

ON THE FINITE GENERATION OF ADDITIVE GROUP INVARIANTS IN POSITIVE CHARACTERISTIC

EMILIE DUFRESNE AND ANDREAS MAURISCHAT

ABSTRACT. Roberts, Freudenburg, and Daigle and Freudenburg have given the smallest counterexample to Hilbert's fourteenth problem as rings of invariants of algebraic groups. The three examples are of an action of the additive group on a finite dimensional vector space over a field of characteristic zero, and thus, they are the kernel of locally nilpotent derivations. In positive characteristic, additive group actions correspond to locally finite iterative higher derivations. We set up characteristic free analogs of the three examples, and show that in every positive characteristic, the invariants are finitely generated.

1. INTRODUCTION

A main topic of interest in Invariant Theory is the question of the finite generation of invariant rings. Namely, if B is a finitely generated algebra over a field \mathbb{k} , and G is a group acting on B via \mathbb{k} -algebra homomorphisms, one asks if the ring of invariants B^G is always finitely generated. This is a special case of Hilbert's Fourteenth Problem. When G is a finite group, this question has a positive answer for any B (from the work of Hilbert and Noether [3, ?]). For an affine algebraic group G acting regularly on B , the ring of invariants is finitely generated, whenever G is reductive (cf. Nagata [?]). On the other hand, if G is not reductive, then Popov (cf. [?]) showed that there exists a finitely generated \mathbb{k} -algebra B and an action of G on B such that B^G is not finitely generated. These results are valid in arbitrary characteristic.

Consider actions on a polynomial ring $B = \mathbb{k}[x_1, \dots, x_n]$ of the simplest non reductive group, the additive group \mathbb{G}_a . In characteristic zero, several facts are known. By the Maurer-Weitzenböck Theorem (cf. [?]), every linear action of \mathbb{G}_a on $B = \mathbb{k}[x_1, \dots, x_n]$ has finitely generated invariants. If $n \leq 3$, then $B^{\mathbb{G}_a}$ is finitely generated for any algebraic action (cf. [?]). In dimensions 5, 6 and 7, however, there are well-known counterexamples. For $n = 7$, Roberts (cf. [4, ?]) gave an example of a \mathbb{G}_a -action where $B^{\mathbb{G}_a}$ is not finitely generated (from now on referred to as (R7)). For $n = 6$ and 5, examples were constructed by Freudenburg (F6), and Daigle and Freudenburg (DF5). These three counterexamples can be used to construct counterexamples in any dimension $n \geq 5$ (Nagata?). The dimension 4 case

Date: 1st Dec, 2009, 08:59.

Key words and phrases. Invariant theory, Hilbert's fourteenth problem.

is still open in general. For more information on \mathbb{G}_a -actions in characteristic zero, we refer the reader to well written book of Freudenburg [2].

In positive characteristic, much less is known. It is known that $B^{\mathbb{G}_a}$ is finitely generated if $n \leq 3$ (cf. [?]), and even polynomial if $n \leq 2$ (cf. [?]). The finite generation of the invariants was also proved for special classes of linear actions of \mathbb{G}_a (cf. e.g. Weitzenböck actions in positive characteristic, [5, 6]), but not for all linear actions. On the other hand, to the authors's knowledge, there is no example of an algebraic \mathbb{G}_a -action on a polynomial ring where the ring of invariants was proved not to be finitely generated.

Locally finite iterative higher derivations (lfihd) are a generalization of locally nilpotent derivations which behave well in all characteristics: an algebraic action of the additive group always corresponds to a lfihd. In this paper, we adopt this point of view, and consider the positive characteristic analogs of the counterexamples (R7), (F6), and (DF5) mentioned above. Our main result is that, in every characteristic $p > 0$, the arising rings of invariants are finitely generated.

The paper is structured as follows. In Section 2, we recall some facts concerning lfihd, and set up the examples. In Section 3, we prove that the invariants are finitely generated. We use the fact that the examples are related by homomorphisms which respect the lfihd. The key of the argument is the existence of a special invariant. We deduce the existence of the special element for (F6) and (R7) from the the existence of the special element for (DF5). Finally in Section 4, we prove the special element exists for (DF5). Our rather technical construction is in the spirit of van den Essen's simpler proof for (DF5) in characteristic zero (cf. [8]).

Acknowledgements. We thank Florian Heiderich for giving us the idea to explore the correspondence between additive group actions and locally finite iterative higher derivations.

