ISRAEL JOURNAL OF MATHEMATICS **190** (2012), 349–363
DOI: 10.1007/s11856-011-0178-2

SCHANUEL PROPERTY FOR ADDITIVE POWER SERIES

BY

Piotr Kowalski*

Instytut Matematyczny, Uniwersytet Wrocławski
pl. Grunwaldzki 2/4, 50-384 Wrocław, Poland
e-mail: pkowa@math.uni.wroc.pl
URL: http://www.math.uni.wroc.pl/~pkowa/

ABSTRACT

We prove a version of Schanuel's Conjecture for a field of Laurent power series in positive characteristic replacing $\mathbb{C}$ and a non-algebraic additive power series replacing the exponential map.

1. Introduction

In [2], James Ax proved the power series version of Schanuel's Conjecture [2, (SP)], which may be regarded as a transcendence statement about the exponential map on an algebraic torus. By the "power series version", we mean that the field of complex numbers is replaced with the non-Archimedean field of power series, where the exponential map is evaluated. In [3], Ax extended [2, (SP)] from a torus to an arbitrary semi-abelian variety. Bertrand noticed in [5] that a semi-abelian variety may be replaced with any commutative algebraic group without additive quotients. Ax also proved a transcendence statement about differential fields of characteristic 0 [2, (SD)], which was used to prove [2, (SP)]. An elliptic curve version was proved by Brownawell and Kubota in [7] and Kirby [12] generalized both these results to the case of semi-abelian varieties.

Trying to extend the power series version of Schanuel's Conjecture to the positive characteristic case one immediately faces a basic problem — there are

* Supported by the Polish grant MEN no. N N201 545938
Received May 12, 2010 and in revised form August 1, 2010

no exponential maps over a field of positive characteristic! Therefore some other formal maps need to be considered. A Schanuel type result was obtained [13, 6.12] for a raising to power map on a characteristic zero algebraic torus replacing the exponential map. A right class of possible powers needs to be specified, since e.g. the identity map obviously does not yield any transcendence results. The class which was isolated in [13] is very natural: it consists of power series (expansions of) X^α, where the algebraic degree of α over $\mathbb{Q}$ is bigger than the dimension of the torus. The main theorem of this paper is analogous to [13, 6.12], where a characteristic 0 torus is replaced with a positive characteristic vector group. It is worth mentioning here a related result [4, Theorem 1.1], which concerns raising to powers in the Archimedean case, however the non-algebraicity condition on the set of the possible powers is rather restrictive there.

The ring of endomorphisms of the (algebraic) additive group over $\mathbb{F}_p$ coincides with the ring of additive polynomials (with composition) over $\mathbb{F}_p$ which we denote $\mathbb{F}_p[\mathrm{Fr}]$. It is isomorphic to the twisted (by Frobenius) polynomial ring over $\mathbb{F}_p$, but since Frobenius acts trivially on $\mathbb{F}_p$, it is isomorphic to the polynomial ring $\mathbb{F}_p[X]$. In the torus case this ring is $\mathbb{Z}$, so both rings are similar to each other, e.g. they are both 1-dimensional. The ring of formal endomorphisms of the additive group of $\mathbb{F}_p$ coincides with the ring of additive power series denoted $\mathbb{F}_p[\![\mathrm{Fr}]\!]$ (with composition) and it is isomorphic to the power series ring $\mathbb{F}_p[\![X]\!]$.

Let $\mathbb{F}_p(\mathrm{Fr})$ denote the fraction field of $\mathbb{F}_p[\mathrm{Fr}]$. If we have in mind that $\mathbb{Z}$ corresponds to $\mathbb{F}_p[\mathrm{Fr}]$, then the main theorem below is of the same form as the theorem about the torus from [13].

THEOREM 1.1: *Let $F \in \mathbb{F}_p[\![\mathrm{Fr}]\!]$ and assume that the algebraic degree of F over $\mathbb{F}_p(\mathrm{Fr})$ is greater than n (e.g. F is transcendental over $\mathbb{F}_p(\mathrm{Fr})$). Let $x_1, \ldots, x_n \in t\mathbb{F}_p[\![t]\!]$ be linearly independent over $\mathbb{F}_p[\mathrm{Fr}]$ and*

$$g := (x_1, \ldots, x_n, F(x_1), \ldots, F(x_n)).$$

Then $\mathrm{trdeg}_{\mathbb{F}_p}(g) \geqslant n + 1$.

Let us note that the assumptions of the above theorem cannot be weakened. Firstly, the linear independence over $\mathbb{F}_p$ does not suffice. For instance t, t^p are $\mathbb{F}_p$-independent but the transcendence degree of $(t, t^p, F(t), F(t^p))$ is not greater than 2, for $F(t^p) = (F(t))^p$. Secondly, we can neither relax the non-algebraicity assumption on F. If F is algebraic over $\mathbb{F}_p(\mathrm{Fr})$ of degree n,

then $t, F(t), \ldots, F^{n-1}(t)$ (compositional powers) are linearly independent over $\mathbb{F}_p[\mathrm{Fr}]$, and for $x := (t, F(t), \ldots, F^{n-1}(t))$, we have $\mathrm{trdeg}_{\mathbb{F}_p}(x, F(x)) \leqslant n$. Using Hensel's Lemma, it is easy to see that for any n which is non-divisible by p, there is an additive power series which is algebraic over $\mathbb{F}_p(\mathrm{Fr})$ of degree n.

There are many other results about transcendence in positive characteristic which are related to Drinfeld modules; see, e.g., [15] and [17]. The main difference between these results and our case is that we do not allow "non-constant coefficients"—this is discussed in Section 6.2.

