the sense of Remark 3.4(2).

**Remark 3.10.** We will give another interpretation of the  $\mathfrak{g}$ -iterativity condition. Suppose that the matrix (in the standard basis) of the  $k$ -linear comultiplication map  $c$  from Remark 3.9 has the form  $(c_{\mathbf{i}, \mathbf{j}}^{\mathbf{k}})$ . Suppose also that  $\mathbb{D} = (D_{\mathbf{i}})_{\mathbf{i}}$  is an  $m$ -truncated  $e$ -dimensional HS-derivation on  $R$  over  $k$ . Then  $\mathbb{D}$  is a  $\mathfrak{g}$ -derivation if and only if for all  $\mathbf{i}, \mathbf{j}$  we have

$$D_{\mathbf{j}} \circ D_{\mathbf{i}} = \sum_{\mathbf{k}} c_{\mathbf{i}, \mathbf{j}}^{\mathbf{k}} D_{\mathbf{k}}.$$

One easily shows the following.

**Fact 3.11.** *If  $\mathfrak{g} = \mathfrak{g}_1 \times \dots \times \mathfrak{g}_e$  (product of finite group schemes), then we have the following.*

(1) *For any  $\mathfrak{g}$ -derivation  $\mathbb{D}$  on  $R$  and  $i \leq e$ ,  $\mathbb{D}_i$  from Remark 3.2 is a  $\mathfrak{g}_i$ -derivation and we have*

$$D_{(i_1, \dots, i_e)} = D_{1, i_1} \circ \dots \circ D_{e, i_e}.$$

- (2) If for any any  $i \leq e$ ,  $\mathbb{D}_i$  is an  $\mathfrak{g}_i$ -derivation, and we have  $D_{i,i'} \circ D_{j,j'} = D_{j,j'} \circ D_{i,i'}$  for all  $i, j \leq e$  and  $i', j' \in \mathbb{N}$ , then the formula

$$D_{(i_1, \dots, i_e)} = D_{1, i_1} \circ \dots \circ D_{e, i_e}$$

defines a  $\mathfrak{g}$ -derivation.

**Example 3.12.** We give below several examples of  $\mathfrak{g}$ -iterativity rules.

- (1) A sequence of  $e$  commuting iterative  $m$ -truncated HS-derivations from [13] is the same as a  $\mathbb{G}_a^e[m]$ -derivation (see Fact 3.11).  
(2) Let  $G$  be the unipotent algebraic group of dimension 2 given by the cocycle

$$\frac{(X + Y)^p - X^p - Y^p}{p},$$

see [26, p. 171].

Assume that  $p = 2$  and  $\mathbb{D}$  is an  $m$ -truncated 2-dimensional HS-derivation. Then  $\mathbb{D}$  is a  $G[m]$ -derivation if and only if

$$D_{(k,l)} \circ D_{(i,j)} = \sum_{t=0}^{\min(j,l)} \frac{(i+k+t)!}{i!k!t!} \frac{(j+l-2t)!}{(j-t)!(l-t)!} D_{(i+k+t, j+l-2t)}.$$

In particular, we have the following formulas which actually describe the  $G[m]$ -iterativity rule fully:

$$D_{(0,j)} \circ D_{(i,0)} = D_{(i,j)} = D_{(i,0)} \circ D_{(0,j)},$$

$$D_{(k,0)} \circ D_{(i,0)} = \binom{i+k}{i} D_{(i+k,0)},$$

$$D_{(0,1)} \circ D_{(0,i)} = (i+1)D_{(0,i+1)} + D_{(1,i-1)}.$$

The first author described in [7] a modification of the theory of separably closed fields with higher derivations from [20] using the iterativity rules coming from algebraic groups similar to the one considered here (groups of Witt vectors).

- (3) Let  $G$  be  $\mathbb{G}_a \rtimes \mathbb{G}_m$ , where the group operation on  $\mathbb{G}_m$  is given by  $X+Y+XY$ . Hence the group operation on  $G$  is given by

$$(X_1, Y_1) * (X_2, Y_2) = (X_1 + X_2 + Y_1 X_2, Y_1 + Y_2 + Y_1 Y_2).$$

Let  $\mathbb{D}$  be an  $m$ -truncated 2-dimensional HS-derivation. Then  $\mathbb{D}$  is a  $G[m]$ -derivation if and only if

$$D_{(k,l)} \circ D_{(i,j)} = \sum_{t=0}^{\min(k,j)} \sum_{s=0}^{\min(l, j-t)} \frac{(i+k)!}{i!(k-t)!t!} \frac{(j+l-t-s)!}{(j-t-s)!(l-s)!s!} D_{(i+k, j+l-t-s)}.$$

In particular, we have

$$D_{(0,l)} \circ D_{(i,0)} = D_{(i,l)}.$$

But the above formula does not apply for the other choice of coordinates

$$D_{(1,0)} \circ D_{(0,1)} = D_{(1,1)} + D_{(1,0)} \neq D_{(1,1)} = D_{(0,1)} \circ D_{(1,0)}.$$

We also have the following ‘‘additive coordinate’’ rule

$$D_{(1,0)} \circ D_{(i,0)} = (i+1)D_{(1+i,0)} = D_{(i,0)} \circ D_{(1,0)},$$



and the “multiplicative coordinate” rule

$$D_{(0,1)} \circ D_{(0,i)} = (i+1)D_{(0,i+1)} + iD_{(0,i)} = D_{(0,i)} \circ D_{(0,1)}.$$

**Remark 3.13.** We see that all the  $e$ -dimensional HS-derivations in the example above are determined by the 1-dimensional HS-derivations  $\mathbb{D}_1, \dots, \mathbb{D}_e$  from Remark 3.2(3). It may be shown (using Lemma 3.14 below) that this is the case for an arbitrary  $F$ -derivation (or a  $\mathfrak{g}$ -derivation).

We will need more precise information about the “structural constants” from Remark 3.10.

**Lemma 3.14.** *Let  $c_{\mathbf{i},\mathbf{j}}^{\mathbf{k}}$  be as in Remark 3.10. For a tuple of natural numbers  $\mathbf{n} = (n_1, \dots, n_e)$ , the sum  $n_1 + \dots + n_e$  is denoted by  $|\mathbf{n}|$ . Then we have the following.*

- (1) *If  $|\mathbf{k}| > |\mathbf{i}| + |\mathbf{j}|$ , then  $c_{\mathbf{i},\mathbf{j}}^{\mathbf{k}} = 0$ .*
- (2) *If  $|\mathbf{k}| = |\mathbf{i}| + |\mathbf{j}|$  and  $\mathbf{k} \neq \mathbf{i} + \mathbf{j}$ , then  $c_{\mathbf{i},\mathbf{j}}^{\mathbf{k}} = 0$ .*
- (3) *If  $\mathbf{k} = \mathbf{i} + \mathbf{j}$ , then*

$$c_{\mathbf{i},\mathbf{j}}^{\mathbf{k}} = \binom{i_1 + j_1}{i_1} \cdots \binom{i_e + j_e}{i_e}.$$

*Proof.* It is clear for  $\mathbf{i} = \mathbf{0}$  or  $\mathbf{j} = \mathbf{0}$ , so we assume that  $\mathbf{i}, \mathbf{j} \neq \mathbf{0}$ . By a truncated version of the formula [5, (14.1.1)], we have (in the notation of Remark 3.9)

$$c(\mathbf{w}_m) = \mathbf{w}_m + \mathbf{v}_m + \mathbf{s}_m,$$

where  $\mathbf{s}_m = (S_1, \dots, S_e)$  for some  $S_1, \dots, S_e$  belonging to the ideal  $(\mathbf{w}_m \cdot \mathbf{v}_m)$ . Therefore for every  $r \in R$  we have

$$\sum_{\mathbf{i},\mathbf{j}} D_{\mathbf{j}} D_{\mathbf{i}}(r) \mathbf{v}_m^{\mathbf{i}} \mathbf{w}_m^{\mathbf{j}} = \sum_{\mathbf{k}} D_{\mathbf{k}}(r) (\mathbf{w}_m + \mathbf{v}_m + \mathbf{s}_m)^{\mathbf{k}}.$$

We get the result by comparing the coefficients at  $\mathbf{v}_m^{\mathbf{i}} \mathbf{w}_m^{\mathbf{j}}$ . □

**Remark 3.15.** Note that for every  $\mathbf{i}, \mathbf{j} \neq \mathbf{0}$  we have the following:

$$D_{\mathbf{j}} \circ D_{\mathbf{i}} = \binom{i_1 + j_1}{i_1} \cdots \binom{i_e + j_e}{i_e} D_{\mathbf{i}+\mathbf{j}} + \mathcal{O}(D_{\mathbf{n}})_{0 < |\mathbf{n}| < |\mathbf{i}+\mathbf{j}|},$$

where  $\mathcal{O}(D_{\mathbf{n}})_{0 < |\mathbf{n}| < |\mathbf{i}+\mathbf{j}|}$  is a  $k$ -linear combination of  $D_{\mathbf{n}}$  for  $0 < |\mathbf{n}| < |\mathbf{i} + \mathbf{j}|$ . We consider the quantity  $\mathcal{O}(\cdot)$  as a “disturbance from the additive iterativity”, because for the additive iterativity condition this linear combination is always zero. Lemma 3.13 from [8] regards the case of  $e = 1$ .

**Lemma 3.16.** *If  $\mathbf{R} = (R, \mathbb{D})$  is a  $\mathfrak{g}$ -ring, then the ring of constants of  $\mathbf{R}$  coincides with the ring of absolute constants of  $(R, \mathbb{D}[1])$ .*

*Proof.* It follows from Lemma 3.14, that for any  $\mathbf{i} \neq \mathbf{0}$ ,  $D_{\mathbf{i}}$  is a  $k$ -linear combination of the compositions of the derivations  $D_{(1,0,\dots,0)}, \dots, D_{(0,\dots,0,1)}$  which gives the result. □

We comment below on a related notion of a restricted Lie algebra action (see [29]).

**Remark 3.17.** For  $m = 1$ , any finite group scheme of the form considered in this paper (i.e. any finite group scheme of the *Frobenius height one*) is equivalent to a *restricted Lie algebra* in the sense of the theorem on page 139 of [23]. Hence a

$\mathfrak{g}$ -derivation ( $m = 1$ ) on  $R$  is equivalent to an action on  $R$  of  $e$  derivations satisfying the commutator and the  $p$ -th composition rules given by the corresponding restricted Lie algebra  $\text{Lie}(\mathfrak{g})$  (see [23]).

We need to know that the unique extension in Proposition 3.3 preserves the  $\mathfrak{g}$ -iterativity condition.

**Proposition 3.18.** *Assume that  $R \rightarrow S$  is étale and  $\mathbb{D}$  is a  $\mathfrak{g}$ -derivation on  $R$ . Then the unique extension of  $\mathbb{D}$  to  $S$  in Proposition 3.3 is a  $\mathfrak{g}$ -derivation.*

*Proof.* The proof of the moreover part of [19, theorem 27.2] may be applied here, similarly as in the proof of Proposition 3.3.  $\square$

**Remark 3.19.** As before, Proposition 3.18 easily generalizes to  $\mathfrak{g}$ -derivations on  $k$ -schemes.

We prove a version of the “Wronskian theorem” [12, Thm. II.1] for the case of  $\mathfrak{g}$ -derivations.

**Proposition 3.20.** *Let  $\mathbf{K}$  be a  $\mathfrak{g}[1]$ -field and  $C$  be its field of constants. Then for any positive integer  $l$  and any  $x_1, \dots, x_l \in K$ , the elements  $x_1, \dots, x_l$  are linearly independent over  $C$  if and only if the rank of the following “Wronskian matrix”*

$$(D_{\mathbf{i}}(x_j))_{\mathbf{i} \in [p]^e, j \leq l}$$

*is strictly smaller than  $l$ .*

*Proof.* Assume that  $x_l = c_1 x_1 + \dots + c_{l-1} x_{l-1}$  for some  $c_1, \dots, c_{l-1} \in C$ . By Lemma 3.16, each  $D_{\mathbf{i}}$  is  $C$ -linear. Hence we obtain that the rank of our Wronskian matrix is smaller than  $l$  as in the standard case (see [12, Thm. II.1]).

