INVARIANTS IN DIVIDED POWER ALGEBRAS

RUDOLF TANGE

Abstract. Let k be an algebraically closed field of characteristic $p > 0$, let $G = \mathrm{GL}_n$ be the general linear group over k, let $\mathfrak{g} = \mathfrak{gl}_n$ be its Lie algebra and let D_s be subalgebra of the divided power algebra of $\mathfrak{g}^*$ spanned by the divided power monomials with exponents $< p^s$. We give a basis for the G-invariants in D_s up to degree n and show that these are also the $\mathfrak{g}$-invariants.

We define a certain natural *restriction property* and show that it doesn't hold when $s > 1$. If $s = 1$, then D_1 is isomorphic to the truncated coordinate ring of $\mathfrak{g}$ of dimension $p^{\dim(\mathfrak{g})}$ and we conjecture that the restriction property holds and show that this leads to a conjectural spanning set for the invariants (in all degrees).

We give similar results for the divided power algebras of several matrices and of vectors and covectors, and show that in the second case the restriction property doesn't hold.

We also give the dimensions of the filtration subspaces of degree $\leq n$ of the centre of the hyperalgebra of the Frobenius kernel G_s.

Introduction

Let k be an algebraically closed field of characteristic $p > 0$, let $G = \mathrm{GL}_n$ be the general linear group over k and let $\mathfrak{g}$ be its Lie algebra: the $n \times n$ matrices with entries in k. For the representation theory of G and $\mathfrak{g}$ it is of interest to understand the centres $U^{[p]}(\mathfrak{g})^{\mathfrak{g}}$ and $\mathrm{Dist}(G)^G$ of the restricted enveloping algebra $U^{[p]}(\mathfrak{g})$ and the hyperalgebra or distribution algebra $\mathrm{Dist}(G)$. In this paper we study their commutative analogues: the truncated symmetric algebra $\overline{S}(\mathfrak{g}) = S(\mathfrak{g})/(x^p \,|\, x \in \mathfrak{g})$ and the divided power algebra $D(\mathfrak{g})$. They are isomorphic to their noncommutative analogues as G-modules under the conjugation action. The connection with the representations of G and $\mathfrak{g}$ is described in more detail in Remark 1.2.3 and Corollary 3 to Theorem 2.1 (the hyperalgebras of G and G_s) and Remark 1.2.4 (the Schur algebra). To state our results it is more convenient to work with $A_1(\mathfrak{g}) = \overline{S}(\mathfrak{g}^*)$ and $D(\mathfrak{g}^*)$. This is harmless, since $\mathfrak{g} \cong \mathfrak{g}^*$ as G-modules.

Initially we were interested in describing the invariants for the group and the Lie algebra in $A_1(\mathfrak{g})$ and its higher analogues $A_s(\mathfrak{g}) = S(\mathfrak{g}^*)/(f^{p^s} \,|\, f \in \mathfrak{g}^*)$. It is easy to see that $A_1(\mathfrak{g})^G$ is bigger than the image of $S(\mathfrak{g}^*)^G$ (or $S(\mathfrak{g}^*)^{\mathfrak{g}}$): the top degree element (unique up to a scalar multiple) of $A_1(\mathfrak{g})^G$ is not in the image of $S(\mathfrak{g}^*)^G$. It turned out to be more convenient to work with the dual versions $D_s(\mathfrak{g}^*)$ of the $A_s(\mathfrak{g})$, inside the divided power algebra $D(\mathfrak{g}^*)$ where we have the

2020 *Mathematics Subject Classification.* 13A50, 16W22.

Key words and phrases. general linear group, divided power algebra, truncated coordinate ring, invariants, centre.

divided power maps. Up to degree n it is easy to give a basis for the invariants in $D(\mathfrak{g}^*)$. In fact we can give three different bases, see Section 1.5. So the task is then to describe the invariants of the subalgebras $D_s(\mathfrak{g}^*)$ in terms of these bases. For one of the three aforementioned bases of $D(\mathfrak{g}^*)$ we obtain a basis of $D_s(\mathfrak{g}^*)$ by forming equivalence class sums for a certain equivalence relation on the basis, for the other two we obtain a basis of $D_s(\mathfrak{g}^*)$ by taking a suitable subset of the basis, see Theorem 2.2.

We also consider the so-called “restriction property” for several families of algebras, see Section 1.6. Intuitively, when the restriction property holds one may expect a universal description of the invariants, independent of the rank n. When it doesn’t hold the description of the invariants will depend on the rank. In all the classical cases (invariants in the coordinate rings of vectors and covectors and of several matrices) the restriction property holds, at least for the group. For the algebras $D(\mathfrak{g}^*)$ and $D_s(\mathfrak{g}^*)$ that we study, the restriction property almost never holds. We can only conjecture it for $D_1(\mathfrak{g}^*) = A_1(\mathfrak{g})$, see Conjecture 2.1.

The paper is organised as follows. In Section 1 we discuss some, mostly well-known, results about divided power algebras, truncated coordinate rings, polarisation and $\mathbb{Z}$-forms, and multilinear invariants of several matrices that we will need later on.

Section 2 contains our main result which describes the G-invariants in the algebra $D_s(\mathfrak{g}^*)$: Theorem 2.2. To prove it, it is more convenient to first work with $D_s(\mathfrak{g})$. Theorem 2.1 is our main result for this algebra. Infinitesimal invariants are discussed in Proposition 2.1. In Corollary 3 to Theorem 2.2 we give the dimensions of the filtration subspaces of degree $\leq n$ of the centre of the hyperalgebra of $\mathrm{Dist}(G_s)$. In Remark 2.3.3 and 4 we show that the restriction property doesn’t hold for the algebras $A_s(\mathfrak{g})$ when $s \geq 2$ and also not for the algebras $D_s(\mathfrak{g}^*)$ when $s \geq 2$. In Section 2.4 we give dimensions for the invariants in the graded pieces of some of the $A_s(\mathfrak{g})$.

In Section 3 we study the divided power algebra and its “truncated” subalgebras for several matrices. Theorem 3.1 describes the G-invariants and Proposition 3.1 describes the infinitesimal invariants. To state and prove these results we first need to state some, mostly well-known, results about conjugacy classes in the symmetric group for a Young subgroup, partial polarisation, and invariants in the full divided power algebra.

In Section 4 we study the divided power algebra and its truncated subalgebras for vectors and covectors. Proposition 4.1(i) describes the G-invariants and Proposition 4.1(ii) describes the infinitesimal invariants. As preliminaries we first state some, mostly well-known, results about partial polarisation, and orbits in the symmetric group for the multiplication action of a product of two Young subgroups. In Remark 4.1.3 we show that the restriction property doesn’t hold in this case.

1. Preliminaries

Throughout this paper k is an algebraically closed field of characteristic $p > 0$ and s is an integer ≥ 1.

1.1. **Lucas's Theorem and Legendre's Theorem.** We remind the reader of two basic results from number theory.

Theorem (Lucas's Theorem). *Let $a = \sum_{i\geq 0} a_i p^i$ and $b = \sum_{i\geq 0} b_i p^i$ be the p-adic expansions of the integers $a, b \geq 0$. Then $\binom{a}{b} \equiv \prod_{i\geq 0} \binom{a_i}{b_i}$ mod p.*

Theorem (Legendre's Theorem). *Let $\nu_p : \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ be the p-adic valuation, let $a \geq 1$ be an integer, and let $s_p(a)$ be the sum of the p-adic digits of a. Then $\nu_p(a!) = \frac{a - s_p(a)}{p-1}$.*

1.2. **The divided power algebra and certain subalgebras.**
Let $V = k \otimes_{\mathbb{Z}} V_{\mathbb{Z}}$ be a vector space over k "defined over $\mathbb{Z}$" where $V_{\mathbb{Z}}$ has $\mathbb{Z}$-basis $(y_1, \ldots, y_m)$. We will denote $1 \otimes y_i \in V$ just by y_i. Inside the symmetric algebra $S(V_{\mathbb{Q}})$ of $V_{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} V_{\mathbb{Z}}$ we can form the divided power monomials $\prod_{i=1}^m y_i^{(t_i)}$ where $t_i \geq 0$ and $x^{(t)} = \frac{1}{t!} x^t$. They are linearly independent over $\mathbb{Q}$ and their $\mathbb{Z}$-span is a $\mathbb{Z}$-subalgebra $D(V_{\mathbb{Z}})$ of $S(V_{\mathbb{Q}})$. Now we put $D(V) = k \otimes_{\mathbb{Z}} D(V_{\mathbb{Z}})$.

