Nagoya Math. J., **233** (2019), 1–31
DOI 10.1017/nmj.2017.25

ON EXISTENCE OF CANONICAL G-BASES

DANIEL MAX HOFFMANN

Abstract. We describe a general method for expanding a truncated G-iterative Hasse–Schmidt derivation, where G is an algebraic group. We give examples of algebraic groups for which our method works.

§1. Introduction

Our motivation for this paper is [3, 14], where some nice model-theoretic properties are obtained for fields equipped with HS-derivations satisfying the standard iterativity rule. Analyzing the reasoning in [3, 14], we deduce that one of the most important properties of an iterative Hasse–Schmidt derivation is Matsumura's *strong integrability* (a notion from [4], see: Definition 2.15). Thus we are especially interested in it.

Briefly, strong integrability means that a truncated iterative HS-derivation can be expanded to a not-truncated one, satisfying the same iterativity conditions. We prove (Theorem 3.8) that the existence of a *canonical basis* (Definition 3.6) implies strong integrability for an arbitrary iterativity condition. However, the converse is not true in general (see Remark 3.9), which is related to the problem of the existence of canonical basis in a given field.

Finding a canonical basis is not an easy task. Matsumura in [4] proved the existence of canonical basis for $\mathbb{G}_a$ (the standard iterativity). Afterward Tyc in [9] did the same for $\mathbb{G}_m$ and one-dimensional formal groups over algebraically closed fields. Ziegler showed existence of canonical bases for powers of $\mathbb{G}_a$ proving the quantifier elimination for the theory of separably closed fields in [13, 14] (see Example 3.7). Before this paper only products of $\mathbb{G}_a$ and $\mathbb{G}_m$ were considered. We cover the case of commutative, connected, unipotent groups of dimension 2 over an algebraically closed field. This leads us to Theorem 4.17, stating that, over an algebraically closed field,

Received December 9, 2014. Revised December 17, 2016. Accepted February 1, 2017.
2010 Mathematics subject classification. 13N15, 14L15, 20G15.

SDG. Part of the work on this paper was conducted during the author's internship at the Warsaw Center of Mathematics and Computer Science. Partially supported by NCN grants 2016/20/T/ST1/00482, 2016/21/N/ST1/01465 and 2015/19/B/ST1/01150.

© 2017 *Foundation Nagoya Mathematical Journal*

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

linear algebraic groups that are connected and commutative have canonical basis if unipotent elements form a subgroup of dimension $\leqslant 2$. This theorem includes all the previous results (mentioned above).

Kowalski and I in [2] are treating iterative HS-derivations in a much more abstract way. Many proofs from [2] would be obvious if canonical bases exist for the HS-derivations considered there (a similar sentence was noted at the end of [3, Section 2]). Moreover, [2, Section 6] suggests possible generalizations for the notion of canonical basis.

§2. Basic notions about F-derivations

2.1 HS-derivations

All the rings considered in this paper are commutative and with unity. Fix a field k of the characteristic $p>0$, $e\in\mathbb{N}_{>0}$ and $m\in\mathbb{N}_{>0}\cup\{\infty\}$. Let R be any k-algebra. In this subsection we recall some definitions and well-known facts about HS-derivations.

Definition 2.1. We say that $\mathbb{D}=(D_{\mathbf{i}}:R\to R)_{\mathbf{i}\in\mathbb{N}^e}$ is an *e-dimensional HS-derivation over k* if the map

$$\mathbb{D}:R\to R[\![\bar{X}]\!],\qquad r\mapsto\sum_{\mathbf{i}\in\mathbb{N}^e}D_{\mathbf{i}}(r)\bar{X}^{\mathbf{i}},$$

where $\bar{X}^{\mathbf{i}}=X_1^{i_1}\cdot\ldots\cdot X_e^{i_e}$ for $\mathbf{i}=(i_1,\ldots,i_e)$, is a k-algebra homomorphism and $D_{\mathbf{0}}=\mathrm{id}_R$.

We introduce $R[\bar{v}]:=R[\bar{X}]/(X_1^{p^m},\ldots,X_e^{p^m})$, so $v_i=X_i+(X_1^{p^m},\ldots,X_e^{p^m})$ and $\bar{v}=(v_1,\ldots,v_e)$ (for $m=\infty$ we set $v_i=X_i$, $R[\bar{v}]=R[\![\bar{X}]\!]$). After composing $\mathbb{D}$ with the natural mapping $R[\bar{X}]\to R[\bar{v}]$ we obtain a truncation of $\mathbb{D}$, denoted by $\mathbb{D}[m]=(D_{\mathbf{i}}:R\to R)_{\mathbf{i}\in[p^m]^e}$. This lead us to the following:

Definition 2.2. A collection $\mathbb{D}=(D_{\mathbf{i}}:R\to R)_{\mathbf{i}\in[p^m]^e}$ is called an *m-truncated e-dimensional HS-derivation over k* if the map

$$\mathbb{D}:R\to R[\bar{v}],\qquad r\mapsto\sum_{\mathbf{i}\in[p^m]^e}D_{\mathbf{i}}(r)\bar{v}^{\mathbf{i}},$$

where $\bar{v}^{\mathbf{i}}=v_1^{i_1}\cdot\ldots\cdot v_e^{i_e}$ for $\mathbf{i}=(i_1,\ldots,i_e)$, is a k-algebra homomorphism and $D_{\mathbf{0}}=\mathrm{id}_R$.

Clearly, any ∞-truncated HS-derivation is just an HS-derivation. We have seen that it is easy to obtain from an HS-derivation an m-truncated one. For a field $R=K$ the converse is also true.

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

THEOREM 2.3. *Let R be a smooth k-algebra, $\mathbb{D} = (D_{\mathbf{i}} : R \to R)_{\mathbf{i} \in [p^m]^e}$ an m-truncated e-dimensional HS-derivation over k. There exists an e-dimensional HS-derivation $\mathbb{D}' = (D'_{\mathbf{i}} : R \to R)_{\mathbf{i} \in \mathbb{N}^e}$ over k such that for every $\mathbf{i} \in [p^m]^e$ we have $D'_{\mathbf{i}} = D_{\mathbf{i}}$.*

Proof. We recursively construct $\mathbb{D}'$ as was done at [4, page 236], but using the following diagram

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[dr, dashed] & R[\overline{X}]/(X_1^{p^n}, \ldots, X_e^{p^n}) \\
k \arrow[u] \arrow[r] & R[\overline{X}]/(X_1^{p^{n+1}}, \ldots, X_e^{p^{n+1}}) \arrow[u, "\pi"']
\end{tikzcd}$$

where $\varphi(x) := \sum_{\mathbf{i} \in [p^n]^e} D_{\mathbf{i}}(x) \bar{X}^{\mathbf{i}} + (X_1^{p^n}, \ldots, X_e^{p^n})$ and π is the quotient map. □

REMARK 2.4. Theorem 2.3 is a generalization of [4, Theorem 6]. Note that the best possible situation is for a k-algebra R which is étale over k. In such a case there exists a unique expansion of every m-truncated e-dimensional HS-derivation.

By [5, Theorem 26.9], separability implies smoothness, so Theorem 2.3 works in particular for a separable fields extension $k \subseteq K$. Because so far we do not demand anything from k we can take $k = \mathbb{F}_p$, hence the assumption about a separable extension $k \subseteq K$ is negligible in the following way:

COROLLARY 2.5. *Every m-truncated e-dimensional HS-derivation on a field K has an extension to an e-dimensional HS-derivation.*

We call an m-truncated e-dimensional HS-derivation $\mathbb{D}$ on R *integrable* if there exists e-dimensional HS-derivation $\mathbb{D}'$ on R such that $D'_{\mathbf{i}} = D_{\mathbf{i}}$ for every $\mathbf{i} \in [p^m]^e$. Corollary 2.5 says that truncated HS-derivations on a field are always integrable, but it is not true for arbitrary rings [4, Example 3]. Moreover, the described situation dramatically changes after adding some iterativity conditions. Before considering iterative HS-derivations, we state more well-known facts about general HS-derivations, which will be needed in the remainder of this article.

LEMMA 2.6. *Assume that $R \xrightarrow{f} S$ is a homomorphism of k-algebras. Let $\mathbb{D}$ be an m-truncated e-dimensional HS-derivation on R over k.*

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

(i) *If S is smooth over R, then there exists an m-truncated e-dimensional HS-derivation $\mathbb{D}'$ on S over k such that for every $i_1, \ldots, i_e < p^m$*

$$fD_{(i_1,\ldots,i_e)} = D'_{(i_1,\ldots,i_e)}f. \tag{1}$$

(ii) *If S is unramified over R, then there exists at most one m-truncated e-dimensional HS-derivation $\mathbb{D}'$ on S over k such that for every $i_1, \ldots, i_e < p^m$*

$$fD_{(i_1,\ldots,i_e)} = D'_{(i_1,\ldots,i_e)}f.$$

Proof. The lemma just reformulates [2, Proposition 3.3]. □

Fact 2.7. For every m-truncated e-dimensional HS-derivation and every $x \in R$ the following holds

$$D_{(i_1,\ldots,i_e)}(x^p) = \begin{cases} D_{(i_1/p,\ldots,i_e/p)}(x)^p & \text{if } p|i_1, \ldots, i_e, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. It follows from the definition (see e.g. [6, Lemma 1.1]). □

2.2 Iterative HS-derivations

In this subsection we deal with iterative HS-derivations. The main purpose is to provide basic properties. Let $F(\bar{v}, \bar{w}) = (F_1(\bar{v}, \bar{w}), \ldots, F_e(\bar{v}, \bar{w})) \in (k[\bar{v}, \bar{w}])^e$ (still $k[\bar{v}, \bar{w}] = k[\![\bar{X}, \bar{Y}]\!]$ for $m = \infty$) and let $\mathbb{D}$ be an m-truncated e-dimensional HS-derivation on R over k. Sometimes we need to distinguish between $\mathbb{D} : R \to R[\bar{v}]$ and $\mathbb{D} : R \to R[\bar{w}]$; Therefore, they will be denoted by $\mathbb{D}_{\bar{v}}$ and $\mathbb{D}_{\bar{w}}$ respectively.

DEFINITION 2.8. We call $\mathbb{D}$ *F-iterative* if the following diagram commutes

$$\begin{tikzcd} R \arrow[r, "\mathbb{D}_{\bar{v}}"] \arrow[d, "\mathbb{D}_{\bar{v}}"'] & R[\bar{v}] \arrow[d, "{\mathbb{D}_{\bar{w}}[\bar{v}]}"] \\ R[\bar{v}] \arrow[r, "\mathrm{ev}_F"'] & R[\bar{v}, \bar{w}] \end{tikzcd}$$

where $\mathbb{D}_{\bar{w}}[\bar{v}](\sum_{\mathbf{i}} r_{\mathbf{i}}\bar{v}^{\mathbf{i}}) := \sum_{\mathbf{i}} \mathbb{D}_{\bar{w}}(r_{\mathbf{i}})\bar{v}^{\mathbf{i}}$. We write shortly *$F$-derivation* for an F-iterative m-truncated e-dimensional HS-derivation over k.

EXAMPLE 2.9. For $m = \infty$ and $e = 1$ we can take $F = \mathbb{G}_a = X + Y$. It encodes the classical iterativity rule

$$D_i \circ D_j = \binom{i+j}{i} D_{i+j}.$$

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

An example of a $\mathbb{G}_a$-derivation is the following collection of functions on $k[X]$:

$$D_n\left(\sum_{i=0}^{k}\alpha_i X^i\right)=\begin{cases}0 & \text{if } n>k,\\ \displaystyle\sum_{i=n}^{k}\alpha_i\binom{i}{n}X^{i-n} & \text{if } n\leqslant k,\end{cases}$$

where $n\in\mathbb{N}$. For the formal group law $F=\mathbb{G}_m=X+Y+XY$ above formulas are more complicated (see [1, Example 3.6]).

