arXiv:1011.0454v2 [math.RA] 3 Nov 2010

WEITZENBÖCK DERIVATIONS OF NILPOTENCY 3

DAVID L. WEHLAU

Abstract. We consider a Weitzenböck derivation Δ acting on a polynomial ring $R = K[\xi_1, \xi_2, \ldots, \xi_m]$ over a field K of characteristic 0. The K-algebra $R^\Delta = \{h \in R \mid \Delta(h) = 0\}$ is called the algebra of constants. Nowicki considered the case where the Jordan matrix for Δ acting on R_1, the degree 1 component of R, has only Jordan blocks of size 2. He conjectured ([N]) that a certain set generates R^Δ in that case. Recently Koury ([Kh]), Drensky and Makar-Limanov ([DM]) and Kuroda ([K]) have given proofs of Nowicki's conjecture. Here we consider the case where the Jordan matrix for Δ acting on R_1 has only Jordan blocks of size at most 3. Here we use combinatorial methods to give a minimal set of generators $\mathcal{G}$ for the algebra of constants R^Δ. Moreover, we show how our proof yields an algorithm to express any $h \in R^\Delta$ as a polynomial in the elements of $\mathcal{G}$.

Contents

1. Introduction

Let K be a field of characteristic zero and let $R = K[\xi_1, \xi_2, \ldots, \xi_m]$ be a polynomial ring over K in m variables each of degree 1. The

Date: November 4, 2010.
2010 *Mathematics Subject Classification.* 13N15; 13A50; 13P10; 14E07.
Key words and phrases. Locally nilpotent derivations; algebra of constants; invariants of unitriangular transformations, Robert's isomorphism.

ring R is graded by polynomial degree: $R = \oplus_{d=0}^{\infty} R_d$. A K-linear operator $\Delta : R \to R$ is called a derivation if $\Delta(ab) = a\Delta(b) + \Delta(a)b$. A derivation $d : R \to R$ is called locally nilpotent if for every $a \in R$ there exists a positive integer k such that $\Delta^k(a) = 0$. A derivation whose matrix representation on R_1 is a Jordan matrix with the zeros on the main diagonal is called a Weitzenböck derivation. It is clear that if Δ is a locally nilpotent derivation then by an appropriate choice of basis we may suppose that Δ is a Weitzenböck derivation. The kernel of Δ is a subalgebra of R called the *algebra of constants* and denoted by R^Δ. Weitzenböck's Theorem ([We]) asserts that if Δ is a Weitzenböck derivation then R^Δ is a finitely generated K-algebra.

Recently the case where the Jordan matrix of Δ on R_1 consists consist of entirely 2×2 blocks has been studied. Nowicki ([N]) conjectured that for this case R^Δ is generated by certain linear and quadratic polynomials. This was proved by Koury ([Kh]), by Drensky and Makar-Lima ([DM]) and also Kuoda ([K]). Here we consider the case where the Jordan matrix of Δ on R_1 has blocks of size at most 3 and exhibit a set of generators for R^Δ in that case. Furthermore, we give an algorithm for expressing any element of R^Δ as a polynomial in those generators.

Rather than studying the kernel of Δ we may shift perspective and consider $\sigma := e^\sigma = 1 + \delta + \delta^2/2! + \delta^3/3! + \ldots$. Then σ acts invertibly on R_1 and R. We consider the infinite cyclic group G of algebra automorphisms of R generated by σ. The $R^\Delta = R^G$, the ring of G invariants. We may use Robert's isomorphism to show that $R^\Delta = R^G \cong S^{\mathrm{SL}_2(K)}$ for a certain polynomial ring S on which $\mathrm{SL}_2(K)$ acts linearly. This allows us to use the classical invariant theory of $\mathrm{SL}_2(\mathbb{C})$ to derive properties of R^Δ. For a discussion of this approach see [W] or [B]. For a modern treatment of Robert's isomorphism see [P, Ch. 15 §1.3 Theorem 1] and [BK].

Another way to proceed is to use $\mathbb{Z}[\xi_1, \xi_2, \ldots, \xi_m]$ in the role of R and then reduce modulo a prime p. In this setting the cyclic group generated by σ is C_p, the cyclic group of order p and we study its ring of invariants $\mathbb{Z}/p\mathbb{Z}[\xi_1, \xi_2, \ldots, \xi_r]^{C_p}$. From this perspective compute $\mathbb{Z}[\xi_1, \xi_2, \ldots, \xi_r]^\Delta = \varprojlim \mathbb{Z}/p\mathbb{Z}[\xi_1, \xi_2, \ldots, \xi_r]^{C_p}_{<p}$. See [W] for a discussion of, and examples of this approach.

Here we use a simple combinatorial method. This is a generalization of the method used in [CSW] where we considered a question related to Weitzenböck derivations with Jordan blocks of size 2.