Let the rank of the matrix  $(D_{\mathbf{i}}(x_j))_{\mathbf{i} \in [p]^e, j \leq l}$  be equal to  $r < l$ . After reordering  $x_1, \dots, x_l$ , we may assume that the matrix  $(D_{\mathbf{i}}(x_j))_{\mathbf{i} \in [p]^e, j \leq r}$  has rank  $r$ . Therefore there exist  $\lambda_1, \dots, \lambda_{r+1} \in K$ , not all equal to 0, such that for each tuple  $\mathbf{k}$  we have

$$(*) \quad \sum_{s=1}^{r+1} \lambda_s D_{\mathbf{k}}(x_s) = 0.$$

Reordering and dividing by  $c_{r+1}$  if need be, we may assume that  $c_{r+1} = 1$ . By Remark 3.10, there are  $c_{\mathbf{i}, \mathbf{j}}^{\mathbf{k}} \in C$  such that for all tuples  $\mathbf{i}, \mathbf{j}$  we have

$$D_{\mathbf{j}} \circ D_{\mathbf{i}} = \sum_{\mathbf{k}} c_{\mathbf{i}, \mathbf{j}}^{\mathbf{k}} D_{\mathbf{k}}.$$

Hence for  $\mathbf{1} := (1, 0, \dots, 0)$  and every tuple  $\mathbf{i}$  we get (using  $(*)$  with  $\mathbf{k} = \mathbf{1}$  for the last equality)

$$\begin{aligned} 0 &= \sum_{s=1}^{r+1} D_{\mathbf{1}}(\lambda_s) D_{\mathbf{i}}(x_s) + \sum_{s=1}^{r+1} \lambda_s D_{\mathbf{1}}(D_{\mathbf{i}}(x_s)) \\ &= \sum_{s=1}^r D_{\mathbf{1}}(\lambda_s) D_{\mathbf{i}}(x_s) + \sum_{\mathbf{1}} c_{\mathbf{1}, \mathbf{i}}^{\mathbf{1}} \sum_{s=1}^{r+1} \lambda_s D_{\mathbf{1}}(x_s) \\ &= \sum_{s=1}^r D_{\mathbf{1}}(\lambda_s) D_{\mathbf{i}}(x_s). \end{aligned}$$

Thus  $D_{(1,0,\dots,0)}(\lambda_s) = 0$  for every  $s \leq r$ . After similar reasoning for the derivations  $D_{(0,1,0,\dots,0)}, \dots, D_{(0,\dots,0,1)}$  we get  $\lambda_1, \dots, \lambda_{r+1} \in C$ . By setting  $\mathbf{k} = \mathbf{0}$  in (\*), we obtain that  $x_1, \dots, x_l$  are linearly dependent over  $C$ .  $\square$

The next result generalizes the first part of [32, Lemma 2.1] (the second part is generalized in Proposition 3.22(1)). For a group scheme action interpretation and more comments, see Remark 3.29.

**Corollary 3.21.** *Let  $\mathbf{K}$  be a  $\mathfrak{g}$ -field and  $C$  its field of constants. Then we have*

$$[K : C] \leq p^e.$$

*Proof.* Let  $l = p^e + 1$  and  $x_1, \dots, x_l \in K$ . The rank of the corresponding Wronskian matrix from Proposition 3.20 is at most  $p^e$ , since there are only  $p^e$  operators of the form  $D_i$ . By Proposition 3.20,  $x_1, \dots, x_l$  are linearly dependent over  $C$ .  $\square$

We can generalize now the appropriate results from [32] to the context of  $\mathfrak{g}$ -derivations. Let  $K$  be a field of characteristic  $p$ . Then  $[K : K^p] = p^l$ , where  $l \in \mathbb{N} \cup \{\infty\}$ . We call  $l$  the *degree of imperfection* of  $K$ . For the definition and properties of separable algebras/field extensions the reader is referred to [19, Sect. 26]. The next result is a crucial characterization of the étale extensions which we will need for the quantifier elimination results in Section 4.

**Lemma 3.22.** *Let  $\mathbf{K} \subseteq \mathbf{L}$  be an extension of  $\mathfrak{g}$ -fields. Let  $C_K$  (resp.  $C_L$ ) be the constant field of  $\mathbf{K}$  (resp.  $\mathbf{L}$ ). Then we have the following.*

- (1) *The field  $K$  is linearly disjoint from  $C_L$  over  $C_K$ .*
- (2) *If  $\mathbf{K}$  is strict (see Def. 3.5(2)), then the extension  $K \subseteq L$  is separable.*
- (3) *If the extension  $K \subseteq L$  is étale and  $K$  has a finite degree of imperfection, then  $\mathbf{K}$  is strict if and only if  $\mathbf{L}$  is strict.*

*Proof.* For (1), we apply Lemma 3.20 as in the standard case (see [12, Cor. 1, p. 87]).

The item (2) follows directly from (1) using [19, Thm. 26.4].

The right-to-left implication in (3) is clear (and only the condition  $L^p \cap K = K^p$  is used). For the left-to-right implication, the étale assumption implies that  $[L : L^p] = [K : K^p]$  and  $KL^p = L$ . Since  $L^p \subseteq C_L$ , by (1) (used for the second equality below) we get

$$[L : L^p] = [K : K^p] = [KC_L : C_L] = [L : C_L].$$

Since  $[L : L^p]$  is finite, we get  $C_L = L^p$ .  $\square$

**3.3. Formal group actions.** Recall that  $F$  is a formal group law over  $k$  which may be identified with a direct system of finite group schemes over  $k$  and  $G$  is an algebraic group over  $k$ .

**Definition 3.23.** We define the following.

- (1) An  $F$ -derivation on  $V$  is a direct system of  $F[m]$ -derivations on  $V$ .
- (2) A  $G$ -derivation is a  $\widehat{G}$ -derivation (see Section 2.1 for the definition of  $\widehat{G}$ ).
- (3) Similarly we get the notions of an  $F$ -derivation and a  $G$ -derivation on  $R$ .

**Remark 3.24.** (1) As in Remarks 3.9, 3.10, any  $F$ -derivation is an  $e$ -dimensional HS-derivation which satisfies the  $F$ -iterativity law.

- (2) Note that a  $G$ -derivation on  $V$  (i.e. a direct system of group scheme actions of  $G[m]$  on  $V$ ) is *not* the same as an algebraic action of  $G$  on  $V$ . Clearly, any algebraic action of  $G$  on  $V$  gives a  $G$ -derivation by restricting the action of  $G$  to  $G[m]$  for each  $m$ . The difference between these two notions is easy to observe for  $R = k[t]$  and  $G = \mathbb{G}_a$ . If  $\mathbb{D}$  is a  $\mathbb{G}_a$ -derivation on  $R$  (i.e. an iterative HS-derivation on  $R$ ), then  $\mathbb{D}$  comes from a  $\mathbb{G}_a$ -action on  $\text{Spec}(R)$  if and only if there is  $n$  such that for all  $i > n$ , we have  $D_i(t) = 0$ .

**Example 3.25.** Let  $R = k[[\mathbf{X}]]$  and  $K = k((\mathbf{X}))$ . Similarly as in [8, Section 3.2], we define a *canonical  $F$ -derivation* on  $R$  and  $K$ . As a  $k$ -algebra map, it is defined on  $R$  as follows

$$\mathbb{D}^F = \text{ev}_F : R \rightarrow R[[Y_1, \dots, Y_e]], \quad \mathbb{D}^F(f) = f(F).$$

By Proposition 3.18,  $\mathbb{D}^F$  uniquely extends to an  $F$ -derivation on  $K$  which we also call canonical and also denote by  $\mathbb{D}^F$ . For any  $m$ , we call  $\mathbb{D}^F[m]$  (on  $R$  or on  $K$ ) a *canonical  $F[m]$ -derivation*.

We point out here that for a given  $\mathfrak{g}$ , there may exist non-isomorphic formal groups  $F_1, F_2$  such that  $F_1[m] = \mathfrak{g} = F_2[m]$ .

**Proposition 3.26.** *The canonical  $F$ -derivation (equivalently,  $F[m]$ -derivation) is strict.*

*Proof.* We introduce the following notation:

$$\partial_1^F = D_{(1,0,\dots,0)}, \dots, \partial_e^F = D_{(0,\dots,0,1)}.$$

Let  $i \leq e$  and  $f \in K$ . By the chain rule, we get

$$(*) \quad \partial_i^F(f) = \left( \frac{\partial F_i}{\partial Y_j}(\mathbf{X}, 0) \right)_{i,j} \cdot \left( \frac{\partial f}{\partial X_1}, \dots, \frac{\partial f}{\partial X_e} \right).$$

Let  $J$  denote the Jacobian matrix appearing in (\*). Then  $J$  is the matrix of the derivative (at  $\mathbf{0}$ ) of the formal map which is the “ $F$ -multiplication by  $\mathbf{X}$ ”. Since this formal map is (formally) invertible, the matrix  $J$  is non-singular. Therefore  $f$  belongs to the field of constants if and only if  $\frac{\partial f}{\partial X_i} = 0$  for each  $i$ . The latter condition occurs if and only if  $f$  is a  $p$ -th power, so the result is proved.  $\square$

In the case when  $F = \widehat{G}$ , we can define a canonical  $F$ -derivation on a localization of a  $k$ -algebra of finite type.

**Example 3.27.** Let  $\mathcal{O}_G$  be the local ring of  $G$  at the identity. Since  $G$  is a smooth variety over  $k$ ,  $\mathcal{O}_G$  is a regular local ring. Let  $\mathbf{x} = (x_1, \dots, x_e)$  be a sequence of local parameters in  $\mathcal{O}_G$ . By [19, Thm 30.6(i)], the ring  $\widehat{\mathcal{O}}_G$  is the power series ring in the variables  $\mathbf{x}$ . If  $F = \widehat{G}$ , then  $F(\mathbf{x}, \mathbf{Y}) \in \mathcal{O}_G[[\mathbf{Y}]]$  (the group action is algebraic!). Hence  $\mathcal{O}_G$  is a  $G$ -subring (after identifying  $\mathbf{x}$  with  $\mathbf{X}$ ) of  $(k[[\mathbf{X}]], \mathbb{D}^F)$ . Therefore the field of rational functions  $k(G)$  has a natural  $G$ -derivation on it which we call the *canonical  $G$ -derivation* on  $k(G)$ . We also get a canonical  $G[m]$ -derivation on  $k(G)$ . If  $G$  is affine, then we also have a canonical  $G$ -derivation on  $k[G]$ . The natural extensions

$$k[G] \subseteq K[[\mathbf{X}]], \quad k(G) \subseteq K((\mathbf{X})),$$

where the local parameters on  $G$  are understood as variables as in [19, Thm 30.6(i)], are  $G$ -extensions by our construction.

**3.4. Strict  $\mathfrak{g}$ -derivations and group scheme actions.** In this subsection we will investigate strict  $\mathfrak{g}$ -rings using group scheme actions. Let us fix  $\mathbb{D}$ , a  $\mathfrak{g}$ -derivation on  $V$ . For the notion of a (free) action of a group scheme on a scheme and its (good) quotient, the reader is advised to consult Section 12 of [23].

**Theorem 3.28.** *We have the following.*

- (1) *The quotient scheme  $V/\mathfrak{g}$  exists.*
- (2) *If  $V = \text{Spec}(R)$ , then  $V/\mathfrak{g} = \text{Spec}(C_{\mathbb{D}})$ , where  $C_{\mathbb{D}}$  is the ring of absolute constants of  $\mathbf{R}$  (see Definition 3.5(3)).*

*Proof.* For (1), we quote [23, Thm 1(A), p. 111].

By the proof of [23, Thm 1(A), p. 111] we have  $V/\mathfrak{g} = \text{Spec}(C')$  where

$$C' = \{r \in R \mid \mathbb{D}(r) = r\}.$$

Clearly  $C'$  coincides with  $C_{\mathbb{D}}$  giving (2). □

**Remark 3.29.** Let  $\mathbb{D}$  be a  $\mathfrak{g}[1]$ -derivation on a field  $K$  with the field of constants  $C$ . Using Proposition 3.20, it is easy to see that if  $x_1, \dots, x_n \in K$  are linearly independent over  $C$ , then  $\mathbb{D}(x_1), \dots, \mathbb{D}(x_n) \in K[\mathbf{v}_1]$  are linearly independent over  $K$ . Therefore the induced  $K$ -linear map

$$\tilde{\mathbb{D}} : K \otimes_C K \rightarrow K[\mathbf{v}_1], \quad \tilde{\mathbb{D}}(a_1 \otimes b_1 + \dots + a_n \otimes b_n) = a_1 \mathbb{D}(b_1) + \dots + a_n \mathbb{D}(b_n)$$

is an embedding. Since we have

$$\dim_K K \otimes_C K = [K : C] \leq p^e, \quad \dim_K K[\mathbf{v}_1] = p^e,$$

the following are equivalent:

- (1)  $[K : C] = p^e$ ,
- (2) the map  $\tilde{\mathbb{D}}$  is onto,
- (3) the map  $\tilde{\mathbb{D}}$  is an isomorphism.