Example 2.10. For every formal group law $F(\bar{X},\bar{Y})\in(k[\![\bar{X},\bar{Y}]\!])^e$ we have *canonical F-derivation*

$$\mathbb{D}^F:=\mathrm{ev}_{F(\bar{X},\bar{Y})}:k[\![\bar{X}]\!]\to k[\![\bar{X}]\!][\![\bar{Y}]\!].$$

Compare with [2, Example 3.25].

Example 2.11. For actions of finite group schemes, which underlying Hopf algebra is defined on $k[\bar{v}]$, we have a natural correspondence with the truncated F-derivations for an appropriate F (see [2, Section 3]). Therefore, we are especially interested in group scheme actions of k-group schemes of the form $\mathfrak{g}=\operatorname{Spec}k[\bar{v}]$ on the scheme $\operatorname{Spec}R$. By [2, Remark 3.9], such a group scheme action corresponds to an F-derivation on R, where F is the Hopf algebra comultiplication given by $\mathfrak{g}$.

Assume that R is a k-algebra with an F-derivation $\mathbb{D}$. The pair $(R,\mathbb{D})$ will be called an *F-ring*. If K is a field and $(K,\mathbb{D})$ is an F-ring, then $(K,\mathbb{D})$ will be called an *F-field*. Let $(R,\mathbb{D})$ be an F-ring, similarly $(S,\mathbb{D}')$. A morphism of k-algebras $f:R\to S$ is an *F-morphism* if for every $\mathbf{i}$, $fD_{\mathbf{i}}=D'_{\mathbf{i}}f$. Moreover, if such f is injective, R is *F-subring* of S (similarly *F-subfield* for F-fields).

Example 2.12. Let G be an algebraic group over k, we denote by $\mathcal{O}_G$ the local ring of G at the identity (it is a regular local ring) and by $\bar{x}=(x_1,\ldots,x_e)$ a choice of its local parameters. For $F=\hat{G}$ we have $F(\bar{x},\bar{Y})\in\mathcal{O}_G[\![\bar{Y}]\!]$, so $(\mathcal{O}_G,\mathbb{D}^F|_{\mathcal{O}_G})$ is an F-subring of $(k[\![\bar{X}]\!],\mathbb{D}^F)$. Hence $k(G)$ is equipped with a natural $\hat{G}$-derivation, which will be denoted by $\mathbb{D}^G$ and called *canonical G-derivation*. It depends on the choice of local parameters, but we prefer the adjective "canonical". For more details check [2, Example 3.27].

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

For an F-ring $(R,\mathbb{D})$ and $\mathbf{i}\in[p^m]^e$ we introduce $C_{\mathbf{i}}:=\ker D_{\mathbf{i}}$, and two more sets:

$$C_R:=C_{(1,0\ldots,0)}\cap\cdots\cap C_{(0,\ldots,0,1)}\qquad\text{(the ring of constants)},$$

and

$$C_R^{\mathrm{abs}}:=\bigcap_{\mathbf{i}\neq\mathbf{0}}C_{\mathbf{i}}\quad\text{(the ring of absolute constants)}.$$

Both, C_R and C_R^{abs}, are subrings of R (see Remark 3.1).

Lemma 2.13. *Assume that $R\xrightarrow{f}S$ is a homomorphism of k-algebras. Let $\mathbb{D}$ be an F-derivation on R.*

(i) *If S is étale (smooth and unramified) over R, then there exists a unique F-derivation $\mathbb{D}'$ on S such that for every $i_1,\ldots,i_e<p^m$*

$$fD_{(i_1,\ldots,i_e)}=D'_{(i_1,\ldots,i_e)}f.$$

(ii) *If S is unramified over R, then there exists at most one F-derivation $\mathbb{D}'$ on S such that for every $i_1,\ldots,i_e<p^m$*

$$fD_{(i_1,\ldots,i_e)}=D'_{(i_1,\ldots,i_e)}f.$$

Proof. Compare to [2, Proposition 3.18]. Part (ii) is, by Lemma 2.6(ii), true even without the iterativity assumption. For the proof of part (i), it is enough to show that an HS-derivation $\mathbb{D}'$ from Lemma 2.6 is F-iterative, that is, the following diagram is commutative

$$\begin{tikzcd}
S \arrow[r, "\mathbb{D}'_{\bar{v}}"] \arrow[d, "\mathbb{D}'_{\bar{v}}"'] & S[\bar{v}] \arrow[d, "\mathbb{D}'_{\bar{w}}{[\bar{v}]}"] \\
S[\bar{v}] \arrow[r, "\mathrm{ev}_F"'] & S[\bar{v},\bar{w}]
\end{tikzcd}$$

It is similar to the proof of [5, Theorem 27.2] and we leave it to the reader. □

Let $F(\bar{v},\bar{w})\in(k[\bar{v},\bar{w}])^e$, $m'\leqslant m$ and let $\bar{v'}$, $\bar{w'}$ denote the m'-truncated variables $(k[\bar{v'},\bar{w'}]=k[\bar{X},\bar{Y}]/(X_1^{p^{m'}},\ldots,X_e^{p^{m'}},Y_1^{p^{m'}},\ldots,Y_e^{p^{m'}}))$. By $F[m']$ we denote the m'-truncation of F which is equal to $\mathrm{ev}_{(\bar{v'},\bar{w'})}F(\bar{v},\bar{w})$ (the image of F in the ring of truncated polynomials $(k[\bar{v'},\bar{w'}])^e$). If $\mathbb{D}$ is F-iterative, then $\mathbb{D}[m']$ is $F[m']$-iterative as well (for the notion of $\mathbb{D}[m]$, check the first lines after Definition 2.1).

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

EXAMPLE 2.14. For every $m \in \mathbb{N}_{>0}$ we get a $\hat{G}[m]$-field structure on $k(G)$–just consider $\mathbb{D}^G[m]$.

DEFINITION 2.15. Let $F(\bar{X}, \bar{Y}) \in (k[\![\bar{X}, \bar{Y}]\!])^e$ and let $\mathbb{D}$ be an $F[m]$-derivation on a k-algebra R. We call $\mathbb{D}$ *strongly integrable* if there exists an F-derivation $\mathbb{D}'$ on R such that $\mathbb{D}'[m] = \mathbb{D}$.

In the next few facts we give simple properties of F-derivations on a k-algebra R. Those facts were intended for a formal group law F, but it is enough to demand that $F(\bar{v}, \bar{w}) \in (k[\bar{v}, \bar{w}])^e$, $F(\bar{v}, \bar{0}) = \bar{v}$ and $F(\bar{0}, \bar{w}) = \bar{w}$. However, we do not consider F-derivations in the case when F is not a formal group law, even the existence for such (nontrivial) derivations is not clear in general.

Fact 2.16. For every $\mathbf{i}$ and $\mathbf{j}$ there exists $\mathbf{r}(D_{\mathbf{j}'})_{0<|\mathbf{j}'|<|\mathbf{i}+\mathbf{j}|}$, a k-linear combination of $D_{\mathbf{j}'}$, where $0 < |\mathbf{j}'| < |\mathbf{i} + \mathbf{j}|$, such that

$$D_{\mathbf{j}} D_{\mathbf{i}} = \binom{i_1 + j_1}{i_1} \cdots \binom{i_e + j_e}{i_e} D_{\mathbf{i}+\mathbf{j}} + \mathbf{r}(D_{\mathbf{j}'})_{0<|\mathbf{j}'|<|\mathbf{i}+\mathbf{j}|}.$$

Proof. It is clear for $\mathbf{i} = \mathbf{0}$ or $\mathbf{j} = \mathbf{0}$, so assume that both $\mathbf{i}$ and $\mathbf{j}$ differ from $\mathbf{0}$. Since $F(\bar{v}, 0) = \bar{v}$, $F(0, \bar{w}) = \bar{w}$, we have $F(\bar{v}, \bar{w}) = (v_1 + w_1 + S_1, \ldots, v_e + w_e + S_e)$ for some $S_1, \ldots, S_e$ belonging to the ideal $(v_i w_j)_{i,j \leqslant e}$. Therefore, for every $r \in R$

$$\sum_{j_1,\ldots,j_e,i_1,\ldots,i_e} D_{(j_1,\ldots,j_e)} D_{(i_1,\ldots,i_e)}(r) v_1^{i_1} \cdot \ldots \cdot v_e^{i_e} \cdot w_1^{j_1} \cdot \ldots \cdot w_e^{j_e}$$
$$= \sum_{k_1,\ldots,k_e} D_{(k_1,\ldots,k_e)}(r)(v_1 + w_1 + S_1)^{k_1} \cdot \ldots \cdot (v_e + w_e + S_e)^{k_e}.$$

We are interested in the coefficients at $A := v_1^{i_1} \cdot \ldots \cdot v_e^{i_e} \cdot w_1^{j_1} \cdot \ldots \cdot w_e^{j_e}$ on the right side of the above equation. First of all, note that $v_i + w_i + S_i$, $i \leqslant e$, is an element of the maximal ideal $(v_1, \ldots, v_e, w_1, \ldots, w_e)$, hence it is of the form

$$\alpha_1 v_1 + \cdots + \alpha_e v_e + \beta_1 w_1 + \cdots + \beta_e w_e,$$

for some $\alpha_1, \ldots, \alpha_e, \beta_1, \ldots, \beta_e \in k[\bar{v}, \bar{w}]$. Each component of the above sum has total degree at least 1, so the total degree of each summand of $(v_i + w_i + S_i)^{k_i}$ is at least k_i. Therefore, the total degree of

$$(v_1 + w_1 + S_1)^{k_1} \cdot \ldots \cdot (v_e + w_e + S_e)^{k_e}$$

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

is at least equal to $k_1 + \cdots + k_e$. On the other hand, the total degree of A is equal to $|\mathbf{i}+\mathbf{j}|$. After comparing degrees, we see that if $k_1 + \cdots + k_e > |\mathbf{i}+\mathbf{j}|$ then there is no chance to find a component of

$$D_{(k_1,\ldots,k_e)}(r)(v_1 + w_1 + S_1)^{k_1} \cdot \ldots \cdot (v_e + w_e + S_e)^{k_e}$$

equal to A multiplied by some element of R.

Let $k_1 + \cdots + k_e = |\mathbf{i}+\mathbf{j}|$. Since $S_1, \ldots, S_e \in (v_i w_j)_{i,j\leqslant e}$, each summand of S_i, $i \leqslant e$, has total degree at least 2. The only component of

$$D_{(k_1,\ldots,k_e)}(r)(v_1 + w_1 + S_1)^{k_1} \cdot \ldots \cdot (v_e + w_e + S_e)^{k_e}$$

for which the total degree will be equal to $|\mathbf{i}+\mathbf{j}|$ “omits” $S_1, \ldots, S_e$. Therefore, we are looking for the coefficient of

$$D_{(k_1,\ldots,k_e)}(r)(v_1 + w_1)^{k_1} \cdot \ldots \cdot (v_e + w_e)^{k_e},$$

which is divisible by A. □

Fact 2.17. Assume that also $\mathbb{D}'$ is an F-derivation on R. If for all $l \leqslant e$ and $i < m$ we have $D_{(0,\ldots,0,\underset{l\text{th place}}{p^i},0,\ldots,0)} = D'_{(0,\ldots,0,\underset{l\text{th place}}{p^i},0,\ldots,0)}$ then $\mathbb{D} = \mathbb{D}'$.