2. Main Theorem

Theorem 2.1 (Main Theorem)**.** *Suppose the Weitzenböck derivation acts on on a polynomial ring R via a Jordan matrix on R_1 consisting entirely of Jordan blocks of size 3. Write*

$$R = K[x_1, y_1, z_1, x_2, y_2, z_2, \ldots, x_n, y_n, z_n]$$

and write

$$\Delta = \sum_{i=1}^{n} \left(x_i \frac{\partial}{\partial y_i} + y_i \frac{\partial}{\partial z_i} \right) \ .$$

Then the algebra of constants R^Δ is minimally generated as a K-algebra by the following elements:

(1) $f_{(i)} := x_i$ *where* $1 \leq i \leq n$*;*
(2) $f_{(i,j)} := x_i y_j - x_j y_i$ *where* $1 \leq i < j \leq n$*;*
(3) $g_{(i,j)} := x_i z_j - y_i y_j + z_i x_j$ *where* $1 \leq i \leq j \leq n$*;*
(4) $g_{(i,j,k)} = \det \begin{pmatrix} x_i & y_i & z_i \\ x_j & y_j & z_j \\ x_k & y_k & z_k \end{pmatrix}$ *where* $1 \leq i < j < k \leq n$*.*

Remark 2.2. *If $n = 2$ we only get three generators $f_{(1)} = x_1$, $f_{(2)} = x_2$ and $f_{(1,2)} = x_1 y_2 - x_2 y_1$. If $n = 1$ we only get the single generator $f_{(1)} = x_1$.*

Remark 2.3. *Note that if the Weitzenböck derivation Δ acts on a polynomial ring P via a Jordan matrix on P_1 consisting of blocks of size at most 3 then we have a surjective algebra homomorphism $\psi : R \to P$ which commutes with the action of Δ. Then $\psi : R^\Delta \to P^\Delta$ is also surjective and $\Psi(\mathcal{G})$ forms a generating set for P^Δ.*

In addition to the usual polynomial degree we will multi-grade $R = K[x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n, z_1, z_2, \ldots, z_n]$ by $\mathbb{N}^n$ where the multi-degree of the monomial $x_1^{a_1} y_1^{b_1} z_1^{c_1} x_2^{a_2} \cdots z_n^{c_n}$ is $(a_1 + b_1 + c_1, a_2 + b_2 + c_2, \ldots, a_n + b_n + c_n)$. We say a polynomial h is *multi-linear* if it is homogeneous of degree $(d_1, d_2, \ldots, d_n)$ where each $d_i \leq 1$.

We will work with monomial orders. For a discussion of lead monomials and monomial orders we refer the reader to [CLO, Ch. 2]. All tensor products are over the base field K.

Let $\mathcal{G}$ denote the set of elements listed in Theorem 2.1. It is easy to verify that each of these elements is annihilated by Δ. Furthermore, by considering multi-degrees it is easy to show that the elements of $\mathcal{G}$ minimally generate some K-algebra Q. We begin by sketching the main steps in our proof that $Q = R^\Delta$.

Suppose that $h \in R^\Delta$ is a homogeneous polynomial of multi-degree $(d_1, d_2, \ldots, d_n)$. We consider the polynomial ring

$$S = K[X_1, Y_1, Z_1, X_2, Y_2, Z_2, \ldots, X_d, Y_d, Z_d]$$

where $d = d_1 + d_2 + \cdots + d_n$. By abuse of notation we consider Δ to be a Weitzenböck derivation on S. via $\Delta(Z_i) = Y_i$, $\Delta(Y_i) = X_i$ and $\Delta(X_i) = 0$ for $i = 1, 2, \ldots, d$.

We will use the classical techniques of polarization and restitution. In the next section we briefly describe these two techniques in a setting tailored to our needs. For a detailed discussion in a general setting, we refer the reader to the excellent book of Procesi ([P, Ch. 3 §2]). Polarization is a K-linear operator $\mathcal{P} : R_(d_1, d_2, \ldots, d_n)^\Delta \to S^\Delta_{(1,1,\ldots,1)}$ and restitution gives a K-linear operator $\mathcal{R}S^\Delta_{(1,1,\ldots,1)}$. These two operators are inverses of one another.

The full polarization $H := \mathcal{R}(h) \in S^\Delta_{(1,1,\ldots,1)}$. We find an explicit basis $\mathcal{B}_d$ for $S^\Delta_{(1,1,\ldots,1)}$ and so may write $H = \sum_{E \in \mathcal{B}_d} c_E E$ for scalars $c_E \in K$. Then restituting H yields $h = \sum_{E \in \mathcal{B}_d} c_E \mathcal{R}(E)$. The theorem then follows from the fact that each $\mathcal{R}(E)$ may be expressed as a polynomial in the elements of $\mathcal{G}$. Since we may give these polynomial expressions explicitly and since we have an algorithm to compute the scalars c_E we get an algorithm for expressing h as a polynomial in the elements of $\mathcal{G}$.

The main difficultly in the proof as outlined above is to find the basis $\mathcal{B}_d$ of $S^\Delta_{(1,1,\ldots,1)}$. We will construct a directed graph, in fact a rooted tree, Γ and consider the set of paths Path_d of length d starting from the root. Naturally associated to each such path γ we have a multi-linear monomial $\Lambda(\gamma) \in S$. We will construct a set map $\theta : \mathrm{Path}_d \to S^\Delta_{(1,1,\ldots,1)}$ such that $\mathrm{LM}(\theta(\gamma)) = \Lambda(\gamma)$. Then showing that $\dim S^\Delta_{(1,1,\ldots,1)} = |\mathrm{Path}_d|$ proves that $\theta(\mathrm{Path}_d)$ is a basis of $S^\Delta_{(1,1,\ldots,1)}$.