In terms of group scheme actions, the above equivalences mean that the action of  $\mathfrak{g}$  on  $\text{Spec}(K)$  is free if and only if  $[K : C] = p^e$ , and if this action is free, then the corresponding quotient  $\text{Spec}(C) = \text{Spec}(K)/\mathfrak{g}$  is a good quotient. Note that the general theorem about group scheme actions [23, Thm 1(B), p. 112] gives the left-to-right implication above.

We comment below on an interpretation of the notion of strictness using group scheme actions.

**Remark 3.30.** Let  $V^{\text{Fr}^m}$  be  $V$  twisted by the  $m$ -th power of the Frobenius automorphism as in Section 2.1. From the universal property of quotients, there is a unique morphism  $\Psi$  making the following diagram commutative

$$\begin{array}{ccc} V & \xrightarrow{\quad} & V/\mathfrak{g} \\ \text{Fr}_V^m \downarrow & \searrow \Psi & \\ V^{\text{Fr}^m} & & \end{array}$$

If  $V = \text{Spec}(R)$  and  $m = 1$ , then  $\mathbf{R}$  is strict if and only if  $\Psi$  is an isomorphism. It is also easy to see that for a reduced  $R$  and arbitrary  $m$ ,  $\mathbf{R}$  is strict if and only if  $\Psi$  is an isomorphism.

We will need the following result in Section 4.2.

**Lemma 3.31.** *Let  $\mathbb{D}$  be a  $\mathfrak{g}$ -derivation on  $R$  and  $C$  be the ring of constants of  $(R, \mathbb{D})$ . Then we have the following.*

- (1)  $C$  is a  $\mathfrak{g}$ -subring.
- (2) A  $\mathfrak{g}$ -action on  $\text{Spec}(C)$  naturally induces a  $\mathfrak{g}[m-1]^{\text{Fr}}$ -action on  $\text{Spec}(C)$ , hence  $C$  is naturally a  $\mathfrak{g}[m-1]^{\text{Fr}}$ -ring.

*Proof.* We work on the level of group scheme actions. By Theorem 3.28(2), we have  $\text{Spec}(C) = \text{Spec}(R)/\mathfrak{g}[1]$ . As in the case of the usual group actions (one can work it out on the level of rational points), we get the induced action of  $\mathbb{D}$  on  $\text{Spec}(C)$  (since  $\mathfrak{g}[1]$  is normal in  $\mathfrak{g}$ ) giving (1).

For (2), a similar argument gives a natural action of  $\mathfrak{g}/\mathfrak{g}[1]$  on  $\text{Spec}(C)$ . By Remark 2.3, we have

$$\mathfrak{g}[m-1]^{\text{Fr}} \cong \mathfrak{g}/\mathfrak{g}[1],$$

which proves (2). □

**Remark 3.32.** We can describe the  $\mathfrak{g}[m-1]^{\text{Fr}}$ -action on  $\text{Spec}(C)$  from Lemma 3.31(2) more specifically, since it is given by  $(D_{\mathbf{p}\mathbf{j}}|_C)_{\mathbf{j} \in [p^{m-1}]^{\times e}}$ . Hence for any  $c \in C$  and  $\mathbf{i}, \mathbf{j} \in [p^{m-1}]^{\times e}$ , we get the following:

$$D_{\mathbf{p}\mathbf{j}}(D_{\mathbf{p}\mathbf{i}}(c)) = \sum_{\mathbf{k} \in [p^{m-1}]^{\times e}} (c_{\mathbf{i}, \mathbf{j}}^{\mathbf{k}})^p D_{\mathbf{p}\mathbf{k}}(c).$$

The next result (Proposition 3.34) is rather easy in the case of full HS-derivations and turned out to be quite problematic for us in the restricted case. The proof follows the lines of the proof of [13, Fact 2.5], but, in the general case here, a different set of values of the highest order operators needs to be taken (see Remark 3.35). Firstly, we need a general lemma.

**Lemma 3.33.** *For  $i \leq e$  and  $j < m$ , we define  $(p^j)_i \in [p^m]^{\times e}$  as a sequence consisting of zeroes, except for the  $i$ -th coordinate where it has  $p^j$ . Assume  $R$  is a  $\mathfrak{g}$ -ring and let  $\mathcal{P}$  be a subset of  $[p^m]^{\times e}$  such that*

$$\{(p^j)_i \mid i \leq e, j < m\} \subseteq \mathcal{P}.$$

*Then for any  $B \subset R$ , the ideal generated by the set*

$$B_{\mathcal{P}} = \{D_{\mathbf{k}}(b) \mid b \in B, \mathbf{k} \in \mathcal{P}\}$$

*is an HS-ideal.*

*Proof.* It follows from Remark 3.10 and Lemma 3.14. □

**Proposition 3.34.** *Any  $\mathfrak{g}$ -field  $\mathbf{K}$  has a strict  $\mathfrak{g}$ -field extension.*

*Proof.* We consider the theory of  $\mathfrak{g}$ -fields as a universal theory in the language of  $\mathfrak{g}$ -fields (containing  $-$  and  $\div$ ). Then any  $\mathfrak{g}$ -field embeds into an existentially closed  $\mathfrak{g}$ -field. Therefore, it is enough to prove that existentially closed  $\mathfrak{g}$ -fields are strict, so we may assume that  $\mathbf{K}$  is existentially closed. Assume that  $\mathbf{K}$  is not strict, i.e. there is  $a \in K \setminus K^p$  which is a constant of  $\mathbf{K}$ . To reach a contradiction (with the assumption that  $\mathbf{K}$  is existentially closed), it is enough to find a  $\mathfrak{g}$ -extension  $\mathbf{K} \subseteq \mathbf{L}$  such that  $a^{1/p} \in L$ . Let  $C$  denote the field of constants of  $\mathbf{K}$  and  $B$  be a  $p$ -basis of  $C$  over  $K^p$  such that  $a \in B$ .

**Claim 1**

There is a  $\mathfrak{g}[m-1]$ -derivation on  $C^{1/p}$  extending the one we have on  $K$  and such that for each  $b \in B$  and each  $\mathbf{j} \in [p^{m-1}]^{\times e}$ , we have

$$D_{\mathbf{j}}(b^{1/p}) = (D_{p\mathbf{j}}(b))^{1/p}.$$

*Proof of Claim 1.* By Lemma 3.31(2) and Remark 3.32,

$$\mathbb{D}' := (D_{p\mathbf{j}}|_C)_{\mathbf{j} \in [p^{m-1}]^{\times e}}$$

is a  $\mathfrak{g}[m-1]^{\text{Fr}}$ -derivation on  $C$ . Let  $\text{Fr}_C^{-1} : C \cong C^{1/p}$ , and  $\mathbb{D}''$  be  $\mathbb{D}'$  transported to  $C^{1/p}$  using  $\text{Fr}_C^{-1}$ . Then  $\mathbb{D}''$  is a  $\mathfrak{g}[m-1]$ -derivation on  $C^{1/p}$  and by the construction it has the required properties (see also Lemma 4.7 and the proof of Proposition 4.8).  $\square$

We consider the following rings (the set  $B$  indexes the variables):

$$R := K \left[ X_b^{(\mathbf{i})} \mid \mathbf{i} \in [p^m]^{\times e}, b \in B \right],$$

$$R' := K \left[ X_b^{(\mathbf{j})} \mid \mathbf{j} \in [p^{m-1}]^{\times e}, b \in B \right];$$

where for each  $b \in B$ ,  $X_b$  is identified with  $X_b^{(0, \dots, 0)}$ . We put a  $\mathfrak{g}$ -ring structure on  $R$  which is  $\mathfrak{g}$ -extending  $\mathbf{K}$  in the following way:

$$D_{\mathbf{j}} \left( X_b^{(\mathbf{i})} \right) := \sum_{\mathbf{f} \in [p^m]^{\times e}} c_{\mathbf{i}, \mathbf{j}}^{\mathbf{f}} X_b^{(\mathbf{f})}.$$

Then  $R'$  is a  $\mathfrak{g}[m-1]$ -subring of  $R$ . Let us define a subset  $W \subset R'$  as follows:

$$W := \left\{ \left( X_b^{(\mathbf{j})} \right)^p - D_{p\mathbf{j}}(b) \mid \mathbf{j} \in [p^{m-1}]^{\times e}, b \in B \right\}.$$

We define the following  $K$ -algebra map

$$\Psi : R' \rightarrow C^{1/p}, \quad \Psi \left( X_b^{(\mathbf{j})} \right) = D_{p\mathbf{j}}(b)^{1/p}$$

and let  $\mathfrak{m} = \ker(\Psi)$ . By Claim 1,  $\Psi$  is a  $\mathfrak{g}[m-1]$ -map, so  $\mathfrak{m}$  is a maximal  $\mathfrak{g}[m-1]$ -ideal of  $R'$  containing  $W$ . We will show that the  $\mathfrak{g}$ -ideal  $J$  in  $R$  which is  $\mathfrak{g}$ -generated by  $\mathfrak{m}$  is prime (then we can take  $L$  as the field of fractions of  $R/J$ ). Let us order the set  $[p^{m-1}]^{\times e}$  as  $\mathbf{k}_{(1)}, \dots, \mathbf{k}_{(p^{(m-1)e})}$  such that for  $i \leq j$ , we have  $|\mathbf{k}_{(i)}| \leq |\mathbf{k}_{(j)}|$  (in particular  $\mathbf{k}_{(1)} = (0, \dots, 0)$ ). We also order  $B = (b_s)_{s < \kappa}$  such that  $b_0 = a$ .

### Claim 2

There is a set of generators of  $\mathfrak{m}$  consisting of elements of the following two types:

$$\left( X_b^{(\mathbf{j})} \right)^p - D_{p\mathbf{j}}(b), \quad X_{b_s}^{(\mathbf{k}_{(j)})} - \sum_{i=1}^{j-1} \sum_{l=0}^{p-1} \alpha_{t,i,l} \left( X_{b_s}^{(\mathbf{k}_{(i)})} \right)^l - \sum_{t < s} \sum_{\mathbf{j} \in [p^{m-1}]^{\times e}} \beta_{t,\mathbf{j}} X_{b_t}^{(\mathbf{j})};$$

where  $b \in B$ ,  $s < \kappa$ ,  $\mathbf{j} \in [p^{m-1}]^{\times e}$ ,  $j \in \{1, \dots, p^{(m-1)e}\}$  and  $\alpha_{i,l}, \beta_{t,\mathbf{j}} \in K$ .

*Proof of Claim 2.* We construct a required set of generators in  $p^{(m-1)e} \cdot \kappa$  steps.

In Step (0,1), we add  $X^p - b_0$  to the (so far empty) set of generators.

In Step (0,2), we consider two cases.

Case 1:  $D_{p\mathbf{k}_{(2)}}(b_0) \notin K^p(b_0)$ .

In this case, we add the element

$$\left( X_{b_0}^{(\mathbf{k}_{(2)})} \right)^p - D_{p\mathbf{k}_{(2)}}(b_0)$$

to the set of generators.

Case 2:  $D_{p\mathbf{k}(2)}(b_0) \in K^p(b_0)$ .

In this case

$$D_{p\mathbf{k}(2)}(b_0) = \sum_{l=0}^{p-1} \alpha_l^p b_0^l,$$

for some  $\alpha_0, \dots, \alpha_{p-1} \in K$ , and we add the element

$$X_{b_0}^{\mathbf{k}(2)} - \sum_{l=0}^{p-1} \alpha_l^p X_{b_0}^l$$

to the set of generators.