2. SETUP OF THE EXAMPLES

We first review a purely algebraic description of \mathbb{G}_a -actions. Let \mathbb{k} be an algebraically closed field,¹ and let B be a finitely generated \mathbb{k} -algebra. An algebraic action of \mathbb{G}_a on B is uniquely determined by a \mathbb{k} -algebra homomorphism $\theta : B \rightarrow B \otimes_{\mathbb{k}} \mathbb{k}[U]$, where $\mathbb{k}[U] \cong \mathbb{k}[\mathbb{G}_a]$ is the ring of regular functions on \mathbb{G}_a . The correspondence is given by $\sigma \cdot b = \theta(b)|_{U=\sigma}$ for all $b \in B$ and $\sigma \in \mathbb{G}_a(\mathbb{k}) = \mathbb{k}$. A \mathbb{k} -algebra homomorphism $\theta : B \rightarrow B[U]$ defines a family of \mathbb{k} -linear maps $(\theta^{(n)})_{n \geq 0}$ via

$$\theta(b) =: \sum_{n=0}^{\infty} \theta^{(n)}(b) U^n$$

¹This is not a restriction: the property of finite generation of invariants is stable under algebraic extensions of the base field.

for all $b \in B$. The family $(\theta^{(n)})_{n \geq 0}$ (resp. θ) corresponds to a \mathbb{G}_a -action if and only if it fulfills the following properties (cf. [?]):

- (1) $\theta^{(0)} = \text{id}_B$,
- (2) for all $n \geq 0$ and $a, b \in B$, one has $\theta^{(n)}(ab) = \sum_{i+j=n} \theta^{(i)}(a)\theta^{(j)}(b)$,
- (3) for all $b \in B$, there is $n \geq 0$ such that $\theta^{(j)}(b) = 0$ for all $j \geq n$,
- (4) for all $j, k \geq 0$ and $b \in B$, one has $\theta^{(j)}(\theta^{(k)}(b)) = \binom{j+k}{j} \theta^{(j+k)}(b)$.

Whereas Properties (2) and (3) are equivalent to θ being a \mathbb{k} -algebra homomorphism, Properties (1) and (4) ensure that θ really determines a \mathbb{G}_a -action. A family $(\theta^{(n)})_{n \geq 0}$ fulfilling these properties (resp. the corresponding θ) is called a *locally finite iterative higher derivation* (lfihd) on B . Throughout this paper, we adopt the point of view of lfihd's.

Note that $\theta^{(1)}$ is a derivation in the usual sense, and in characteristic zero, Property (4) implies that $\theta^{(n)} = \frac{1}{n!}(\theta^{(1)})^n$. Thus, in characteristic zero, lfihd's are in one to one correspondence with those derivations which are locally nilpotent (by Property (3)). Accordingly, the \mathbb{k} -algebra $B^\theta := \{b \in B \mid \theta^{(n)}(b) = 0 \forall n \geq 1\}$ is often called the ring of constants of θ . Since, it is also the ring of invariants $B^{\mathbb{G}_a}$ of the corresponding \mathbb{G}_a -action, we will refer to B^θ as the “ring of invariants”.

In characteristic zero, (DF5), (F6) and (R7) are realised as \mathbb{k} -algebras with a locally nilpotent derivation: the counterexample of Daigle and Freudenburg (DF5) is given by

$$\mathbb{k}[x, s, t, u, v] \quad \text{and} \quad \theta^{(1)} = x^3 \frac{\partial}{\partial s} + s \frac{\partial}{\partial t} + t \frac{\partial}{\partial u} + x^2 \frac{\partial}{\partial v},$$

the counterexample of Freudenburg (F6) is given by

$$\mathbb{k}[x, y, s, t, u, v] \quad \text{and} \quad \theta^{(1)} = x^3 \frac{\partial}{\partial s} + y^3 s \frac{\partial}{\partial t} + y^3 t \frac{\partial}{\partial u} + x^2 y^2 \frac{\partial}{\partial v},$$

and the counterexample of Roberts (R7) is given by

$$\mathbb{k}[x_1, x_2, x_3, y_1, y_2, y_3, v] \quad \text{and} \quad \theta^{(1)} = x_1^3 \frac{\partial}{\partial y_1} + x_2^3 \frac{\partial}{\partial y_2} + x_3^3 \frac{\partial}{\partial y_3} + x_1^2 x_2^2 x_3^2 \frac{\partial}{\partial v}.$$

As there are denominators in the first two examples, to obtain lfihd which make sense in all positive characteristic, we must rescale the variables t and v by a factor of 2 and 6, respectively. Characteristic-free formulations of the examples are therefore given by:

Daigle-Freudenburg's example (DF5):

$$B_5 := \mathbb{k}[x, s, t, u, v],$$

$$\begin{aligned} \theta(x) &= x, & \theta(s) &= s + x^3 U, \\ \theta(t) &= t + 2sU + x^3 U^2, & \theta(u) &= u + 3tU + 3sU^2 + x^3 U^3, \\ \theta(v) &= v + x^2 U. \end{aligned}$$