3. Polarization and Restitution

Here we give a brief description of the classical techniques of polarization and restitution. Our discussion tailored to our needs. For a complete discussion in a general setting, see Procesi [P, Ch. 3 §2]. Suppose that $f(x_1, y_1, z_1, x_2, y_2, z_2, \ldots, x_n, y_n, z_n) \in R$ is a homogeneous polynomial of multi-degree $(d_1, d_2, \ldots, d_n)$. We consider the polynomial rings $T = K[x_1, y_1, \ldots, z_n, X_1, Y_1, Z_1, X_2, Y_2, Z_2, \ldots, Z_d]$ and $S = K[X_1, Y_1, Z_1, X_2, Y_2, Z_2, \ldots, Z_d]$ where $d = d_1 + d_2 + \cdots + d_n$. We view both S and R as subalgebras of T. By abuse of notation we consider Δ to be a Weitzenböck derivation on both T and S by declaring that $\Delta(Z_i) = Y_i$, $\Delta(Y_i) = X_i$ and $\Delta(X_i) = 0$ for $i = 1, 2, \ldots, d$.

Let $D_{i,j}$ denote the differential operator

$$D_{i,j} := X_{r_i+j}\frac{\partial}{\partial x_i} + Y_{r_i+j}\frac{\partial}{\partial y_i} + Z_{r_i+j}\frac{\partial}{\partial z_i}$$

where $r_i = d_1 + d_2 + \cdots + d_{i-1}$. Then the full polarization of f is the element

$$\mathcal{P}(f) := \frac{1}{d_1!d_2!\cdots d_n!}\prod_{i=1}^{n}\prod_{j=1}^{d_i} D_{i,j} f \ .$$

The full polarization $\mathcal{P}(f)$ is multi-linear, i.e., it lies in $S_{(1,1,\ldots,1)}$. Note that

$$S_{(1,1,\ldots,1)} \cong K[X_1, Y_1, Z_1]_1 \otimes \cdots \otimes K[X_d, Y_d, Z_d]_1 \cong V_3 \otimes V_3 \otimes \cdots \otimes V_3 \ .$$

Corresponding to the full polarization is restitution. This is the algebra map $\mathcal{R} : S \to R$ determined by $\mathcal{R}(X_j) = x_i$, $\mathcal{R}(Y_j) = y_i$ and $\mathcal{R}(Z_j) = z_i$ where j is defined by $r_i < j \leq r_{i+1}$ and $r_i = d_1 + d_2 + \cdots + d_{i-1}$. Thus we have a full polarization operator and a restitution homomorphism for each multi-degree $(d_1, d_2, \ldots, d_n)$ of R.

The following theorem summarizes the properties of polarization and restitution we will use. Proofs may be found in [P, Ch.3 §2].

Theorem 3.1.

(1) $\mathcal{P} : R_{(d_1,d_2,\ldots,d_n)} \to S_{(1,1,\ldots,1)}$ *is a* K*-linear operator.*
(2) $\mathcal{R} : S \to R$ *is an algebra hommorphism.*
(3) $\mathcal{P} : R^{\Delta}_{(d_1,d_2,\ldots,d_n)} \to S^{\Delta}_{(1,1,\ldots,1)}$.
(4) $\mathcal{R} : S^{\Delta}_{(1,1,\ldots,1)} \to R^{\Delta}_{(d_1,d_2,\ldots,d_n)}$.
(5) $\mathcal{R}(\mathcal{P}(f)) = f$ *and* $\mathcal{P}(\mathcal{R}(F)) = F$, *i.e.,* $\mathcal{P}$ *and* $\mathcal{R}$ *are inverse set maps.*

4. Tensor Products of Jordan Matrices

We seek to find the Jordan form for Δ on $\otimes^d V_3$ where d is a positive integer. Let $J_n(\lambda)$ denote the $n \times n$ Jordan matrix with a single Jordan block and eigenvalue λ.

The derivation Δ on $S_{(1,1,\ldots,1)} \cong \otimes^d V_3$ has Jordan decomposition

$$\oplus_{h=1}^{\infty} \mu^d(h) J_h(0)$$

for some integers $\mu^d(h) \in \mathbb{N}$. Here we write $tJ_h(0)$ to denote the direct sum of t Jordan blocks of size h and eigenvalue 0.

It is not hard to see that the action of $\sigma = e^{\Delta}$ on $\otimes^d V_3$ has Jordan matrix given by $\oplus_{h=1}^{\infty} \mu^d(h) J_h(1)$. In particular, the matrix of σ on V_3 has Jordan form $J_3(1)$. To determine the numbers $\mu^d(h)$ we work with σ rather than with Δ directly. Hence we need to find the Jordan form for the Kronecker power $\otimes^d J_3(1)$. To do this inductively it suffices to decompose the Kronecker product $J_m(1) \otimes J_n(1)$ into a sum of Jordan blocks.