The algebra $S(V_{\mathbb{Q}})$ has the divided power map $\gamma_i = (x \mapsto x^{(i)}) : I_{\mathbb{Q}} \to S(V_{\mathbb{Q}})$ where $I_{\mathbb{Q}}$ consists of the polynomials without constant term. The γ_i, $i \geq 1$, preserve $I_{\mathbb{Z}} = D(V_{\mathbb{Z}}) \cap I_{\mathbb{Q}}$ and therefore induce divided power maps $\gamma_i : I_{\mathbb{Z}} \to D(V_{\mathbb{Z}})$. These γ_i preserve $pI_{\mathbb{Z}}$ for $i \geq 1$ and, reducing mod p and extending from $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ to k, we obtain divided power maps $\gamma_i = (x \mapsto x^{(i)}) : I \to D(V)$, where $I = k \otimes I_{\mathbb{Z}}$, which satisfy:

(1) $\gamma_0(x) = 1$, $\gamma_1(x) = x$ and $\gamma_i(x) \in I$ for $i \geq 1$ and for all $x \in I$,
(2) $\gamma_i(x + y) = \sum_{j=0}^{i} \gamma_j(x)\gamma_{i-j}(y)$ for $i \geq 0$ and for $x, y \in I$,
(3) $\gamma_i(xy) = x^i \gamma_i(y)$ for $i \geq 0$, $x \in D(V)$ and $y \in I$,
(4) $\gamma_i(x)\gamma_j(x) = \binom{i+j}{i}\gamma_{i+j}(x)$ for $i, j \geq 0$ and $x \in I$, and
(5) $\gamma_i(\gamma_j(x)) = \frac{(ij)!}{(i!)^j j!}\gamma_{ij}(x)$ for $i, j \geq 0$ and $x \in I$.

The algebra $D(V)$ is commutative and graded and has a $\mathrm{GL}(V)$-action which is "defined over $\mathbb{Z}$", so it is clear that the γ_i are $\mathrm{GL}(V)$-equivariant. The span $D_s(V)$ of the (divided power) monomials $\prod_i y_i^{(t_i)}$, $0 \leq t_i < p^s$ is a $\mathrm{GL}(V)$-stable graded subalgebra of $D(V)$ of dimension p^{sm}. It can be characterised as the distribution algebra or hyperalgebra of the s-th Frobenius kernel $V_{a,s}$ of the additive group scheme V_a, see [9, I.4.25]. We denote the graded pieces of degree r of $D(V)$ and $D_s(V)$ by $D^r(V)$ and $D_s^r(V)$.

Lemma 1.1. *Let $B = \bigoplus_{r\geq 2} D_1^r(V)$. Then B is stable under multiplication and under the $\gamma_i, i \geq 1$.*

Proof. Clearly, B is stable under multiplication. Note that $\binom{\sum_i a_i p^i}{\sum_i b_i p^i}$ is nonzero mod p if $0 \leq b_i \leq a_i < p$ for all i by Lucas's Theorem, and $\frac{p^{i+1}!}{(p^i!)^p p!}$ is nonzero mod p by Legendre's Theorem. So in view of (4) and (5) it is enough to show that B is stable under γ_p. Clearly, B is stable under the γ_i, $1 \leq i < p$, so by (2) it is enough to show that $\gamma_p(u) = 0$ for any divided power monomial u in the y_i of degree j with $2 \leq j < p$. If u involves at least two variables, then this follows immediately from (3). So assume $u = y_i^{(j)}$ for some i. Then $\gamma_p(u) = \frac{(jp)!}{(j!)^p p!} y_i^{(jp)}$ by (5). By Legendre's Theorem the p-adic valuation of $\frac{(jp)!}{(j!)^p p!}$

is $\frac{jp-s_p(jp)}{p-1}-(\frac{p(j-s_p(j))}{p-1}+1)$, where $s_p(j)$ denotes the sum of the p-adic digits of j. Now $s_p(jp)=s_p(j)=j$, since $j<p$, so this p-adic valuation equals $j-1$ which is ≥ 1. So $\frac{(jp)!}{(j!)^p p!}=0 \mod p$. □

1.3. **Truncated coordinate rings.** Define the ideal I_s of the coordinate ring $A=A(V)=k[V]=S(V^*)$ of V by $I_s=(f^p\,|\,f\in V^*)=({x_i}^{p^s}\,|\,1\leq i\leq m)$, where $(x_1,\ldots,x_m)$ is the dual basis of $(y_1,\ldots,y_m)$. Put $A_s=A_s(V)=k[V]/I_s$. We call $A_s(V)$ the *s-th truncated coordinate ring of V*. It is a commutative graded algebra of dimension p^{sm} and can be characterised as the coordinate ring of the aforementioned infinitesimal group scheme $V_{a,s}$. We denote the graded pieces of degree r of $A(V)$ and $A_s(V)$ by $A^r(V)$ and $A^r_s(V)$. There is a $\mathrm{GL}(V)$-equivariant isomorphism of graded Hopf algebras $D_s(V)\cong A_s(V)^*$. It maps $\prod_{i=1}^m y_i^{(t_i)}$, $0\leq t_i<p^s$, to the dual basis element of $\prod_{i=1}^m {x_i}^{t_i}$. Put $A^r_s=A^r_s(V)$. The top degree of A_s is $N=(p^s-1)m$ and $A_s(N)=k\prod_{i=1}^m {x_i}^{p^s-1}$ is 1-dimensional. Since $\mathrm{GL}(V)$ acts through $\det^{1-p^s}$ on $A_s(N)$, the multiplication defines an $\mathrm{GL}(V)$-invariant pairing $A^r_s\times(A^{N-r}_s\otimes\det^{p^s-1})\to k$. This pairing is nondegenerate, so we obtain isomorphisms $(A^r_s)^*\cong A^{N-r}_s\otimes\det^{p^s-1}$ and $D_s(V)\cong A_s(V)^*\cong A_s(V)\otimes\det^{p^s-1}$ of $\mathrm{GL}(V)$-modules. The latter maps $\prod_{i=1}^m y_i^{(t_i)}$ to $\prod_{i=1}^m x_i^{p^s-t_i}$.

1.4. **The polarisation map and $\mathbb{Z}$-forms.** The polarisation map

$$P: S^r(V^*)\to(S^rV)^*$$

in degree r sends $f\in S^r(V^*)$ to the the multi-homogeneous component of degree $(1,\ldots,1)$ of the r-variable polynomial function $(v_1,\ldots,v_r)\mapsto f(v_1+\cdots+v_r)$. Let $F:V^{\oplus r}\to k$ be r-linear, and let $f=(v\mapsto F(v,\ldots,v))\in S^r(V^*)$, then

$$P(f)=((v_1,\ldots,v_r)\mapsto\sum_{\sigma\in S_r}F(v_{\sigma(1)},\ldots,v_{\sigma(1)}))\,,$$

where S_r denotes the symmetric group or rank r. We extend P to a linear map from $k[V]=S(V^*)$ to the graded dual $S(V)^{*\mathrm{gr}}$ of $S(V)$ and this is an algebra homomorphism. The multiplication on this graded dual comes from the comultiplication on $S(V)$, see [3, III.11].

Inside $S(V^*_{\mathbb{Q}})$ we have the "divided power $\mathbb{Z}$-form" $D(V^*_{\mathbb{Z}})$. The polarisation map over $\mathbb{Q}$ maps this $\mathbb{Z}$-form onto the standard $\mathbb{Z}$-form of the graded dual of $S(V_{\mathbb{Q}})$. Reducing mod p we obtain an isomorphism from $D\overset{\mathrm{def}}{=}D(V^*)$ to $S(V)^{*\mathrm{gr}}$. We now identify these two. Then $D^r\overset{\mathrm{def}}{=}D^r(V^*)=S^r(V)^*=((V^{\otimes r})^*)^{S_r}$: the space of symmetric r-linear functions $V^{\oplus r}\to k$, and $D^r_s=D^r_s(V^*)$ consists of the symmetric r-linear functions that vanish when p^s arguments are the same. Furthermore the polarisation map over k can now be identified with the map $k[V]=S(V^*)\to D(V^*)$ given by inclusion of $\mathbb{Z}$-forms. We note that for a symmetric r-linear function $V^{\oplus r}\to k$ to vanish when p^s arguments are the same it is enough to check that this holds for r-tuples of basis vectors. This follows from the fact that the S_{p^s}-stabiliser of a nonconstant map $\{1,\ldots,p^s\}\to\{1,\ldots,t\}$, t any integer ≥ 2, is a proper Young subgroup of S_{p^s}, so the orbit of such a map has size divisible by p.