Proof. Induction on $|\mathbf{j}|$. Clearly, $D_{(0,\ldots,0)} = \mathrm{id}_R = D'_{(0,\ldots,0)}$. Take $\mathbf{j} = (j_1, \ldots, j_e) \neq (0, \ldots, 0)$ and assume that $D_{\mathbf{j}'} = D'_{\mathbf{j}'}$ for every $\mathbf{j}'$ such that $|\mathbf{j}'| < |\mathbf{j}|$. Without loss of generality, we set $j_1 \neq 0$. Let $j_1 = \gamma_0 + \gamma_1 p + \cdots + \gamma_s p^s$, where $\gamma_0, \ldots, \gamma_s < p$ and $\gamma_s \neq 0$. Fact 2.16 implies that

$$D_{(p^s,0,\ldots,0)} D_{(j_1-p^s,j_2,\ldots,j_e)} = \gamma_s D_{\mathbf{j}} + \mathbf{r}(D_{\mathbf{j}'})_{0<|\mathbf{j}'|<|\mathbf{j}|},$$
$$D'_{(p^s,0,\ldots,0)} D'_{(j_1-p^s,j_2,\ldots,j_e)} = \gamma_s D'_{\mathbf{j}} + \mathbf{r}(D'_{\mathbf{j}'})_{0<|\mathbf{j}'|<|\mathbf{j}|}.$$

A k-linear combination $\mathbf{r}(D_{\mathbf{j}'})_{0<|\mathbf{j}'|<|\mathbf{j}|}$ is unique for F (what can be deduced from the proof of Fact 2.16), hence, by the inductive assumption, it is equal to $\mathbf{r}(D'_{\mathbf{j}'})_{0<|\mathbf{j}'|<|\mathbf{j}|}$. Moreover, it follows from the inductive assumption that

$$D_{(p^s,0,\ldots,0)} D_{(j_1-p^s,j_2,\ldots,j_e)} = D'_{(p^s,0,\ldots,0)} D'_{(j_1-p^s,j_2,\ldots,j_e)},$$

so $D_{\mathbf{j}} = D'_{\mathbf{j}}$. □

LEMMA 2.18. *Let $(K, \mathbb{D})$ be an F-field and let $\partial_1, \ldots, \partial_{p^e}$ be all different elements of $\{D_{(i_0,\ldots,i_e)} \mid i_0, \ldots, i_e < p\}$. Take any $x_1, \ldots, x_n \in K$. Elements $x_1, \ldots, x_n$ are linearly dependent over C_K if and only if the rank of the matrix $(\partial_i(x_j))_{i\leqslant p^e, j\leqslant n}$ is smaller than n.*

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

Proof. The proof of [2, Proposition 3.20] works well for the above, more general lemma. ∎

COROLLARY 2.19. *For every F-field extension $K \subseteq L$, K and C_L are linearly disjoint over C_K.*

DEFINITION 2.20. We call an F-field $(K, \mathbb{D})$ *strict* if $C_K = K^p$.

REMARK 2.21. Let $K \subseteq L$ be an F-field extension. If K is strict, then $K \subseteq L$ is separable.

Proof. By Corollary 2.19, K and $L^p \subseteq C_L$ are linearly disjoint over $K^p = C_K$, so by [5, Theorem 26.4] L is separable over K. ∎

LEMMA 2.22. *For any F-field $(K, \mathbb{D})$ we have $[K : C_K] \leqslant p^e$.*

Proof. It follows from Lemma 2.18. ∎

2.3 Commutative HS-derivations

In this subsection we deal with formulas for $D_{\mathbf{i}}^{(p)}$ (the pth composition) in the case of an F-derivation $\mathbb{D} = (D_{\mathbf{i}})_{\mathbf{i} \in [p^m]^e}$ for a commutative F (i.e., $F(\bar{v}, \bar{w}) = F(\bar{w}, \bar{v})$). The main idea follows [1, Section 3.3], but improves the reasoning of [1, Proposition 3.11] and [1, Remark 3.12.(4)]. The idea to focus on the ring of symmetric polynomials comes from Kowalski. We assume only that $F(\bar{v}, \bar{w}) \in (k[\bar{v}, \bar{w}])^e$ is commutative and that $(R, \mathbb{D})$ is an F-ring. Obviously:

Fact 2.23. We have the following

$$D_{\mathbf{j}} \circ D_{\mathbf{i}} = D_{\mathbf{i}} \circ D_{\mathbf{j}}.$$

For every $N \geqslant 1$ we introduce the following k-algebra homomorphism

$$E_N : R[\bar{v}_1, \ldots, \bar{v}_{N-1}] \to R[\bar{v}_1, \ldots, \bar{v}_N],$$
$$E_N = \mathbb{D}_{\bar{v}_N}[\bar{v}_1, \ldots, \bar{v}_{N-1}],$$

where $\bar{v}_1, \ldots, \bar{v}_N$ are e-tuples of m-truncated variables and

$$\mathbb{D}_{\bar{v}_N}[\bar{v}_1, \ldots, \bar{v}_{N-1}]\left(\sum_{\mathbf{i}_1, \ldots, \mathbf{i}_{N-1}} \alpha_{\mathbf{i}_1, \ldots, \mathbf{i}_{N-1}} \bar{v}_1^{\mathbf{i}_1} \cdot \ldots \cdot \bar{v}_{N-1}^{\mathbf{i}_{N-1}}\right)$$
$$= \sum_{\mathbf{i}_1, \ldots, \mathbf{i}_N} D_{\mathbf{i}_N}(\alpha_{\mathbf{i}_1, \ldots, \mathbf{i}_{N-1}}) \bar{v}_1^{\mathbf{i}_1} \cdot \ldots \cdot \bar{v}_N^{\mathbf{i}_N}.$$

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

For $N \geqslant 1$ we define inductively

$$F_1(\bar{v}_1) := \bar{v}_1,$$
$$F_{N+1}(\bar{v}_1, \ldots, \bar{v}_{N+1}) := F_N(\bar{v}_1, \ldots, \bar{v}_{N-1}, F(\bar{v}_N, \bar{v}_{N+1})).$$

LEMMA 2.24. *For every $N \geqslant 1$ the following diagram commutes*

$$\begin{tikzcd}
R \arrow[rr, "E_N \circ \cdots \circ E_1"] \arrow[dr, "E_1"'] & & R[\bar{v}_1, \ldots, \bar{v}_N] \\
& R[\bar{v}_1] \arrow[ur, "\mathrm{ev}_{F_N}"'] &
\end{tikzcd}$$

Proof. It is clear for $N = 1$, so assume for the induction step that the last diagram is commutative. Consider

$$\begin{tikzcd}
R \arrow[r, "E_{N-1} \circ \cdots \circ E_1"] \arrow[d, "E_1"'] & R[\bar{v}_1, \ldots, \bar{v}_{N-1}] \arrow[r, "E_N"] \arrow[d, "E_N"'] & R[\bar{v}_1, \ldots, \bar{v}_N] \arrow[d, "E_{N+1}"] \\
R[\bar{v}_1] \arrow[r, "\mathrm{ev}_{F_N}"'] & R[\bar{v}_1, \ldots, \bar{v}_N] \arrow[r, "\mathrm{ev}_{(\bar{v}_1, \ldots, \bar{v}_{N-1}, F(\bar{v}_N, \bar{v}_{N+1}))}"'] & R[\bar{v}_1, \ldots, \bar{v}_{N+1}]
\end{tikzcd}$$

Left part is commutative by the inductive assumption. For commutativity of the right side, just apply the functor

$$R \to R[\bar{v}_1, \ldots, \bar{v}_{N-1}]$$

to the diagram from the F-iterativity definition and change $\bar{v}$, $\bar{w}$ to $\bar{v}_N$, $\bar{v}_{N+1}$. Finally

$$\mathrm{ev}_{(\bar{v}_1, \ldots, \bar{v}_{N-1}, F(\bar{v}_N, \bar{v}_{N+1}))} \circ \mathrm{ev}_{F_N} = \mathrm{ev}_{F_{N+1}}. \qquad \square$$

Note that the following composition of mappings

$$R \xrightarrow{E_1} R[\bar{v}_1] \xrightarrow{E_2} R[\bar{v}_1, \bar{v}_2] \to \cdots \xrightarrow{E_p} R[\bar{v}_1, \ldots, \bar{v}_p]$$

is a k-algebra homomorphism such that $\mathrm{im}(E_p \circ \cdots \circ E_1)$ is, by Fact 2.23, a subset of the ring of symmetric polynomials in $\bar{v}_1, \ldots, \bar{v}_p$, that is, elements of $R[\bar{v}_1, \ldots, \bar{v}_p]$ invariant under the action of S_p,

$$\sigma : \bar{v}_i = (v_{i,1}, \ldots, v_{i,e}) \mapsto \bar{v}_{\sigma(i)} = (v_{\sigma(i),1}, \ldots, v_{\sigma(i),e}),$$

for $\sigma \in S_p$ and $i \leqslant p$. In other words the map $E_p \circ \cdots \circ E_1$ factors as in following the diagram

$$\begin{tikzcd}
R \arrow[rr, dashed] \arrow[drr, "E_p\circ\cdots\circ E_1"'] & & R[\bar{v}_1, \ldots, \bar{v}_p]^{S_p} \arrow[d, "\subseteq"] \\
& & R[\bar{v}_1, \ldots, \bar{v}_p]
\end{tikzcd}$$

For $\varphi : R[\bar{v}_1, \ldots, \bar{v}_p]^{S_p} \to R[\bar{v}_1^{1/p}]$, given by $v_{i,j} \mapsto v_{1,j}^{1/p}$, where $i \leqslant p$ and $j \leqslant e$, also the map φ factors as in the following diagram

$$\begin{tikzcd}
R[\bar{v}_1, \ldots, \bar{v}_p]^{S_p} \arrow[rr, dashed] \arrow[drr, "\varphi"'] & & R[\bar{v}_1] \arrow[d, "\subseteq"] \\
& & R[\bar{v}_1^{1/p}]
\end{tikzcd}$$

Therefore, $\varphi : \mathrm{im}(E_p \circ \cdots \circ E_1) \to R[\bar{v}_1]$, defined is a well-defined k-algebra homomorphism.

For any $N \geqslant 1$ we define inductively the “multiplication by N map”:

$$[1]_F := \bar{v},$$
$$[N+1]_F := F(\bar{v}, [N]_F).$$

For example $[2]_F = F(\bar{v}, \bar{v})$.

COROLLARY 2.25. *For any $r \in R$ we have*

$$\sum_{\mathbf{i}} D_{\mathbf{i}}^{(p)}(r)\bar{v}^{\mathbf{i}} = \mathrm{ev}_{[p]_F(\bar{v}^{1/p})}\left(\sum_{\mathbf{i}} D_{\mathbf{i}}(r)\bar{v}^{\mathbf{i}}\right).$$

Proof. By Lemma 2.24 we know that

$$E_p \circ \cdots \circ E_1(r) = \mathrm{ev}_{F_p} \circ E_1(r),$$

so

$$\sum_{\mathbf{i}} D_{\mathbf{i}}^{(p)}(r)\bar{v}_1^{\mathbf{i}} = \varphi \circ E_p \circ \cdots \circ E_1(r) = \varphi \circ \mathrm{ev}_{F_p} \circ E_1(r)$$
$$= \mathrm{ev}_{[p]_F(\bar{v}_1^{1/p})}\left(\sum_{\mathbf{i}} D_{\mathbf{i}}(r)\bar{v}_1^{\mathbf{i}}\right).$$

The first equality is similar to [1, Lemma 3.7], the last follows from definitions of $[p]_F$, F_p and φ. For example let $p = 2$:

$$\varphi \circ \mathrm{ev}_{F_2(\bar{v}_1, \bar{v}_2)} = \mathrm{ev}_{F_2(\bar{v}_1^{1/p}, \bar{v}_1^{1/p})} = \mathrm{ev}_{[2]_F(\bar{v}_1^{1/p})}.$$ □

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

§3. Canonical G-bases and the integrability

The results of this section focus on proving the integrability for a field equipped with an iterative HS-derivation and endowed with a p-basis of a special kind. For the notion of p-independence, p-basis and their basic properties, the reader is referred to [5, page 202]. Recall that k is a perfect field. Assume that G is an algebraic group over k of dimension e (perhaps not commutative). We write $G[m]$-derivation, $G[m]$-ring, $G[m]$-field, ... instead of $\hat{G}[m]$-derivation, $\hat{G}[m]$-ring, $\hat{G}[m]$-field, ...