A possible line of further research is to replace an additive power series with a formal map between algebraic groups in positive characteristic. The most natural example of such a map is a formal isomorphism between an ordinary elliptic curve and the multiplicative group. Such formal maps will be considered in a forthcoming paper.

This paper is organized as follows. In Section 2 we recall Vojta's notion of higher differential forms and prove a technical result about linear dependence of differential forms. This result replaces the usage of the Lie derivative in Ax's proof. We find in Section 3 a non-zero additive power series which vanishes on g in a certain strong sense. In Section 4, we use this power series to find additive polynomials vanishing on g. In Section 5 we show how these polynomials affect the degree of F over $\mathbb{F}_p(\mathrm{Fr})$. In Section 6 we discuss generalizations of Theorem 1.1 and its relationship to some other results.

Acknowledgement. I would like to thank Boris Zilber for suggesting this topic to me, Daniel Bertrand for his comments, Amador Martin-Pizarro for many stimulating discussions and the referee for her/his helpful report.

2. Linear dependence of differential forms

In this section we prove a technical result about dependence of (higher) differential forms under certain assumptions. Throughout this section C is a perfect field of positive characteristic p and T is a C-algebra. We will use Vojta's higher forms from [16]. Its usage here is not absolutely necessary, but it simplifies some arguments. For $m \in \mathbb{N}$ let $\mathrm{HS}^m_{T/C}$ (we suppress "$/C$" in the sequel) denote the T-**algebra** of higher differential forms which comes with the universal Hasse–Schmidt derivation over C (HS-derivation for short) of order m

$$(\mathrm{d}_0, \ldots, \mathrm{d}_m) : T \to \mathrm{HS}^m_T\,.$$

For precise definitions, the reader should consult [16]. The T-algebra HS_T^m is generated by the symbols of the form $\mathrm{d}_i(t)$ for $0 \leqslant i \leqslant m$ and $t \in T$ which satisfy the following relations:

- for each $t \in T$, $\mathrm{d}_0(t) = t$,
- for each $c \in C$ and $1 \leqslant i \leqslant m$, $\mathrm{d}_i(c) = 0$,
- for each $t, t' \in T$ and $0 \leqslant i \leqslant m$,

$$\mathrm{d}_i(t + t') = \mathrm{d}_i(t) + \mathrm{d}_i(t'), \quad \mathrm{d}_i(tt') = \sum_{k+l=i} \mathrm{d}_k(t)\mathrm{d}_l(t').$$

In particular, we have $\mathrm{d}_{p^{n+1}}(t^p) = \mathrm{d}_{p^n}(t)^p$ and $\mathrm{d}_1(t^p) = 0$. Let us also notice that $\mathrm{HS}_T^0 = T$ and $\mathrm{HS}_T^1 = S(\Omega_T)$ (the symmetric algebra). We will use the following easy observation.

LEMMA 2.1: *Let $C \subseteq L$ be a field extension, $a \in L$ and $m \in \mathbb{N}$. Then the following are equivalent:*

(1) $a \in L^{p^{m+1}}$,
(2) $\mathrm{d}_1(a) = \mathrm{d}_2(a) = \cdots = \mathrm{d}_{p^m}(a) = 0$,
(3) $\mathrm{d}_{p^m}(a) = 0$.

Proof. Only (3) to (1) requires an argument. Assume $a \in L \setminus L^{p^{m+1}}$. Therefore, there is $n \in \{0, \ldots, m\}$ and $b \in L \setminus L^p$ such that $a = b^{p^n}$. We can extend $\{b\}$ to B, a p-basis of L over C. Since C perfect, the extension $C \subseteq L$ is separable. Thus, by [14, Theorem 26.8], B is algebraically independent over C and L is étale over $C(B)$. There is an HS-derivation D on $C(B)$ vanishing on C such that $D_{p^{m-n}}(b) \neq 0$. Therefore

$$D_{p^m}(a) = D_{p^{m-n}}(b)^{p^n} \neq 0.$$

By [14, Theorem 27.2], D extends (uniquely) to an HS-derivation D' on L. Since $D'_{p^m}(a) \neq 0$, we have $\mathrm{d}_{p^m}(a) \neq 0$. ∎

Additive power series give rise to infinite sequences having a certain property which motivates the following definition.

Definition 2.2: A sequence $(h_m \in T)_m$ is **compatible** if $h_{m+1} - h_m \in T^{p^{m+1}}$ for each $m \in \mathbb{N}$.

If $T = C[X_1, \ldots, X_k]$, then any additive power series in k variables is a limit of a compatible sequence of additive polynomials from T. Obviously, there are many compatible sequences of additive polynomials converging to the same

power series (there is the most natural choice though). However, (h_m) and (t_m) converge to the same power series if and only if for each m, we have $h_m - t_m \in T^{p^{m+1}}$. This observation motivates the next definition.

Definition 2.3: Let $h := (h_m)$ be a compatible sequence on T and $k \in \mathbb{N}$.

- The sequence h **vanishes** if for each m, we have $h_m \in T^{p^{m+1}}$.
- We write $h \in T^{p^{k+1}}$ if $h_k \in T^{p^{k+1}}$.

Note that h vanishes if and only if, for each $k \in \mathbb{N}$, $h \in T^{p^{k+1}}$ and that $h \in T^{p^{k+1}}$ if and only if, for each $0 \leqslant i \leqslant k$, $h_i \in T^{p^{i+1}}$.

If we have a homomorphism of C-algebras $T_1 \to T_2$, then using this homomorphism we can send any compatible sequence on T_1 to a compatible sequence on T_2, so we sometimes say that a compatible sequence on T_1 vanishes on T_2.