We now return to the polarisation map in characteristic p. It follows easily from the definition that P has image D_1 and kernel I_1, so it induces a $\mathrm{GL}(V)$-equivariant isomorphism $A_1 = A_1(V) \xrightarrow{\sim} D_1(V^*) = D_1$ of graded algebras.

1.5. **Adjoint invariants and symmetric functions.** From now on until the end of Section 2 we specialise V to $\mathfrak{g} = \mathfrak{gl}_n = \mathrm{End}(k^n)$ with $G = \mathrm{GL}_n$ acting by conjugation. So $D = D(\mathfrak{g}^*)$ and $A = A(\mathfrak{g})$. The symbol V may now denote another vector space. We work with the bases $(E_{ij})_{1\le i,j\le n}$ of $\mathfrak{g}$ with dual basis $(x_{ij})_{1\le i,j\le n}$ of $\mathfrak{g}^*$, where E_{ij} is the elementary matrix which is 1 in row i and column j and 0 elsewhere. Note that the trace form on $\mathfrak{g}$ is nondegenerate and gives an isomorphism $\mathfrak{g} \xrightarrow{\sim} \mathfrak{g}^*$ of G-modules which maps E_{ij} to x_{ji}. Note also that the G-action factors through the $\mathrm{SL}(\mathfrak{g})$-action, so we have isomorphisms of G-modules $D^r_s \cong (A^r_s)^* \cong A^{N-r}_s$, where $N = (p^s-1)n^2$ is the top degree. The G-invariants in $D^r = ((\mathfrak{g}^{\otimes r})^*)^{S_r}$ are the S_r-invariants in the space of G-invariants of $(\mathfrak{g}^{\otimes r})^*$. By "Schur-Weyl duality" [4, Sect 4], the space of G-invariants of $(\mathfrak{g}^{\otimes r})^*$ can be described as the image of the group algebra kS_r of the symmetric group S_r under the S_r-equivariant linear map

$$\pi \mapsto f_\pi\,,$$

where $f_\pi(X_1,\dots,X_r) = \prod_{i=1}^r \mathrm{tr}(X_{\sigma_i})$, $\pi = \sigma_1\cdots\sigma_s$ is the disjoint cycle form of π (including 1-cycles), $\mathrm{tr}(X_\sigma) \overset{\mathrm{def}}{=} \mathrm{tr}(X_{i_1}\cdots X_{i_t})$ for any cycle $\sigma = (i_1,\dots,i_t)$, and the S_r-action on kS_r is by conjugation. This map is injective when $r \le n$. If we work with $\mathfrak{g}^{\otimes r}$ instead of the isomorphic module $(\mathfrak{g}^{\otimes r})^*$, then the map is given by $\pi \mapsto E_\pi$, where $E_\pi = \sum_{i\in\{1,\dots,n\}^r} \otimes_{l=1}^r E_{i_{\pi(l)}i_l}$.[1]

We make some observations about symmetric functions. For the basics we refer to [10]. For an integer $i \ge 1$ and $X \in \mathrm{Mat}_n$ we define $e_i(X) = \mathrm{tr}(\wedge^i X), h_i(X) = \mathrm{tr}(S^i X)$ and $p_i(X) = \mathrm{tr}(X^i)$. Clearly, the e_i, h_i, p_i can be considered as elements of $k[\mathfrak{g}]$ and therefore also as elements of $D(\mathfrak{g})$, see Section 1.4. For a partition λ of r we define e_λ to be the product of the e_{λ_i} and we define h_λ and p_λ in the same way. Via the Chevalley Restriction Theorem (CRT) we can identify these functions with the equally named symmetric functions. Writing λ in the form $\lambda = 1^{m_1}2^{m_2}\cdots$ we define $z_\lambda = \prod_{i\ge1} i^{m_i} m_i!$ and $u_\lambda = \prod_{i\ge1} m_i!$. Recall that z_λ is the order of the centraliser in S_r of a permutation of cycle type λ. We will call $\frac{1}{z_\lambda}p_\lambda, \frac{1}{u_\lambda}h_\lambda, \frac{1}{u_\lambda}e_\lambda \in S(\mathfrak{g}^*_{\mathbb{Q}})$ *divided* p_λ, h_λ and e_λ.

For the divided e_λ's and h_λ's, λ a partition of r, it is clear that by reduction mod p they can be considered as elements of $(D^r)^G$: $e_\lambda = \prod_{i\ge1} e_i^{(m_i)}$, $h_\lambda = \prod_{i\ge1} h_i^{(m_i)}$. We claim that the same is true for the divided p_λ's and that, for $n \ge r$, these three families form three bases of $(D^r)^G$. For the first claim we work over $\mathbb{Q}$. By [10, Ex I.6.10, p 110] the $\mathbb{Z}$-span of the p_λ's is the same as that of the $u_\lambda m_\lambda$'s, where the m_λ's are the monomial symmetric functions. Taking the "dual" lattices, i.e. everything that is integral on the lattice via the canonical form, we obtain that the $\mathbb{Z}$-span of the divided p_λ's is the same as that of the divided h_λ's, see [10, I.4.5, I.4.7]. Applying the involution ω we see

[1] Identifying $\mathfrak{g}^{\otimes r}$ with $\mathrm{End}((k^n)^{\otimes r})$, the action of S_r on tensor space is given by $\pi \mapsto E_{\pi^{-1}}$.

that $\mathbb{Z}$-span of the divided p_λ's is also the same as that of the divided e_λ's, see [10, I.2.6-13]. So $\frac{1}{z_\lambda}p_\lambda$ belongs to $D(\mathfrak{g}^*_\mathbb{Z})$.

To prove the second claim we return to the above S_r-equivariant linear map from kS_r onto the G-invariant multilinear functions of r matrices. It is injective when $n \geq r$. So in this case $(D^r)^G$ is simply the image of the centre $(kS_r)^{S_r}$ of kS_r. If $\pi \in S_r$ has cycle type λ, then $p_\lambda = (X \mapsto f_\pi(X, \ldots, X))$, so, as an element of $S^r(\mathfrak{g}_\mathbb{Q})^*$ via the polarisation map P, it is $\sum_{\sigma\in S_r} f_{\sigma\pi\sigma^{-1}}$. Therefore the sum of the conjugacy class $[\pi]$ is mapped to divided p_λ. So the divided p_λ's form a basis and therefore the divided e_λ's and h_λ's as well.

Example 1.1. Take $p = 2$. Put $u = \text{divided}\, p_{21} + \text{divided}\, p_{1^3} = \frac{1}{2}p_2p_1 + \frac{1}{6}p_1^3 \in D(\mathfrak{g}^*_\mathbb{Z})$. Then $u = (X \mapsto \frac{1}{2}\mathrm{tr}(X^2)\mathrm{tr}(X) + \frac{1}{6}\mathrm{tr}(X)^3)$ corresponds to the symmetric 3-linear function

$$(X, Y, Z) \mapsto \mathrm{tr}(XY)\mathrm{tr}(Z) + \mathrm{tr}(XZ)\mathrm{tr}(Y) + \mathrm{tr}(YZ)\mathrm{tr}(X) + \mathrm{tr}(X)\mathrm{tr}(Y)\mathrm{tr}(Z)\,.$$

In characteristic p, this function vanishes when 2 arguments are the same, so the reduction mod p of u belongs to D_1. When $n = 2$ this function is nonzero (take e.g. $X = E_{12}, Y = E_{21}, Z = E_{11}$), but is zero on triples of diagonal 2×2-matrices. The same is true for any symmetric r-linear function $r\mathfrak{gl}_2 \to k$, $r > 2$, which vanishes when 2 arguments are the same. Similarly, $\text{divided}\, p_3 = \frac{1}{3}p_3 = ((X, Y, Z) \mapsto \mathrm{tr}(XYZ) + \mathrm{tr}(YXZ))$ vanishes in characteristic 2 when 2 arguments are the same. This function is clearly nonzero for $n \geq 2$, but is zero on triples of diagonal matrices for all $n \geq 1$. Note that $e_4 = e_2^{(2)}$ on the diagonal matrices for $p = 2$ and any $n \geq 4$, but not on the $n \times n$ matrices.

1.6. **The restriction properties.** Recall that for a $\mathfrak{g}$-module V the subspace of $\mathfrak{g}$-invariants in V is defined by $V^\mathfrak{g} = \{v \in V \,|\, x \cdot v = 0 \text{ for all } x \in \mathfrak{g}\}$. If V is a commutative k-algebra on which $\mathfrak{g}$ acts by derivations, for example the differentiated action of an action of G by automorphisms, then any p-th power is a $\mathfrak{g}$-invariant.