Let $(K, \mathbb{D})$ be a $G[m]$-field. For every $s \in \{0, \ldots, m-1\}$ we introduce

$$F_s := \bigcap_{j=0}^{s} C_{(p^j,0,\ldots,0)} \cap C_{(0,p^j,0,\ldots,0)} \cap \cdots \cap C_{(0,\ldots,0,p^j)}, \qquad F_{-1} := K.$$

REMARK 3.1. Sets F_s are, due to Fact 2.17, subfields of K. In fact F_s is equal to the field of constants of order s (the absolute constants of $\mathbb{D}[s+1]$).

For the clarity of the following proofs, we note an obvious fact:

Fact 3.2. Let $L \subseteq L'$ be an extension of fields. If $y \in L^{1/p} \backslash L \subseteq L'$, then $[L(y) : L] = p$.

LEMMA 3.3. *Let $z_1, \ldots, z_e \in K$ form a p-basis of (or equivalently, by Lemma 2.22, “are p-independent in”) K over $C_K = F_0$. For every $s \in \{0, \ldots, m-1\}$ we have*

$$[F_{s-1} : F_s] = p^e, \qquad F_{s-1} = F_s(z_1^{p^s}, \ldots, z_e^{p^s}).$$

Proof. Being a p-basis for K over F_0, due to $K^p \subseteq F_0$, means that $K = F_0(z_1, \ldots, z_e)$ and that $[F_0(z_1, \ldots, z_e) : F_0] = p^e$. Notice that, by [2, Lemma 3.31] and Lemma 2.22,

$$[F_s(z_1^{p^s}, \ldots, z_e^{p^s}) : F_s] \leqslant [F_{s-1} : F_s] \leqslant p^e.$$

It is enough to show that $[F_s(z_1^{p^s}, \ldots, z_e^{p^s}) : F_s] = p^e$. We know that $\{z_1^{i_1} \cdot \ldots \cdot z_e^{i_e} \mid 0 \leqslant i_1, \ldots, i_e < p\}$ is F_0-linearly independent, thus $\{z_1^{i_1 p^s} \cdot \ldots \cdot z_e^{i_e p^s} \mid 0 \leqslant i_1, \ldots, i_e < p\}$ is $F_0^{p^s}$-linearly independent. Consider

$$(K^{p^s}, \mathbb{D}[s+1]|_{K^{p^s}}) \subseteq (F_{s-1}, \mathbb{D}[s+1]|_{F_{s-1}}).$$

By [2, Lemma 3.31], it is an extension of $G[1]^{\mathrm{Fr}^{p^s}}$-fields. Therefore, by Corollary 2.19, K^{p^s} is linearly disjoint from constants of$\mathbb{D}[s+1]|_{F_{s-1}}$

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

over constants of $\mathbb{D}[s+1]|_{K^{p^s}}$. So $F_0^{p^s}$-linear independence of $\{z_1^{i_1p^s}\cdot\ldots\cdot z_e^{i_ep^s}\mid 0\leqslant i_1,\ldots,i_e<p\}$ implies its F_s-linear independence. Hence $[F_s(z_1^{p^s},\ldots,z_e^{p^s}):F_s]=p^e$. □

Remark 3.4. The equality

$$[F_{s-1}:F_s]=p^e,$$

where $s\in\{0,\ldots,m-1\}$, does not depend on the choice of a p-basis. Therefore, it is true if $[K:C_K]=p^e$.

Proposition 3.5. *Let $z_1,\ldots,z_e\in K$ form a p-basis of (or equivalently "are p-independent in") K over $C_K=F_0$. Then there exists a subset $\mathcal{B}_0\subseteq C_K^{abs}=F_{m-1}$, for which $\mathcal{B}:=\mathcal{B}_0\cup\{z_1,\ldots,z_e\}$ is a p-basis for K over k.*

Proof. In particular, Lemma 3.3 implies that the set $\{z_1^{p^m},\ldots z_e^{p^m}\}$ is p-independent over k in F_{m-1}. Let $\mathcal{B}'$ be a p-basis $\mathcal{B}'$ of the field F_{m-1} over k of the form$\mathcal{B}'=\mathcal{B}_0\cup\{z_1^{p^m},\ldots,z_e^{p^m}\}$. We show that $\mathcal{B}:=\mathcal{B}_0\cup\{z_1,\ldots,z_e\}$ is a p-basis of K over k. Since for $s=m$, $\mathcal{B}_0\cup\{z_1^{p^m},\ldots,z_e^{p^m}\}=\mathcal{B}'$ is, as above, a p-basis for F_{m-1} over k, it is enough to show the following induction step

$$\text{if } \mathcal{B}_0\cup\{z_1^{p^s},\ldots,z_e^{p^s}\} \text{ is } p\text{-basis for } F_{s-1} \text{ over } k,$$
$$\text{then } \mathcal{B}_0\cup\{z_1^{p^{s-1}},\ldots,z_e^{p^{s-1}}\} \text{ is } p\text{-basis for } F_{s-2} \text{ over } k,$$

where s descends from m to 1.

Firstly, we argue for the p-independence of $\mathcal{B}_0$ in F_{s-2}. For any $n\in\mathbb{N}$ and pairwise distinct $x_1,\ldots,x_n\in\mathcal{B}_0$, by Lemma 3.3, we have

$$[F_{s-2}^p(x_1,\ldots,x_n):F_{s-1}^p]=[F_{s-1}^p(z_1^{p^s},\ldots,z_e^{p^s},x_1,\ldots,x_n):F_{s-1}^p]=p^{n+e},$$

using Lemma 3.3 again, we get

$$\begin{aligned}p^{n+e}&=[F_{s-2}^p(x_1,\ldots,x_n):F_{s-2}^p]\cdot[F_{s-1}^p(z_1^{p^s},\ldots,z_e^{p^s}):F_{s-1}^p]\\&=[F_{s-2}^p(x_1,\ldots,x_n):F_{s-2}^p]\cdot p^e.\end{aligned}$$

Elements $x_1,\ldots,x_n$ were chosen arbitrary, so indeed $\mathcal{B}_0$ is p-independent over k in F_{s-2}.

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

We show now the p-independence of $\mathcal{B}_0 \cup \{z_1^{p^{s-1}}, \ldots, z_e^{p^{s-1}}\}$ in F_{s-2}. For any $n \in \mathbb{N}$, pairwise distinct $x_1, \ldots, x_n \in \mathcal{B}_0$,

$$\begin{aligned}
&[F_{s-2}^p(z_1^{p^{s-1}}, \ldots, z_e^{p^{s-1}}, x_1, \ldots, x_n) : F_{s-2}^p] \\
&\quad = [F_{s-2}^p(z_1^{p^{s-1}}, \ldots, z_e^{p^{s-1}}, x_1, \ldots, x_n) : F_{s-2}^p(x_1, \ldots, x_n)] \\
&\qquad \cdot [F_{s-2}^p(x_1, \ldots, x_n) : F_{s-2}^p].
\end{aligned}$$

To show the p-independence of $\mathcal{B}_0 \cup \{z_1^{p^{s-1}}, \ldots, z_e^{p^{s-1}}\}$ over k in F_{s-2} we need only to prove

$$[F_{s-2}^p(z_1^{p^{s-1}}, \ldots, z_e^{p^{s-1}}, x_1, \ldots, x_n) : F_{s-2}^p(x_1, \ldots, x_n)] = p^e.$$

By Fact 3.2 it reduces to show that for each $i \leqslant e$ we have

$$z_i^{p^{s-1}} \notin F_{s-2}^p(z_{i+1}^{p^{s-1}}, \ldots, z_e^{p^{s-1}}, x_1, \ldots, x_n)$$

(clearly $z_i^{p^s} \in F_{s-2}^p$). It holds due to Lemma 3.3 and

$$F_{s-2}^p(z_{i+1}^{p^{s-1}}, \ldots, z_e^{p^{s-1}}, x_1, \ldots, x_n) \subseteq F_{s-1}(z_{i+1}^{p^{s-1}}, \ldots, z_e^{p^{s-1}}).$$

Finally, we see that

$$\begin{aligned}
F_{s-2} &= F_{s-1}(z_1^{p^{s-1}}, \ldots, z_e^{p^{s-1}}) \\
&= F_{s-1}^p(\mathcal{B}_0 \cup \{z_1^{p^s}, \ldots, z_e^{p^s}\})(z_1^{p^{s-1}}, \ldots, z^{p^{s-1}}) \\
&= F_{s-1}^p(z_1^{p^s}, \ldots, z_e^{p^s})(\mathcal{B}_0 \cup \{z_1^{p^{s-1}}, \ldots, z^{p^{s-1}}\}) \\
&= F_{s-2}^p(\mathcal{B}_0 \cup \{z_1^{p^{s-1}}, \ldots, z^{p^{s-1}}\}),
\end{aligned}$$

and that ends proof of the induction, after last step we obtain that $\mathcal{B}_0 \cup \{z_1, \ldots z_e\}$ is a p-basis for $F_{1-2} = K$ over k. □

In the spirit of [2, Definition 6.1] we introduce the following term:

DEFINITION 3.6. Let $(K, \mathbb{D}[m])$ be a $G[m]$-field. A subset $B \subseteq K$ is called a *canonical G-basis* if:

- $|B| = e$;
- B is p-independent in K over C_K;
- there is an embedding of $G[m]$-fields $(k(G), \mathbb{D}^G[m]) \to (K, \mathbb{D}[m])$ (see Example 2.12) such that B is the image of the set of canonical parameters of G corresponding to the canonical G-derivation.

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

EXAMPLE 3.7. Let us take $G = \mathbb{G}_a^e$. By [5, Theorem 27.3] and Lemma 4.15 if $[K : C_K] = p^e$ then $(K, \mathbb{D}[m])$ has a canonical $\mathbb{G}_a^e$-basis. This fact was used in [14], to obtain the quantifier elimination for the theory of separably closed strict $\mathbb{G}_a^e$-fields, satisfying $[K : C_K] = p^e$.

THEOREM 3.8. *Assume that a $G[m]$-field $(K, \mathbb{D}[m])$ has a canonical G-basis, then $\mathbb{D}[m]$ is strongly integrable.*

Proof. Let $B = \{z_1, \ldots, z_e\}$ be a canonical G-basis of $(K, \mathbb{D}[m])$ and let $\bar{X}$ be an e-tuple of variables. By a choice of local parameters of G at the identity we get an embedding $k(\bar{X}) \subseteq k(G)$. Proposition 3.5 assures the existence of a set $B_0 \subseteq C_K^{\text{abs}}$ such that $B_0 \cup B$ is a p-basis of K over k. Let $K' := k(B_0)$. Because $B_0 \cup B$ is algebraically independent over k, B_0 is algebraically independent over $k(B)$. Moreover, $k(B) \cong k(\bar{X}) \subset k(G)$ is an algebraic extension, thus B_0 is algebraically independent over $k(G)$. Therefore, K' and $k(G)$ are linearly disjoint over k, so the "multiplication" map $\mu : k(G) \otimes_k K' \to K$ is an injection, and therefore it extends to $\tilde{\mu} : (k(G) \otimes_k K')_0 \to K$.