Freudentburg's example (F6):

$$B_6 := \mathbb{k}[x, y, s, t, u, v],$$

$$\begin{aligned} \theta(x) &= x, & \theta(y) &= y, \\ \theta(s) &= s + x^3U, & \theta(t) &= t + 2y^3sU + x^3y^3U^2, \\ \theta(u) &= u + 3y^3tU + 3y^6sU^2 + x^3y^6U^3, & \theta(v) &= v + x^2y^2U. \end{aligned}$$

Roberts' example (R7):

$$B_7 := \mathbb{k}[x_1, x_2, x_3, y_1, y_2, y_3, v],$$

$$\begin{aligned} \theta(x_i) &= x_i, & \theta(y_i) &= y_i + x_i^3U \quad (i = 1, 2, 3), \\ \theta(v) &= v + x_1^2x_2^2x_3^2U. \end{aligned}$$

On the \mathbb{k} -algebras B_5, B_6, B_7 , we define gradings w_5, w_6, w_7 by assigning the following degrees:

$$\begin{aligned} w_5(x) &= 1, \quad w_5(s) = w_5(t) = w_5(u) = 3, \quad w_5(v) = 2; \\ w_6(x) &= w_6(y) = 1, \quad w_6(s) = 3, \quad w_6(t) = 6, \quad w_6(u) = 9, \quad w_6(v) = 4; \\ w_7(x_i) &= 1, \quad w_7(y_i) = 3, \quad (i = 1, 2, 3), \quad w_7(v) = 6, \quad (i = 1, 2, 3). \end{aligned}$$

With respect to these gradings, the lfhd and the corresponding \mathbb{G}_a -actions are homogeneous, and so the ring of invariants are graded subalgebras. This provides useful additional structure. We will also use an additional grading w_4 on B_5 which is given by:

$$w_4(x) = 0, \quad w_4(s) = 1, \quad w_4(t) = 2, \quad w_4(u) = 3, \quad w_4(v) = 1.$$

We now have the proper setup to state our main theorem:

Theorem 2.1. *In every positive characteristic, the rings of invariants B_5^θ , B_6^θ , and B_7^θ , are finitely generated.*

3. MAIN RESULTS

This section presents the main steps of our argument to prove Theorem 2.1. First, we need a connection between the examples:

Lemma 3.1.

- i) *The ring B_5 is isomorphic to $B_6/(y - 1)$ and the lfhd on B_5 is the one induced from the lfhd on B_6 by this isomorphism.*
- ii) *There is a homomorphism $\alpha : B_6 \rightarrow B_7$ which respects the lfhd's, given by:*

$$\begin{aligned} \alpha(x) &= x_1, & \alpha(y) &= x_2x_3, \\ \alpha(s) &= y_1, & \alpha(t) &= (x_3^3y_2 + x_2^3y_3)y_1 - x_1^3y_2y_3, \\ \alpha(v) &= v, & \alpha(u) &= (x_2^6y_3^2 + x_2^3x_3^3y_2y_3 + x_3^6y_2^2)y_1 - (x_3^3y_2 + x_2^3y_3)x_1^3y_2y_3 \end{aligned}$$

Proof. This can be verified by a short computation. \square

Proposition 3.2. *In each of B_5 , B_6 , and B_7 , there exists a homogeneous invariant of the form $v^p - b$ such that v does not appear in b .*

Proof. By Theorem 4.4, there is a w_5 -homogeneous element $v^p - b \in B_5^\theta$, such that $w_4(b) = p$. Since $w_5(v^p) = 2p$, we have $w_5(b) = 2p$. Furthermore, $B_5 \cong B_6/(y-1)$, and so we obtain a w_6 -homogeneous invariant element $v^p - \tilde{b}$ in $B_6[\frac{1}{y}]$ by homogenizing b inside $B_6[\frac{1}{y}]$, that is, by setting

$$\tilde{b} := y^{4p} \cdot b \left(\frac{x}{y}, \frac{s}{y^3}, \frac{t}{y^6}, \frac{u}{y^9} \right).$$

Denote by d_x, d_s, d_t, d_u the exponents in a monomial of b of the variables x, s, t, u , respectively. By the conditions on b , we have $2p = w_5(b) = d_x + 3d_s + 3d_t + 3d_u$, and $p = w_4(b) = d_s + 2d_t + 3d_u$. It follows that

$$d_x + 3d_s + 6d_t + 9d_u \leq d_x + 3d_s + 3d_t + 3d_u + 2d_s + 4d_t + 6d_u = 2p + 2p = 4p.$$

Hence, the exponent of y in the denominator of $b(\frac{x}{y}, \frac{s}{y^3}, \frac{t}{y^6}, \frac{u}{y^9})$ is less or equal to $4p$, and so $\tilde{b} \in B_6$.