We will occasionally indicate the dependence of our algebras A_s and D_s on the rank n with an extra left subscript n. The embedding $X \mapsto \left(\begin{smallmatrix} X & 0 \\ 0 & 0 \end{smallmatrix}\right) : \mathfrak{gl}_{n-1} \hookrightarrow \mathfrak{gl}_n$ induces a GL_{n-1}-equivariant surjections ${}_nA \twoheadrightarrow {}_{n-1}A$ and ${}_nA_s \twoheadrightarrow {}_{n-1}A_s$ and therefore restriction maps

$$({}_nA_s)^{\mathrm{GL}_n} \to ({}_{n-1}A_s)^{\mathrm{GL}_{n-1}}. \tag{1}$$

$$({}_nA_s)^{\mathfrak{gl}_n} \to ({}_{n-1}A_s)^{\mathfrak{gl}_{n-1}}. \tag{2}$$

We say that the algebras $({}_nA_s)_{n\geq1}$ have the *group restriction property* if the above maps (1) are surjective for all $n \geq 2$. The *infinitesimal restriction property*, or *Lie algebra restriction property*, can be defined analogously using the maps (2) and one can define similar restriction maps for the algebras ${}_nA = k[\mathfrak{gl}_n]$, ${}_nD$ and ${}_nD_s$.

As is well known, $e_1, \ldots, e_n$ are algebraically independent and generate A^G. Clearly, e_i for $\mathfrak{gl}_n$ restricts to e_i for $\mathfrak{gl}_{n-1}$, so the algebras ${}_nA$, $n \geq 1$, have the group restriction property. Furthermore, by Veldkamp's Theorem for A, A is generated by A^p and A^G, see [13, Sect 3.5] and the references there. So the algebras ${}_nA$, $n \geq 1$, also have the infinitesimal restriction property.

Remarks 1.2. 1. Although the S_r-invariants of kS_r, i.e. the centre of kS_r, in general ($r > n$) does not surject onto the S_r-invariants in $((\mathfrak{g}^{\otimes r})^*)^G$, it seems that this image does contain the symmetric G-invariant multilinear functions of r matrices which vanish when p arguments are the same. The first statement is equivalent to the statement that the algebras ${}_nD$ don't have the restriction property, see Remark 2.3.4. The second statement is implied by Conjecture 2.1.
2. From our discussion of $(D^r)^G$ we get an isomorphism from $(kS_r)^{S_r}$ to the projective limit $\varprojlim_n (S^r(\mathfrak{gl}_n)^*)^{\mathrm{GL}_n}$. This map is a characteristic p version the "characteristic map" from [10, I.7.3].
3. The map $f \mapsto (X \mapsto f(X - I)) : k[\mathfrak{g}] \to k[G]$, I the identity matrix, induces G-equivariant filtration preserving algebra isomorphisms $A_s \overset{\sim}{\to} k[G_s]$, $s \geq 1$. Here the filtrations are given by the powers of the maximal ideals of 0 resp. I. Taking duals we obtain G-equivariant filtration preserving coalgebra isomorphisms $\mathrm{Dist}(G_s) \overset{\sim}{\to} D_s(\mathfrak{g}) \cong D_s$, $s \geq 1$, where $\mathrm{Dist}(G_s)$ is the distribution or hyperalgebra of the s-th Frobenius kernel G_s of G. These fit together to give a G-equivariant filtration preserving coalgebra isomorphism

$$\mathrm{Dist}(G) \overset{\sim}{\to} D(\mathfrak{g}) \cong D \tag{$*$}$$

of which the associated graded is a G-equivariant isomorphism of Hopf algebras. All this holds in much bigger generality, see [6, Sect 2]. We note that the algebra $\mathrm{Dist}(G_1)$ is isomorphic to the restricted enveloping algebra $U^{[p]}(\mathfrak{g})$ of $\mathfrak{g}$.

In [11, Sect 14,15] Okounkov and Olshanski studied the "special symmetrisation" map $\sigma : S(\mathfrak{g}_\mathbb{C}) \to U(\mathfrak{g}_\mathbb{C})$. It maps the divided power $\mathbb{Z}$-form onto the Kostant $\mathbb{Z}$-form and after reduction mod p one obtains the inverse of the map (*). Via the Chevalley restriction and Harish Chandra map, the restriction of σ to the invariants corresponds to the map φ from symmetric functions to "shifted symmetric functions" which maps the Schur function s_λ to the shifted Schur function s^*_λ. It is not clear to me how to obtain elementary formulas for the images of the symmetric functions e_λ, h_λ and p_λ under φ.
4. The Schur algebra $S(n, r)$ is isomorphic to D^r as $G\times G$-module, so the centre of $S(n, r)$ is isomorphic to $(D^r)^G$ as vector spaces. Computer calculations suggest that $(D^r)^G$ has dimension equal to the number of partitions of r of length $\leq n$, independent of p, and that a spanning set can be obtained by dividing each h_λ, λ a partition of r, by the biggest possible integer in the $D(\mathfrak{gl}^*_{n,\mathbb{Z}})$ and then reducing mod p.

2. The algebras D_s and $D_s(\mathfrak{g})$

2.1. **Group invariants.** Call a partition *s-reduced* if it has $< p^s$ ones. To any partition we can associate an s-reduced partition by repeatedly replacing p^s occurrences of 1 by p^{s-1} occurrences of p. We will call two partitions *s-equivalent* if their associated s-reduced partitions are the same. Call two elements of the symmetric group S_r *s-equivalent* if their cycle types are s-equivalent. Recall the definition of E_π, $\pi \in S_r$, from Section 1.5.

Theorem 2.1. *The sums of the E_π over the s-equivalence classes belong to $D_s(\mathfrak{g})^G$, and when $n \geq r$ they form a basis of $D^r_s(\mathfrak{g})^G$.*

Proof. As we have seen in Section 1.5, the E_π span the G-invariants in $\mathfrak{g}^{\otimes r}$ and they form a basis when $n \geq r$. So if $n \geq r$, then the sums of the E_π over the conjugacy classes form a basis of $D^r(\mathfrak{g})^G = (\mathfrak{g}^{\otimes r})^{G \times S_r}$. The subspace $D^r_s(\mathfrak{g})$ consists of those elements u of $D^r(\mathfrak{g})$ for which $(x_{i_1j_1} \otimes \cdots \otimes x_{i_rj_r})(u) = 0$ for all $i, j \in \{1, \ldots, n\}^r$ such that $(i_lj_l)_{l \in \{1,\ldots,r\}}$ has at least p^s repetitions. First we observe that $(x_{i_1j_1} \otimes \cdots \otimes x_{i_rj_r})(E_\pi) = 1$ if $j = i \circ \pi$ and 0 otherwise. So, if we put $E_S = \sum_{\sigma \in S} E_\sigma$ for $S \subseteq S_r$, then $(x_{i_1j_1} \otimes \cdots \otimes x_{i_rj_r})(E_S) = |\{\sigma \in S \,|\, j = i \circ \sigma\}| \mod p$. We will now show the following:

Lemma. *Let $\Lambda \subseteq \{1, \ldots, r\}$ be a set of p^s indices and let $i, j \in \{1, \ldots, n\}^r$ such that (i_l, j_l) is constant for $l \in \Lambda$. We extend the permutations in* $\mathrm{Sym}(\Lambda)$ *to $\{1, \ldots, r\}$ by letting them fix the elements outside Λ. Let $\pi \in S_r$.*

(i) *If $j \neq i \circ \pi$ or the centraliser $C_{\mathrm{Sym}(\Lambda)}(\pi)$ of π in* $\mathrm{Sym}(\Lambda)$ *does not contain a p^s-cycle, then $(x_{i_1j_1} \otimes \cdots \otimes x_{i_rj_r})(E_{\mathrm{Sym}(\Lambda)\cdot\pi}) = 0$.*

(ii) *If $j = i \circ \pi$ and $C_{\mathrm{Sym}(\Lambda)}(\pi)$ contains a p^s-cycle, then Λ is π-stable, and $(x_{i_1j_1} \otimes \cdots \otimes x_{i_rj_r})(E_{\mathrm{Sym}(\Lambda)\cdot\pi})$ equals*[2]
$$\begin{cases} 1 & \textit{if } \pi|_\Lambda = \mathrm{id}, \\ -1 & \textit{if } \pi|_\Lambda \textit{ is a product of } p^{s-1} \textit{ disjoint } p\textit{-cycles, and} \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Let Ω be the set of permutations π with $j = i \circ \pi$. Note that Ω is $C_{S_r}(i) \times C_{S_r}(j)$-stable, so $\mathrm{Sym}(\Lambda)$ acts on Ω by conjugation.