In Step (0,3), we proceed as in Step (0,2) with the field  $K^p(b_0, D_{p\mathbf{k}(2)}(b_0))$  replacing the field  $K^p(b_0)$ .

Continuing like this, after  $p^{(m-1)e}$  steps we obtain our desired set of generators for  $b_0$ . We continue in a similar way (although e.g. Step (1,1) already consist of two cases) for  $(b_i)_{i>0}$ .  $\square$

By Lemma 3.33, it is enough to apply to the generators from Claim 2 the operators  $D_{\mathbf{i}}$ , where  $\mathbf{i} \in [p^{m-1}]^{\times e}$  or where  $\mathbf{i}$  is of the form  $(p^{m-1})_i$  (see Lemma 3.33 for the definition of  $(p^{m-1})_i$ ). If  $\mathbf{i} \in [p^{m-1}]^{\times e}$  then we get elements of  $\mathfrak{m}$ , so we may focus on the other case. To treat the first type of the generators from Claim 2, we just need to use that there is  $\mathbf{l} \in [p^{m-1}]^{\times e}$  such that  $\mathbf{i} = p\mathbf{l}$ . We obtain the following:

$$\begin{aligned} D_{p\mathbf{l}} \left( (X_b^{(j)})^p - D_{p\mathbf{j}}(b) \right) &= \left( D_{\mathbf{l}} \left( X_b^{(j)} \right) \right)^p - D_{p\mathbf{l}} \left( D_{p\mathbf{j}}(b) \right) \\ &= \left( \sum_{\mathbf{k} \in [p^{m-1}]^{\times e}} c_{\mathbf{i}, \mathbf{j}}^{\mathbf{k}} X_b^{(\mathbf{k})} \right)^p - \sum_{\mathbf{k} \in [p^{m-1}]^{\times e}} (c_{\mathbf{i}, \mathbf{j}}^{\mathbf{k}})^p D_{p\mathbf{k}}(b) \\ &= \sum_{\mathbf{k} \in [p^{m-1}]^{\times e}} (c_{\mathbf{i}, \mathbf{j}}^{\mathbf{k}})^p \left( (X_b^{(\mathbf{k})})^p - D_{p\mathbf{k}}(b) \right), \end{aligned}$$

where the second equality holds by Remark 3.32, since  $b \in C$ . Hence we get that  $D_{p\mathbf{l}}((X_b^{(j)})^p - D_{p\mathbf{j}}(b))$  belongs to the ideal generated by  $W$  in  $R'$ , so it also belongs to  $\mathfrak{m}$ .

After applying  $D_{\mathbf{i}}$  to the second type of generators, by Lemma 3.14 we get the following:

$$\begin{aligned} D_{\mathbf{i}} \left( X_{b_s}^{(\mathbf{k}(j))} - \sum_{i=1}^{j-1} \sum_{l=0}^{p-1} \alpha_{i,l} \left( X_{b_s}^{(\mathbf{k}(i))} \right)^l - \sum_{t < s} \sum_{\mathbf{j} \in [p^{m-1}]^{\times e}} \beta_{t,\mathbf{j}} X_{b_t}^{(\mathbf{j})} \right) &= \\ \binom{\mathbf{k}(j) + \mathbf{i}}{\mathbf{i}} X_{b_s}^{(\mathbf{k}(j) + \mathbf{i})} + \sum_{i=1}^{j-1} \sum_{l=0}^{p-1} d_{i,l} \left( X_{b_s}^{(\mathbf{k}(i) + \mathbf{i})} \right)^l + Q, \end{aligned}$$

for some  $d_{i,l} \in K$ , where

$$\binom{\mathbf{i} + \mathbf{j}}{\mathbf{i}} := \binom{i_1 + j_1}{i_1} \cdots \binom{i_e + j_e}{i_e},$$

and where

$$Q \in K \left[ X_{b_t}^{(\mathbf{r})}, X_{b_s}^{(\mathbf{j})} \mid t < s, \mathbf{r} \in [p^m]^{\times e}, \mathbf{j} \in [p^{m-1}]^{\times e} \right].$$



We forget now about the HS-differential structure on  $R$  and  $J$ . The obtained set of generators of  $J$  is of the form  $J_1 \cup J_2$ , where  $J_1 \subseteq \mathfrak{m}$  and  $J_2 \subseteq R'[X_\gamma]_{\gamma \in \mathcal{I}}$  (after renaming variables), and

$$\mathcal{I} := \kappa \times \{1, \dots, e\} \times (\mathbf{k}_i)_{i \in \{1, \dots, p^{(m-1)e}\}}$$

with the lexicographical order. Moreover, there is a subset  $\mathcal{I}_0 \subset \mathcal{I}$  such that without loss of generality (since  $p$  does not divide  $\binom{k_i^{(j)+1}}{i}$ ), we have

$$J_2 = \{X_\gamma - Q_\gamma \mid \gamma \in \mathcal{I}_0\},$$

where for each  $\gamma \in \mathcal{I}_0$ ,  $Q_\gamma \in R'[X_\delta]_{\delta < \gamma}$ . Therefore, the ring  $R/J$  is isomorphic to a polynomial ring over  $R'/\mathfrak{m}$ , so the ideal  $J$  is prime.  $\square$

**Remark 3.35.** (1) The proof above may seem to be technical, but the idea is very simple. For  $\mathbf{j} \in [p^{m-1}]^{\times e}$ , the value  $D_{\mathbf{j}}(a^{1/p})$  is determined by Claim 1. For  $i \leq e$ , we set  $D_{(p^{m-1})_i}(a^{1/p})$  as a new formal variable. The values of the remaining operators on  $a^{1/p}$  are determined by the  $\mathfrak{g}$ -iterativity rule.

(2)

(3) The above proof may be also used to show that a  $\mathfrak{g}$ -field is strict if and only if it is *differentially perfect*, i.e. each of its differential extension is separable. This generalizes a result of Kolchin (see Chapter II, Section 3., Proposition 5.(a) in [12]).

We need one more lemma for the proof of the amalgamation property for a class of  $\mathfrak{g}$ -fields.

**Lemma 3.36.** *Assume that  $\mathbf{R}$  and  $\mathbf{S}$  are  $\mathfrak{g}$ -rings. Then there is a unique  $\mathfrak{g}$ -ring structure on  $R \otimes_k S$  such that the natural maps  $\mathbf{R} \rightarrow \mathbf{R} \otimes_k \mathbf{S}$ ,  $\mathbf{S} \rightarrow \mathbf{R} \otimes_k \mathbf{S}$  are  $\mathfrak{g}$ -homomorphisms.*

*Proof.* It is convenient to show a more general result. Assume that  $V, W$  are schemes over  $k$  and  $\mathbb{D}_V$  and  $\mathbb{D}_W$  are  $\mathfrak{g}$ -derivations on  $V$  and  $W$  respectively. As in the case of the usual group actions, we get a unique  $\mathfrak{g}$ -derivation on  $V \times W$  such that the projections  $V \times W \rightarrow V, W$  are  $\mathfrak{g}$ -invariant. By considering the affine schemes and dualizing, we get what we need.  $\square$

**Proposition 3.37.** *Let  $\mathbf{K} \subseteq \mathbf{L}_1, \mathbf{K} \subseteq \mathbf{L}_2$  be  $\mathfrak{g}$ -field extensions and assume that  $\mathbf{K}$  is strict. Then  $\mathbf{L}_1$  and  $\mathbf{L}_2$  can be  $\mathfrak{g}$ -amalgamated over  $\mathbf{K}$  into a  $\mathfrak{g}$ -field.*

*Proof.* By Proposition 3.18, we can assume that  $L_1, L_2$  are separably closed (since separable algebraic extensions are étale). Then  $K^{\text{sep}}$  is a subfield of  $L_1$  and  $L_2$ . By Remark 3.4(5), it is a  $\mathfrak{g}$ -subfield. By Lemma 3.22 (using Corollary 3.21), the  $\mathfrak{g}$ -field structure on  $K^{\text{sep}}$  is strict. Therefore we can assume that  $K$  is separably closed as well.

The proof will be finished exactly as in [32, Prop. 2.6]. We can assume that  $L_1, L_2$  are subfields of a big field  $\Omega$  and that they are algebraically disjoint over  $K$ . By Lemma 3.22, the extension  $K \subseteq L_1$  is separable. Since  $K$  is separably closed, this extension is regular (see [15, p. 367]). By [15, Thm. VIII 4.12],  $L_1$  and  $L_2$  are linearly disjoint over  $K$ , thus  $L_1 \otimes_K L_2$  is a domain. By Lemma 3.36, there is a  $\mathfrak{g}$ -structure on  $L_1 \otimes_K L_2$  extending those on  $L_1$  and  $L_2$ . By Proposition 3.18 again, we get the required  $\mathfrak{g}$ -structure on the field of fractions of  $L_1 \otimes_K L_2$ .  $\square$

## 4. MODEL COMPANIONS

In this section we turn our attention to the model-theoretic properties of (truncated) HS-fields. Our results here generalize the corresponding results from [32] and [13], and our proofs do not differ much.

**4.1. Existentially closed  $\mathfrak{g}$ -fields.** In this subsection, we assume that  $\mathfrak{g}$  is of the form  $W[m]$  for a formal group law  $W$  (see Remark 2.2).

Let  $K$  be a field of characteristic  $p$  and  $\lambda$  be the following  $p$ -th root function:

$$\lambda : K \rightarrow K, \quad \lambda(x) = \begin{cases} x^{1/p} & \text{for } x \in K^p, \\ 0 & \text{for } x \notin K^p. \end{cases}$$

We introduce several languages.

- Let  $L^\lambda$  be the language of rings expanded by a unary function symbol  $\lambda$ .
- Let  $L_{e,m}$  be the language of  $k$ -algebras (so there are constants in the language for the elements of  $k$ ) with  $m$ -truncated  $e$ -dimensional HS-derivations.
- Let  $L_{e,m}^\lambda = L^\lambda \cup L_{e,m}$ .

**Lemma 4.1.** *Each field of characteristic  $p$  has a natural  $L^\lambda$ -structure and we have the following.*

- (1) *A field extension  $K \subseteq L$  is an  $L^\lambda$ -extension if and only if  $L^p \cap K = K^p$ .*
- (2) *If  $\mathbf{K} \subseteq \mathbf{L}$  is an  $L_{e,m}$ -extension and  $\mathbf{K}$  is strict, then  $\mathbf{K} \subseteq \mathbf{L}$  is an  $L_{e,m}^\lambda$ -extension.*
- (3) *Suppose  $R$  is a subring of a field  $L$ ,  $K$  is the field of fractions of  $R$  and  $R \subseteq L$  is an  $L^\lambda$ -extension. Then  $K \subseteq L$  is an  $L^\lambda$ -extension.*

*Proof.* The item (1) is clear and (2) follows from Lemma 3.22(2). The last item follows by an easy computation.  $\square$

We need the following well-known description of elementary extensions of separably closed fields.

**Lemma 4.2.** *Let us assume that  $\mathbf{K}$  and  $\mathbf{L}$  are  $\mathfrak{g}$ -fields such that  $K$  and  $L$  are separably closed and that  $K$  has finite imperfection degree. Then the following are equivalent.*

- (1) *The fields  $K$  and  $L$  have the same (absolute)  $p$ -basis.*
- (2) *The  $K$ -algebra  $L$  is étale.*
- (3) *The extension  $K \subseteq L$  is elementary (in the language of rings).*
- (4) *The extension  $\mathbf{K} \subseteq \mathbf{L}$  is  $L_{e,m}^\lambda$ -elementary.*
- (5) *The extension  $\mathbf{K} \subseteq \mathbf{L}$  is  $L_{e,m}$ -elementary.*

*Proof.* By the proof of [4, Theorem 2.1] and by [4, Claim 2.2], the extension  $K \subseteq L$  is elementary if and only if  $K$  and  $L$  have the same (absolute)  $p$ -basis. By [19, Theorem 26.7], it happens if and only if this extension is étale, so we get the equivalence of (1), (2) and (3).

Since both the  $\lambda$ -function and the  $\mathfrak{g}$ -derivation are defined (over the field of the  $p^m$ -th powers) using the field operations and the elements of a  $p$ -basis, we get the equivalence of (3) with (4) and (5).  $\square$

We introduce now several theories.