For a compatible sequence $h = (h_m)$ on T, we define $\mathrm{d}_{p^k}(h)$ as $\mathrm{d}_{p^k}(h_k)$. Note that for each $l \geqslant k$, we have $\mathrm{d}_{p^k}(h) = \mathrm{d}_{p^k}(h_l)$. By 2.1 we obtain the following corollary.

COROLLARY 2.4: *Let h be a compatible sequence on L and $k \in \mathbb{N}$. Then we have:*

(1) *$h \in L^{p^{k+1}}$ if and only if $\mathrm{d}_{p^k}(h) = 0$,*
(2) *h vanishes if and only if $\mathrm{d}_{p^k}(h) = 0$ for all k.*

The next lemma replaces the usage of the Lie derivative in Ax's proof from [3] (see also [12] and [13]).

PROPOSITION 2.5: *Let $C \subseteq L \subseteq K$ be a tower of fields. Assume that $L \nsubseteq K^p$, $K^{p^\infty} = C$ and $\mathrm{trdeg}_C L \leqslant n$. Let $a_1, \ldots, a_n$ be compatible sequences on L vanishing on K. Then $\mathrm{d}_1(a_1), \ldots, \mathrm{d}_1(a_n) \in \Omega_L$ are linearly dependent over C. Moreover, if $a_1, \ldots, a_n \in L^{p^k}$ for some $k > 0$, then $\mathrm{d}_{p^k}(a_1), \ldots, \mathrm{d}_{p^k}(a_n) \in \mathrm{HS}_L^{p^k}$ are linearly dependent over C.*

Proof. We fix $m \in \mathbb{N}$ and denote $L \cap K^{p^m}$ by L_m. Since $L \nsubseteq K^p$, then $L^{p^m} \nsubseteq K^{p^{m+1}}$; in particular, we have $L_m \nsubseteq K^{p^{m+1}}$. By 2.1, the natural map

$$\phi : \Omega_{L_m} \to \Omega_{K^{p^m}}$$

is non-zero.

Since the extension $C \subseteq L_m$ is separable, by [14, 26.8] we have

$$\dim_{L_m} \Omega_{L_m} \leqslant \mathrm{trdeg}_C(L_m) \leqslant n.$$

For each i, we have $a_{i,m} \in L_{m+1} \subseteq L_m$, for a_i vanishes on K. Therefore $\mathrm{d}_1(a_{i,m}) \in \Omega_{L_m}$ and

$$\mathrm{d}_1(a_{1,m}), \ldots, \mathrm{d}_1(a_{n,m}) \in \ker(\phi).$$

Since ϕ is non-zero, $\dim_{L_m}(\ker(\phi)) < n$, therefore $\mathrm{d}_1(a_{1,m}), \ldots, \mathrm{d}_1(a_{n,m})$ are linearly dependent over L_m in Ω_{L_m}. However, for each i, $\mathrm{d}_1(a_i) = \mathrm{d}_1(a_{i,m})$ in Ω_L, hence $\mathrm{d}_1(a_1), \ldots, \mathrm{d}_1(a_n)$ are linearly dependent over L_m in Ω_L for each m. Since $C = \bigcap L_m$, we get that $\mathrm{d}a_1, \ldots, \mathrm{d}a_n$ are linearly dependent over C.

For the 'moreover' clause, notice that if b is a compatible sequence on L which vanishes on K and such that $b \in L^{p^k}$, then

$$(\sqrt[p^k]{b_k},\ \sqrt[p^k]{b_{k+1}}, \ldots)$$

is a compatible sequence on L which vanishes on K. Then we can use the case of $k = 0$ proved above, since $\mathrm{d}_{p^k}(b_k) = \mathrm{d}_1(\sqrt[p^k]{b_k})^{p^k}$. ∎

3. A vanishing power series

We proceed towards the proof of 1.1. Let us assume that $\mathrm{trdeg}_{\mathbb{F}_p}(g) \leqslant n$ and we want to show that $x_1, \ldots, x_n$ are linearly dependent over $\mathbb{F}_p[\mathrm{Fr}]$. We will prove this in Section 5. In this section, we find a non-zero power series of a special form which vanishes on g in the sense of 2.3.

Let us define:

$$L = \mathbb{F}_p(g),\ K = \mathbb{F}_p((t)),\ \bar{X} = (X_1, \ldots, X_n),\ \bar{Y} = (Y_1, \ldots, Y_n).$$

To apply 2.5 to our situation we need to know whether $L \nsubseteq K^p$. It need not be the case, but we will show below that without loss of generality we may assume it is. Assume that for each i we have $x_i = y_i^p$. Since $F(y_i^p) = (F(y_i))^p$, we get

$$\mathrm{trdeg}_{\mathbb{F}_p}(x_1, F(x_1), \ldots, x_n, F(x_n)) = \mathrm{trdeg}_{\mathbb{F}_p}(y_1, F(y_1), \ldots, y_n, F(y_n)).$$

It is also easy to see that the linear dependence of $y_1, \ldots, y_n$ over $\mathbb{F}_p[\mathrm{Fr}]$ implies the linear dependence of $x_1, \ldots, x_n$. Thus we can replace $x_1, \ldots, x_n$ with $y_1, \ldots, y_n$. Then the only problem could be that $x_1, \ldots, x_n \in K^{p^\infty}$, but since $K^{p^\infty} = \mathbb{F}_p$, we would get the $\mathbb{F}_p$-dependence then.

We have a $\mathbb{F}_p$-algebra homomorphism

$$\mathbb{F}_p[\overline{X}, \overline{Y}] \ni w \mapsto w(g) \in L,$$

so it is meaningful to say that a compatible sequence on $\mathbb{F}_p[\overline{X},\overline{Y}]$ vanishes on L.