(i). If $j \neq i \circ \pi$, then $j \neq i \circ \rho$ for all $\rho \in \mathrm{Sym}(\Lambda) \cdot \pi$. Therefore we have $(x_{i_1j_1} \otimes \cdots \otimes x_{i_rj_r})(E_{\mathrm{Sym}(\Lambda)\cdot\pi}) = 0$. Now assume that $j = i \circ \pi$. Then $\mathrm{Sym}(\Lambda)\cdot\pi \subseteq \Omega$ and $(x_{i_1j_1} \otimes \cdots \otimes x_{i_rj_r})(E_{\mathrm{Sym}(\Lambda)\cdot\pi}) = |\mathrm{Sym}(\Lambda)\cdot\pi| \mod p$. So it suffices to show that $\mathrm{Sym}(\Lambda) \cdot \pi$ has size divisible by p. Now also assume that $C_{\mathrm{Sym}(\Lambda)}(\pi)$ does not contain a p^s-cycle. Then the same holds for $C_{\mathrm{Sym}(\Lambda)}(\rho)$ for all $\rho \in \mathrm{Sym}(\Lambda)\cdot\pi$. Now let $\sigma \in \mathrm{Sym}(\Lambda)$ be any p^s-cycle. Then $\langle\sigma\rangle$ is a p-group and all $\langle\sigma\rangle$-orbits on $\mathrm{Sym}(\Lambda) \cdot \pi$ have size divisible by p. So $\mathrm{Sym}(\Lambda) \cdot \pi$ has size divisible by p.

(ii). Since $j = i \circ \pi$, we have $(x_{i_1j_1} \otimes \cdots \otimes x_{i_rj_r})(E_{\mathrm{Sym}(\Lambda)\cdot\pi}) = |\mathrm{Sym}(\Lambda) \cdot \pi| \mod p$, as we have seen in the proof of (i). Let $\sigma \in C_{\mathrm{Sym}(\Lambda)}(\pi)$ be a p^s-cycle. Then Λ is π-stable, since π commutes with σ. So Λ is a union of $\langle\pi\rangle$-orbits. These orbits are permuted transitively by $\langle\sigma\rangle$. So they all have the same size, p^t say, $t \in \{0, \ldots, s\}$.

We have $|\mathrm{Sym}(\Lambda)\cdot\pi| = |\mathrm{Sym}(\Lambda)\cdot(\pi|_\Lambda)| = \frac{p^s!}{(p^t)^{p^{s-t}} p^{s-t}!}$, see [10, I.B.3(1) p171]. If we apply the p-adic valuation to this we get by Legendre's Theorem
$$\frac{p^s - 1}{p - 1} - (tp^{s-t} + \frac{p^{s-t} - 1}{p - 1})\,.$$
If $t = 0$, then $\pi|_\Lambda = \mathrm{id}$ and $|\mathrm{Sym}(\Lambda) \cdot \pi| = 1$. Now assume $t = 1$. Then $\pi|_\Lambda$ is a product of p^{s-1} disjoint p-cycles. Clearly, $|\mathrm{Sym}(\Lambda) \cdot \pi|$ is nonzero mod p (the p-adic valuation is zero), so we may assume that $p > 2$. For each $a \in \{1, \ldots, p-1\}$

[2] The reader may want to check that the centraliser of a product of s disjoint t-cycles always contains an st-cycle.

we count how often a p-power multiple of a number with remainder a mod p occurs in the list $p^s, p^s-1, \dots, p^{s-1}+1$ of factors of $\frac{p^s!}{p^{s-1}!}$. It occurs as $a+bp$ for $b=p^{s-2},\dots,p^{s-1}-1$, as $ap+bp^2$ for $b=p^{s-3},\dots,p^{s-2}-1,\dots$, as $ap^{s-2}+bp^{s-1}$ for $b=1,\dots,p-1$ and finally as ap^{s-1} for $a>1$ and as p^s for $a=1$. That is in total $(p^{s-1}-p^{s-2})+(p^{s-2}-p^{s-3})+\cdots+(p-1)+1=p^{s-1}$ times. The product of the nonzero numbers in the prime field is -1. So $|\mathrm{Sym}(\Lambda)\cdot\pi|=(-1)^{p^{s-1}}=-1$ mod p.

Finally assume that $t\geq 2$. Then we have to show that $\frac{p^s-1}{p-1}>tp^{s-t}+\frac{p^{s-t}-1}{p-1}$, i.e. $p^s>tp^{s-t+1}-tp^{s-t}+p^{s-t}$, i.e. that $p^t>tp-t+1$. This we do by induction on t. For $t=2$ this follows from the fact that $p>2-\frac{1}{p}$. Now assume it holds for t. Then we have $p\geq 2>1+\frac{1}{p^{t-1}}-\frac{1}{p^t}$. So $p^{t+1}>p^t+p-1>tp-t+1+p-1=(t+1)p-(t+1)+1$. So $\mathrm{Sym}(\Lambda)\cdot\pi$ has size divisible by p. □

So for i,j and Λ as in the lemma, the $\mathrm{Sym}(\Lambda)$-orbits S for which the value $(x_{i_1j_1}\otimes\cdots\otimes x_{i_rj_r})(E_S)$ is nonzero, leave Λ stable and come in "associated pairs": one has cycle structure 1^{p^s} on Λ and value 1, the other has cycle structure $p^{p^{s-1}}$ on Λ and value -1. When T is an s-equivalence class, then E_T can be written as a sum of certain E_S, S a $\mathrm{Sym}(\Lambda)$-orbit and with any such orbit which has nonzero value the associated orbit is also present, so $(x_{i_1j_1}\otimes\cdots\otimes x_{i_rj_r})(E_T)=0$. It follows that $E_T\in D_s(\mathfrak{g})$.

Now assume that $n\geq r$. Let $\Lambda\subseteq\{1,\dots,r\}$ be a set of p^s indices, assume $\pi\in S_r$ stabilises Λ, $\pi|_\Lambda$ is a product of p^{s-1} disjoint p-cycles and $\pi'\in S_r$ is the identity on Λ and equal to π outside Λ. Denote the S_r-conjugacy class of $\sigma\in S_r$ by $[\sigma]$. Note that $[\pi]\neq[\pi']$. Recall from our discussion in Section 1.5 that the $E_{[\sigma]}$ form a basis of $D^r(\mathfrak{g})^G$. To prove the theorem it is enough to show that for any Λ, π and π' as above, and any $u\in D^r_s(\mathfrak{g})^G$, $E_{[\pi]}$ and $E_{[\pi']}$ occur with the same coefficient in u. Define $i\in\{1,\dots,n\}^r$ by $i_l=l$ for $l\in\{1,\dots,r\}\setminus\Lambda$ and $i_l=\min(\Lambda)$ for $l\in\Lambda$. Put $j=i\circ\pi=i\circ\pi'$. By our definition of i and j, $j=i\circ\sigma$ implies $\sigma=\pi$ outside Λ. So the $\mathrm{Sym}(\Lambda)$-orbits of π and π' form the only associated pair (relative to i,j and Λ) and the only $\mathrm{Sym}(\Lambda)$-orbit S in $[\pi]$ resp $[\pi']$ for which E_S has nonzero value is that of π resp. π'. So for $u\in(D^r)^G$, written as a linear combination of the $E_{[\sigma]}$, $(x_{i_1j_1}\otimes\cdots\otimes x_{i_rj_r})(u)$ equals the coefficient of $E_{[\pi']}$ minus the coefficient of $E_{[\pi]}$. This ends the proof of the theorem. □

Theorem 2.2.

(i) *The sums of the divided p_λ's over the s-equivalence classes of the partitions of r belong to $(D^r_s)^G$, and when $n\geq r$ they form a basis of $(D^r_s)^G$.*

(ii) *The divided h_λ's and the divided e_λ's, both with $\lambda=1^{m_1}2^{m_2}\cdots$ such that $m_1<p^s$, belong to $(D^r_s)^G$, and when $n\geq r$ they form two bases of $(D^r_s)^G$.*

Proof. (i). This is just a reformulation of Theorem 2.1, where we now work in the divided power algebra D of $\mathfrak{g}^*$ rather than $\mathfrak{g}$. As we have seen in Section 1.5 divided p_λ corresponds to the sum of the E_π over the conjugacy class labelled by λ.