Finally, applying the homomorphism α from Lemma 3.1 to $v^p - \tilde{b}$ yields an invariant of the required form in B_7 . \square

As the lfhd's θ are triangular, the restriction induces lfhd's on $A_5 = \mathbb{k}[x, s, t, u]$, $A_6 = \mathbb{k}[x, y, s, t, u]$, and $A_7 = \mathbb{k}[x_1, x_2, x_3, y_1, y_2, y_3]$ also denoted by θ .

Lemma 3.3. *The subrings of invariants $A_5^\theta \subseteq B_5$, $A_6^\theta \subseteq B_6$, and $A_7^\theta \subseteq B_7$ are finitely generated.*

Proof. We apply the characteristic-free version (cf. [6] or [1]) of van den Essen's Algorithm (cf. [7]). We do the details for (DF5), the other examples are done similarly. Since $\theta(s) = s + x^3U$ is a polynomial of degree 1 in U with leading coefficient x^3 , the invariants of the localized ring $\mathbb{k}[x, s, t, u, \frac{1}{x}]$ are generated by $1/x$, $\theta(x)|_{U=-s/x^3} = x$, $\theta(t)|_{U=-s/x^3} = t - s^2/x^3$, and $\theta(u)|_{U=-s/x^3} = u - 3st/x^3 + 2s^3/x^6$. Hence, $A_5^\theta = \mathbb{k}[x, x^3t - s^2, x^6u - 3x^3st + 2s^3, 1/x] \cap A_5$. To obtain generators for A_5^θ , we must look at the relation ideal modulo x of the generators $f_1 := x^3t - s^2$ and $f_2 := x^6u - 3x^3st + 2s^3$, that is, the preimage of the ideal (x) for the map $\pi_1 : \mathbb{k}[X_1, X_2] \rightarrow \mathbb{k}[x, x^3t - s^2, x^6u - 3x^3st + 2s^3]$, $X_1 \mapsto f_1, X_2 \mapsto f_2$. This is clearly generated by $4X_1^3 + X_2^2$, and so we obtain a new generator for $\mathbb{k}[x, s, t, u]^\theta$, namely

$$f_3 := \frac{1}{x^6} \pi_1(4X_1^3 + X_2^2) = x^6u^2 + 2x^3t(2t^2 - 3su) + s^2(4su - 3t^2).$$

Now consider $\pi_2 : \mathbb{k}[X_1, X_2, X_3] \rightarrow \mathbb{k}[x, f_1, f_2, f_3]$, $X_i \mapsto f_i$, ($i = 1, 2, 3$). Then $\pi_2^{-1}((x)) = (4X_1^3 + X_2^2) \subseteq \mathbb{k}[X_1, X_2, X_3]$, and so we don't get new generators. It follows that $\mathbb{k}[x, s, t, u]^\theta = \mathbb{k}[x, f_1, f_2, f_3]$.

For the other examples, the algorithm yields:

$$\begin{aligned} A_6^\theta &= \mathbb{k}[x, y, x^3t - y^3s^2, x^6u - 3x^3x^3st + 2y^6s^3, \\ &\quad x^6u^2 + 2x^3y^3t(2t^2 - 3su) + y^6s^2(4su - 3t^2)], \end{aligned}$$

and

$$A_7^\theta = \mathbb{k}[x_1, x_2, x_3, x_1^3 y_2 - x_2^3 y_1, x_1^3 y_3 - x_3^3 y_1, x_2^3 y_3 - x_3^3 y_2]. \quad \square$$

We end the section with the proof of our main theorem:

Proof of Theorem 2.1. We now show that the finite generation of the invariants modulo v (Lemma 3.3) together with the existence of an invariant of the form $v^p - b$ (Proposition 3.2) imply that the ring of invariants is finitely generated. As the argument is the same for the three examples, we write B to denote the rings B_5 , B_6 , and B_7 , and A to denote the rings A_5 , A_6 , and A_7 .

If $f \in B^\theta$, then $f = q \cdot (v^p - b) + r$, where $\deg_v(r) < p$. Applying θ shows that $q, r \in B^\theta$. Hence, B^θ is generated by $v^p - b$ and invariants of degree less than p as polynomials in v .

For each degree $m < p$ the set

$$I_m = \{a \in A^\theta \mid a \text{ is the leading coefficient of some } f \in B^\theta, \deg_v(f) = m\}$$

is an ideal in A^θ , and hence finitely generated by Lemma 3.3.

Therefore, B^θ is generated by generators of A^θ , $v^p - b$, and a (finite) set of polynomials whose leading coefficients generate the ideal I_m for each $0 < m < p$. \square

4. THE 5-DIMENSIONAL EXAMPLE

The purpose of this section is to construct, for the 5-dimensional example of Daigle and Freudenberg (DF5) and for each characteristic $p > 0$, an invariant of the form $v^p + vb' - b$, where $b, b' \in \mathbb{k}[x, s, t, u] \subset B_5$ such that $w_5(b) = w_5(b') = 2p$ and $w_4(b) = p$ and $w_4(b') = p - 1$.