We have noted that any additive power series $h \in \mathbb{F}_p[\![\overline{X},\overline{Y}]\!]$ is the limit of a compatible sequence $(h_m \in \mathbb{F}_p[\overline{X},\overline{Y}])$ and it is the limit of some other compatible sequence (h'_m) if and only if $(h_m - h'_m)$ vanishes. Therefore, it makes sense to say that h vanishes on L (or K) and that $h \in L^{p^{m+1}}$. Similarly, for any $m \in \mathbb{N}$, the differential form $\mathrm{d}_{p^m}(h(g)) \in \mathrm{HS}_L^{p^m}$ is well defined as $\mathrm{d}_{p^m}(h_m(g))$ for any compatible sequence (h_m) converging to h.

PROPOSITION 3.1: *There is* $(h_1,\dots,h_n) \in \mathbb{F}_p[\![\mathrm{Fr}]\!]^n \setminus \{0\}$ *such that*

$$h := h_1 \circ (Y_1 - F(X_1)) + \cdots + h_n \circ (Y_n - F(X_n))$$

vanishes on L.

Proof. In this proof, by a permutation we mean $\sigma \in S_n$ applied both to $\overline{X}$- and $\overline{Y}$-coordinates. Let us define $f_i := Y_i - F(X_i) \in \mathbb{F}_p[\![\overline{X},\overline{Y}]\!]$. From the assumptions in 1.1, each f_i vanishes on K.

By 2.5 (for $C = \mathbb{F}_p$), the forms $\mathrm{d}_1(f_1(g)),\dots,\mathrm{d}_1(f_n(g)) \in \Omega_L$ are linearly dependent over $\mathbb{F}_p$. After applying a permutation, there is $0 \leqslant r_0 < n$ such that $\{\mathrm{d}_1(f_1(g)),\dots,\mathrm{d}_1(f_{r_0}(g))\}$ is a basis of the $\mathbb{F}_p$-linear span of these forms. For each $r_0 < l \leqslant n$, there are $\alpha_{l,1},\dots,\alpha_{l,r_0} \in \mathbb{F}_p$ such that

$$\mathrm{d}_1(f_l(g)) = \sum_{i=1}^{r_0} \alpha_{l,i}\mathrm{d}_1(f_i(g)).$$

We define now new additive power series. For each $1 \leqslant l \leqslant r_0$ we set $f_l^{(1)} := f_l^p$ and for each $r_0 < l \leqslant n$ we set $f_l^{(1)} := f_l - \sum_{i=1}^{r_0} \alpha_{l,i} f_i$.

Note that $f_1^{(1)}(g),\dots,f_n^{(1)}(g) \in L^p$ by 2.4. Since each $f^{(i)}$ still vanishes on K, by 2.5 the forms $\mathrm{d}_p(f_1^{(1)}(g)),\dots,\mathrm{d}_p(f_n^{(1)}(g)) \in \mathrm{HS}_L^p$ are linearly dependent over $\mathbb{F}_p$. Since for each $1 \leqslant l \leqslant r_0$ we have

$$\mathrm{d}_p(f_l^{(1)}(g)) = \mathrm{d}_1(f_l(g))^p,$$

the forms $\mathrm{d}_p(f_1^{(1)}(g)),\dots,\mathrm{d}_p(f_{r_0}^{(1)}(g))$ are linearly independent over $\mathbb{F}_p$ (since $\mathbb{F}_p$ is perfect). Therefore, after applying a permutation, there is $r_0 \leqslant r_1 < n$ such that $\{\mathrm{d}_p(f_1^{(1)}(g)),\dots,\mathrm{d}_p(f_{r_1}^{(1)}(g))\}$ is a basis of the $\mathbb{F}_p$-linear span of $\{\mathrm{d}_p(f_1^{(1)}(g)),\dots,\mathrm{d}_p(f_n^{(1)}(g))\}$.

We define now new power series $f_i^{(2)}$ in the same fashion as we have defined the power series $f_i^{(1)}$. Note that $f_1^{(2)}(g), \dots, f_n^{(2)}(g) \in L^{p^2}$ and each $f_i^{(2)}$ vanishes on K.

If we continue like this we get a sequence $0 \leqslant r_0 \leqslant r_1 \leqslant r_2 \leqslant \cdots < n$. Let $m \in \mathbb{N}$ be such that for each $j \geqslant m$ we have $r_m = r_j$. Let $f_{<n}$ denote $(f_1, \dots, f_{n-1})$. Note that

$$f_1^{(m)} = t_1(f_{<n}),\ \dots\ ,\ f_{n-1}^{(m)} = t_{n-1}(f_{<n}),\ f_n^{(m)} = f_n - t_n(f_{<n}) \tag{1}$$

for certain additive polynomials $t_1, \dots, t_n$.

For any $k \in \mathbb{N}$, there are $\alpha_{1,k}, \dots, \alpha_{n-1,k} \in \mathbb{F}_p$ such that if we set

$$w_k := \alpha_{1,k}(f_1^{(m)})^{p^k} + \cdots + \alpha_{n-1,k}(f_{n-1}^{(m)})^{p^k}, \tag{2}$$

$$h^{(k+1)} := f_n^{(m)} - w_0 - \cdots - w_k, \tag{3}$$

we get that $h^{(k)}$ is an additive power series such that $h^{(k)}(g) \in L^{p^{k+m}}$. Clearly $(h^{(k)})_k$ is a compatible sequence in the ring of power series; in particular, it is a Cauchy sequence. From (1), (2) and (3), $h := \lim(h^{(k)})$ is our required power series. ∎

4. An algebraic subgroup

In this section we replace the additive power series h from 3.1 with an algebraic group.