- Let  $\mathfrak{g} - \text{DF}$  be the theory of  $\mathfrak{g}$ -fields in the language  $L_{e,m}$ .
- Let  $\mathfrak{g} - \text{DF}_\lambda$  be the theory of strict  $\mathfrak{g}$ -fields in the language  $L_{e,m}^\lambda$  i.e.  $\mathfrak{g} - \text{DF}_\lambda$  contains the natural interpretation of  $\lambda$  and the following extra axiom:

$$\forall x \left( (x \neq 0 \wedge \lambda(x) = 0) \rightarrow (D_{(1,0,\dots,0)}(x) \neq 0 \vee \dots \vee D_{(0,\dots,0,1)}(x) \neq 0) \right).$$

- Let  $\mathfrak{g} - \text{DCF}$  be the theory  $\mathfrak{g} - \text{DF}$  with the extra axioms for strict  $\mathfrak{g}$ -fields, and for separably closed fields of imperfectness degree  $e$ .
- Similarly for  $\mathfrak{g} - \text{DCF}_\lambda$ .

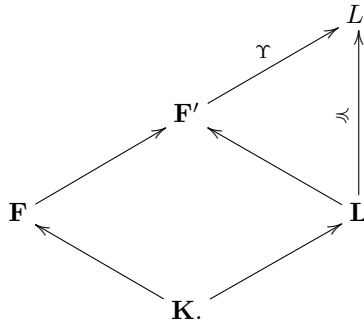
**Lemma 4.3.** *The theories  $\mathfrak{g} - \text{DCF}$  and  $\mathfrak{g} - \text{DCF}_\lambda$  are consistent.*

*Proof.* We take the canonical  $F$ -derivation  $\mathbb{D}^F$  on the field  $K$  from Example 3.25. By Proposition 3.26,  $\mathbf{K}$  is strict and clearly the imperfection degree of  $K$  is  $e$ . By Proposition 3.18,  $\mathbb{D}^F$  extends to the separable closure of  $K$  (a separable algebraic extension is étale, see [19, Thm. 26.7]). By Lemma 3.22(3), this extension is still strict. Since it is étale, the degree of imperfection does not change.  $\square$

The main technical result needed for quantifier elimination is the proposition below. It does not differ much from [32, 3.1] where the case of full (i.e. non-truncated) HS-derivations is considered. For reader's convenience we include a proof following the lines of the proof of [32, 3.1].

**Proposition 4.4.** *Let us take  $\mathbf{L} \models \mathfrak{g} - \text{DCF}_\lambda$ ,  $\mathbf{F}$  being a strict  $\mathfrak{g}$ -field and assume that  $\mathbf{K}$  is an  $L_{e,m}^\lambda$ -substructure of both  $\mathbf{F}$  and  $\mathbf{L}$ . Then there is an  $L_{e,m}^\lambda$ -embedding of  $\mathbf{F}$  over  $\mathbf{K}$  into an elementary extension of  $\mathbf{L}$ .*

*Proof.* By Remark 3.4(1), Proposition 3.18 and Lemma 4.1(3), we can assume that  $K$  is a field. By Lemma 4.1(1), we have  $K^p = L^p \cap K$ . Since  $\mathbf{L} \models \mathfrak{g} - \text{DCF}_\lambda$ ,  $\mathbf{L}$  is strict and hence  $\mathbf{K}$  is strict as well. By Proposition 3.37 and Lemma 4.1(2), we can  $L_{e,m}^\lambda$ -amalgamate  $\mathbf{F}$  and  $\mathbf{L}$  over  $\mathbf{K}$  into a strict  $\mathfrak{g}$ -field  $\mathbf{F}'$ . Since the extension  $L \subseteq F'$  is separable, by [4, Claim 2.2] there is an elementary extension in the language of fields  $L \preceq L'$  and a field embedding  $\Upsilon : F' \rightarrow L'$  over  $L$ . The situation is described in the following diagram:



By Lemma 4.2, the extension  $L \subseteq L'$  is étale. The  $\mathfrak{g}$ -field  $\mathbf{F}'$  is strict, so by Corollary 3.21, we have  $[F' : (F')^p] \leq p^e$ . Since the extension  $L \subseteq F'$  is separable and  $[L : L^p] = p^e$ , by the equivalence between (1) and (2) in Lemma 4.2, the extension  $L \subseteq F'$  is étale. Then the extension  $F' \subseteq L'$  is étale as well. By Proposition 3.18, there is a  $\mathfrak{g}$ -derivation on  $L'$  extending the one on  $F'$  (hence also extending the one on  $L$ ). By Lemma 4.2, the extension  $\mathbf{L} \subseteq \mathbf{L}'$  is  $L_{e,m}^\lambda$ -elementary and we are done.  $\square$

We are ready to prove the main result of this subsection.

**Theorem 4.5.** *We have the following.*

- (1) *The theory  $\mathfrak{g} - \text{DCF}_\lambda$  has quantifier elimination in the language  $L_{e,m}^\lambda$ .*
- (2) *Each model of  $\mathfrak{g} - \text{DF}$  embeds into a model of  $\mathfrak{g} - \text{DCF}$ .*
- (3) *The theory  $\mathfrak{g} - \text{DCF}$  is a model companion of the theory  $\mathfrak{g} - \text{DF}$ .*
- (4) *The theory  $\mathfrak{g} - \text{DCF}_\lambda$  is a model completion of the theory  $\mathfrak{g} - \text{DF}_\lambda$ .*

*Proof.* For (1), we use the criterion from [25, Theorem 13.1] (and Proposition 4.4) exactly as in [32, 3.1].

For (2), let us take any  $\mathfrak{g}$ -field  $\mathbf{F}$ . By Proposition 3.34, we may assume that  $\mathbf{F}$  is strict. By Lemma 4.3, there is  $\mathbf{L} \models \mathfrak{g} - \text{DCF}_\lambda$ . Clearly,  $k$  with the trivial  $\mathfrak{g}$ -structure is a common  $L_{e,m}^\lambda$ -substructure of both  $\mathbf{F}$  and  $\mathbf{L}$ . By Proposition 4.4,  $\mathbf{F}$  embeds into an elementary extension of  $\mathbf{L}$ , which is clearly a model of  $\mathfrak{g} - \text{DCF}_\lambda$  as well.

By (1),  $\mathfrak{g} - \text{DCF}_\lambda$  is model complete, so using Lemma 4.1(2) and Lemma 4.2, we get that  $\mathfrak{g} - \text{DCF}$  is model complete as well. By (2),  $\mathfrak{g} - \text{DCF}$  is a model companion of the theory  $\mathfrak{g} - \text{DF}$ , so we get (3).

By Proposition 3.37 and the item (1), we get (4).  $\square$

- Remark 4.6.** (1) The theory  $\mathfrak{g} - \text{DF}$  does not have the amalgamation property. The theory  $\mathfrak{g} - \text{DCF}$  does not have quantifier elimination and the theory  $\mathfrak{g} - \text{DCF}$  is not a model completion of the theory  $\mathfrak{g} - \text{DF}$ .
- (2) We have (after taking  $k = \mathbb{F}_p$ )

$$\mathbb{G}_a^e[m] - \text{DCF} = \text{SCH}_{p,e,m},$$

where  $\text{SCH}_{p,e,m}$  is the theory considered in [13].

- (3) If we take the algebraic group  $U$  from Example 3.12(2), then a  $U(1)$ -field is the same as a field with two derivations  $\partial_1, \partial_2$  such that  $\partial_1^{(p)} = \partial_2$  and  $\partial_2^{(p)} = 0$ . Hence  $U(1) - \text{DCF}$  corresponds to Wood's theory 2 - DCF, see [31]. It should be possible to find algebraic groups governing the iterative rules for Wood's theories  $m - \text{DCF}$  for an arbitrary  $m$ .
- (4) After dropping the iterativity assumptions rather strange things happen. In the case of characteristic zero, model companions exist and are analyzed in [22]. In the case of positive characteristic, it is shown in [22, Prop 7.2] that (in our terminology) the theory of fields with  $m$ -truncated  $e$ -dimensional HS-derivations has a model companion if and only if  $m = 1$ .

**4.2. Existentially closed  $F$ -fields.** Let  $L_e$  be the language of  $k$ -algebras with  $e$ -dimensional HS-derivations. The main model-theoretic advantage of HS-derivations (over truncated HS-derivations) is that we do not need to consider the extra operator  $\lambda$  to get quantifier elimination results.

We define two  $L_e$ -theories.

- Let  $F - \text{DF}$  be the theory of  $F$ -fields.
- Let  $F - \text{DCF}$  be the theory  $F - \text{DF}$  with the extra axioms for strict  $F$ -fields, and for separably closed fields of imperfection degree  $e$ .

The main algebraic difference between  $\mathfrak{g}$ -derivations and  $F$ -derivations is given by the proposition below which generalizes [32, Lemma 2.4]. First we need an obvious lemma which is a general fact about group scheme actions.

**Lemma 4.7.** *Let  $f \in \text{Aut}(k)$  and let  $\varphi : R \rightarrow S$  be an isomorphism of rings extending  $f$ . For any  $\mathfrak{g}$ -derivation  $\mathbb{D}$  on  $R$ , we define:*

$$\mathbb{D}^\varphi : S \rightarrow S[\mathbf{v}_m], \quad \mathbb{D}^\varphi := \varphi[\mathbf{v}_m] \circ \mathbb{D} \circ \varphi^{-1}.$$

*Then  $\mathbb{D}^\varphi$  is a  $\mathfrak{g}^f$ -derivation, where  $\mathfrak{g}^f$  is the group scheme  $\mathfrak{g}$  twisted by  $f$ .*

**Proposition 4.8.** *Let  $\mathbf{K} = (K, \mathbb{D})$  be an  $F$ -field. Then there is a smallest strict  $F$ -field extending  $\mathbf{K}$ .*

*Proof.* Let  $C$  be the field of constants of  $\mathbf{K}$ . It is enough to show that there is a unique  $F$ -derivation  $\mathbb{D}'$  on  $C^{1/p}$  extending  $\mathbb{D}$ . By Lemma 3.31(1),  $C$  is an  $F$ -subfield of  $K$ . For  $\mathbf{i} \in \mathbb{N}^e$  and  $a \in C^{1/p}$ , we have the only option (as in [32, Lemma 2.4]):

$$D'_{\mathbf{i}}(a) := (D_{\mathbf{p}\mathbf{i}}(a^p))^{1/p}.$$

Clearly, each  $D'_{\mathbf{i}}$  extends  $D_{\mathbf{i}}$ . We need to show that  $\mathbb{D}' = (D'_{\mathbf{i}})_{\mathbf{i} \in \mathbb{N}^e}$  is an  $F$ -derivation. By Lemma 3.31(2), the sequence of maps

$$\mathbb{D}'' := (D_{\mathbf{p}\mathbf{i}}(b))_{\mathbf{i} \in [p^m]^e}$$

is an  $F[m-1]^{\text{Fr}}$ -derivation on  $C$ . It is easy to see that  $\mathbb{D}'[m-1]$  coincides with  $\mathbb{D}''$  “transported” to  $C^{1/p}$  using the ring isomorphism  $\text{Fr}_C^{-1} : C \rightarrow C^{1/p}$ . By Lemma 4.7,  $\mathbb{D}'[m-1]$  is an  $F[m-1]$ -derivation. Since it happens for all  $m \in \mathbb{N}$ , we get that  $\mathbb{D}'$  is an  $F$ -derivation.  $\square$

Proceeding similarly as in the proof of [32, Prop. 2.6] (or Proposition 3.37) and using Proposition 4.8 one shows the following.

**Proposition 4.9.** *The class of  $F$ -fields has the amalgamation property.*

We can conclude now as in Section 4.1.

**Theorem 4.10.** *The theory  $F$  – DCF is a model completion of the theory  $F$  – DF (so it eliminates quantifiers).*

**Remark 4.11.** (1) The extra property which makes the theory  $F$  – DF nicer than the theory  $\mathfrak{g}$  – DF is the existence of the *smallest* strict extensions (Proposition 4.8). It gives the amalgamation property for *all* (i.e. not necessarily strict)  $F$ -fields (Proposition 4.9) and the quantifier elimination for  $F$  – DCF.

(2) In this context, quantifier elimination for  $F$  – DCF implies elimination of imaginaries for  $F$  – DCF exactly as in Section 4 of [32].