The question of the Jordan decomposition of the Kronecker product of Jordan matrices was considered early in the last century. The following theorem which provides the solution for the Jordan decomposition of $J_n(\lambda) \otimes J_m(\mu)$was ennunciated at that time (see [A, L, R]). However, it was not until rather later that a correct proof of this result [Br, MR] was given. For a discussion of the history of this problem see [Br] or [W].

Theorem 4.1. *Let $1 \leq m \leq n$. Then*

$$J_m(1) \otimes J_n(1) = J_{n-m+1}(1) \oplus J_{n-m+3}(1) \oplus J_{n-m+5}(1) \oplus \cdots \oplus J_{n+m-1}(1)\ .$$

This yields the following.

Lemma 4.2. *Suppose h is an odd positive integer. Then*

$$\mu^0(h) = \delta_h^1,$$

and

$$\mu^{d+1}(h) = \begin{cases} \mu^d(3), & \text{if } h = 1; \\ \mu^d(h-2) + \mu^d(h) + \mu^d(h+2), & \text{if } 3 \leq h. \end{cases}$$

for $d \geq 1$.

5. The Representation Graph

In this section we introduce a directed graph Γ which encodes the Jordan decomposition of tensor powers of $J_3(1)$. In order to simplify the exposition, we will consider Γ as embedded in the xy-plane in the first quadrant.

Γ is tree with root at the point $(1, 0)$. The vertices of Γ are the integer lattice points in (h, d) in the first quadrant with h odd and which lie on or above the line $y = x-1$, i.e., the points $(2a+1, d)$ with $a, d \in \mathbb{Z}$ and $0 \leq 2a \leq d$. We will also attach labels to the edges of Γ. Every vertex $(2a + 1, d)$ of Γ has a directed edge going up and to the right to the vertex at $(2a + 3, d + 1)$. We label this edge with the symbol X_{d+1}. If $2a+1 \geq 3$ there is also a directed edge going straight up from $(2a + 1, d)$ to $(2a + 1, d + 1)$. This vertical edge is labelled Y_{d+1}. Finally , if $2a + 1 \geq 3$ there is also an edge from $(2a + 1, d)$ up and leftward to $(2a - 1, d + 1)$. This edge is labelled Z_{d+1}.

Consider a path in the directed graph from the root $(1, 0)$ to a vertex $(2a + 1, d)$. Reading the edge labels of this path yields d labels, each from the set $\{X_1, Y_1, Z_1, X_2, Y_2, Z_2, \ldots, X_d, Y_d, Z_d\}$. Furthermore each of the subscripts $1, 2, \dots, d$ occurs exactly once. Multiplying these labels together yields a monomial of degree d in $S_{(1,1,\dots,1)} \cong \otimes^d V_3$. Thus to each path γ of length d originating from the root we have associated a monomial which we denote by $\Lambda(\gamma)$. We call the monomials which can be constructed in this manner, *path monomials* and we denote by M_d the path monomials arising from paths of length d.. We will show that these path monomials are exactly the lead monomials of elements of $S^{\Delta}_{(1,1,\dots,1)} \cong (\otimes^d V_3)^{\Delta}$.

We begin by counting paths in Γ. Let $\nu^d(h)$ denote the number of distinct paths in Γ from the root $(1, 0)$ to the vertex (h, d). With this notation we have the following lemma whose proof is left to the reader.

Lemma 5.1.

$$\nu^0(h) = \delta^1_h,$$

and

$$\nu^{d+1}(h) = \begin{cases} \nu^d(3), & \text{if } h = 1; \\ \nu^d(h-2) + \nu^d(h) + \nu^d(h+2), & \text{if } 3 \leq h. \end{cases}$$

The following corollary is immediate.

Corollary 5.2. *For all $d \in \mathbb{N}$ and all odd positive integers h we have*

$$\mu^d(h) = \nu^d(h) \ .$$

6. A Vector Space Basis for $S^{\Delta}_{(1,1,\dots,1)}$

We define the following multi-linear elements of S^{Δ}:

(1) $F_{\{i\}} := X_i$ where $1 \leq i \leq n$;
(2) $F_{\{i,j\}} := X_i Y_j - X_j Y_i$ where $1 \leq i < j \leq n$;
(3) $G_{\{i,j\}} := X_i Z_j - Y_i Y_j + Z_i Y_j$ where $1 \leq i < j \leq n$;
(4) $G_{\{i,j,k\}} = \det \begin{pmatrix} X_i & Y_i & Z_i \\ X_j & Y_j & Z_j \\ X_k & Y_k & Z_k \end{pmatrix}$ where $1 \leq i < j < k \leq n$.

From these elements we inductively construct two families of multi-linear elements of S^{Δ} as follows.