Let $\mathbb{G}_{\mathrm{a}}$ denote the (algebraic) additive group over $\mathbb{F}_p^{\mathrm{alg}}$ (the algebraic closure of $\mathbb{F}_p$) and A denote $\mathbb{G}_{\mathrm{a}}^{2n}$. Assume that $W \subseteq A$ is an irreducible affine subvariety such that 0 is a smooth point of W. Let $\mathcal{O}_A$ and $\mathcal{O}_W$ denote the coordinate rings over $\mathbb{F}_p^{\mathrm{alg}}$ and let I_W be the kernel of the restriction map $\pi_W : \mathcal{O}_A \to \mathcal{O}_W$. Let $\widehat{\mathcal{O}}_W$ denote the completion of $\mathcal{O}_W$ with respect to the ideal $\mathfrak{m}_{W,0}$. We identify $\widehat{\mathcal{O}}_W$ with the inverse limit of the inverse system $(\mathcal{O}_W/\mathfrak{m}_{W,0}^{p^{m+1}})_{m\in\mathbb{N}}$. We would like to emphasize that $\mathfrak{m}_{W,0}^{p^m}$ denotes here the p^m-th power of the ideal $\mathfrak{m}_{W,0}$ and not the image of $\mathfrak{m}_{W,0}$ by the p^m-th power of the Frobenius map (which is contained in $\mathfrak{m}_{W,0}^{p^m}$), although, for any C-algebra T, T^{p^m} still denotes the image of T by the m-th power of the Frobenius map. Let $C(W)$ denote the fraction field of $\mathcal{O}_W$ (the field of rational functions on W). In the lemma below we note the relation between compatible sequences on $C(W)$ and elements of $\widehat{\mathcal{O}}_W$. This

relation also justifies the choice of indices in the inverse system representing $\widehat{\mathcal{O}}_W$.

LEMMA 4.1: *Let $f = (f_m)_{m\in\mathbb{N}}$ be a compatible sequence on $C(W)$ such that each f_m belongs to $\mathfrak{m}_{W,0}$. Then*

$$\widehat{f} := (f_m + \mathfrak{m}_{W,0}^{p^{m+1}})_{m\in\mathbb{N}} \in \widehat{\mathcal{O}}_W.$$

Moreover, if f vanishes on $C(W)$, then $\widehat{f} = 0$.

Proof. Since $\mathfrak{m}_{W,0}$ is maximal, we can replace $\mathcal{O}_W$ with its localization at $\mathfrak{m}_{W,0}$, i.e., with the local ring of W at 0. Since 0 is a smooth point, $\mathcal{O}_W$ is regular, in particular normal. Therefore, for each $m \in \mathbb{N}$ we have

$$C(W)^{p^m} \cap \mathfrak{m}_{W,0} \subseteq \mathrm{Fr}^m(\mathfrak{m}_{W,0}) \subseteq \mathfrak{m}_{W,0}^{p^m}$$

and the result follows. ∎

Clearly the converse to neither clause in the lemma above holds.

We consider $\mathcal{O}_W$ as a subring of $\widehat{\mathcal{O}}_W$. We identify $\widehat{\mathcal{O}}_A$ with $\mathbb{F}_p[\![\overline{X}, \overline{Y}]\!]$, in particular $h \in \widehat{\mathcal{O}}_A$, where h comes from 3.1. Since $\pi_W(\mathfrak{m}_{A,0}) = \mathfrak{m}_{W,0}$, we get the induced epimorphism $\widehat{\pi}_W : \widehat{\mathcal{O}}_A \to \widehat{\mathcal{O}}_W$.

We note a classical result which will be needed in the next section.

LEMMA 4.2: *For W, A as above we have* $\ker(\widehat{\pi}_W) = I_W\widehat{\mathcal{O}}_A$.

Proof. This is well-known and follows directly from [11, Theorem 7.2(a)] and [11, Lemma 7.15]. ∎

We say that h vanishes on W if h vanishes on the function field of W (as a compatible sequence, note the discussion in the beginning of the previous section).

LEMMA 4.3: *If h vanishes on W, then $h \in \ker(\widehat{\pi}_W)$.*

Proof. It follows directly from 4.1. ∎

For any $\mathcal{O}_A$-module N, denote by $\widehat{N}$ the completion of N with respect to $\mathfrak{m}_{A,0}$. Then $N \mapsto \widehat{N}$ is an exact functor [11, Lemma 7.15], $\widehat{\mathcal{O}}_W = \widehat{\mathcal{O}_W}$ and $\widehat{\pi}_W = \widehat{\pi_W}$.

For $W_1, W_2 \subseteq A$ subvarieties, let $W_1 + W_2$ denotes the Zariski closure of the set $\{w_1 + w_2 | w_1 \in W_1, w_2 \in W_2\}$.