In the proof of Theorem 4.4, we will require a sequence $c_n \in \mathbb{Q}[s, t, u]$. Therefore let $B := \mathbb{Q}[x, s, t, u, v]$ be Example (DF5) over \mathbb{Q} and let $A := \mathbb{Q}[x, s, t, u]$ be the subalgebra of B with restricted lfhd. The lfhd θ on A induces a lfhd $\bar{\theta}$ on the quotient $C := A/(x - 1) \cong \mathbb{Q}[s, t, u]$, where $\bar{\theta}(f) = \overline{\theta(f)}$. The ring of invariants is $C^{\bar{\theta}} = \mathbb{Q}[t_1, u_1]$, where $t_1 = t - s^2$, and $u_1 = u - 3st + 2s^3$. The w_4 -grading on B induces a grading on C which will also be denoted by w_4 .

Proposition 4.1. *Let $e : \mathbb{N} \rightarrow \mathbb{N}$ be given by $e(n) := \lfloor \frac{2n}{3} \rfloor$. There exists a sequence $(h_n)_{n \in \mathbb{N}}$ in $\mathbb{Q}[t_1, u_1] = C^{\bar{\theta}}$ such that $h_0 = 1$, $h_1 = 0$, and for all $n \geq 2$, the element*

$$c_n := \sum_{i=0}^n \binom{n}{i} h_{n-i} s^i \in \mathbb{Q}[s, t, u]$$

has degree $\deg(c_n) \leq e(n)$ with respect to the standard grading \deg on $\mathbb{Q}[s, t, u]$. Furthermore, for all primes p , the coefficients of h_0, h_1, \dots, h_{p-2} and h_p are in the local ring $\mathbb{Z}_{(p)}$ and the coefficients of h_{p-1} are in $\frac{1}{p}\mathbb{Z}_{(p)}$.

Remark 4.2. For all $k, n \in \mathbb{N}$, the sequence $(c_n)_{n \in \mathbb{N}}$ satisfies $\bar{\theta}^{(k)}(c_n) = \binom{n}{k} c_{n-k}$, since

$$\begin{aligned} \bar{\theta}^{(k)}(c_n) &= \sum_{i=0}^n \binom{n}{i} h_{n-i} \binom{i}{k} s^{i-k} = \sum_{j=0}^{n-k} \binom{n}{j+k} h_{n-k-j} \binom{j+k}{k} s^j \\ &= \sum_{j=0}^{n-k} \binom{n}{k} \binom{n-k}{j} h_{n-k-j} s^j = \binom{n}{k} c_{n-k}. \end{aligned}$$

Proof of Proposition 4.1. Let $C = \bigoplus_{n \geq 0} C_n$ be the decomposition into homogeneous parts with respect to the w_4 -grading. For $n \geq k$, we have $\bar{\theta}^{(k)}(C_n) = C_{n-k}$.

We will show by induction on n that the sequences h_n and c_n can be constructed with the property $h_n, c_n \in C_n$. When $n \equiv 2, 3, 4, 5 \pmod{6}$, we explain how to obtain h_n from h_j , where $0 \leq j \leq n-1$. The cases $n \equiv 0 \pmod{6}$ and $n \equiv 1 \pmod{6}$ must be constructed in one step together, that is, when $n \equiv 1 \pmod{6}$, we show we can construct h_{n-1} and h_n from h_j , where $0 \leq j \leq n-2$.

Assume that $n \equiv 2, 3, 4, 5 \pmod{6}$, and that we already have $h_j \in C_j$ for all $0 \leq j \leq n-1$ such that the denominators of the coefficients of h_j are only divisible by primes smaller than n . By the induction hypothesis, c_{n-1} has standard degree at most $e(n-1)$ for $j > 2$ and at most $e(2) = 1$ for $n = 2$, and is w_4 -homogeneous of w_4 -degree $n-1$. The same computation as in Remark 4.2 shows that $c := \sum_{i=1}^n \binom{n}{i} h_{n-i} s^i \in \mathbb{Q}[s, t, u]$ satisfies $\bar{\theta}^{(1)}(c) = n c_{n-1}$. Thus, it will suffice to find $h_n \in \mathbb{Q}[s, t, u]^{\bar{\theta}}$ such that $\deg(c + h_n) \leq e(n)$.