(1) $F_{\{i_1,i_2,\dots,i_t\}} := F_{\{i_2,i_4,i_5,i_6\dots,i_t\}} G_{\{i_1,i_3\}} - F_{\{i_1,i_4,i_5,i_6\dots,i_t\}} G_{\{i_2,i_3\}}$ where $1 \leq i_1 < i_2 < \cdots < i_t \leq n$ and $t \geq 3$.
(2) $G_{\{i_1,i_2,\dots,i_t\}} := G_{\{i_2,i_4,i_5,i_6\dots,i_t\}} G_{\{i_1,i_3\}} - G_{\{i_1,i_4,i_5,i_6\dots,i_t\}} G_{\{i_2,i_3\}}$ where $1 \leq i_1 < i_2 < \cdots < i_t \leq n$ and $t \geq 4$.

We denote the union of these families by $\mathcal{B}$ and we write $\mathcal{B}_d$ to denote those products of elements of $\mathcal{B}$ which have total degree d and lie in $S_{(1,1,\dots,1)}$.

We use the lexicographic order on S determined by

$$Z_n > Y_n > X_n > Z_{n-1} > Y_{n-1} > X_{n-1} > \cdots > Z_1 > Y_1 > X_1 \ .$$

The following lemma exhibits the two largest terms for elements of $\mathcal{B}$.

Lemma 6.1. *Let $1 < i_1 < i_2 \cdots < i_t \leq n$. Then*

(1) $F_{\{i_1,i_2,\ldots,i_t\}} = X_{i_1}Y_{i_2}Y_{i_3}Y_{i_4}\cdots Y_{i_t} - Y_{i_1}X_{i_2}Y_{i_3}Y_{i_4}\cdots Y_{i_t} + \ l.o.t.$, *if $t \geq 2$.*

(2) $G_{\{i_1,i_2,\ldots,i_t\}} = X_{i_1}Y_{i_2}Y_{i_3}Y_{i_4}\cdots Y_{i_{t-1}}Z_{i_t} - Y_{i_1}X_{i_2}Y_{i_3}Y_{i_4}\cdots Y_{i_{t-1}}Z_{i_t} + \ l.o.t.$, *if $t \geq 3$.*

Proof. The proof is by induction on t. The result is straightforward to verify for $t = 2, 3$. For higher values of t we have (using induction)

$$\begin{aligned}
&f_{\{i_1,i_2,\ldots,i_t\}} = f_{\{i_2,i_4,i_5\ldots,i_t\}}g_{\{1,3\}} - f_{\{i_1,i_4,i_5,i_6\ldots,i_t\}}g_{\{i_2,i_3\}}\\
&\quad = (X_{i_2}Y_{i_4}Y_{i_5}\cdots Y_t - Y_{i_1}X_{i_2}Y_{i_3}\cdots Y_{i_t} + \text{ l.o.t.})(X_{i_1}Z_{i_3} - Y_{i_1}Y_{i_3} + Z_{i_1}Y_{i_3})\\
&\qquad - (X_{i_1}Y_{i_4}Y_{i_5}\cdots Y_t - Y_{i_1}X_{i_4}Y_{i_5}\cdots Y_{i_t} + \text{ l.o.t.})(X_{i_2}Z_{i_3} - Y_{i_2}Y_{i_3} + Z_{i_2}Y_{i_3})\\
&\quad = X_{i_1}X_{i_2}Z_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_t} - X_{i_1}Y_{i_2}Z_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_t} + \text{ l.o.t.}\\
&\qquad - Y_{i_1}X_{i_2}Y_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_t} + Y_{i_1}Y_{i_2}Y_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_t} + \text{ l.o.t.}\\
&\qquad + Z_{i_1}X_{i_2}X_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_t} - Z_{i_1}Y_{i_2}X_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_t} + \text{ l.o.t.}\\
&\qquad - X_{i_1}X_{i_2}Z_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_t} + Y_{i_1}X_{i_2}Z_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_t} + \text{ l.o.t.}\\
&\qquad + X_{i_1}X_{i_2}Z_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_t} - Y_{i_1}Y_{i_2}Y_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_t} + \text{ l.o.t.}\\
&\qquad - X_{i_1}Z_{i_2}X_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_t} + Y_{i_1}Z_{i_2}X_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_t} + \text{ l.o.t.}\\
&\quad = X_{i_1}Y_{i_2}Y_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_t} - Y_{i_1}x_{i_2}Y_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_t} + \text{ l.o.t.}
\end{aligned}$$

The proof for (2) is similar with the cases $t = 3, 4$ being easily verified.