**Theorem 4.12.** *The theories  $F[m]$  – DCF form an increasing chain and we have*

$$F - \text{DCF} = \bigcup_{m=1}^{\infty} F[m] - \text{DCF}.$$

*Proof.* It follows just by inspecting the axioms of the theories in question.  $\square$

**4.3. Bi-interpretability with a theory of separably closed fields.** Clearly, each model of  $F$  – DCF restricts to a model of  $\text{SCF}_{p,e}$ . In this subsection, we discuss the opposite problem: can any model of  $\text{SCF}_{p,e}$  be expanded to a model of  $F$  – DCF? The same question can be asked for  $\mathfrak{g}$  in place of  $F$ . Ziegler showed in [32] that the answer is affirmative for  $F = \widehat{\mathbb{G}}_a^e$ . The second author showed the same in [13] for  $\mathfrak{g} = \mathbb{G}_a^e[m]$ . In this subsection, we generalize the above results to the case when  $F$  is of the form  $\widehat{G}$  and  $\mathfrak{g}$  of the form  $G[m]$ .

We actually show more, i.e. we will see that (after adding some extra constants) the theory  $G - \text{DCF}$  is *extension by definitions* (see [27, page 59]) of the theory  $\text{SCF}_{p,e}$ .

By  $L$ , we denote the language of  $k$ -algebras, and by  $\text{SCF}_{p,e}$ , the theory of separably closed  $k$ -algebras with the degree of imperfection  $e$  in the language  $L$  (so our notation does not reflect the dependence on  $k$ , we hope it will not cause any confusion). Recall that  $L_e$  denotes the language of  $k$ -algebras with  $e$ -dimensional HS-derivations. We introduce two new languages (obtained after adding  $e$  extra constant symbols):

$$L^{\mathbf{b}} := L \cup \{b_1, \dots, b_e\}, \quad L_e^{\mathbf{b}} := L_e \cup \{b_1, \dots, b_e\}.$$

Let  $\beta$  be a sentence in the language  $L^{\mathbf{b}}$  saying that  $b_1, \dots, b_e$  form a  $p$ -basis. Now we add  $\beta$  to the theory  $\text{SCF}_{p,e}$  and to the theory  $F - \text{DCF}$  to obtain the theory

$$\text{SCF}_{p,e}^{\mathbf{b}} := \text{SCF}_{p,e} \cup \{\beta\}$$

in the language  $L^{\mathbf{b}}$ , and the theory

$$F - \text{DCF}^{\mathbf{b}} := F - \text{DCF} \cup \{\beta\}$$

in the language  $L_e^{\mathbf{b}}$ .

**Lemma 4.13.** *There are  $x_1, \dots, x_e \in k(G)$  algebraically independent over  $k$  such that the field extension  $k(x_1, \dots, x_e) \subseteq k(G)$  is finite and separable.*

*Proof.* Let  $x_1, \dots, x_e \in \mathcal{O}_G$  be a sequence of local parameters (see Example 3.27). By Example 3.27, [19, 30.6(ii)] and Proposition on page 276 of [17],  $\{x_1, \dots, x_e\}$  is a  $p$ -basis of  $\mathcal{O}_G$ , so it is also a  $p$ -basis of  $k(G)$ . Hence the field extension  $k(x_1, \dots, x_e) \subseteq k(G)$  is finite and separable.  $\square$

Let  $x_1, \dots, x_e$  be as in Lemma 4.13. By Abel's theorem, there is  $y \in k(G)$  such that  $k(G) = k(x_1, \dots, x_e, y)$ . Let  $H(X_1, \dots, X_e, Y) \in k[X_1, \dots, X_e, Y]$  be such that  $H(x_1, \dots, x_e, y) = 0$  and the polynomial  $H(x_1, \dots, x_e, Y)$  is irreducible.

We need to add one more constant to the languages we consider to obtain the following languages:

$$L^{\mathbf{b},c} := L \cup \{b_1, \dots, b_e, c\}, \quad L_e^{\mathbf{b},c} := L_e \cup \{b_1, \dots, b_e, c\}.$$

The meaning of this extra constant  $c$  is that it generates the field  $k(G)$  over  $k$  extended by the chosen  $p$ -basis. Formally, we specify one more axiom  $\gamma$  in the language  $L^{\mathbf{b},c}$

$$\gamma := \beta \wedge (H(b_1, \dots, b_e, c) = 0).$$

We define the following theories.

$$\text{SCF}_{p,e}^{\mathbf{b},c} := \text{SCF}_{p,e} \cup \{\gamma\}, \quad F - \text{DCF}^{\mathbf{b},c} := F - \text{DCF} \cup \{\gamma\}.$$

**Theorem 4.14.** *The theory  $G - \text{DCF}^{\mathbf{b},c}$  is an extension by definitions of the theory  $\text{SCF}_{p,e}^{\mathbf{b},c}$ .*

*Proof.* Take  $x_1, \dots, x_e \in k(G)$  as in Lemma 4.13, denote  $(x_1, \dots, x_e)$  by  $\mathbf{x}$  and let  $y \in k(G)$  be separable algebraic over  $k(\mathbf{x})$  such that  $k(\mathbf{x}, y) = k(G)$  (such  $y$  exists by Lemma 4.13 and Abel's theorem). Then for any  $\mathbf{i}, \mathbf{j} \in \mathbb{N}^e$ , there are polynomials  $F_{\mathbf{j},\mathbf{i}}, H_{\mathbf{j},\mathbf{i}} \in k[\mathbf{X}, Y]$  such that for the canonical  $F$ -derivation  $\mathbb{D}^F = (D_{\mathbf{j}}^F)_{\mathbf{j} \in \mathbb{N}^e}$  on  $k(G)$ , we have

$$D_{\mathbf{j}}^F(\mathbf{x}^{\mathbf{i}}) = \frac{F_{\mathbf{j},\mathbf{i}}(\mathbf{x}, y)}{H_{\mathbf{j},\mathbf{i}}(\mathbf{x}, y)} \in k(G).$$

We describe now an extension by definitions of the theory  $\text{SCF}_{p,e}^{\mathbf{b},c}$  coinciding with the theory  $G\text{-DCF}^{\mathbf{b},c}$ . To ease the notation, we will also denote by  $\mathbf{b}$  the tuple (of constant symbols or elements of a model)  $(b_1, \dots, b_e)$ . Take  $\mathbf{j} = (j_1, \dots, j_e) \in \mathbb{N}^e$ , for every  $n \geq \max\{j_1, \dots, j_e\}$  we add to the theory  $\text{SCF}_{p,e}^{\mathbf{b},c}$  the following defining axiom

$$(\clubsuit) \quad D_{\mathbf{j}}(x) = y \leftrightarrow \left( \exists^{i \in [p^n]^e} \alpha_i \right) \left( x = \sum_{i \in [p^n]^e} \alpha_i^{p^n} \mathbf{b}^i \wedge y = \sum_{i \in [p^n]^e} \alpha_i^{p^n} \frac{F_{\mathbf{j},i}(\mathbf{b}, c)}{H_{\mathbf{j},i}(\mathbf{b}, c)} \right).$$

Take any  $(K, \mathbf{b}, c) \models \text{SCF}_{p,e}^{\mathbf{b},c}$ . It is not hard to verify that the defining axioms  $(\clubsuit)$  determine well-defined functions on  $K$ . The axioms  $\beta, \gamma$  guarantee that

$$k(\mathbf{b}, c) \cong_k k(G)$$

and that  $\mathbb{D} := (D_{\mathbf{j}})_{\mathbf{j} \in \mathbb{N}^e}$  restricted to  $k(\mathbf{b}, c)$  corresponds to the canonical  $G$ -derivation on  $k(G)$ . Because  $\mathbf{b}$  is a  $p$ -basis of  $K$ , the extension  $k(\mathbf{b}) \subseteq K$  is étale (see [19, Theorem 26.8]). Hence the extension  $k(\mathbf{b}, c) \subseteq K$  is also étale. Due to Proposition 3.3, we can extend the canonical  $G$ -derivation from  $k(G)$  to the field  $K$ . Let  $\mathbb{D}' = (D'_{\mathbf{j}})_{\mathbf{j} \in \mathbb{N}^e}$  denote the  $G$ -derivation on  $K$  extending the canonical  $G$ -derivation on  $k(G)$ .

Note that  $D'_{\mathbf{j}}(x) = D_{\mathbf{j}}(x)$  for every  $x \in K$ , hence  $\mathbb{D}' = \mathbb{D}$ . Moreover the canonical  $G$ -derivation on  $k(G)$  is strict, so also  $\mathbb{D}'|_{k(\mathbf{b},c)}$  is strict. Lemma 3.22 implies that  $\mathbb{D}' = \mathbb{D}$  is strict, so  $(K, \mathbb{D}, \mathbf{b}, c) \models G\text{-DCF}^{\mathbf{b},c}$ .  $\square$

**Remark 4.15.** In many cases, the theory  $G\text{-DCF}^{\mathbf{b}}$  is an extension by definitions of the theory  $\text{SCF}_{p,e}^{\mathbf{b}}$ , so in such cases the constant symbol  $c$  is not necessary. For example, it is the case for  $G$  being the group of Witt vectors, see [7].

It is unclear to us how to proceed in the case of an arbitrary formal group  $F$ . The crucial question is whether the canonical derivation on  $k((\mathbf{X}))$  can be restricted to  $k(\mathbf{X})$  or to  $k(\mathbf{X})^{\text{sep}}$ . This question has been investigated in [9] (it is related to Matsumura's *integrability question*). To prove a partial result (Theorem 4.17), we need the following lemma.

**Lemma 4.16.** *Assume that  $F_1$  and  $F_2$  are one-dimensional formal group laws over  $k$  such that  $F_1 \cong F_2$ . Then the theory  $F_1\text{-DCF}$  is an extension by definitions of the theory  $F_2\text{-DCF}$ .*

*Proof.* Let  $f \in Xk[[X]]$  be an isomorphism between  $F_1$  and  $F_2$ . For any  $F_1$ -derivation  $\mathbb{D} : K \rightarrow K[[X]]$ , the following composition

$$K \xrightarrow{\mathbb{D}} K[[X]] \xrightarrow{\text{ev}_f} K[[X]]$$

is an  $F_2$ -derivation. It is easy to see that for each positive integer  $n$ , there are  $c_{n,1}, \dots, c_{n,n} \in k$  such that if  $\mathbb{D} = (D_i)_{i \in \mathbb{N}}$  then the corresponding  $F_2$ -derivation  $\text{ev}_f \circ \mathbb{D}$  is of the form

$$(\text{id}, c_{1,1}D_1, c_{2,1}D_1 + c_{2,2}D_2, \dots),$$

hence the result follows.  $\square$

Using [11] and [1] (which we needed to prove the crucial [9, Thm. 4.3]), we can now show the following.

**Theorem 4.17.** *Suppose that  $F$  is a one-dimensional formal group law over an algebraically closed field  $k$  (in particular  $e = 1$ ). Then the theory  $F - \text{DCF}^{\mathbf{b}}$  is an extension by definitions of the theory  $\text{SCF}_{p,1}^{\mathbf{b}}$ .*

*Proof.* By [9, Thm. 4.3], there is a formal group law  $\tilde{F}$  over  $k$  such that  $F \cong \tilde{F}$  and the canonical  $\tilde{F}$ -derivation restricts to  $k[X]$ . By Lemma 4.16, we can assume that  $F = \tilde{F}$ . We can repeat now the proof of Theorem 4.14 (and we do not need to worry about the extra constant  $c$ ).  $\square$

**Remark 4.18.** Passing from the base field  $k$  to its algebraic closure expands the language with extra constants. But any existentially closed  $F$ -field is separably closed, so its field of absolute constants contains  $k^{\text{alg}}$ . Hence such an expansion is not important for the theories we consider, since the models of  $F - \text{DCF}$  in the language with constants for elements of  $k$  are the same as models of  $F - \text{DCF}$  in the language with constants for elements of  $k^{\text{alg}}$ . Therefore, the assumption in Theorem 4.17 that  $k$  is algebraically closed is harmless.

## 5. GEOMETRIC AXIOMS

In this section, we give geometric axioms for the theories  $\mathfrak{g} - \text{DCF}$  and  $F - \text{DCF}$ . The presentation follows the one in [13], however (unlike in [13]) we notice here that the existence of canonical  $p$ -bases (see Section 6.1) is *not* necessary for the geometric axioms. We do *not* assume in this section that  $\mathfrak{g}$  is of the form  $W[m]$  for a formal group law  $W$ .