Writing

$$c = \sum_{i+2j+3k=n} \alpha_{i,j,k} s^i t^j u^k,$$

where $\alpha_{i,j,k} \in \mathbb{Q}$, one gets

$$\begin{aligned} \bar{\theta}^{(1)}(c) &= \sum_{i+2j+3k=n} \alpha_{i,j,k} \left(i s^{i-1} t^j u^k + 2j s^{i+1} t^{j-1} u^k + 3k s^i t^{j+1} u^{k-1} \right) \\ &= \sum_{i+2j+3k=n} \left((i+2) \alpha_{i+2,j-1,k} + 2j \alpha_{i,j,k} + 3(k+1) \alpha_{i+1,j-2,k+1} \right) s^{i+1} t^{j-1} u^k, \end{aligned}$$

where $\alpha_{p,q,r} := 0$ for $p < 0$ or $q < 0$. Since $\deg(\bar{\theta}^{(1)}(c)) \leq e(n)$, we have

$$(i+2) \alpha_{i+2,j-1,k} + 2j \alpha_{i,j,k} + 3(k+1) \alpha_{i+1,j-2,k+1} = 0$$

for all i, j, k such that $i+2j+3k = n$ and $i+j+k \geq e(n)+1$. Hence, each $\alpha_{i,j,k}$ is a linear combination of certain $\alpha_{p,q,r}$'s with $q < j$ and $p+q+r \geq i+j+k$. Consequently, each $\alpha_{i,j,k}$ with $i+j+k \geq e(n)+1$ is a linear combination of the $\alpha_{p,q,r}$'s with $q = 0$ and $p+r \geq e(n)+1$. Therefore, it suffices to prove that there exists $h \in C_n^{\bar{\theta}}$ such that for all i, k with $i+3k = n$ and $i+k \geq e(n)+1$, the coefficient of $s^i u^k$ in h is the same as the coefficient of $s^i u^k$ in c , and to take $h_n = -h$. (Take into account that h trivially satisfies

$\deg(\bar{\theta}^{(1)}(h)) \leq e(n)$, since it is a constant, and hence its coefficients also satisfy these linear relations.)

The “relevant” $s^i u^k$ are those where $i + 3k = n$ and $i + k \geq e(n) + 1$, that is, where $0 \leq k \leq \left\lfloor \frac{n-e(n)-1}{2} \right\rfloor = \left\lfloor \frac{n-1}{6} \right\rfloor$. For short, we write $d := \left\lfloor \frac{n-1}{6} \right\rfloor$ for the maximum value k of a relevant $s^i u^k$.

By assumption, h is a linear combination of the “monomials” $(-t_1)^l u_1^m$, where $2l + 3m = n$, that is, where $m \in [0, \lfloor \frac{n}{3} \rfloor]$, $m \equiv n \pmod{2}$, and $l = \frac{n-3m}{2}$. Thus, for n odd, we have $m = 2m' + 1$, where $0 \leq m' \leq \lfloor \frac{n-3}{6} \rfloor$, and for n even, we have $m = 2m'$ where $0 \leq m' \leq \lfloor \frac{n}{6} \rfloor$. The coefficient of $s^i u^k$ in $(-t_1)^l u_1^m = (s^2 - t)^l (u - 3st + 2s^3)^m$ is $\binom{m}{k} 2^{m-k}$.

Therefore, if $n \equiv 2, 3, 4$ or $5 \pmod{6}$, the number of admissible “monomials” in h equals $d + 1$. Hence, we obtain a system of linear equations $Mx = \alpha$ for the coefficient vector $(x_0, \dots, x_d)^T$ of h , where $\alpha = (\alpha_{n,0,0}, \dots, \alpha_{n-3d,0,d})^T$ and M is the square matrix $M = (a_{k,m'})_{0 \leq k, m' \leq d}$, given by $a_{k,m'} = \binom{2m'+1}{k} 2^{2m'+1-k}$, if n is odd, and by $a_{k,m'} = \binom{2m'}{k} 2^{2m'-k}$, if n is even.

By Lemma 4.3, in both cases M is invertible over $\mathbb{Z}[\frac{1}{2}]$. Hence, the system has a unique solution, and the primes which might occur in the denominators of the coefficients of h are 2 and the primes occurring in the denominators of the coefficients of some h_j ($0 \leq j \leq n-1$). This proves the assertion in these cases.

If $n \equiv 1 \pmod{6}$, the number of coefficients is less than d , which might lead to an unsolvable linear equation. Hence, we cannot use the exact same argument. We construct h_{n-1} and h_n in one step. Again by induction, we may assume that the denominators of the coefficients of h_0, \dots, h_{n-2} only contain primes less than $n-1$.