(ii). Since these two families are independent, see Section 1.5, and have the same cardinality as the basis from part (i), it is enough to show that they lie in D_s. Recall that D_s is spanned by the divided power monomials in the x_{ij}'s with exponents $< p^s$. Both the divided h_λ's and the divided e_λ's are products of divided powers with exponent $< p^s$ of $e_1 = h_1$ and divided powers of elements in the span $B \subseteq D_1$ of the divided power monomials in the x_{ij}'s of degree ≥ 2 and with exponents $< p$. Using (2) it follows that $\gamma_i(e_1) \in D_s$ for all $i < p^s$. So it is enough to show that B is stable under all divided powers γ_i, $i \geq 1$. This follows from Lemma 1.1. □

Corollary 1. *The monomials $\prod_{i=1}^n e_i^{(m_i)}$, $m_1 < p^s$, belong to D_s^G. Furthermore, for $r \leq n$, those with $\sum_{i=1}^n im_i = r$ form a basis of $(D_s^r)^G$.*

Proof. This is just a reformulation of the statement about the e_λ's in Theorem 2.2. □

Remarks 2.1. 1. Let $\overline{A^G}$ denote the image of A^G in $A_1 = D_1$. By Veldkamp's Theorem for $k[\mathfrak{g}]$, see Section 1.6, $\overline{A^G}$ is also the image of $A^{\mathfrak{g}}$ in A_1. Furthermore, by [12, Thms 8.2 or 8.4] it has the monomials in the e_i with exponents $< p$ as a basis. From Corollary 1 it is clear that when $n \geq 2p$ the first degree where a "new" invariant (i.e. not in $\overline{A^G}$) shows up in A_1 is $2p$. Indeed $(A_1^{2p})^G$ is the direct sum of the image of $(A^{2p})^G$ and $ke_2^{(p)}$. In the introduction of [15] it is pointed out that $A_1^{\mathfrak{g}}$ modulo $\overline{A^G}$ is isomorphic to $H^1(G_1, I_1)$, where I_1 is the ideal from Section 1.3. We note that conjecturally $A_1^{\mathfrak{g}}$ and A_1^G are the same, see the remarks after Conjecture 2.1.
2. For R a commutative ring, put $A_{1,R} = R[(x_{ij})_{1\leq i,j\leq n}]/(x_{ij}^p \,|\, 1 \leq i,j \leq n)$. We define $\varphi_p : A_{1,\mathbb{Z}}^+ \to A_{1,\mathbb{Z}}$, $A_{1,\mathbb{Z}}^+$ the truncated polynomials without constant term, by $\varphi_p(u) = \frac{u^p}{p}$. Then φ_p descends to a map $\varphi_p : A_{1,\mathbb{F}_p}^+ \to A_{1,\mathbb{F}_p}$. We have $A_{1,\mathbb{F}_p} = D_{1,\mathbb{F}_p}$, and when $u \in A_{1,\mathbb{F}_p}^+$ has no linear or constant term, then $\varphi_p(u)$ can also be computed in the divided power algebra $D_\mathbb{Z}$ by the same formula. Let $\overline{u} \in D_\mathbb{Z}$ be a lift of u (without linear or constant term), let $m \geq 0$ be an integer, let $m = \sum_{i=0}^t a_i p^i$ be the p-adic expansion of m and write $m! = qp^{\nu_p(m!)}$, where p does not divide q. By Legendre's Theorem we have $\nu_p(m!) = \sum_{i=1}^t a_i \frac{p^i-1}{p-1} = \sum_{i=1}^t a_i \nu_p(p^i!)$. So $\overline{u}^{(m)} = \frac{1}{q}\prod_{i=1}^t (\frac{\overline{u}^{p^i}}{p^{\nu_p(p^i!)}})^{a_i} = \frac{1}{q}\prod_{i=1}^t (\varphi_p^i(\overline{u}))^{a_i}$ and therefore

$$u^{(m)} = \frac{1}{q}\prod_{i=1}^t (\varphi_p^i(u))^{a_i}\,.$$

In particular, any divided power monomial $\prod_{i=1}^n e_i^{(m_i)}$ with $m_1 < p$ can be expressed as a monomial in $e_1, \ldots, e_n$ together with the iterates of φ_p on $e_2, \ldots, e_n$.

2.2. **Infinitesimal invariants.**

Lemma 2.1. *Let $V = k^n$ be the natural module for G, let $r, t \geq 1$ with $n \geq r, t$, and put $W = V^{\oplus r} \oplus (V^*)^{\oplus t}$. For $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, t\}$ let $x_i : W \to V$ and $y_j : W \to V^*$ be the i-th vector component and j-th covector component function and $\langle x_i, y_j\rangle = ((v, w) \mapsto w_j(v_i)) \in k[W]^G$ be the bracket function. Then*

(i) *the monomials in the* $\langle x_i, y_j\rangle$ *with exponents* $< p$ *form a basis of* $k[W]^{\mathfrak{g}}$ *over* $k[W]^p$*, and*

(ii) $((V^{\otimes r} \otimes (V^*)^{\otimes t})^*)^{\mathfrak{g}} = ((V^{\otimes r} \otimes (V^*)^{\otimes t})^*)^G$.

Proof. (i). We will verify the hypotheses of [14, Thm 5.5]. Using the notation in [14] we have that $\mathfrak{c}_{\mathfrak{g}}(W) = \dim \mathfrak{g} - \min_{x\in W} \dim \mathfrak{g}_x = n^2 - (n-r)(n-t) = (r+t)n - rt$, since $n \geq r, t$, and $\dim(W) - \mathfrak{c}_{\mathfrak{g}}(W) = rt$. Let $U \subseteq W$ be the set of points $(v, w) \in W$ where the differentials $d_{(v,w)}\langle x_i, y_j\rangle$ are linearly dependent. We have $d_{(v,w)}\langle x_i, y_j\rangle = ((z, u) \mapsto \langle v_i, u_j\rangle + \langle z_i, w_j\rangle) = f_j(v_i) + g_i(w_j) \in W^* = (V^*)^{\oplus r} \oplus V^{\oplus t}$, where f_j embeds V in the $(r+j)$-th position in W^* and g_i embeds V^* in the i-th position of W^*. It is now easy to check that the differentials of the $\langle x_i, y_j\rangle$ at (v, w) will be independent if $v \in V^{\oplus r}$ is independent or if $w \in (V^*)^{\oplus t}$ is independent. Since $n \geq r, t$ we can indeed choose v and w like this, so we obtain that $\operatorname{codim}(W \setminus U) \geq 2$.
(ii). This follows from (i), since $((V^{\otimes r} \otimes (V^*)^{\otimes t})^*)^{\mathfrak{g}}$ consists of the multilinear functions in $k[W]^{\mathfrak{g}}$, so the p-th powers cannot be involved. □

Proposition 2.1. *Assume* $r \leq n$ *and put* $N = (p^s-1)n^2$. *Then* $(D^r)^{\mathfrak{g}} = (D^r)^G$ *and* $(A_s^{N-r})^{\mathfrak{g}} = (A_s^{N-r})^G$ *for* $r \leq n$.

Proof. Since $A_s^{N-r} \cong D_s^r$ as G-modules and D_s^r is a G-submodule of D^r, it is enough to prove the first assertion. Put $V = k^n$. Since $D_s^r \subseteq D^r \subseteq (\mathfrak{g}^{\otimes r})^* \cong (V^{\otimes r} \otimes (V^*)^{\otimes r})^*$ it is enough to show that $((V^{\otimes r} \otimes (V^*)^{\otimes r})^*)^{\mathfrak{g}}$ equals $((V^{\otimes r} \otimes (V^*)^{\otimes r})^*)^G$ for $r \leq n$ which follows from Lemma 2.1(ii). □

One can form the divided power algebra of a vector space $V = k \otimes_{\mathbb{Z}} V_{\mathbb{Z}}$ where $V_{\mathbb{Z}}$ is any free $\mathbb{Z}$-module. If $(x_i)_{i\in I}$ is a basis of $V_{\mathbb{Z}}$ one just has to work with monomials $\prod_{i\in I} x_i^{(m_i)}$ with all but finitely many m_i zero. For a family of variables $(x_i)_{i\in I}$ we put $D((x_i)_{i\in I}) = D(k\otimes_{\mathbb{Z}} V_{\mathbb{Z}})$ and $D_s((x_i)_{i\in I}) = D_s(k\otimes_{\mathbb{Z}} V_{\mathbb{Z}})$ where $V_{\mathbb{Z}}$ is the free $\mathbb{Z}$-module on $(x_i)_{i\in I}$.