**5.1. Prolongation and comultiplication.** The notions introduced in this subsection are special cases of the notions considered in [21]. These notions originate from Buium [2] and also appeared (among others) in [24] and [14].

We fix a field  $K$  with a  $\mathfrak{g}$ -derivation  $\mathbb{D}$ . Our first definitions do not use the  $\mathfrak{g}$ -iterativity condition.

- Let  $\mathcal{D}$  be the functor from the category of  $K$ -algebras to the category of  $K[\mathbf{v}_m]$ -algebras defined in the following way:

$$\mathcal{D}(R) = R \otimes_{K, \mathbb{D}} K[\mathbf{v}_m].$$

Since  $\mathcal{D}$  commutes with localizations, it also defines a functor from  $K$ -schemes to  $K[\mathbf{v}_m]$ -schemes.

- The functor  $\mathcal{D}$  considered as a functor from  $K$ -algebras to  $K$ -algebras has a left-adjoint functor  $\nabla$  which extends to  $K$ -schemes. A crucial natural bijection is the following one:

$$(\nabla V)(R) \longleftrightarrow V(\mathcal{D}(R)).$$

- For any  $K$ -scheme  $V$  we have a (non-algebraic!) map

$$\mathbb{D}_V : V(K) \rightarrow V(\mathcal{D}(K)) = \nabla V(K)$$

induced by the  $K$ -algebra homomorphism  $\mathbb{D} : K \rightarrow K[\mathbf{v}_m] = \mathcal{D}(K)$ .

**Remark 5.1.** Our notation here differs from the notation used in [2] and [21], where the left-adjoint functor considered above is denoted  $\tau$ , and the notation  $\nabla$  is used for  $\mathbb{D}_V$ .

The second set of definitions uses the  $\mathfrak{g}$ -iterativity condition.



- We have a natural transformation (of functors on the category of  $K$ -algebras) given by the Hopf algebra comultiplication (coming from  $\mathfrak{g}$ )

$$\mu : \mathcal{D} \rightarrow \mathcal{D} \circ \mathcal{D}.$$

- We define a natural transformation of functors on the category of  $K$ -schemes

$$c : \nabla \rightarrow \nabla \circ \nabla$$

using the commutative diagram below

$$\begin{array}{ccc} V(\mathcal{D}(R)) & \xrightarrow{V(\mu)} & V(\mathcal{D}(\mathcal{D}(R))) \\ \cong \uparrow & & \cong \uparrow \\ \nabla V(R) & \xrightarrow{c_V} & \nabla(\nabla V)(R). \end{array}$$

Below we give explicit descriptions of the maps  $\mathbb{D}_V$  and  $c_V$ .

For any positive integer  $n$ , our HS-derivation  $\mathbb{D}$  naturally extends to the following HS-derivation

$$\left( D_{\mathbf{j}} : K[X_1, \dots, X_n] \rightarrow K[X_1^{(\mathbf{i})}, \dots, X_n^{(\mathbf{i})} \mid \mathbf{i} \in [p^m]^e] \right)_{\mathbf{j} \in [p^m]^e}, \quad \mathbb{D}_{\mathbf{j}}(X) = X^{(\mathbf{j})},$$

where  $X_k^{(\mathbf{0})} = X_k$  and for  $\mathbf{j} \neq \mathbf{0}$ ,  $X_k^{(\mathbf{j})}$  is a new variable. We will use the following notation

$$K\{X_1, \dots, X_n\} := K[X_1^{(\mathbf{i})}, \dots, X_n^{(\mathbf{i})} \mid \mathbf{i} \in [p^m]^e].$$

If  $R = K[X_1, \dots, X_n]/I$ , then  $\nabla(R) = K\{X_1, \dots, X_n\}/(\mathbb{D}(I))$ . Hence, for an affine variety  $V = \text{Spec}(R)$ , the variety  $\nabla(V)$  is defined by the ideal  $(\mathbb{D}(I))$  and  $\mathbb{D}_V$  is given in coordinates as the  $n$ -th Cartesian product of  $\mathbb{D}$  (considered as a map from  $K$  to  $K^{p^m}$ ).

Let  $c_n$  denote  $c_{\mathbb{A}^{np^m}}$ . For every  $(b_{\mathbf{i},1}, \dots, b_{\mathbf{i},n})_{\mathbf{i} \in [p^m]^e} \in K^{np^m}$  we have

$$c_n \left( (b_{\mathbf{i},1}, \dots, b_{\mathbf{i},n})_{\mathbf{i} \in [p^m]^e} \right) = \left( \sum_{\mathbf{k} \in [p^m]^e} c_{\mathbf{i},\mathbf{j}}^{\mathbf{k}} b_{\mathbf{k},1}, \dots, \sum_{\mathbf{k} \in [p^m]^e} c_{\mathbf{i},\mathbf{j}}^{\mathbf{k}} b_{\mathbf{k},n} \right)_{\mathbf{i},\mathbf{j} \in [p^m]^e},$$

where  $c_{\mathbf{i},\mathbf{j}}^{\mathbf{k}}$  are the “structural constants” from Remark 3.10. We will need the following.

**Lemma 5.2.** *Let  $V$  be a  $K$ -scheme and suppose that  $(K, \mathbb{D}) \subseteq (L, \mathbb{D}')$  is an extension of  $m$ -truncated  $e$ -dimensional HS-fields. Then for any  $a \in V(L)$ , we have  $\mathbb{D}'_V(a) \in \nabla V(L)$ .*

*Proof.* It is enough to notice that if  $\mathbb{D}'$  extends  $\mathbb{D}$ , then the  $k$ -algebra map  $\mathbb{D}' : L \rightarrow \mathbb{D}'(L)$  is  $K$ -linear.  $\square$

The following lemma corresponds to [13, Lemma 1.1(ii)] and is a direct consequence of the  $\mathfrak{g}$ -iterativity condition.

**Lemma 5.3.** *For any  $K$ -scheme  $V$  we have the following:*

$$\mathbb{D}_{\nabla(V)} \circ \mathbb{D}_V = c_V \circ \mathbb{D}_V.$$

Let us fix a  $|K|^+$ -saturated algebraically closed field  $\Omega$  containing  $K$ . We want to describe possible extensions of  $\mathbb{D}$  to subfields of  $\Omega$  in terms of the functor  $\nabla$ . Let  $b_0 \in \Omega^n$ ,  $b = (b_0, \dots, b_{p^{m_e}-1}) \in \Omega^{np^{m_e}}$  and we set

$$V = \text{locus}_K(b_0), \quad W = \text{locus}_K(b).$$

As in [13, Lemma 3.3], we can show the following.

**Lemma 5.4.** *If  $b \in \nabla V(\Omega)$  and  $K(b_0) = K(b)$ , then there is an  $m$ -truncated  $e$ -dimensional HS-derivation  $\mathbb{D}'$  on  $K(b)$  extending  $\mathbb{D}$  such that  $\mathbb{D}'_V(b_0) = b$ .*

Finally, we obtain the following lemma by using Lemmas 5.2, 5.3, 5.4 (as in [13]).

**Lemma 5.5.** *The following are equivalent.*

- (1) *There is a  $\mathfrak{g}$ -field extension  $(K, \mathbb{D}) \subseteq (K(b), \mathbb{D}')$  such that  $\mathbb{D}'_V(b_0) = b$ .*
- (2) *There is a  $\mathfrak{g}$ -field extension  $(K, \mathbb{D}) \subseteq (L, \mathbb{D}')$  such that  $\mathbb{D}'_V(b_0) = b$ .*
- (3)  *$c_n(W) \subseteq \nabla(W)$ .*

**5.2. Geometric axioms.** In this subsection, we give geometric axioms for the theories  $\mathfrak{g}$ -DCF and  $F$ -DCF. In the case of  $F = \widehat{\mathbb{G}}_a^e$ , we will recover (and actually we will also correct, thanks to referee's comment, by adding the assumption that  $K$  is separably closed) the geometric axioms for  $\text{SCH}_{p,e}$  from [13, Theorem 4.3]. First we deal with the truncated case.

#### Geometric axioms for $\mathfrak{g}$ -DCF

- (1) The field  $K$  is separably closed.
- (2) For each positive integer  $n$ , suppose that  $V \subseteq \mathbb{A}^n$  and  $W \subseteq \nabla(V)$  are absolutely irreducible  $K$ -varieties, and  $Z$  is a proper  $K$ -subvariety of  $W$ . If  $W$  projects generically onto  $V$ , and  $c_V(W) \subseteq \nabla(W)$ , then there is  $a \in V(K)$  such that  $\mathbb{D}_V(a) \in W(K) \setminus Z(K)$ .

These axioms are first-order, since for a separably closed field  $K$ , any  $K$ -irreducible variety is absolutely irreducible.

**Theorem 5.6.** *The  $\mathfrak{g}$ -field  $(K, \mathbb{D})$  is an existentially closed  $\mathfrak{g}$ -field if and only if  $(K, \mathbb{D})$  satisfies the geometric axioms above.*

*Proof.* Assume that  $(K, \mathbb{D})$  is an existentially closed  $\mathfrak{g}$ -field. Then by Proposition 3.18,  $K$  is separably closed (since a separable algebraic field extension is étale). Take any  $K$ -irreducible  $K$ -varieties  $V \subseteq \mathbb{A}^n$ ,  $W \subseteq \nabla(V)$  and  $Z \subsetneq W$ . If  $W$  projects generically onto  $V$  then there is  $b_0 \in \Omega^n$  and  $b = (b_0, \dots, b_{p^{m_e}-1}) \in \Omega^{np^{m_e}}$  such that  $V = \text{locus}_K(b_0)$  and  $W = \text{locus}_K(b)$ . Since  $c_V(W) \subseteq \nabla(W)$ , Lemma 5.5 implies that there exists a  $\mathfrak{g}$ -field extension  $(K, \mathbb{D}) \subseteq (K(b), \mathbb{D}')$  such that  $\mathbb{D}'_V(b_0) = b$ . We have

$$\mathbb{D}'_V(b_0) = b \in W(K(b)) \setminus Z(K(b))$$

and  $b_0 \in V(K(b))$ . Since  $(K, \mathbb{D})$  is existentially closed, there is  $b'_0 \in V(K)$  such that  $\mathbb{D}_V(b'_0) \in W(K) \setminus Z(K)$ .

Assume now that  $(K, \mathbb{D})$  is a model of the “geometric axioms for  $\mathfrak{g}$ -DCF” and let  $(K, \mathbb{D}) \subseteq (L, \mathbb{D}')$  be an extension of  $\mathfrak{g}$ -fields. Take any quantifier-free formula  $\varphi(x_0, \dots, x_{p^{m_e}-1})$  over  $K$  (in the language of fields), where each  $x_i$  is an  $n$ -tuple of variables for an arbitrary (but fixed) positive integer  $n$ . Suppose that  $(L, \mathbb{D}') \models (\exists x_0) \varphi(\mathbb{D}'(x_0))$ . Take  $b_0 \in L^n$  such that  $(L, \mathbb{D}') \models \varphi(\mathbb{D}'(b_0))$  and set

$$V = \text{locus}_K(b_0), \quad b = \mathbb{D}'_V(b_0), \quad W = \text{locus}_K(b), \quad Z_0 = \{d \in W \mid \neg \varphi(d)\}.$$

Let  $Z$  denote the intersection of all  $K$ -subvarieties of  $W$  containing  $Z_0$ . Clearly  $b \in W(L) \setminus Z(L)$  and the second condition of Lemma 5.5 is satisfied, so  $c_V(W) \subseteq \nabla(W)$ . Hence all the assumptions of the “geometric axioms for  $\mathfrak{g}$  – DCF” hold. Therefore there is  $b'_0 \in V(K)$  such that  $\mathbb{D}(b'_0) \in W(K) \setminus Z(K)$  and  $(K, \mathbb{D}) \models (\exists x_0)\varphi(\mathbb{D}(x_0))$ .  $\square$

**Remark 5.7.** Note that the results of Section 4 are not used in the proof of Theorem 5.6 which suggests a possibility of generalizations, e.g. to the context of  $\mathcal{D}$ -fields from [21].