$$\begin{aligned}
&G_{\{i_1,i_2,\ldots,i_t\}} = G_{\{i_2,i_4,i_5\ldots,i_t\}}G_{\{1,3\}} - G_{\{i_1,i_4,i_5,i_6\ldots,i_t\}}G_{\{i_2,i_3\}}\\
&\quad = (X_{i_2}Y_{i_4}Y_{i_5}\cdots Y_t - Y_{i_1}X_{i_2}Y_{i_3}\cdots Y_{i_{t-1}}Z_{i_t} + \text{ l.o.t.})(X_{i_1}Z_{i_3} - Y_{i_1}Y_{i_3} + Z_{i_1}Y_{i_3})\\
&\qquad - (X_{i_1}Y_{i_4}Y_{i_5}\cdots Y_t - Y_{i_1}X_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + \text{ l.o.t.})(X_{i_2}Z_{i_3} - Y_{i_2}Y_{i_3} + Z_{i_2}Y_{i_3})\\
&\quad = X_{i_1}X_{i_2}Z_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} - X_{i_1}Y_{i_2}Z_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + \text{ l.o.t.}\\
&\qquad - Y_{i_1}X_{i_2}Y_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + Y_{i_1}Y_{i_2}Y_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + \text{ l.o.t.}\\
&\qquad + Z_{i_1}X_{i_2}X_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} - Z_{i_1}Y_{i_2}X_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + \text{ l.o.t.}\\
&\qquad - X_{i_1}X_{i_2}Z_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + Y_{i_1}X_{i_2}Z_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + \text{ l.o.t.}\\
&\qquad + X_{i_1}X_{i_2}Z_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} - Y_{i_1}Y_{i_2}Y_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + \text{ l.o.t.}\\
&\qquad - X_{i_1}Z_{i_2}X_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + Y_{i_1}Z_{i_2}X_{i_3}X_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + \text{ l.o.t.}\\
&\quad = X_{i_1}Y_{i_2}Y_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} - Y_{i_1}X_{i_2}Y_{i_3}Y_{i_4}Y_{i_5}\cdots Y_{i_{t-1}}Z_{i_t} + \text{ l.o.t.}
\end{aligned}$$

$\square$

In Proposition 8.1, we will prove that $\mathcal{B}_d$ is a vector space basis for $S^{\Delta}_{(1,1,\ldots,1)}$.

7. Definition of θ and ϕ

We will define a set maps

$$\phi : M_d \to S^{\Delta}_{(1,1,\ldots,1)}$$

and

$$\theta : \mathrm{Path}_d \to S^{\Delta}_{(1,1,\ldots,1)}$$

such that $\mathrm{LM}(\theta(\gamma)) = \Lambda(\gamma)$. Furthermore, $\theta(\gamma)$ will be a product of elements from $\mathcal{B}$ and so $\theta(\gamma) \in \mathcal{B}_d$. Since $\theta = \phi \circ \Lambda$ it will suffice to define ϕ.

Let α be a monomial in S. Put $\mathrm{supp}_X(\alpha) = \{i \mid X_i \text{ divides } \alpha\}$, $\mathrm{supp}_Y(\alpha) = \{i \mid Y_i \text{ divides } \alpha\}$, $\mathrm{supp}_Z(\alpha) = \{i \mid Z_i \text{ divides } \alpha\}$ and $\mathrm{supp}(\alpha) = \mathrm{supp}_X(\alpha) \cup \mathrm{supp}_Y(\alpha) \cup \mathrm{supp}_Z(\alpha)$. Suppose that $\alpha \in M_d$. Note that $\mathrm{supp}(\alpha)$ is the interval $[1, d]$.

We define $\phi(\alpha)$ as follows. Write $\mathrm{supp}_Z(\alpha) = \{k_1, k_2, \ldots, k_s\}$ where $k_1 < k_2 < \cdots < k_s$. We begin by defining $\{i_1, i_2, \ldots, i_s\} \subset \mathrm{supp}_X(\alpha)$ with $i_1 > i_2 > \cdots > i_s$. Let $i_1 := \max\{i \in \mathrm{supp}_X(\alpha) \mid i < k_1\}$ and put $I_i := [i_1, k_1]$ (an interval). Let $i_2 := \max\{i \in \mathrm{supp}_X(\alpha) \mid i < i_1\}$ and $I_2 := [i_2, k_2] \setminus I_1$. In general, $i_q := \max\{i \in \mathrm{supp}_X(\alpha) \mid i < i_{q-1}\}$ and $I_q := [i_q, k_q] \setminus (\sqcup_{\ell=1}^{q-1} I_\ell)$ for $q = 2, \ldots, s$.

Define $\overline{\alpha} := \alpha / (\prod_{\ell=1}^{s} \mathrm{LM}(G_{I_\ell}))$. Then $\mathrm{supp}(\overline{\alpha}) = [1, d] \setminus (\sqcup_{\ell=1}^{s} I_\ell)$. For each $j \in \mathrm{supp}_Y(\overline{\alpha})$ we define $\mathrm{succ}(j) := \min\{i \in \mathrm{supp}(\overline{\alpha}) \mid i > j\}$. Let $\{j_1, j_s, \ldots, j_t\} = \{j \in \mathrm{supp}_Y(\overline{\alpha}) \mid \mathrm{succ}(j) \notin \mathrm{supp}_Y(\overline{\alpha})\}$ where $j_1 < j_2 < \cdots < j_t$. Next we define $\{i'_1, i'_2, \ldots, i'_t\} \subset \mathrm{supp}_X(\overline{\alpha})\}$ with $i'_1 > i'_2 > \cdots > i'_t$ as follows. Let $i'_1 := \max\{i \in \mathrm{supp}_X(\overline{\alpha}) \mid i < j_1\}$ and $I'_1 := [i'_1, j_1] \cap \mathrm{supp}(\overline{\alpha})$. Let $i'_2 := \max\{i \in \mathrm{supp}_X(\overline{\alpha}) \mid i < i_2\}$ and $I'_2 := ([i'_2, j_2] \setminus I'_1) \cap \mathrm{supp}(\overline{\alpha})$. In general, $i'_q := \max\{i \in \mathrm{supp}_X(\overline{\alpha}) \mid i_q < i_{q-1}\}$ and $I'_q := ([i'_q, j_q] \setminus (\sqcup_{\ell=1}^{q-1} I'_\ell)) \cap \mathrm{supp}(\overline{\alpha})$. We put $I'' := [1, d] \setminus ((\sqcup_{\ell=1}^{s} I_\ell) \sqcup (\sqcup_{\ell=1}^{t} I'_\ell))$. Note that $I'' \subseteq \mathrm{supp}_X(\overline{\alpha})$.