We want $h_{n-1} = \sum_{m'=0}^d x_{m'} (-t_1)^l u_1^{2m'}$ and $h_n = \sum_{m'=0}^{d-1} y_{m'} (-t_1)^l u_1^{2m'+1}$ such that adding h_{n-1} to $\sum_{i=2}^n \binom{n-1}{i-1} h_{n-i} s^{i-1}$ cancels out the coefficient vector α of $\{s^{n-1}, s^{n-4}u, \dots, s^{n-3d+2}u^{d-1}\}$, and such that adding $h_n + nh_{n-1}s$ to $\sum_{i=2}^n \binom{n}{i} h_{n-i} s^i$ cancels out the coefficient vector β of $\{s^n, s^{n-3}u, \dots, s^{n-3d}u^d\}$. Thus, we must solve $Mx = -\alpha$ and $Ny + nLx = -\beta$, where

$$\begin{aligned} M &\in \text{Mat}(d \times (d+1)), & M_{k,m'} &= \binom{2m'}{k} 2^{2m'-k}, \\ N &\in \text{Mat}((d+1) \times d), & N_{k,m'} &= \binom{2m'+1}{k} 2^{2m'+1-k}, \\ L &\in \text{Mat}((d+1) \times (d+1)), & L_{k,m'} &= \binom{2m'}{k} 2^{2m'-k}. \end{aligned}$$

Since L is invertible by Lemma 4.3, the equations are equivalent to

$$x = -\frac{1}{n} L^{-1}(\beta + Ny) \quad \text{and} \quad ML^{-1}Ny = -ML^{-1}\beta + n\alpha.$$

But $ML^{-1}N$ is just the $d \times d$ matrix with entries $\binom{2m'+1}{k} 2^{2m'+1-k}$ and hence invertible by Lemma 4.3.

Therefore we can find unique vectors x and y . Due to the given equations, the denominators of the entries of y are only divisible by primes less than $n-1$, and those of x can have the additional factor n , if n is prime itself. \square

Lemma 4.3. *For $d \in \mathbb{N}$, let $M_e, M_o \in \text{Mat}((d+1) \times (d+1), \mathbb{Z})$ be given by*

$$(M_e)_{k,m} := \binom{2m}{k} 2^{2m-k} \quad \text{and} \quad (M_o)_{k,m} := \binom{2m+1}{k} 2^{2m+1-k}$$

for all $k, m = 0, \dots, d$. Then one has

$$\det(M_e) = 2^{d(d+1)} \quad \text{and} \quad \det(M_o) = 2^{(d+1)^2}.$$

Proof. For arbitrary x_0, \dots, x_d denote by $V(x_0, \dots, x_d)$ the Vandermonde matrix

$$V(x_0, \dots, x_d) = \begin{pmatrix} 1 & x_0 & \dots & x_0^d \\ 1 & x_1 & \dots & x_1^d \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_d & \dots & x_d^d \end{pmatrix}.$$

By definition of the binomial coefficients, we obtain

$$V(x_0, \dots, x_d) \cdot M_e \equiv V((2+x_0)^2, \dots, (2+x_d)^2) \pmod{(x_0^{d+1}, \dots, x_d^{d+1})}$$

and therefore also the determinants are congruent modulo $(x_0^{d+1}, \dots, x_d^{d+1})$. Since $\det(V(x_0, \dots, x_d)) = \prod_{j>i} (x_j - x_i)$, and

$$\begin{aligned} \det(V((2+x_0)^2, \dots, (2+x_d)^2)) &= \prod_{j>i} ((2+x_j)^2 - (2+x_i)^2) \\ &= \prod_{j>i} (x_j - x_i) \prod_{j>i} (4 + x_j + x_i), \end{aligned}$$

we obtain

$$\prod_{j>i} (x_j - x_i) \cdot \left[\det(M_e) - \prod_{j>i} (4 + x_j + x_i) \right] \equiv 0 \pmod{(x_0^{d+1}, \dots, x_d^{d+1})}.$$

But this implies that the coefficient of $x_1 x_2^2 \dots x_d^d$ of the left hand side, namely $\det(M_e) - \prod_{j>i} 4$, has to vanish. Hence $\det(M_e) = 2^{d(d+1)}$.

The proof for M_o goes the same way by recognizing that $V(x_0, \dots, x_d) \cdot M_o$ is congruent to

$$\begin{pmatrix} 2+x_0 & (2+x_0)^3 & \dots & (2+x_0)^{2d+1} \\ 2+x_1 & (2+x_1)^3 & \dots & (2+x_1)^{2d+1} \\ \vdots & \vdots & \ddots & \vdots \\ 2+x_d & (2+x_d)^3 & \dots & (2+x_d)^{2d+1} \end{pmatrix}$$

modulo $(x_0^{d+1}, \dots, x_d^{d+1})$, and that the determinant of this matrix equals $\prod_{l=0}^d (2+x_l) \cdot \det(V((2+x_0)^2, \dots, (2+x_d)^2))$. \square

Now, we are prepared to proof the existence of the special invariant.

Theorem 4.4. *Let \mathbb{k} be a field of positive characteristic p and let (B_5, θ) be as in Example (DF5) over \mathbb{k} .*

There exists a w_5 -homogeneous invariant in B_5 of the form $v^p + vb' - b$, where $b', b \in \mathbb{k}[x, s, t, u] \subset B_5$ have w_4 -degree $w_4(b) = p$ and $w_4(b') = p - 1$.