By [5, Theorem 26.8], $K'(B)$ is purely transcendental over K' and $K'(B) \subseteq K$ is 0-étale. Hence we have $K'(B) \cong K'(\bar{X}) \cong (k(\bar{X}) \otimes_k K')_0 \subseteq (k(G) \otimes_k K')_0$ ($k(G) \otimes_k K'$ is a domain as a subring of K). Therefore, we have a natural mapping $K'(B) \to (k(G) \otimes_k K')_0 =: K'(G)$.

Note that the following diagram commutes

$$\begin{tikzcd}
 & K'(G) \arrow[dr, "\tilde{\mu}"] & \\
K'(B) \arrow[ur] \arrow[rr, "\subseteq"'] & & K
\end{tikzcd}$$

The extension of fields $K'(B) \subseteq K$ is smooth, and by [5, Theorem 26.9] it is also separable. In particular, $K'(G)$ is separable over $K'(B)$. The algebraicity of the extension $k(B) \subseteq k(G)$ implies the algebraicity of the extension $K'(B) \subseteq K'(G)$, and that, due to [5, Theorem 26.1], means that $K'(B) \subseteq K'(G)$ is 0-étale. Therefore, also $\tilde{\mu} : K'(G) \to K$ is 0-étale. We have the following tower of k-algebras

$$k(G) \otimes_k K' \subseteq (k(G) \otimes_k K')_0 = K'(G) \xrightarrow{\tilde{\mu}} K,$$

where both extensions are 0-étale. By [5, Theorem 26.7] $k(G) \otimes_k K' \xrightarrow{\mu} K$ is 0-étale.

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

Now we are going to define a G-ring structure on $R := k(G) \otimes_k K'$. For every $\mathbf{i} \in \mathbb{N}^e$, $v \in k(G)$ and $w \in K'$ we define

$$D'_{\mathbf{i}}(v \otimes w) := D^G_{\mathbf{i}}(v) \otimes w.$$

Note that for every $\mathbf{i} \in [p^m]^e$, we have $\mu \circ D'_{\mathbf{i}} = D_{\mathbf{i}} \circ \mu$. Thus $(R, \mathbb{D}'[m]) \xrightarrow{\mu} (K, \mathbb{D})$ is a $G[m]$-morphism. By Lemma 2.13 for $(R, \mathbb{D})$, there exists a unique G-derivation $\tilde{\mathbb{D}}$ on K. Since both $\mathbb{D}$ and $\tilde{\mathbb{D}}[m]$ extend $\mathbb{D}'[m]$, by Lemma 2.13 for every $\mathbf{i} \in [p^m]^e$ we have $D_{\mathbf{i}} = \tilde{D}_{\mathbf{i}}$. □

REMARK 3.9. The converse to Theorem 3.8 is not true in general. First of all, we need enough “space” to have a canonical G-basis, so we assume

$$[K : C_K] = p^e \tag{2}$$

for an integrable $G[m]$-field $(K, \mathbb{D})$. For example $D_{\mathbf{i}} = 0$, for all $\mathbf{i} \neq \mathbf{0}$, is integrable, but $[K : C_K] = 1$ and there are not enough p-independent elements to form a G-basis. Equality (2) in dimension $e = 1$ means that $D_1 \neq 0$ and such an assumption is needed in [5, Theorem 27.3(ii)] to obtain the existence of a one-element canonical basis. Hence it is morally justified to assume (2) in the next Section, where we find a canonical G-basis for a special algebraic group G. Perhaps there are no general reasons for the converse theorem to hold and finding a canonical G-basis is the only possibility for proving the existence of such a basis for a given algebraic group G.

§4. New examples of groups with canonical G-bases

4.1 Unipotent groups of dimension two

In this subsection, we are going to find a canonical G-basis for an algebraic group G of a special type. Firstly we provide a well-known fact about derivations, then define G and its group law. After this we specify which tuples satisfy the canonical G-basis condition in this case and prove the existence of such basis for a $G[m]$-field $(K, \mathbb{D})$ satisfying $[K : C_K] = p^e$.

Fact 4.1. Let L be a field, $\partial \in \mathrm{Der}_C(L)$, $\ker \partial = C \neq L$, $\partial^{(p)} = 0$, then:

(i) there exists an element $z \in L$ such that $\partial(z) = 1$, and $1, z, z^2, \ldots, z^{p-1}$ form a basis of L over C;

(ii) $\ker \partial^{(p-1)} = \mathrm{im}\, \partial$.

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

Proof. The first item is contained in [5, Theorem 27.3]. The second item is in [13, Lemma 3.], but for reader's convenience, we include a short proof. The derivation ∂ is a C-linear map, after computing ∂ on $1, z, z^2, \ldots, z^{p-1}$ we see that $\dim_C \ker \partial = 1$. Therefore, $\dim_C \operatorname{im} \partial = p-1$, moreover $\dim_C \ker \partial^{(p-1)} \leqslant p-1$. The condition $\partial^{(p)} = 0$ implies that $\operatorname{im} \partial \subseteq \ker \partial^{(p-1)}$, but $\dim_C \ker \partial^{(p-1)} \leqslant \dim_C \operatorname{im} \partial$. □

For $i \leqslant p$ let $\lambda_i := (p-1)!/(p-i)!i! \mod p$, which is equal to the image of $(1/p)\binom{p}{i}$ in $\mathbb{F}_p$. Following the [7, page 171], we define

$$\begin{aligned} H_n(X_2, Y_2) &:= \left[\frac{1}{p}((X_2+Y_2)^p - X_2^p - Y_2^p)\right]^{p^n} \\ &= \frac{1}{p}((X_2^{p^n} + Y_2^{p^n})^p - X_2^{p^{n+1}} - Y_2^{p^{n+1}}) \in \mathbb{F}_p[X_2, Y_2], \\ H_n(X_2, Y_2) &= \sum_{i=1}^{p-1} \lambda_i X_2^{ip^n} Y_2^{(p-i)p^n}. \end{aligned}$$

Consider the extension of commutative algebraic groups

$$0 \to \mathbb{G}_a \to G \to \mathbb{G}_a \to 0,$$

where the group operation $*$ on G is given by

$$\begin{aligned} (X_1, X_2) * (Y_1, Y_2) &= F(X_1, X_2, Y_1, Y_2) \\ &:= \left(X_1 + Y_1 + \sum_{n=0}^{M} \alpha_n H_n(X_2, Y_2), X_2 + Y_2\right), \end{aligned}$$

for a fixed $M \in \mathbb{N}$ and $\alpha_i \in k$ for $i \leqslant M$. We are interested in the following m-truncation

$$F[m](v_1, v_2, w_1, w_2) = \left(v_1 + w_1 + \sum_{n=0}^{N} \alpha_n H_n(v_2, w_2), v_2 + w_2\right),$$

where v_1, v_2, w_1 and w_2 are m-truncated variables and $N := \min\{M, m-1\}$. Without loss of generality we assume that $N = m-1$. Let $(K, \mathbb{D})$ be a $G[m]$-field (i.e., $(K, \mathbb{D})$ is a $\hat{G}[m]$-field, but $\hat{G} = \hat{F} = F$, so we consider just an $F[m]$-field), such that $[K : C_K] = p^2$.

LEMMA 4.2. *We have the following:*

(i) $D_{(i,j)} = D_{(i,0)} D_{(0,j)} = D_{(0,j)} D_{(i,0)}$;

(ii) $D_{(i_2,0)} \circ D_{(i_1,0)} = \binom{i_1+i_2}{i_1} D_{(i_1+i_2,0)}$;

(iii) $[p]_{F[m]}(v_1, v_2) = (-\sum_{n=0}^{N} \alpha_n v_2^{p^{n+1}}, 0)$;

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

(iv) $D^{(p)}_{(i,j)} = 0$ *for every* $i, j \leqslant p^{m-1}$ *such that* $i \neq 0$*;*
(v) *if* $j < m$ *then*

$$D^{(p)}_{(0,p^j)} = -\alpha_j D_{(1,0)} + \sum_{n=p}^{p^j} \beta_n D_{(n,0)},$$

for some $\beta_n \in k$*.*

Proof. The first two items are easy. For the proof of third item it is sufficient to prove inductively the following

$$[l]_F(v_1, v_2) = \left(lv_1 + \sum_{n=0}^{N} \alpha_n \left[\left(\frac{1}{p}(l^p - l) \right) v_2^p \right]^{p^n}, lv_2 \right).$$

The fourth and the fifth item use the third part and Corollary 2.25. Specifically, one needs to show

$$D^{(p)}_{(0,j)} = \sum_{i_0+i_1p+\cdots+i_Np^N=j} (-1)^{i_0+\cdots+i_N} \cdot \frac{(i_0+\cdots+i_N)!}{i_0! \cdot \ldots \cdot i_N!} \alpha_0^{i_0} \cdot \ldots \cdot \alpha_N^{i_N} D_{(i_0+\cdots+i_N,0)},$$

for every $j \leqslant p^{m-1}$. We leave it to the reader. ∎

Let us consider the canonical F-derivation from Example 2.10:

$$\mathrm{ev}_F : k[\![X_1, X_2]\!] \to (k[\![X_1, X_2]\!])[\![Y_1, Y_2]\!],$$

where

$$X_1 \mapsto X_1 + Y_1 + \sum_{n=0}^{N} \alpha_n \sum_{i=1}^{p-1} \lambda_i X_2^{ip^n} Y_2^{(p-i)p^n},$$
$$X_2 \mapsto X_2 + Y_2.$$

As in Example 2.12, the above F-derivation could be considered as a G-derivation on $k(G)$ (because $F = \hat{G}$). In this situation $k(G) = k(X_1, X_2)$, so we need to find an embedding φ of $(k(X_1, X_2), \mathbb{D}^G[m])$ in $(K, \mathbb{D})$ such that for $x = \varphi(X_1)$ and $y = \varphi(X_2)$ we have:

(i) $[C_K(x, y) : C_K] = p^2$;

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

(ii) $\sum_{i,j=0}^{p^m-1} D_{(i,j)}(x)v_1^i v_2^j = x + v_1 + \sum_{n=0}^{N} \alpha_n \sum_{i=1}^{p-1} \lambda_i y^{ip^n} v_2^{(p-i)p^n}$;
(iii) $\sum_{i,j=0}^{p^m-1} D_{(i,j)}(y)v_1^i v_2^j = y + v_2$.

The conditions (i), (ii) and (iii) above are equivalent to

$$D_{(1,0)}(x)=1, \quad D_{(0,1)}(x)=\alpha_0\lambda_1 y^{p-1}, \ldots,$$
$$D_{(p^n,0)}(x)=0, \quad D_{(0,p^n)}(x)=\alpha_n\lambda_1 y^{(p-1)p^n}, \ldots$$
$$D_{(1,0)}(y)=0, \quad ,D_{(0,1)}(y)=1, \quad D_{(p,0)}(y)=0, \quad D_{(0,p)}(y)=0, \ldots$$

(since $D_{(1,0)}(x)=1$, $D_{(1,0)}(y)=0$ and $D_{(0,1)}(y)=1$ imply, by Fact 3.2, that $[C_K(x,y):C_K]=p^2$). We are concerned now only with the terms of the form $D_{(p^i,0)}$ and $D_{(0,p^j)}$. It will turn out later that it is enough to consider such terms to obtain expected G-basis. Recall that G is commutative, so each subset of constants is preserved, that is,

$$D_{(i,j)}(C_{(i',j')}) \subseteq C_{(i',j')},$$

for every $i, j, i', j' < p^m$.

Recall also that $[F_{s-1}:F_s]=p^2$ for every $s \in \{0,\ldots,m-1\}$ (Remark 3.4).

Fact 4.3. There exists $x, y \in K$ such that $D_{(1,0)}(x)=1$, $D_{(1,0)}(y)=0$ and $D_{(0,1)}(y)=1$.