Finally, we define

$$\phi(\alpha) := (\prod_{\ell=1}^{s} G_{I_\ell}) \cdot (\prod_{\ell=1}^{t} F_{I'_\ell}) \cdot (\prod_{i \in I''} F_{\{i\}}) \ .$$

For each $\ell = 1, 2, \ldots, s$ we have $\min I_\ell = i_\ell$ and $\max I_\ell = k_\ell$. Define $J_\ell := \{j \in I_\ell \mid i_\ell < j < k_\ell\}$. Then $\mathrm{LM}(G_{I_\ell}) = X_{i_\ell} \cdot (\prod_{j \in J_\ell} Y_j) \cdot Z_{k_\ell}$.

For each $\ell = 1, 2, \ldots, t$ we have $\min I'_\ell = i'_\ell$ and $\max I'_\ell = j_\ell$. Define $J'_\ell := I'_\ell \setminus \{i'_\ell\}$. Then $\mathrm{LM}(F_{I'_\ell}) = X_{i'_\ell} \cdot (\prod_{j \in J'_\ell} Y_j)$.

Therefore $\mathrm{LM}(\phi(\alpha)) = \alpha$ as required. Furthermore, $\phi(\alpha)$ is a product of elements of $\mathcal{B}$ and thus $\phi(\alpha) \in \mathcal{B}_d$.

8. Proof of the Main Theorem

We now prove that path monomials are exactly the lead monomials of multi-linear constants and so θ provides a bijection between paths of length d and a basis of the degree d multi-linear constants, $S^{\Delta}_{(1,1,\ldots,1)}$

Proposition 8.1.

$$M_d = \{\mathrm{LM}(f) \mid \deg(f) = d, f \in S^{\Delta}_{(1,1,\ldots,1)}\} \ .$$

Moreover, $\{\theta(\gamma) \mid \gamma \in Path_d\}$ is a vector space basis for $S^{\Delta}_{(1,1,\ldots,1)}$.

Proof. Since $\mathrm{LM}(\phi(\alpha)) = \alpha$ for all $\alpha \in M_d$ it follows that $M_d \subseteq \{\mathrm{LM}(f) \mid \deg(f) = d, f \in S^{\Delta}_{(1,1,\ldots,1)}\}$. Since $\#M_d = \#\mathrm{Path}_d = \sum_{h \text{ odd}, h \le d} \nu_h(d) = \sum_{h \text{ odd}, h \le d} \mu_h(d) = \dim S^{\Delta}_{(1,1,\ldots,1)}\} = \#\{\mathrm{LM}(f) \mid \deg(f) = d, f \in S^{\Delta}_{(1,1,\ldots,1)}\}$, we see that $M_d = \{\mathrm{LM}(f) \mid \deg(f) = d, f \in S^{\Delta}_{(1,1,\ldots,1)}\}$.

Furthermore, $\mathrm{LM}(\phi(\alpha)) = \alpha$ for all $\alpha \in M_d$ implies that the set $\phi(M_d) = \theta(\mathrm{Path}_d)$ is linearly independent. Therefore $\theta(\mathrm{Path}_d)$ is a basis of $S^{\Delta}_{(1,1,\ldots,1)}$. $\square$

Remark 8.2. *In fact it is possible to show that if γ is a path from the root to (h, d) then $\theta(\gamma)$ is an eigenvector corresponding to a Jordan block of size h.*

Suppose h lies in the algebra of constants R^{Δ}. Further suppose that h is homogeneous of multi-degree $(d_1, d_2, \ldots, d_n)$ and put $d := d_1 + d_2 + \cdots + d_n$. Let H denote the full polarization $\mathcal{P}(f)$ of h. Then $H \in S^{\Delta}_{(1,1,\ldots,1)}$. Thus $H = \sum_{E \in \mathcal{B}_d} c_E E$. In fact we may compute these coefficients c_E as follows. We know $\mathrm{LM}(H) = \Lambda(\gamma_1)$ for some $\gamma_1 \in \mathrm{Path}_d$. Then the lead term of H is $c_{\gamma_1}\Lambda(\gamma_1)$ for some scalar c_{γ_1}. Thus $\mathrm{LM}(H) > \mathrm{LM}(H - c_{\gamma_1}\theta(\gamma_1))$. By induction on lead monomials we may may compute the coefficients c_{γ_i} in the expansion $H = \sum_{i=1}^{r} c_{\gamma_i}\theta(\gamma_i)$.