PROPOSITION 4.4: *Let $W_1, W_2 \subseteq A$ be subvarieties having 0 as a smooth point and assume $h \in \ker(\widehat{\pi}_{W_1}) \cap \ker(\widehat{\pi}_{W_2})$. Then $h \in \ker(\widehat{\pi}_{W_1+W_2})$.*

Proof. From the definition of $W_1 + W_2$, $\ker(\pi_{W_1+W_2})$ coincides with the kernel of the following composition:

$$\mathcal{O}_A \xrightarrow{\mu} \mathcal{O}_A \otimes \mathcal{O}_A \xrightarrow{\pi_V \otimes \pi_W} \mathcal{O}_V \otimes \mathcal{O}_W,$$

where μ is the coaddition map. Therefore, $\ker(\widehat{\pi}_{W_1+W_2})$ coincides with the kernel of the following composition:

$$\widehat{\mathcal{O}}_A \xrightarrow{\widehat{\mu}} \widehat{\mathcal{O}}_A \widehat{\otimes} \widehat{\mathcal{O}}_A \xrightarrow{\widehat{\pi}_V \otimes \widehat{\pi}_W} \widehat{\mathcal{O}}_V \widehat{\otimes} \widehat{\mathcal{O}}_W.$$

Since h is additive, $\widehat{\mu}(h) = h\widehat{\otimes}1 + 1\widehat{\otimes}h$, hence h belongs to the kernel of the above composition. ∎

Let as assume that $V \subseteq A$ is an irreducible subvariety. By a theorem of Chevalley (see Chapter II Section 7 in [8]), V generates in finitely many steps H, a coset of an algebraic subgroup of A. Clearly, if V is defined over $\mathbb{F}_q$, then H is defined over $\mathbb{F}_q$. By the locus of g over $\mathbb{F}_p^{\mathrm{alg}}$ we mean the smallest algebraic subvariety V of A which is defined over $\mathbb{F}_p^{\mathrm{alg}}$ and such that $g \in V(\mathbb{F}_p((t)))$. Since $\mathbb{F}_p^{\mathrm{alg}}$ is algebraically closed, V is irreducible. Let us recall the power series h from the statement of 3.1 which plays an important role in the main result of this section below.

PROPOSITION 4.5: *Let V be the locus of g over $\mathbb{F}_p^{\mathrm{alg}}$ and H be the coset generated by V. Then H is an algebraic subgroup defined over $\mathbb{F}_p$, $g \in H(\mathbb{F}_p((t)))$ and $h \in \ker(\widehat{\pi}_H)$.*

Proof. Since $\mathbb{F}_p((t))$ is linearly disjoint from $\mathbb{F}_p^{\mathrm{alg}}$ over $\mathbb{F}_p$ (in $\mathbb{F}_p^{\mathrm{alg}}((t))$), we have

$$\mathbb{F}_p^{\mathrm{alg}}[g] = \mathbb{F}_p^{\mathrm{alg}}\mathbb{F}_p[g] \cong \mathbb{F}_p^{\mathrm{alg}} \otimes_{\mathbb{F}_p} \mathbb{F}_p[g].$$

Therefore, V is defined over $\mathbb{F}_p$ and H is defined over $\mathbb{F}_p$ as well.

By 3.1, h vanishes on $\mathbb{F}_p(g)$. Let $c \in V(\mathbb{F}_p^{\mathrm{alg}})$ be a smooth point and $V_c := V - c$. Then V_c generates a group G whose coset is H. Since $\mathbb{F}_p(g)$ is a subfield of the function field of V_c and 0 is a smooth point of V_c, h vanishes on V_c. By 4.3, $h \in \ker(\widehat{\pi}_{V_c})$. Since G is generated in finitely many steps by V_c, we get by 4.4 that $h \in \ker(\widehat{\pi}_G)$.

We will show that $c \in G(\mathbb{F}_p^{\mathrm{alg}})$, which clearly implies that $g \in G(\mathbb{F}_p((t)))$ and $H = G$. Assume that $c \notin G(\mathbb{F}_p^{\mathrm{alg}})$ and we will reach a contradiction. There is

an additive polynomial w which vanishes on $g - c$ and $w(c) \neq 0$. Hence there are $\alpha_1, \ldots, \alpha_{2n} \in \mathbb{F}_p^{\mathrm{alg}}[\mathrm{Fr}]$ such that

$$\sum_{i=1}^{n} \alpha_i(x_i) + \sum_{j=n+1}^{2n} \alpha_j(F(x_i)) \in t\mathbb{F}_p^{\mathrm{alg}}[\![t]\!] \cap \{w(c)\} = \emptyset,$$

a contradiction. ∎

The main fact behind 4.5 can be stated much more generally. Assume G is an algebraic group, V a subvariety containing the identity element of G and $\mathcal{H}$ a formal subgroup of $\widehat{G}$, the formalization of G. Proceeding as in the proof of 4.4, one can show that if $\widehat{V} \subseteq \mathcal{H}$, then $\widehat{H} \subseteq \mathcal{H}$, where H is the algebraic subgroup of G generated by V.

5. The conclusion of the proof

In this section we finish the proof of 1.1 in a similar way as in the proof of [13, 6.12]. We need to show that x belongs to a proper algebraic subgroup of $\mathbb{G}_{\mathrm{a}}^n$ defined over $\mathbb{F}_p$.

Let us take h from 3.1 and H from 4.5. For $1 \leqslant i \leqslant 2n$, let $\pi_i : \mathbb{G}_{\mathrm{a}}^{2n} \to \mathbb{G}_{\mathrm{a}}^i$ denote the projection on the first i coordinates. If $\pi_n(H) \neq \mathbb{G}_{\mathrm{a}}^n$, then we are done by 4.5. Assume not. We will show that $\pi_n(H) = \mathbb{G}_{\mathrm{a}}^n$ implies that the algebraic degree of F over $\mathbb{F}_p(\mathrm{Fr})$ is at most n.

Let us recall the form of h from 3.1:

$$h = h_1 \circ (Y_1 - F(X_1)) + \cdots + h_n \circ (Y_n - F(X_n)), \tag{1}$$

where $h_1, \ldots, h_n$ is a non-zero n-tuple of elements from $\mathbb{F}_p[\![\mathrm{Fr}]\!]$.