Proof. Note that $D_{(1,0)} \in \mathrm{Der}_{C_{(1,0)}}(F_{-1})$ and $D_{(1,0)}^{(p)}=0$, so we can use Lemma 2.22 and obtain $[F_{-1}:C_{(1,0)}] \leqslant p$ (Lemma 2.22 works for iterative HS-derivations, but by [5, Theorem 27.4], $D_{(1,0)}^{(p)}=0$ implies $\mathbb{G}_a$-iterativity). Moreover, from Lemma 4.2,

$$D_{(0,1)}^{(p)}|_{C_{(1,0)}} = -\alpha_0 D_{(1,0)}|_{C_{(1,0)}} = 0,$$

so similarly $[C_{(1,0)}:F_0] \leqslant p$. Since $[F_{-1}:F_0]=[K:C_K]=p^2$, both $D_{(1,0)} \in \mathrm{Der}_{C_{(1,0)}}(F_{-1})$ and $D_{(0,1)}|_{C_{(1,0)}} \in \mathrm{Der}_{F_0}(C_{(1,0)})$ are nonzero, so they satisfy assumptions of Fact 4.1(i). □

LEMMA 4.4. *Let $n \geqslant 0$ and $i, j < p^{n+1}$, be such that $(i,j) \neq (0,0)$. Then we have $F_n \subseteq C_{(i,j)}$.*

Proof. We argue inductively on $l=i+j$ to show that $D_{(i,j)}|_{F_n}=0$ for $i, j < p^{n+1}$ such that $(i,j) \neq (0,0)$. For $l=1$ it is clear. Assume that $i, j < p^{n+1}$, $(i,j) \neq (0,0)$ and for every $i'+j' < i+j$ such that $(i',j') \neq (0,0)$

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

we have $D_{(i',j')}|_{F_n} = 0$. If $i = \gamma_0 + \cdots + \gamma_r p^r$, $j = \beta_0 + \cdots + \beta_s p^s$, $r, s \leqslant n$, $0 \leqslant \gamma_0, \ldots, \gamma_r, \beta_0, \ldots, \beta_s < p$, and $\gamma_r, \beta_s \neq 0$, then from Fact 2.16

$$\gamma_r \beta_s D_{(i,j)} = D_{(i-p^r, j-p^s)} \circ D_{(p^r,p^s)} - \mathbf{r}(D_{(i',j')})_{0<i'+j'<i+j}.$$

By Lemma 4.2 $F_n \subseteq \ker D_{(p^r,0)} \subseteq \ker D_{(p^r,p^s)}$. □

Lemma 4.5. *For each $n \geqslant -1$ sets F_n and $F_n \cap C_{(p^{n+1},0)}$ are subfields of K.*

Proof. By Remark 3.1 F_n is a subfield. Using Lemma 4.4, we get that $D_{(p^{n+1},0)}|_{F_n} \in \mathrm{Der}(F_n)$ and therefore $\ker D_{(p^{n+1},0)}|_{F_n}$, equal to $F_n \cap C_{(p^{n+1},0)}$, also is a subfield. □

4.1.1 Finding y

Fact 4.6. There exists an element $y \in K$ such that:

(i) $D_{(1,0)}(y) = 0$ and $D_{(0,1)}(y) = 1$;
(ii) for every $0 < n < m$ we have $D_{(p^n,0)}(y) = D_{(0,p^n)}(y) = 0$.

Proof. For the proof of (i) consider the element $y \in K$ from Fact 4.3. For the proof of (ii) we inductively correct y. Take the maximal $0 < l < m$ such that for every $0 < l' < l$

$$D_{(p^{l'},0)}(y) = D_{(0,p^{l'})}(y) = 0.$$

Assume that $D_{(p^l,0)}(y) \neq 0$ or $D_{(0,p^l)}(y) \neq 0$, otherwise we have nothing to do.

Let $D_{(p^l,0)}(y) \neq 0$, clearly $D_{(p^l,0)}(y) \in F_{l-1}$, so $D_{(p^l,0)}(y) \in \ker D_{(p^l,0)}|_{F_{l-1}}^{(p-1)}$ equal, due to Fact 4.1, to the image of $D_{(p^l,0)}|_{F_{l-1}}$. There exists $z \in F_{l-1}$ such that $D_{(p^l,0)}(y) = D_{(p^l,0)}(z)$. We exchange y with $y - z$.

Now let $D_{(p^l,0)}(y) = 0$ and $D_{(0,p^l)}(y) \neq 0$. We have $D_{(0,p^l)}(y) \in F_{l-1} \cap C_{(p^l,0)}$ and as before $D_{(0,p^l)}(y) \in \ker D_{(0,p^l)}|_{F_{l-1} \cap C_{(p^l,0)}}^{(p-1)}$. Again, we would like to use Fact 4.1, so it is enough to check that $D_{(0,p^l)}|_{F_{l-1} \cap C_{(p^l,0)}}^{(p)} = 0$, which follows from Lemmas 4.2 and 4.4. □

For the rest of this subsection we fix $y \in K$ as in the fact above.

Remark 4.7. If $p^q \leqslant n < p^{q+1}$ and $D_{(p^q,0)}(a) = 0$, then also $D_{(n,0)}(a) = 0$.

Proof. It is a property of the standard iterativity rule. □

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

The values of $D_{(p^n,0)}$ and $D_{(0,p^n)}$ $(n < m)$ at the element y determine the value of $D_{(i,j)}$ (for every (i,j)) at y, which we show below. Moreover, the proposition below assures us that y fulfills the canonical G-basis conditions.

PROPOSITION 4.8. *We have the following:*

(i) *for all* $n > 0$ $D_{(n,0)}(y) = 0$*;*
(ii) $D_{(n,0)}(y^s) = 0$ *for all* $n > 0$ *and* $1 \leqslant s \leqslant p-1$*;*
(iii) *for all* $n > 1$ $D_{(0,n)}(y) = 0$*;*
(iv) $D_{(0,p^n)}(y^s) = 0$ *for all* $n > 1$ *and* $1 \leqslant s \leqslant p-1$*;*
(v)

$$D_{(i,j)}(y) = \begin{cases} y & \textit{if } (i,j) = (0,0), \\ 1 & \textit{if } (i,j) = (0,1), \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. The item (i) follows from Remark 4.7. The item (ii) is a consequence of the equality $D_{(n,0)}(y^s) = yD_{(n,0)}(y^{s-1})$. Our iterativity rule forces (by Fact 2.16) that

$$(3) \qquad D_{(0,j_2)}D_{(0,j_1)} = \binom{j_1+j_2}{j_1} D_{(0,j_1+j_2)} + \mathbf{r}(D_{(i,j)})_{\substack{0<i+j<j_1+j_2 \\ i\neq 0}}.$$

For the proof of item (iii) we use the equation above in an induction argument. If $p = 2$, then $D_{(0,2)}(y) = 0$. For $p > 2$ we have

$$0 = D_{(0,1)}D_{(0,1)}(y) = 2D_{(0,2)}(y) + \mathbf{r}(D_{(0,j)}D_{(i,0)})_{i\neq 0}(y) = 2D_{(0,2)}(y).$$

Assume that $n \geqslant 2$ and $D_{(0,2)}(y) = \cdots = D_{(0,n)}(y) = 0$. Take $n+1 = \gamma_0 + \gamma_1 p + \cdots + \gamma_s p^s$, where $\gamma_0, \ldots, \gamma_s < p$, $\gamma_s \neq 0$.

$$\begin{aligned} D_{(0,n+1-p^s)}D_{(0,p^s)}(y) &= \gamma_s D_{(0,n+1)}(y) + \mathbf{r}(D_{(0,j)}D_{(i,0)})_{i\neq 0}(y) \\ &= \gamma_s D_{(0,n+1)}(y). \end{aligned}$$

If $s = 0$, then the left-hand side of the last expression is equal to $D_{(0,n)}D_{(0,1)}(y) = 0$, if $s \neq 0$ we proceed similarly due to the equation $D_{(0,p^s)}(y) = 0$. The proof of the item (iv) uses the equation

$$D_{(0,l)}(y^s) = yD_{(0,l)}(y^{s-1}) + D_{(0,l-1)}(y^{s-1})$$

and it is a simple induction on s. The item (v) follows from Lemma 4.2(i). ∎

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

4.1.2 Finding x

Fact 4.9. There exists an element $w \in K$ such that:

(i) $D_{(1,0)}(w) = 1$ and $D_{(0,1)}(w) = 0$;
(ii) for every $0 < n < m$ we have $D_{(p^n,0)}(w) = D_{(0,p^n)}(w) = 0$.

Proof. We define $D^*_{(0,1)} := D_{(0,1)}|_{C_{(1,0)}}$, note that $D^{*(p)}_{(0,1)} = 0$ and $D^*_{(0,1)} \neq 0$. We start with an element x from the statement of Fact 4.3, for which we have $D_{(0,1)}(x) \in C_{(1,0)}$. Naturally $D_{(0,1)}(x) \in \ker D^{*(p-1)}_{(0,1)} = \operatorname{im} D^*_{(0,1)}$. Hence there exists an element $z \in C_{(1,0)}$ such that $D_{(0,1)}(x) = D_{(0,1)}(z)$. Taking $w = x - z$ give us the first part. The second part follows as in the proof of Fact 4.6. □

Lemma 4.10. *There exists an element $x \in K$ satisfying:*

(i) $D_{(1,0)}(x) = 1,\ D_{(0,1)}(x) = \alpha_0 y^{p-1}$;
(ii) $D_{(p^n,0)}(x) = 0$ *and* $D_{(0,p^n)}(x) = \alpha_n y^{(p-1)p^n}$ *for each* $0 < n \leqslant N$;
(iii) $D_{(p^n,0)}(x) = D_{(0,p^n)}(x) = 0$ *for each* $N < n < m$.

Proof. The proof of item (ii) is more complicated, but reasoning is similar to the proof of the point (i).

(i) We start with $x \in K$ from Fact 4.3. If $\alpha_0 = 0$, we proceed like in the proof of Fact 4.6. Assume $\alpha_0 \neq 0$, we need $x' \in C_{(1,0)}$ such that $D_{(0,1)}(x + x') = \alpha_0 y^{p-1}$. We have

$$D_{(1,0)}(\alpha_0 y^{p-1} - D_{(0,1)}(x)) = \alpha_0 D_{(1,0)}(y^{p-1}) = 0,$$

therefore $\alpha_0 y^{p-1} - D_{(0,1)}(x) \in \ker D_{(1,0)} \subseteq \ker D^{(p-1)}_{(1,0)} = \operatorname{im} D_{(1,0)}$. So there exists $z \in K$ such that

$$\alpha_0 y^{p-1} - D_{(0,1)}(x) = D_{(1,0)}(z) = -\frac{1}{\alpha_0} D^{(p)}_{(0,1)}(z).$$

The last equality comes from Lemma 4.2, since $D^{(p)}_{(0,1)} = -\alpha_0 D_{(1,0)}$. Then we can take $x' = -(1/\alpha_0) D^{(p-1)}_{(0,1)}(z)$, since:

$$D_{(1,0)}\left(x - \frac{1}{\alpha_0} D^{(p-1)}_{(0,1)}(z)\right) = 1 - \frac{1}{\alpha_0} D^{(p-1)}_{(0,1)}(D_{(1,0)}(z)),$$

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

but

$$\begin{aligned} D^{(p-1)}_{(0,1)}(D_{(1,0)}(z)) &= D^{(p-1)}_{(0,1)}(\alpha_0 y^{p-1} - D_{(0,1)}(x)) \\ &= \alpha_0 D^{(p-1)}_{(0,1)}(y^{p-1}) - D^{(p)}_{(0,1)}(x) \\ &= \alpha_0(p-1)! + \alpha_0 D_{(1,0)}(x) = \alpha_0((p-1)!+1) \end{aligned} \tag{4}$$

and by Wilson's theorem it is equal to 0.