Proof. It suffices to find $b \in \mathbb{k}[x, s, t, u]$ such that $\theta(b) = b + x^2b'U + x^{2p}U^p$, since this implies $\theta(b') = b'$ and

$$\begin{aligned} \theta(v^p + vb' - b) &= \theta(v)^p + \theta(v)\theta(b') - \theta(b) \\ &= (v + x^2U)^p + (v + x^2U) \cdot b' - (b + x^2b'U + x^{2p}U^p) = v^p + vb' - b. \end{aligned}$$

If $p = 2$, then $\theta(xt) = xt + x^4U^2$, and we are done.

Suppose $p > 2$. Let $\mathcal{O} := \mathbb{W}(\mathbb{k})$ be the Witt ring of \mathbb{k} , and let \mathbb{K} be the field of fractions of \mathcal{O} . Hence \mathbb{K} is a discrete valued field of unequal characteristic with valuation ring \mathcal{O} , valuation ideal (p) and residue class field \mathbb{k} . Example (DF5) over \mathbb{K} has a lfhd which restricts to $\mathcal{O}[x, s, t, u, v]$. Reduction modulo p then leads to Example (DF5) over \mathbb{k} . Thus, to obtain $b, b' \in \mathbb{k}[x, s, t, u]$ such that $\theta(b) = b + x^2b'U + x^{2p}U^p$, it suffices to find $\tilde{b}, \tilde{b}' \in \mathcal{O}[x, s, t, u] \subseteq \mathbb{K}[x, s, t, u]$ such that $\theta(\tilde{b}) \equiv \tilde{b} + x^2\tilde{b}'U + x^{2p}U^p \pmod{p}$. Let $c_n \in \mathbb{Q}[s, t, u] \subseteq \mathbb{K}[s, t, u]$ be the sequence constructed in Proposition 4.1. Set

$$b_n := x^{2p}c_n\left(\frac{s}{x^3}, \frac{t}{x^3}, \frac{u}{x^3}\right) \text{ for } 0 \leq n \leq p,$$

that is, b_n is the homogenization of c_n of degree $2p$ with respect to the grading w_5 . By construction of c_n , the elements b_n are indeed in $\mathbb{K}[x, s, t, u]$ and have coefficients in $\mathbb{Z}_{(p)} \subseteq \mathcal{O}$ resp. $\frac{1}{p}\mathbb{Z}_{(p)}$ for $n = p - 1$. Moreover, we have $b_0 = x^{2p}$, and x^2 divides b_{p-1} . A similar calculation as in Remark 4.2 shows that $\theta^{(k)}(b_p) = \binom{p}{k}b_{p-k}$ for all $0 \leq k \leq p$, and $\theta^{(k)}(b_p) = 0$ for $k > p$. Hence, $\theta(b_p) \equiv b_p + x^2\left(\frac{pb_{p-1}}{x^2}\right)U + x^{2p}U^p \pmod{p}$, as desired. \square

REFERENCES

- [1] Harm Derksen and Gregor Kemper. Computing Invariants of Algebraic Groups in Arbitrary Characteristic. *Adv. Math.*, 217(5):2089–2129, 2008. arXiv:math.AC/0704.2594.
- [2] Gene Freudenberg. *Algebraic Theory of Locally Nilpotent Derivations*. Encyclopaedia of Mathematical Sciences. Springer, Berlin Heidelberg, 2006.
- [3] Emmy Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.*, 77(1):89–92, 1915.
- [4] Paul Roberts. An infinitely generated symbolic blow-up in a power series ring and a new counterexample to Hilbert’s fourteenth problem. *J. Algebra*, 132(2):461–473, 1990.
- [5] Ryuji Tanimoto. On the polynomiality of invariant rings for codimension one \mathbb{G}_a -modules. *J. Algebra*, 305(2):1084–1092, 2006.
- [6] Ryuji Tanimoto. An algorithm for computing the kernel of a locally finite iterative higher derivation. *J. Pure Appl. Algebra*, 212(10):2284–2297, 2008.
- [7] Arno van den Essen. An algorithm to compute the invariant ring of a \mathbf{G}_a -action on an affine variety. *J. Symbolic Comput.*, 16(6):551–555, 1993.

- [8] Arno van den Essen. A simple solution of Hilbert's fourteenth problem in dimension five. *Colloq. Math.*, 105(1):167–170, 2006.

Emilie Dufresne, Mathematics Center of Heidelberg (MATCH), Heidelberg University, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
E-mail address: emilie.dufresne@iwr.uni-heidelberg.de

Andreas Maurischat, Interdisciplinary Center for Scientific Computing (IWR), Heidelberg University, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
E-mail address: andreas.maurischat@iwr.uni-heidelberg.de