Corollary 2 (to Theorem 2.2)**.**

$$\varprojlim_n ({}_nD_s)^{\mathfrak{gl}_n} = \varprojlim_n ({}_nD_s)^{\mathrm{GL}_n} = D_s(e_1) \otimes D((e_i)_{i\geq 2}),$$

where $D((e_i)_{i\geq 2})$ *is graded such that* $e_i^{(m)}$ *has degree* mi*, and the limit is in the category of graded* k*-algebras.*

Proof. This follows from Proposition 2.1 and Corollary 1 to Theorem 2.2. □

Corollary 3 (to Theorem 2.2)**.** *Denote the centre of* $\mathrm{Dist}(G_s)$ *by* Z_s *and for a subspace* W *of* $\mathrm{Dist}(G_s)$ *denote by* F^rW *the intersection of* W *with the* r*-th filtration subspace of* $\mathrm{Dist}(G_s)$*. Assume that* $r \leq n$.

(i) $F^rZ_s = F^r\mathrm{Dist}(G_s)^G = F^r\mathrm{Dist}(G_s)^{\mathfrak{g}}$.

(ii) *The dimension of* F^rZ_s *is the number of partitions of* $0, 1, \ldots, r$ *with* $< p^s$ *ones.*

Proof. This follows from Remark 1.2.3, Proposition 2.1 and Theorem 2.1. □

Remarks 2.2. 1. The referee mentioned to me the following generalisation of Lemma 2.1. Call a polynomial dominant weight, i.e. a partition of length $\leq n$,

p^s-restricted if $\lambda_i - \lambda_{i+1} < p^s$ for $i = 1, \ldots, n-1$, and $\lambda_n < p^s$. Furthermore, call a semisimple G-module *p^s-restricted* if all its irreducible submodules have *p^s-restricted* highest weight. Then we have the following result.

Proposition. *Let M and N be finite dimensional polynomial G-modules, homogeneous of degrees r and t. If $r \leq t$ and N has p^s-restricted socle or if $r \geq t$ and M has p^s-restricted head, then* $\mathrm{Hom}_G(M,N) = \mathrm{Hom}_{G_s}(M,N)$.

This result is not hard to prove using standard facts about polynomial modules, see [9, App A.1-3], contravariant duality, see [9, II.1.16,2.12,2.13] or [7, 2.7,5.4c], and the arguments from [9, II.3.16]: One first reduces to the first alternative using contravariant duality, then one reduces to the case that N is an injective indecomposable in the polynomial category, and then one proves the assertion by induction on the number of composition factors, where the assumption $r \leq t$ is needed for the basis case that M is irreducible.

From the above result one easily deduces Lemma 2.1. Indeed for $n \geq r$ we have $\mathrm{Hom}_G(V^{\otimes r}, X) \cong X_\omega$ where X_ω is the ω-weight space and $\omega = (1, \ldots, 1, 0, \ldots, 0)$ (r ones), see [9, A.22,23] or[7, 6.2g Rem 1, 6.4f, 6.4b]. So $V^{\otimes r}$ has p-restricted head, and, by contravariant duality, p-restricted socle.
2. The conclusion of Lemma 2.1 does not hold when $n < r$ or $n < t$. For example, if we have $n = 1, r \geq 2, t \geq 1$ then $x_1^h x_2^{p-h}$, $1 < h < p$ is a $\mathfrak{g}$-invariant, but it doesn't belong to the $k[X]^p$-algebra generated by the $x_i y_j$.
3. I checked with the computer that $\dim(D^r)^{\mathfrak{g}} > \dim(D^r)^G$ when $p = 2, n = 2$ or $n = 3$, and $r = n+1$. In the first case I got $8 > 5$, in the second case $31 > 23$. When $p = 3, n = 2$, and $r = 5$ I got $45 > 42$.

For $p = 2, n = 2, r = 3$ one can easily describe a $\mathfrak{g}$-invariant in $D^r(\mathfrak{g}) = (\mathfrak{g}_n^{\otimes r})^{S_r}$ which is not a G-invariant. One can take the sum of the 3 S_3-conjugates of $(E_{11} + E_{22}) \otimes E_{12} \otimes E_{12}$, i.e. $(E_{11} + E_{22})E_{12}^{(2)}$.
4. Take $n = 2$. Let H be the group of diagonal matrices in G and let $\mathfrak{h}$ be its Lie algebra. It is easy to check that the nonzero H-weights in A_1 are also nonzero for $\mathfrak{h}$. So the H-action on $A_1^{\mathfrak{g}}$ is trivial. Of course the same holds for all G-conjugates of H. From the density of the semisimple elements in H it now follows that $A_1^{\mathfrak{g}} = A_1^G$. This argument was mentioned to me by S. Donkin. It is not difficult to show that $\dim(A_1^G) = \frac{3p^2-p}{2}$ and that $e_1 = \mathrm{tr}, e_2 = \det$ and $e_2^{(2)}$ generate A_1^G by reducing to the $\mathfrak{sl}_2$-case when $p > 2$.

2.3. **The restriction property.** Recall that there is a G-equivariant isomorphism $D_1 \cong A_1$ of graded algebras.

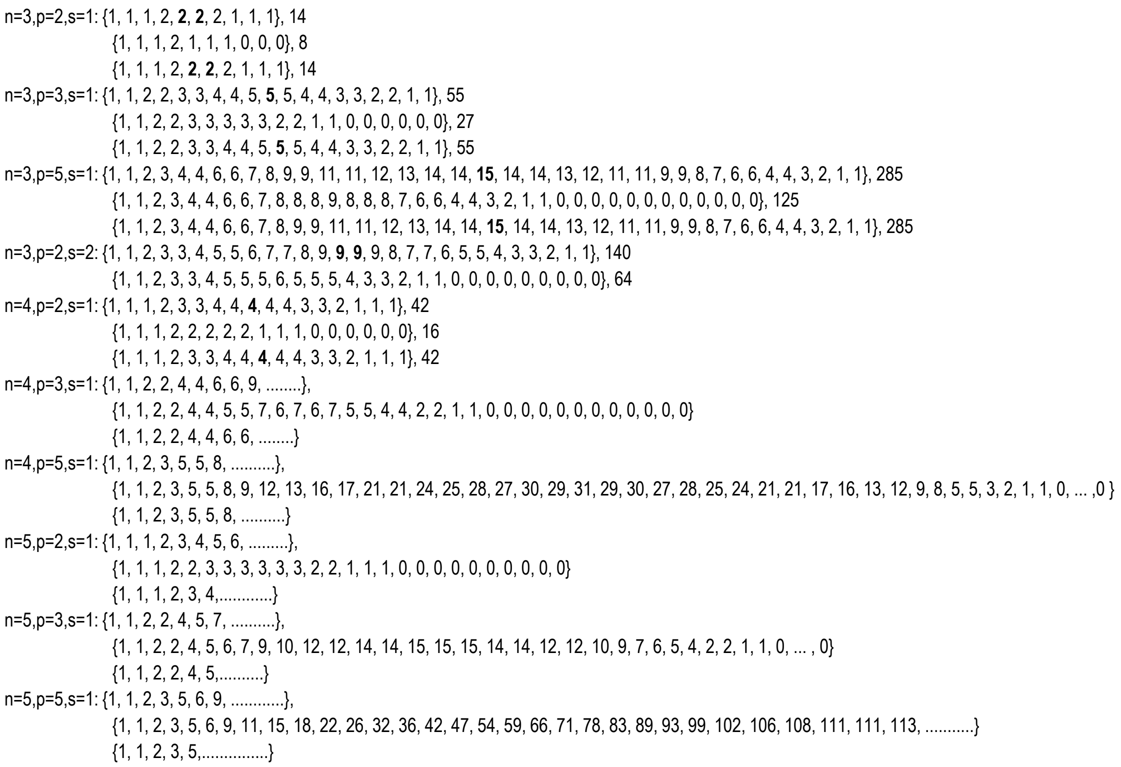
Conjecture 2.1. *The algebras $({}_nA_1)_{n \geq 1}$ have the infinitesimal restriction property.*

If this conjecture holds, then $A_1^{\mathfrak{g}} = A_1^G$ by Proposition 2.1 and the monomials $\prod_{i=1}^n e_i^{(m_i)}$, $m_1 < p$, span $A_1^{\mathfrak{g}}$ by Corollary 1 to Theorem 2.2. The point is that the restriction property allows us to reduce to the situation that n is $\geq$ the degree r. Conversely, if these monomials span $A_1^{\mathfrak{g}}$, then $A_1^{\mathfrak{g}} = A_1^G$ and the algebras $({}_nA_1)_{n \geq 1}$ have the infinitesimal restriction property. Note that by Remark 1.2.3 $A_1^{\mathfrak{g}} = A_1^G$ implies that the centre $U^{[p]}(\mathfrak{g})^{\mathfrak{g}}$ of $U^{[p]}(\mathfrak{g})$ is contained in the centre $\mathrm{Dist}(G)^G$ of $\mathrm{Dist}(G)$, see [8, Lem 6.5].