Since $H \neq \mathbb{G}_{\mathrm{a}}^{2n}$, then after applying a permutation of the $\bar{X}$-coordinates and the corresponding permutation of the $\bar{Y}$-coordinates, we can assume that there is $n \leqslant i < 2n$ such that

$$\dim(\pi_i(H)) = \dim(H) = i.$$

Then for each $i < j \leqslant 2n$ there are additive polynomials

$$f_j \in \mathbb{F}_p[\mathrm{Fr}], \quad g_j \in \mathbb{F}_p[\bar{X}, Y_1, \ldots, Y_i]$$

such that

$$I_H = (g_{i+1} - f_{i+1}(Y_{i+1-n}), \ldots, g_{2n} - f_{2n}(Y_n)).$$

By 4.2, there are $\alpha_{i+1}, \dots, \alpha_{2n} \in \mathbb{F}_p[\![\bar{X}, \bar{Y}]\!]$ such that:

$$h = (g_{i+1} - f_{i+1}(Y_{i+1-n}))\alpha_{i+1} + \cdots + (g_{2n} - f_{2n}(Y_n))\alpha_{2n}. \tag{2}$$

For each j, let f_j^{-1} denote the compositional inverse of f_j in $\mathbb{F}_p(\mathrm{Fr})$ and let $t_j := f_j^{-1} \circ g_j$. Then we have

$$t_j = \sum_{k=1}^{n} (t_{j,k}(X_k) + s_{j,k}(Y_k)), \tag{3}$$

for some $t_{j,k}, s_{j,k} \in \mathbb{F}_p[\mathrm{Fr}]$.

From (2) we get

$$h(X_1, \dots, X_n, Y_1, \dots, Y_i, t_{i+1}, \dots, t_{2n}) = 0. \tag{4}$$

Then by (1) and (4) we have

$$\sum_{k=1}^{i} h_k \circ (Y_k - F(X_k)) + \sum_{k=i+1}^{n} h_k \circ (t_{n+k} - F(X_k)) = 0. \tag{5}$$

We focus now on the variables $X_{k+1}, \dots, X_n$ in (5). Using (3), for each $k \in \{i+1, \dots, n\}$ we have the following equation in the field $\mathbb{F}_p((\mathrm{Fr}))$:

$$h_{i+1-n} \circ t_{i+1,k} + \cdots + h_n \circ t_{2n,k} = h_k \circ F. \tag{$*_k$}$$

The equations $*_{i+1}, \dots, *_n$ mean that F is a characteristic value of the linear map given by the matrix $(t_{j,k}) \in M_{2n-i}(\mathbb{F}_p(\mathrm{Fr}))$. By the Cayley–Hamilton theorem, F is algebraic over $\mathbb{F}_p(\mathrm{Fr})$ of degree not greater than $2n - i \leqslant n$, which finishes the proof of Theorem 1.1.

6. Other formal maps

In this section we discuss transcendence results related to power series of a more general form than the one considered in Theorem 1.1.

6.1. Power series over a perfect field. Let us replace $\mathbb{F}_p$ with C, an arbitrary perfect field of characteristic p. As the referee has pointed out, for an extension of commutative domains $R \subseteq S$ and $s \in S$ the following conditions are equivalent:

(1) the element s is algebraic over (the fraction field of) R of degree at most n,

(2) there is $r \in R \setminus \{0\}$ and an R-algebra embedding of $R[rs]$ into the ring of n-by-n matrices over R,

(3) there is $r \in R \setminus \{0\}$ such that rs is an eigenvalue of a non-zero n-by-n matrix over R.

The conditions (2) and (3) make sense for rings which are not necessarily commutative. We can prove 1.1 for C, after replacing the algebraicity condition with the condition (3) for $R = C[\mathrm{Fr}]$. We do not know if the conditions (2) and (3) are equivalent for arbitrary rings, or even for the rings of the form $C[\mathrm{Fr}]$.

For $m \in \mathbb{N}_{>0}$, we obtain a result over $\mathbb{F}_{p^m}$ generalizing Theorem 1.1. Let us take an additive power series F with coefficients from $\mathbb{F}_{p^m}$ and let Fr denote the Frobenius map.

THEOREM 6.1: *Assume that for each* $(\alpha_0, \ldots, \alpha_n) \in \mathbb{F}_{p^m}[\mathrm{Fr}]^{n+1} \setminus \{0\}$ *we have*

$$\alpha_n \mathrm{Fr}^{m-1}(F)^n + \cdots + \alpha_1 \mathrm{Fr}^{m-1}(F) + \alpha_0 \neq 0$$

in the ring $(\mathbb{F}_{p^m}[\![\mathrm{Fr}]\!], +, \circ)$. *Let* $x_1, \ldots, x_n \in t\mathbb{F}_{p^m}[\![t]\!]$ *be linearly independent over* $\mathbb{F}_{p^m}[\mathrm{Fr}]$ *and*

$$g := (x_1, \ldots, x_n, F(x_1), \ldots, F(x_n)).$$

Then $\mathrm{trdeg}_{\mathbb{F}_p}(g) \geqslant n + 1$.

Proof. Let us notice first that for $G, H \in X\mathbb{F}_{p^m}[\![X]\!]$ we have

$$\mathrm{Fr}(G \circ H) = G^{\mathrm{Fr}} \circ \mathrm{Fr}(H) = \mathrm{Fr}(G) \circ H, \tag{1}$$

where for any $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^m})$, $(\sum a_i X^i)^\sigma$ denotes $\sum \sigma(a_i) X^i$.