(ii) As in the proof of 4.6, we take the maximal $0 < l \leqslant N$ such that for every $0 < l' < l$

$$D_{(p^{l'},0)}(x) = 0, \qquad D_{(0,p^{l'})}(x) = \alpha_{l'} y^{(p-1)p^{l'}}.$$

Case 1. $D_{(p^l,0)}(x) \neq 0$.

Clearly, $D_{(p^l,0)}(x) \in C_{(p^{l'},0)}$ for every $0 \leqslant l' < l$. Moreover, for every $0 \leqslant l' < l$

$$\begin{aligned} D_{(0,p^{l'})} D_{(p^l,0)}(x) &= D_{(p^l,0)} D_{(0,p^{l'})}(x) \\ &= D_{(p^l,0)}(\alpha_{l'} y^{(p-1)p^{l'}}) \\ &= \alpha_{l'} D_{(p^{l-l'},0)}(y^{p-1})^{p^{l'}} = 0, \end{aligned} \tag{5}$$

by Proposition 4.8(ii) where the last equation follows. This means that $D_{(p^l,0)}(x) \in F_{l-1}$ and furthermore $D_{(p^l,0)}(x) \in \ker D_{(p^l,0)}|^{(p-1)}_{F_{l-1}} = \operatorname{im} D_{(p^l,0)}|_{F_{l-1}}$. Hence there exists $z \in F_{l-1}$ such that $D_{(p^l,0)}(x) = D_{(p^l,0)}(z)$ and we replace x with $x - z$.

Case 2. $D_{(p^l,0)}(x) = 0$ and $D_{(0,p^l)}(x) \neq \alpha_l y^{(p-1)p^l}$.

If $\alpha_l = 0$ we argue similarly as many times before (compare also with the proof of item (iii)), so let $\alpha_l \neq 0$. The aim of this part is to find an element $x' \in F_{l-1} \cap C_{(p^l,0)}$ such that

$$D_{(0,p^l)}(x + x') = \alpha_l y^{(p-1)p^l}.$$

We introduce

$$W := C_{(0,1)} \cap C_{(p^l,0)} \cap \bigcap_{1 \leqslant l' < l} C_{(p^{l'},0)} \cap C_{(0,p^{l'})}.$$

Note that the element w from Fact 4.9 satisfies $w \in W \setminus \ker D^*_{(1,0)}$, where $D^*_{(1,0)} := D_{(1,0)}|_W$.

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

Claim. $\ker D^*_{(1,0)} \subseteq \operatorname{im} D^*_{(1,0)}$.

Proof of the Claim. Note that $W_0 := W \cap C_{(1,0)} = F_{l-1} \cap C_{(p^l,0)} = \ker D^*_{(1,0)}$ is a subfield of K (by Lemma 4.5). Using Lemma 4.4 we obtain that W is a vector space over W_0. Now take $a \in W$ such that $D^*_{(1,0)}(a) = 0$, that means $a \in W_0$. The element $a \cdot w$ belongs to W and moreover $D^*_{(1,0)}(aw) = aD^*_{(1,0)}(w) = a$, so $a \in \operatorname{im} D^*_{(1,0)}$. □

It is not to hard to see that

$$\alpha_l y^{(p-1)p^l} - D_{(0,p^l)}(x) \in F_{l-1}.$$

Moreover, since $D_{(1,0)}(y) = 0$, we have

$$D_{(p^l,0)}(\alpha_l y^{(p-1)p^l}) = \alpha_l D_{(1,0)}(y^{(p-1)})^{p^l} = \alpha_l (p-1)(y^{p-2} D_{(1,0)}(y))^{p^l} = 0.$$

We conclude that

$$\alpha_l y^{(p-1)p^l} - D_{(0,p^l)}(x) \in F_{l-1} \cap C_{(p^l,0)} = W \cap C_{(1,0)}.$$

In other words $\alpha_l y^{(p-1)p^l} - D_{(0,p^l)}(x) \in \ker D^*_{(1,0)} \subseteq \operatorname{im} D^*_{(1,0)}$, and there is $z \in W$ such that

$$\alpha_l y^{(p-1)p^l} - D_{(0,p^l)}(x) = D_{(1,0)}(z).$$

From Lemma 4.2 we know that

$$D^{(p)}_{(0,p^l)} = -\alpha_l D_{(1,0)} + \sum_{n=p}^{p^l} \beta_n D_{(n,0)},$$

for some $\beta_n \in k$. By Remark 4.7 for every $p \leqslant i \leqslant p^l$ $D_{(i,0)}|_W = 0$, consequently $D_{(1,0)}(z) = -(1/\alpha_l) D^{(p)}_{(0,p^l)}(z)$. For x' take $-(1/\alpha_l) D^{(p-1)}_{(0,p^l)}(z)$, only an argument for $D^{(p-1)}_{(0,p^l)}(z) \in C_{(1,0)}$ is missing, and it is straightforward modification of the equation (4).

(iii) It follows the proof of Fact 4.6, we need to check only that $D_{(p^l,0)}(x), D_{(0,p^l)}(x) \in F_{l-1}$ for $l > N$. Obviously, $D_{(p^l,0)}(x), D_{(0,p^l)}(x) \in \bigcap_{l'=0}^{l-1} C_{(p^{l'},0)} \cap \bigcap_{l'=N+1}^{l-1} C_{(0,p^{l'})}$. Let $0 \leqslant l' \leqslant N$, then

$$D_{(p^l,0)} D_{(0,p^{l'})}(x) = D_{(p^l,0)}(\alpha_{l'} y^{(p-1)p^{l'}}) = \alpha_{l'} D_{(p^{l-l'},0)}(y^{p-1})^{p^{l'}} = 0,$$

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

as in (5). Furthermore,

$$D_{(0,p^l)}D_{(0,p^{l'})}(x)=D_{(0,p^l)}(\alpha_{l'}y^{(p-1)p^{l'}})=\alpha_{l'}D_{(0,p^{l-l'})}(y^{p-1})^{p^{l'}},$$

so we are done if $D_{(0,p^{l-l'})}(y^{p-1})=0$, which is a part of Proposition 4.8. □

We fix $x\in K$ as in the above fact.

LEMMA 4.11. *We have the following:*

(i) *for all* $n>1$ $D_{(n,0)}(x)=0$*;*
(ii) *for all* $n>0$

$$D_{(0,n)}(x)=\begin{cases}\alpha_l\lambda_i y^{(p-i)p^l} & \textit{if } 0\leqslant l\leqslant N, 1\leqslant i<p, n=ip^l,\\ 0 & \textit{otherwise.}\end{cases}$$

Proof. The item (i) for $n\geqslant p$ follows from Remark 4.7, and for $1<n<p$ from Lemma 4.2 and $D_{(1,0)}(x)=1$. To prove the item (ii) we argue inductively. Note that $\lambda_1=1$, so for $n=1$ it is clear. Assume that for every $n'<n$ our thesis is true. Let $n=\gamma_0+\gamma_1 p+\cdots+\gamma_s p^s$, where $\gamma_0,\ldots,\gamma_s<p$ and $\gamma_s\neq 0$.

Claim 1.

$$D_{(0,n-p^s)}D_{(0,p^s)}(x)=\gamma_s D_{(0,n)}(x), \tag{6}$$

$$D_{(0,n-\gamma_s p^s)}D_{(0,\gamma_s p^s)}(x)=D_{(0,n)}(x). \tag{7}$$

Proof of the Claim 1. Both equations have similar proofs, so we consider only the first one. We start with the equation (3) for $j_1=p^s$ and $j_s=n-p^s$:

$$D_{(0,n-p^s)}D_{(0,p^s)}=\gamma_s D_{(0,n)}+\mathbf{r}(D_{(i,j)})_{\substack{0<i+j<n\\ i\neq 0}}.$$

Our aim is to show that $D_{(i,j)}(x)=0$ for $0<i+j<n$, $i\neq 0$. The component with $D_{(1,0)}$ $(i=1$ and $j=0)$ does not occur. To see this, we compare the sides of the equation from the iterativity definition for our chosen iterativity rule, where on the left-hand side we focus on $D_{(0,n-p^s)}D_{(0,p^s)}$. A nonzero component with $D_{(1,0)}$ implies that $n=p^{s+1}$ and this is impossible. Let us assume that $i=1$ and $j>0$. Because of $j<n$, $D_{(0,j)}(x)$ is, due to the inductive assumption, equal to βy^r for some $\beta\in k$ and $r>0$, and then $D_{(1,0)}D_{(0,j)}(x)=D_{(1,0)}(\beta y^r)=0$. If $i>1$, then $D_{(i,j)}(x)=D_{(0,j)}D_{(i,0)}(x)=0$. □

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

Claim 2. For every $0 \leqslant l \leqslant N$ and $0 < i < p$ we have $D_{(0,ip^l)}(x) = \alpha_l \lambda_i y^{(p-i)p^l}$.

Proof of the Claim 2. It is quite an obvious induction, using Claim 1:

$$\begin{aligned} D_{(0,(1+i)p^l)}(x) &= \frac{1}{i+1} D_{(0,p^l)} D_{(0,ip^l)}(x) = \frac{1}{i+1} D_{(0,p^l)}(\alpha_l \lambda_i y^{(p-i)p^l}) \\ &= \frac{\alpha_l \lambda_i}{i+1} D_{(0,1)}(y^{p-i})^{p^l} = \frac{\alpha_l \lambda_i}{i+1}(p-i) y^{(p-i-1)p^l} \\ &= \alpha_l \lambda_{i+1} y^{(p-i-1)p^l}. \end{aligned}$$ □

Now we are going to the proof of the main induction step. We deal with several cases. If $s > N$, then $D_{(0,p^s)}(x) = 0$ and the equation (6) implies that $D_{(0,n)}(x) = 0$. We can assume that $s \leqslant N$ and $n - \gamma_s p^s \neq 0$ (otherwise we apply claim 2),

$$D_{(0,n)}(x) = D_{(0,n-\gamma_s p^s)} D_{(0,\gamma_s p^s)}(x) = \alpha_s \lambda_{\gamma_s} D_{(0,n-\gamma_s p^s)}((y^{p-\gamma_s})^{p^s}).$$

Recall that for every $a \in K$ the element a^{p^s} belongs to F_{s-1}, thus by Lemma 4.4 $D_{(0,n-\gamma_s p^s)}(a^{p^s}) = 0$. □

We show below that fixed element x satisfies the required properties.

Proposition 4.12.

$$D_{(i,j)}(x) = \begin{cases} x & \textit{if } (i,j) = (0,0), \\ 1 & \textit{if } (i,j) = (1,0), \\ \alpha_l \lambda_i y^{(p-i)p^l} & \textit{if } (i,j) = (0, ip^l), 0 \leqslant l \leqslant N, 1 \leqslant i < p, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. By Lemma 4.2(i) we decompose $D_{(i,j)}$ into $D_{(0,j)} D_{(i,0)}$. For $i \geqslant p$ Remark 4.7 and $D_{(p^n,0)}(x) = 0$, where $0 < n < m$, ensure us that $D_{(i,0)}(x) = 0$, thus also $D_{(i,j)}(x) = 0$. For $1 < i < p$ Remark 4.7(ii) used in an inductive argument give $D_{(i,0)}(x) = 0$. If $i = 1$, then $D_{(i,j)}(x) = D_{(j,0)}(1)$. Hence $D_{(i,j)}(x) \neq 0$ if and only if $j = 0$. The case with $i = 0$ is exactly Lemma 4.11. □

By Propositions 4.8 and 4.12 the pair $\{x, y\}$ is a canonical G-basis (see the beginning of Section 4.1). Thus we end with the following:

Corollary 4.13. *For G as defined above, any $m \in \mathbb{N}_{>0}$ and any $G[m]$-field $(K, D[m])$ such that $[K : C_K] = p^2$, there is a canonical G-basis in K.*

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

4.2 Canonical G-bases for commutative and connected groups

In the previous subsection we showed the existence of a canonical G-basis for every $G[m]$-field $(K, \mathbb{D})$ such that $[K : C_K] = p^e$, where G was very specific. Now we are going to apply those results to a more general class of algebraic groups.