We turn now to the case of  $F$ -derivations and assume that  $(K, \mathbb{D})$  is an  $F$ -field. By Theorem 4.12, the geometric axioms for  $F$  – DCF are given as the union (over  $m$ ) of the geometric axioms for  $F[m]$  – DCF. We state these axioms explicitly below, where  $\nabla_m$  denotes the functor  $\nabla$  with respect to  $\mathbb{D}[m]$  (similarly for  $c_m$ ).

### Geometric axioms for $F$ – DCF

- (1) The field  $K$  is separably closed.
- (2) For any positive integers  $n, m$ , suppose that  $V \subseteq \mathbb{A}^n$  and  $W \subseteq \nabla_m(V)$  are absolutely irreducible  $K$ -varieties, and  $Z$  is a proper  $K$ -subvariety of  $W$ . If  $W$  projects generically onto  $V$ , and  $c_{m,V}(W) \subseteq \nabla_m(W)$ , then there is  $a \in V(K)$  such that  $\mathbb{D}[m]_V(a) \in W(K) \setminus Z(K)$ .

We get a result generalizing [13, Theorem 4.3].

**Theorem 5.8.** *The  $F$ -field  $\mathbf{K}$  is an existentially closed  $F$ -field if and only if  $\mathbf{K}$  is a model of the geometric axioms for  $\mathfrak{g}$  – DCF.*

**Remark 5.9.** Unlike in the proof of Theorem 5.6, the results of Section 4 *are* used for the proof of Theorem 5.8, since Theorem 4.12 is necessary for the geometric axiomatization and the proof of Theorem 4.12 requires the algebraic axiomatizations of  $\mathfrak{g}$  – DCF and  $F$  – DCF. However, one can also prove Theorem 4.12 (but for a limited class of formal groups  $F$  only) in another fashion as it was done in [13] for  $F = \widehat{\mathbb{G}}_a^c$ . This approach will be discussed in Section 6.1.

## 6. FIELDS WITH OPERATORS AND CANONICAL $G$ -TUPLES

As we have mentioned several times,  $F$ -iterative fields fit to the more general setup of *iterative  $\mathcal{D}$ -fields*, see [21]. Model companions of the theories of iterative  $\mathcal{D}$ -fields are analyzed in [22], however only the case of characteristic 0 and only the “trivial” iterativity maps (see [22, Section 6.1]) are considered there. One could wonder whether our techniques may be generalized to include the case of iterative  $\mathcal{D}$ -fields of positive characteristic. It seems likely in the case where an iterative system  $(\underline{\mathcal{D}}, \Delta)$  is the inverse limit of finite iterative systems  $(\mathcal{D}_m, \Delta_m)_m$  resembling the ones given by Hopf algebra comultiplications  $\mu_m : \mathcal{D}_m \rightarrow \mathcal{D}_m \circ \mathcal{D}_m$  (see Section 5.1). More precisely, our techniques may apply to the iterative systems  $(\underline{\mathcal{D}}, \Delta)$  where each morphism  $\Delta_{p^m} : \mathcal{D}_{2p^m} \rightarrow \mathcal{D}_{p^m} \circ \mathcal{D}_{p^m}$  factors through the projection morphism  $\mathcal{D}_{2p^m} \rightarrow \mathcal{D}_{p^m}$ . It is easy to see that each direct system of finite group schemes provides such an iterative system, and, for example, étale group schemes (corresponding to actual groups) would correspond to systems governing actions of groups on fields by field automorphisms.

A geometric axiomatization of the class of existentially closed  $(\mathcal{D}_m, \Delta_m)$ -fields

should not be very difficult, see Remark 5.7. The crucial technical point allowing a geometric axiomatization of the class of existentially closed  $(\underline{\mathcal{D}}, \Delta)$ -fields may require an appropriate generalization of Theorem 4.12. The proof given in this paper seems to be too specific for a possible generalization to this more general context. However, one could have proceeded in Section 5 differently, more in the fashion of [13] where Ziegler’s notion of a *canonical  $p$ -basis* is used (however we would get then Theorem 5.8 only for a limited class of formal groups  $F$ ). We sketch this approach below.

**6.1. Canonical  $G$ -tuples.** We generalize the notion of a canonical  $p$ -basis (see [32]) from the case of the formalization of a vector group to the case of the formalization of an arbitrary algebraic group.

**Definition 6.1.** Let  $\mathbb{D}$  be a  $G[m]$ -derivation on  $K$ . A subset  $B \subseteq K$  is called a *canonical  $G$ -tuple*, if  $|B| = e$  and there is a  $G[m]$ -embedding  $(k(G), \mathbb{D}[m]^G) \rightarrow \mathbf{K}$  such that  $B$  is the image of the set of canonical parameters of  $G$ , where  $\mathbb{D}[m]^G$  is the canonical  $G[m]$ -derivation from Example 3.27.

**Remark 6.2.** If  $\mathbf{L}$  is strict and of imperfection degree  $e$ , then any canonical  $G$ -tuple in  $L$  is a  $p$ -basis. For  $G = \mathbb{G}_a^e$ , we recover the notion of a *canonical  $p$ -basis* from [32].

We define below a general property of algebraic groups.

**Definition 6.3.** We say that *canonical  $G$ -tuples exist* if for any  $m$  and any separably closed  $G[m]$ -field  $\mathbf{L}$ , whenever  $[L : C_L] = p^e$ , there is a canonical  $G$ -tuple in  $L$ .

**Remark 6.4.** (1) Definition 6.1 can be phrased in a (much) greater generality using group scheme actions. Let  $\mathfrak{G}_0$  be a group subscheme of a group scheme  $\mathfrak{G}$ . Assume that  $\mathfrak{G}_0$  acts (as a group scheme) on a scheme  $V$ . We say that this action has a *canonical  $\mathfrak{G}$ -basis*, if there is an  $\mathfrak{G}_0$ -invariant morphism  $V \rightarrow \mathfrak{G}$  such that the induced map

$$V \rightarrow \mathfrak{G} \times_{\mathfrak{G}/\mathfrak{G}_0} V/\mathfrak{G}_0$$

is an isomorphism.

- (2) The existence of canonical  $\mathbb{G}_a^e$ -tuples is shown in [32] and the existence of canonical  $\mathbb{G}_m$ -tuples is shown in [8]. Combining these results, one can show the existence of canonical  $G$ -tuples for  $G$  of the form  $\mathbb{G}_a^e \times \mathbb{G}_m^f$ .
- (3) We do not attack here the problem of the *existence* of canonical  $G$ -tuples for a given algebraic group  $G$ . This will be done in [6] (as well as possible applications to the notion of “ $G$ -thinness”).
- (4) The existence of canonical  $G$ -tuples implies (*strong*) *integrability* of  $G$ -derivations, as in (morally) [18] or as in [8] (see also [29])

The existence of canonical  $G$ -tuples gives rather directly (see [13, Thm. 2.3]) another proof of Theorem 4.12 which is the only ingredient needed in Section 5 requiring specific differential-algebraic arguments. The interpretation of the notion of the existence of canonical  $G$ -tuples from Remark 6.4(1) looks promising for possible generalizations beyond the context of HS-derivations.

## REFERENCES

- [1] Malkhaz Bakuradze. Calculating mod  $p$  Honda formal group law. Available on <http://arxiv.org/pdf/1502.04152v1.pdf>.
- [2] A. Buium. *Differential Algebraic Groups of Finite Dimension*. Springer-Verlag, 1992.
- [3] Stephen U. Chase. Infinitesimal group scheme actions on finite field extensions. *American Journal of Mathematics*, 98(2):441–480, 1976.
- [4] Françoise Delon. Separably closed fields. In Elisabeth Bouscaren, editor, *Model theory, algebra, and geometry: An Introduction to E. Hrushovskis proof of the geometric Mordell-Lang conjecture*, volume 1696 of *Lecture Notes in Mathematics*, pages 143–176. Springer, Berlin, 1998.
- [5] Michiel Hazewinkel. *Formal Groups and Applications*. Academic Press, 1978.
- [6] Daniel Hoffmann. On existence of canonical  $G$ -bases. Submitted, available on <http://arxiv.org/abs/1412.2224>.
- [7] Daniel Hoffmann. Witt vectors and separably closed fields with higher derivations. Submitted, available on <http://arxiv.org/abs/1510.00218>.
- [8] Daniel Hoffmann and Piotr Kowalski. Integrating Hasse-Schmidt derivations. *J. Pure Appl. Algebra*, 219(4):875–896, 2015.
- [9] Daniel Hoffmann and Piotr Kowalski. A note on integrating group scheme actions. *Journal of Algebra*, 446C:275–290, 2016. doi:10.1016/j.jalgebra.2015.08.031.
- [10] Ehud Hrushovski. The Elementary Theory of the Frobenius Automorphisms. Preprint (24 July 2012), available on <http://www.ma.huji.ac.il/~ehud/FR0B.pdf>.
- [11] Lubin (<http://mathoverflow.net/users/11417/lubin>). Formal group law over  $\mathbb{F}_p$ . MathOverflow. URL:<http://mathoverflow.net/q/196233> (version: 2015-02-11).
- [12] E.R. Kolchin. *Differential Algebra and Algebraic Groups*. Pure and applied mathematics. Academic Press, 1973.
- [13] Piotr Kowalski. Geometric axioms for existentially closed Hasse fields. *Annals of Pure and Applied Logic*, 135:286–302, 2005.
- [14] Piotr Kowalski and Anand Pillay. On the isotriviality of projective iterative  $\partial$ -varieties. *Journal of Pure and Applied Algebra*, 216(1):20–27, 2012.
- [15] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2002.
- [16] Yu I. Manin. The theory of commutative formal groups over fields of finite characteristic. *Russ. Math. Surv.*, 18(6):1–83, 1963.
- [17] H. Matsumura. *Commutative Algebra*. Math Lecture Notes Series. Benjamin/Cummings Publishing Company, 1980.
- [18] Hideyuki Matsumura. Integrable derivations. *Nagoya Math. J.*, 87:227–245, 1982.
- [19] Hideyuki Matsumura. *Commutative ring theory*. Cambridge University Press, 1986.
- [20] Margit Messmer and Carol Wood. Separably closed fields with higher derivation I. *Journal of Symbolic Logic*, 60(3):898–910, 1995.
- [21] Rahim Moosa and Thomas Scanlon. Generalized Hasse-Schmidt varieties and their jet spaces. *Proc. Lond. Math. Soc.*, 103(2):197–234, 2011.
- [22] Rahim Moosa and Thomas Scanlon. Model theory of fields with free operators in characteristic zero. *Journal of Mathematical Logic*, 14(02):1450009, 2014.
- [23] D. Mumford. *Abelian varieties*. Tata Institute of fundamental research studies in mathematics. Published for the Tata Institute of Fundamental Research, Bombay [by] Oxford University Press, 1974.
- [24] Anand Pillay and Martin Ziegler. Jet spaces of varieties over differential and difference fields. *Selecta Mathematica*, 9:579–599, 2003.
- [25] G.E. Sacks. *Saturated model theory*. Mathematics lecture note series. World Scientific Publishing Company, Incorporated, 2010.
- [26] J.P. Serre. *Algebraic Groups and Class Fields: Translation of the French Edition*. Graduate Texts in Mathematics Series. Springer-Verlag New York Incorporated, 1988.
- [27] J.R. Shoenfield. *Mathematical logic*. Addison-Wesley series in logic. Addison-Wesley Pub. Co., 1967.
- [28] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer-Verlag, 1986.
- [29] 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.

- [30] William C. Waterhouse. *Introduction to Affine Group Schemes*. Springer-Verlag, 1979.
- [31] C. Wood. Notes on the stability of separably closed fields. *Journal of Symbolic Logic*, 44:412–416, 1979.
- [32] M. Ziegler. Separably closed fields with Hasse derivations. *Journal of Symbolic Logic*, 68:311–318, 2003.

†INSTYTUT MATEMATYCZNY, UNIWERSYTET WROCLAWSKI, WROCLAW, POLAND  
*E-mail address*: `daniel.hoffmann@math.uni.wroc.pl`

♣INSTYTUT MATEMATYCZNY, UNIWERSYTET WROCLAWSKI, WROCLAW, POLAND  
*E-mail address*: `pkowa@math.uni.wroc.pl`  
*URL*: `http://www.math.uni.wroc.pl/~pkowa/`