It is also clear that for $F_1, F_2 \in \mathrm{Fr}^{m-1}(X\mathbb{F}_{p^m}[\![X]\!])$, we have

$$F_1 \circ F_2 = F_2 \circ F_1. \tag{2}$$

Proceeding as in the proof of 1.1 we obtain $0 < l \leqslant n$ and t_{ij}, h_k such that for each $0 \leqslant k \leqslant l$ we have

$$h_1 \circ t_{1,k} + \cdots + h_l \circ t_{l,k} = h_k \circ F. \tag{$*_k$}$$

Applying Fr^{2m-2} and using $2m-2$ times (1) we get

$$\sigma(h_1^\sigma) \circ \sigma(t_{1,k}) + \cdots + \sigma(h_l^\sigma) \circ \sigma(t_{l,k}) = \sigma(h_k^\sigma) \circ \sigma(F), \tag{$**_k$}$$

where $\sigma = \mathrm{Fr}^{m-1}$.

Using (2), we see that all the elements involved in $(**_1), \ldots, (**_l)$ commute with each other, so we can finish as in Section 5. ∎

6.2. Drinfeld modules. There is a rich theory of algebraic independence in positive characteristic related to Drinfeld modules. For a survey of this theory the reader is referred to [6]. In this subsection we briefly describe how our results are related to this theory. In [10], Drinfeld introduced elliptic modules, which are now called Drinfeld modules. In our setting, Drinfeld modules are certain homomorphisms between $\mathbb{F}_q[X]$ and $K[\mathrm{Fr}]$, where q is a power of p and $K = \mathbb{F}_q((\theta))$ is the non-Archimedean field of Laurent series over $\mathbb{F}_q$. An additive power series over K is associated to each Drinfeld module and this series is entire on K. A number of very interesting transcendence results for such additive power series is obtained; see, e.g., [17]. A special case of such a series was introduced by Carlitz (before the invention of Drinfeld's modules) and it is called the Carlitz exponential. Several Schanuel-type results for the Carlitz exponential were obtained in [9] and a Carlitz exponential version of the (still open) conjecture on algebraic independence of logarithms of algebraic numbers was proved in [15, 1.2.6].

The power series we consider in this paper do not fit in the above framework, since we consider power series with *constant coefficients* only, i.e., there is no transcendental element θ present in the coefficients of our series.

6.3. Non-additive power series. The transcendence statement 1.1 was obtained for certain additive power series, i.e., for sufficiently non-algebraic formal maps between vector groups. It is natural to try to extend Theorem 1.1 to the context of an arbitrary "sufficiently non-algebraic" formal map between (the formalizations of) algebraic groups, e.g., a formal isomorphism between an abelian variety and an algebraic torus. Such a general statement was obtained [13, 5.5] in the case of characteristic 0. We aim to state and prove a positive characteristic version of [13, 5.5] in a forthcoming paper. It is worth mentioning here a related result [1, Théorème 1] concerning raising one point in a multiplicative group to several linearly independent p-adic powers.

References

[1] J.-P. Allouche, M. Mendès-France and A. J. van der Poorten, *Indépendance algébrique de certaines séries formelles* Bulletin de la Société Mathématique se France **116** (1988), 449–454.

[2] J. Ax, *On Schanuel's conjectures*, Annals of Mathematics **93** (1971), 252–268.

[3] J. Ax, *Some topics in differential algebraic geometry. I. Analytic subgroups of algebraic groups*, American Journal of Mathematics **94** (1972), 1195–1204.

[4] M. Bays, J. Kirby and A. Wilkie, *A Schanuel property for exponentially transcendental powers*, The Bulletin of the London Mathematical Society **42** (2010), 917–922.

[5] D. Bertrand, *Schanuel's conjecture for non-isoconstant elliptic curves over function fields*, in *Model theory with applications to algebra and analysis. Vol. 1*, London Math. Soc. Lecture Note Ser. vol. 349, Cambridge University Press, Cambridge, 2008, pp. 41–62.

[6] W. D. Brownawell, *Transcendence in positive characteristic*, in *Number theory (Tiruchirapalli, 1996)*, Vol. 210 of Contemporary Mathematics, American Mathematical Society, Providence, RI, 1998, pp. 317–332.

[7] W. D. Brownawell and K. Kubota, *Algebraic independence of Weierstrass functions* Acta Arithmetica **33** (1977), 111–149.

[8] C. Chevalley, *Théorie des groupes de Lie, vol II, Groupes algébriques*, Springer, Berlin, 1951.

[9] L. Denis, *Indépendance algébrique et exponentielle de Carlitz*, Acta Arithmetica **69** (1995), 75–89.

[10] V. G. Drinfeld, *Elliptic modules* (Russian), MatematicheskiĭSbornik. Novaya Seriya **94** (1974), 594–627. English translation: Mathematics of the USSR-Sbornik **23** (1976), 561–592.

[11] D. Eisenbud, *Commutative Algebra with a View Towards Algebraic Geometry*, Springer, Berlin, 1996.

[12] J. Kirby, *The theory of the exponential differential equations of semiabelian varieties*, Selecta Mathematica **15** (2009), 445–486.

[13] P. Kowalski, *A note on a theorem of Ax*, Annals of Pure and Applied Logic **156** (2008), 96–109.

[14] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1986.

[15] M. Papanikolas, *Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms*, Inventiones Mathematicae **171** (2008), 123–174.

[16] P. Vojta, *Jets via Hasse–Schmidt derivations* in *Diophantine Geometry, Proceedings* (U. Zannier, ed.), Edizioni della Normale, Pisa, 2006, pp. 335–361.

[17] J. Yu, *Transcendence and Drinfeld modules*, Inventiones Mathematicae **83** (1986), 507–517.