Definition 4.14. Let G be an algebraic group over k

(1) We call G *integrable* if for any $m \in \mathbb{N}_{>0}$, every $G[m]$-derivation on a field K such that $[K : C_K] = p^{\dim G}$ is strongly integrable.

(2) If for any $m \in \mathbb{N}_{>0}$, every $G[m]$-field K such that $[K : C_K] = p^{\dim G}$ has a canonical G-basis, we call G *canonically integrable.*

By Theorem 3.8 each canonically integrable algebraic group is integrable.

Lemma 4.15. *Let G and H be algebraic groups over k. If both are canonically integrable, then also $G \times H$ is canonically integrable.*

Proof. Introduce $A := G \times H$, $e_1 : \dim G$, $e_2 := \dim H$ and let $(K, \mathbb{D})$ be an $A[m]$-field such that $[K : C_K] = p^{e_1+e_2}$. We define

$$\mathbb{D}' := (D'_{(j_1,\ldots,j_{e_1})} := D_{(j_1,\ldots,j_{e_1},\underbrace{0,\,\ldots\,,0}_{e_2 \text{ times}})})_{j_1,\ldots,j_{e_1}<p^m},$$

$$\mathbb{D}'' := (D''_{(j_{e_1+1},\ldots,j_{e_1+e_2})} := D_{(\underbrace{0,\,\ldots\,,0}_{e_1 \text{ times}},j_{e_1+1},\ldots,j_{e_1+e_2})})_{j_{e_1+1},\ldots,j_{e_1+e_2}<p^m}.$$

From the $A[m]$-iterativity diagram (see Definition 2.8) it follows that

$$D_{(j_1,\ldots,j_{e_1+e_2})} = D'_{(j_1,\ldots,j_{e_1})} D''_{(j_{e_1+1},\ldots,j_{e_1+e_2})},$$

$\mathbb{D}'$ is $G[m]$-iterative and the second one, $\mathbb{D}''$ is $H[m]$-iterative.

Taking any p-basis of K over C_K and using Remark 3.4 assures us that for every $s < m$ $[F_{s-1} : F_s] = p^{e_1+e_2}$. Thus $[K : C_K^{\mathrm{abs}}] = p^{m(e_1+e_2)}$. For $s < m$ we introduce

$$F'_s := \bigcap_{j=0}^{s} C_{(p^j,0,\ldots,0)} \cap \cdots \cap C_{(0,\ldots,0,p^j,\underbrace{0,\,\ldots\,,0}_{e_2 \text{ times}})}, \qquad F'_{-1} := K,$$

$$F''_s := \bigcap_{j=0}^{s} C_{(\underbrace{0,\,\ldots\,,0}_{e_1 \text{ times}},p^j,0\ldots,0)} \cap \cdots \cap C_{(0,\ldots,0,p^j)}, \qquad F''_{-1} := K.$$

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

Consider the following tower of subfields

$$K\supseteq F_0'\supseteq F_1'\supseteq\cdots\supseteq F_{m-1}'\supseteq F_{m-1}'\cap F_0''\supseteq F_{m-1}'\cap F_1''\supseteq\cdots F_{m-1}'\cap F_{m-1}''.$$

For every $s<m$, due to Lemma 2.22 and $[K:C_K^{\mathrm{abs}}]=p^{m(e_1+e_2)}$, we have

$$[F_{s-1}':F_s']=p^{e_1},\qquad [F_{m-1}'\cap F_{s-1}'':F_{m-1}'\cap F_s'']=p^{e_2}.$$

In particular

$$[F_{m-1}':F_{m-1}'\cap F_0'']=p^{e_2},$$

so there exists a canonical $H[m]$-basis $\{\beta_1,\ldots,\beta_{e_2}\}$ of $(F_{m-1}',\mathbb{D}'')$. Analogously, there exists a canonical $G[m]$-basis $\{b_1,\ldots,b_{e_1}\}$ of $(F_{m-1}'',\mathbb{D}')$. Elements $\beta_1,\ldots,\beta_{e_2}$ are p-independent in F_{m-1}' over $F_{m-1}'\cap F_0''$. By Corollary 2.19, they are also p-independent in K over F_0''. Similarly for elements $b_1,\ldots,b_{e_1}$, Corollary 2.19 implies that they are p-independent in F_0'' over $F_0''\cap F_0'$. We have

$$[F_0'':F_0''\cap F_0']\leqslant p^{e_1},$$

hence $F_0(b_1,\ldots,b_{e_1})=F_0''$ (note that $C_K=F_0=F_0''\cap F_0'$). Now we have all the ingredients to state that $B:=\{b_1,\ldots,b_{e_1},\beta_1,\ldots,\beta_{e_2}\}$ is a p-basis of K over C_K. Verification that B is also a canonical A-basis is not hard and left to the reader. □

We note the obvious fact:

Fact 4.16. Let G and H be isomorphic algebraic groups over k. If G is canonically integrable, then also H is canonically integrable.

We can prove now the main theorem of this paper.

THEOREM 4.17. *Let G be a commutative and connected linear algebraic group over an algebraically closed field k. If maximal unipotent subgroup of G has dimension at most 2, then G is integrable.*

Proof. Due to "Jordan decomposition" (last theorem on [10, page 70]), G decomposes as $G_U\times G_S$, where G_U consists of unipotent elements and G_S of semisimple elements. If the dimension of G_U is equal to 2 we know by [7, Proposition 8, page 171] that G_U is isomorphic to the group defined at the beginning of the previous subsection, so it is canonically integrable. If $\dim G_U=1$, then by [8, Theorem 3.4.9] it is isomorphic to $\mathbb{G}_a$, so canonically integrable by [1, Proposition 4.5]. We focus now on the semisimple part.

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

By [8, Lemma 2.4.2(ii)], G_S is diagonalizable, and by [8, Corollary 3.2.7(ii)] it is a torus. Proposition 4.10 from [1] states that also $\mathbb{G}_m$ is canonically integrable, so our group G is isomorphic to the product of canonically integrable groups. Finally, we use Lemma 4.15, Fact 4.16 and Theorem 3.8. □

In most cases of applications of the model theory to the differential algebra, we are dealing with an algebraic group G over a field k, which is assumed only to be perfect. One may wonder if Theorem 4.17 can be used for such $G[m]$-fields, that is, for models of $G[m]-\mathrm{DCF}$ [2]. The answer is positive, because separable closure of k, which is also algebraic closure, is contained in the absolute constants for models of $G[m]-\mathrm{DCF}$ (for an argument check e.g. proof of [12, Theorem 10]).

4.3 Possible generalizations

The desired generalization is to drop, in the assumptions of Theorem 4.17, the condition for the dimension of the unipotent component of group G. Unfortunately, the ideas from the above proof do not work in the case of unipotent groups of dimension higher than 2. There are several reasons for that, which will be explained below.

First of all, we are using in Section 4.1 formulas for the group law of our group G. Commutative, connected unipotent groups of dimension 2 are characterized by [7, Proposition 8, page 171], so the explicit formulas for the group law are known. For the unipotent groups of dimension 3 or greater, the best known to the author results coincide with [7, Theorem 1, page 176] and [7, Theorem 2, page 177]. It is unknown how the condition “being a subgroup” translates to the case of iterative derivations, hence the last reference does not help in finding a canonical basis. However, there is a hope to use [7, Theorem 1, page 176]. We sketch this idea and reveal difficulties in extending our technique to this context.

Assume that G is isogenous to W_n (the Witt group of dimension n). We should give a modification of [1, Lemma 2.6], from which we would conclude that G is integrable if and only if W_n is integrable. If this can be done, then we need to check whether W_n is integrable. Unluckily, the whole procedure from Section 4.1 cannot be extended to show the existence of a canonical basis for W_n. Even in the case $p=2$ and $n=3$, some issues appear. If we translate the group law of W_3 (given by e.g. the formulas (a) and (b) in [11, page 128]) for $p=2$ into the conditions for a canonical basis:

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

(i) $[C_K(x, y, z) : C_K] = 2^3$;
(ii) $\sum_{i,j,l=0}^{2^m-1} D_{(i,j,l)}(x) v_1^i v_2^j v_3^l = x + v_1 - yv_2 + yzv_3 + zv_2v_3 - zv_3^3 - z^3v_3$;
(iii) $\sum_{i,j,l=0}^{2^m-1} D_{(i,j,l)}(y) v_1^i v_2^j v_3^l = y + v_2 - zv_3$;
(iv) $\sum_{i,j,l=0}^{2^m-1} D_{(i,j,l)}(z) v_1^i v_2^j v_3^l = z + v_3$;

we can notice occurrence of equations of a new kind:

$$D_{(0,1,1)}(x) = z.$$

Proofs from Section 4.1 involve only "one-dimensional differential equations" and the above equation is not of such a form. The "one-dimensional differential equations" appear, because after diminishing the dimension by 1, at the induction step, we deal with one-dimensional subgroup, what is the case for two-dimensional group G.

To summarize, generalizations of Theorem 4.17 to the higher dimensional unipotent component case need to involve new proofs. It is also possible that such a generalization cannot be done without some additional assumptions, or even cannot be done at all.

Acknowledgments. I thank my advisor, Piotr Kowalski, for his invaluable contribution. I am also grateful to the referee for a very useful report.

References

[1] D. Hoffmann and P. Kowalski, *Integrating Hasse–Schmidt derivations*, J. Pure Appl. Algebra **219**(4) (2015), 875–896.
[2] D. Hoffmann and P. Kowalski, *Existentially closed fields with G-derivations*, J. Lond. Math. Soc. **93**(3) (2016), 590–618.
[3] P. Kowalski, *Geometric axioms for existentially closed Hasse fields*, Ann. Pure Appl. Logic **135** (2005), 286–302.
[4] H. Matsumura, *Integrable derivations*, Nagoya Math. J. **87** (1982), 227–245.
[5] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1986.
[6] K. Okugawa, *Basic properties of differential fields of an arbitrary characteristic and the Picard–Vessiot theory*, J. Math. Kyoto Univ. **2**(3) (1962), 295–322.
[7] J. P. Serre, *Algebraic Groups and Class Fields: Translation of the French Edition*, Graduate Texts in Mathematics Series, Springer-Verlag New York Incorporated, 1988.
[8] T. A. Springer, *Linear Algebraic Groups*, 2nd ed., Birkhäuser, Basel, 1998.
[9] A. Tyc, *On F-integrable actions of the restricted Lie algebra of a formal group F in characteristic $p > 0$*, Nagoya Math. J. **115** (1989), 125–137.
[10] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Springer, 1979.
[11] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p*, J. Reine Angew. Math. **176** (1937), 126–140.

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press

[12] C. Wood, *The model theory of differential fields of characteristic* $p \neq 0$, Proc. Amer. Math. Soc. **40**(2) (1973), 577–584.

[13] M. Ziegler, Canonical p-bases. Available on http://home.mathematik.uni-freiburg.de/ziegler/preprints/canonical-p-bases.pdf.

[14] M. Ziegler, *Separably closed fields with Hasse derivations*, J. Symbolic Logic **68** (2003), 311–318.

Instytut Matematyczny
Uniwersytet Wrocławski
Wrocław
Poland
daniel.hoffmann@math.uni.wroc.pl

https://doi.org/10.1017/nmj.2017.25 Published online by Cambridge University Press