Then $h = \mathcal{R}(H) = \sum_{i=1}^{r} c_{\gamma_i}\mathcal{R}(\theta(\gamma_i))$ where each $\theta(\gamma_i) \in \mathcal{B}_d$. Each $E \in \mathcal{B}_d$ is of the form $E = \prod_{I \in A} F_I \cdot \prod_{I' \in A'} G_{I'}$ for some index sets A and A'. Thus $\mathcal{R}(E) = \prod_{I \in A} \mathcal{R}(F_I) \cdot \prod_{I' \in A'} \mathcal{R}(G_{I'})$.

Lemma 8.3. *Let Q denote the K-algebra generated by $\mathcal{G}$.*

1. *$\mathcal{R}(F_I) \in Q$ for all index sets I.*
2. *$\mathcal{R}(G_{I'}) \in Q$ for all index sets I' with $\#I' \ge 2$.*

Proof. We prove the first assertion; the proof of the second is similar. The proof is by induction on $\#I$. If $\#I = 1$ then $\mathcal{R}(F_I) = x_i \in \mathcal{G}$ for some i. If $\#I = 2$ then $\mathcal{R}(F_I) = x_i y_j - x_j y_i$ for some $i \leq j$ and so either $\mathcal{R}(F_I) \in \mathcal{G}$ or $\mathcal{R}(F_I) = 0$. If $\#I \geq 3$ then $F_I = F_A G_B - F_C G_D$ for some index sets A, B, C, D and $\mathcal{R}(F_I) = \mathcal{R}(F_A)\mathcal{R}(G_B) - \mathcal{R}(F_C)\mathcal{R}(G_D)$ lies in Q by induction. □

This lemma completes the proof that R^Δ is the K-algebra generated by $\mathcal{G}$. Moreover, the proof of the above lemma provides an inductive algorithm for writing any element of $\mathcal{B}$ as a polynomial in the elements of $\mathcal{G}$.

I thank Megan Wehlau for a number of useful discussions which led to this work. The computer algebra program Magma ([BCP]) was very helpful in my early explorations of this problem. The author was partially supported by grants from NSERC and ARP.

References

[A] A.C. Aitken, *The normal form of compound and induced matrices*, Proc. London Math. Soc. **38** (1934) 354–376.

[BCP] W. Bosma, J.J. Cannon and C. Playoust, *The Magma algebra system I: the user language*, J. Symbolic Comput. **24** (1997) 235–265.

[B] Leonid Bedratyuk, *A note about the Nowicki conjecture on Weitzenböck derivations* Serdica Math. J. **35** (2009), 311-316.

[Br] Richard A. Brualdi, *Combinatorial verification of the elementary divisors of tensor products*, Linear Algebra Appl., **71** (1985) 31–47.

[BK] Roger M. Bryant and Gregor Kemper, *Global degree bounds and the transfer principle for invariants*, J. Algebra **284** (2005), no. 1, 80–90.

[CSW] H.E.A. Campbell, R.J. Shank and David L. Wehlau, *Vector invariants for the two dimensional modular representation of a cyclic group of prime order*, Advances in Mathematics **225** (2010) no. 2, 1069–1094 (doi:10.1016/j.aim.2010.03.018, arXiv:0901.2811).

[CLO] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag, 1992.

[DM] Vesselin Drensky and Leonid Makar-Limanov, *The conjecture of Nowicki on Weitzenbck derivations of polynomial algebras*, J. Algebra Appl. **8** (2009), no. 1, 41-51.

[Kh] J. Khoury, *A Groebner basis approach to solve a conjecture of Nowicki*, J. Symbolic Comput. **43** (2008), no. 12, 908–922.

[K] Shigeru Kuroda, *A simple proof of Nowicki's conjecture on the kernel of an elementary derivation*, Tokyo J. Math. **32** (2009), no. 1, 247–251.

[L] D.E. Littlewood, *On induced and compound matrices*, Proc. London Math. Soc. **40** (1936) 370–381.

[MR] Marvin Marcus and Herbert Robinson, *Elementary divisors of tensor products*, Comm. ACM **18** (1975) 36–39.

[N] A. Nowicki, *Polynomial Derivations and Their Rings of Constants* (Uniwersytet Mikolaja Kopernika, Torun, 1994). [Available at: www-users.mat.umk.pl/∼anow/ps-dvi/pol-der.pdf.]

[P] Claudio Procesi, Lie groups. *An approach through invariants and representations*, Universitext. Springer, New York, 2007. xxiv+596 pp. ISBN: 978-0-387-26040-2; 0-387-26040-4.

[R] W.E. Roth, *On direct product matrices*, Bull. AMS **40** (1934) 461–468.

[W] David L. Wehlau, *Invariants for the Modular Cyclic Group of Prime Order via Classical Invariant Theory*, (preprint) arXiv:0912.1107.

[We] R. Weitzenböck, *Über die Invarianten von linearen Gruppen*, Acta Math. **58** (1932) 231-293.

Department of Mathematics and Computer Science,
Royal Military College, Kingston, Ontario, Canada, K7K 5L0
E-mail address: wehlau@rmc.ca