Remarks 2.3. 1. We consider the surjectivity of the map $({}_NA_1)^{\mathrm{GL}_N} \to ({}_nA_1)^{\mathrm{GL}_n}$, $N > n$. By Remark 2.2.4 it is surjective for $n = 2$, since the generators there lift to any $({}_NA_1)^{\mathrm{GL}_N}$. I also checked that it is surjective for $n = 3$ and $p = 2, 3, 5$, $n = 4$ and $p = 2$, 3 (up to degree 8), $n = 5$ and $p = 2$ (up to degree 7), $p = 3$ (up to degree 6). This was done by checking in each of these cases that the monomials from Corollary 1 to Theorem 2.2, span $({}_nA_1^r)^{\mathrm{GL}_n} = ({}_nD_1^r)^{\mathrm{GL}_n}$.
2. We consider the conjecture $A_1^{\mathfrak{g}} = A_1^G$. By Remark 2.2.4 it holds for $n = 2$. I checked it with the computer for $n = 3$ and $p = 2, 3, 5$, $n = 4$ and $p = 2$, 3 (up to degree 7) and 5 (up to degree 6), $n = 5$ and $p = 2$ (up to degree 5), 3 (up to degree 5).
3. The algebras $({}_nA_s)_{n\geq 1}$, $s \geq 2$, don't have the group or Lie algebra restriction property. I checked this for the restriction ${}_3A_2^{10} \to {}_2A_2^{10}$ when $p = 2$: $({}_2A_2^{10})^{\mathrm{GL}_2}$ is spanned by $x_{11}^2x_{12}^3x_{21}^3x_{22}^2 + x_{11}^3x_{12}^2x_{21}^2x_{22}^3$ and $x_{11}^3x_{12}^3x_{21}^3x_{22} + x_{11}^2x_{12}^3x_{21}^3x_{22}^2 + x_{11}x_{12}^3x_{21}^3x_{22}^3$, but the image in ${}_2A_2$ of $({}_3A_2^{10})^{\mathfrak{b}_3}$, $\mathfrak{b}_3$ the upper triangular matrices in $\mathfrak{gl}_3$, is spanned by the first element.
4. The algebras $({}_nD_s)_{n\geq 1}$, $s \geq 2$, and $({}_nD)_{n\geq 1}$ don't have the group or Lie algebra restriction property. By Proposition 2.1 and Theorem 2.2(i) it is enough to check that the dimension of the span of the sums of the divided p_λ's is $< \dim({}_nD_s^r)^G$. First we consider the case $n = 2$. For $r = 5$, $p = 2$ I got $1 < 2$ for $s = 2$ and $2 < 3$ for $s \geq 3$, for $r = 8$, $p = 3$ I got $4 < 5$ for $s \geq 2$, and for $r = 14$, $p = 5$ I got $7 < 8$ for $s \geq 2$. In the case $n = 3$, $r = 6$, $p = 2$ I got $4 < 5$ for $s = 2$ and $6 < 7$ for $s \geq 3$.

2.4. **Dimensions of some of the A_s^r.** We give some dimensions that we calculated using a computer program. For $n = 2$ the dimensions of the A_s^r were always given as the coefficients of the polynomial $\frac{1-T^{p^s}}{1-T} \times \frac{1-T^{3(p^s-1)+2}}{1-T^2} \in \mathbb{Z}[T]$ which we calculate as $\frac{1-T^{p^s}}{1-T^2} \times \frac{1-T^{3(p^s-1)+2}}{1-T}$ for $p = 2$. The total dimension was always $p^{2s} + \frac{p^s(p^s-1)}{2}$. We checked the cases $s = 2, p = 2, 3, 5$ and $s = 3, p = 2$. For the case $s = 1$, see Remark 2.2.4.

In the table below we give dimensions for $n \geq 3$. Let $\overline{A^G}$ denote the image of A^G in A_s. The first row gives the dimensions of the $(A_s^r)^G$, the second row gives the dimensions of the graded pieces of $\overline{A^G}$, and the third row, if it exists, gives the dimensions of the $(A_s^r)^{\mathfrak{g}}$. If the dimensions can be computed in all degrees, then the single number to the right gives the total dimension.



n=3,p=2,s=1: {1, 1, 1, 2, **2**, **2**, 2, 1, 1, 1}, 14

{1, 1, 1, 2, 1, 1, 1, 0, 0, 0}, 8

{1, 1, 1, 2, **2**, **2**, 2, 1, 1, 1}, 14

n=3,p=3,s=1: {1, 1, 2, 2, 3, 3, 4, 4, 5, **5**, 5, 4, 4, 3, 3, 2, 2, 1, 1}, 55

{1, 1, 2, 2, 3, 3, 3, 3, 3, 2, 2, 1, 1, 0, 0, 0, 0, 0, 0}, 27

{1, 1, 2, 2, 3, 3, 4, 4, 5, **5**, 5, 4, 4, 3, 3, 2, 2, 1, 1}, 55

n=3,p=5,s=1: {1, 1, 2, 3, 4, 4, 6, 6, 7, 8, 9, 9, 11, 11, 12, 13, 14, 14, **15**, 14, 14, 13, 12, 11, 11, 9, 9, 8, 7, 6, 6, 4, 4, 3, 2, 1, 1}, 285

{1, 1, 2, 3, 4, 4, 6, 6, 7, 8, 8, 8, 9, 8, 8, 8, 7, 6, 6, 4, 4, 3, 2, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}, 125

{1, 1, 2, 3, 4, 4, 6, 6, 7, 8, 9, 9, 11, 11, 12, 13, 14, 14, **15**, 14, 14, 13, 12, 11, 11, 9, 9, 8, 7, 6, 6, 4, 4, 3, 2, 1, 1}, 285

n=3,p=2,s=2: {1, 1, 2, 3, 3, 4, 5, 5, 6, 7, 7, 8, 9, **9**, **9**, 9, 8, 7, 7, 6, 5, 5, 4, 3, 3, 2, 1, 1}, 140

{1, 1, 2, 3, 3, 4, 5, 5, 5, 6, 5, 5, 5, 4, 3, 3, 2, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0}, 64

n=4,p=2,s=1: {1, 1, 1, 2, 3, 3, 4, 4, **4**, 4, 4, 3, 3, 2, 1, 1, 1}, 42

{1, 1, 1, 2, 2, 2, 2, 2, 1, 1, 1, 0, 0, 0, 0, 0, 0}, 16

{1, 1, 1, 2, 3, 3, 4, 4, **4**, 4, 4, 3, 3, 2, 1, 1, 1}, 42

n=4,p=3,s=1: {1, 1, 2, 2, 4, 4, 6, 6, 9, ...},

{1, 1, 2, 2, 4, 4, 5, 5, 7, 6, 7, 6, 7, 5, 5, 4, 4, 2, 2, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}

{1, 1, 2, 2, 4, 4, 6, 6, ...}

n=4,p=5,s=1: {1, 1, 2, 3, 5, 5, 8, ...},

{1, 1, 2, 3, 5, 5, 8, 9, 12, 13, 16, 17, 21, 21, 24, 25, 28, 27, 30, 29, 31, 29, 30, 27, 28, 25, 24, 21, 21, 17, 16, 13, 12, 9, 8, 5, 5, 3, 2, 1, 1, 0, ... ,0 }

{1, 1, 2, 3, 5, 5, 8, ...}

n=5,p=2,s=1: {1, 1, 1, 2, 3, 4, 5, 6, ...},

{1, 1, 1, 2, 2, 3, 3, 3, 3, 3, 3, 2, 2, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}

{1, 1, 1, 2, 3, 4,............}

n=5,p=3,s=1: {1, 1, 2, 2, 4, 5, 7, ...},

{1, 1, 2, 2, 4, 5, 6, 7, 9, 10, 12, 12, 14, 14, 15, 15, 15, 14, 14, 12, 12, 10, 9, 7, 6, 5, 4, 2, 2, 1, 1, 0, ... , 0}

{1, 1, 2, 2, 4, 5,..........}

n=5,p=5,s=1: {1, 1, 2, 3, 5, 6, 9, ...},

{1, 1, 2, 3, 5, 6, 9, 11, 15, 18, 22, 26, 32, 36, 42, 47, 54, 59, 66, 71, 78, 83, 89, 93, 99, 102, 106, 108, 111, 111, 113, ...}

{1, 1, 2, 3, 5,...............}

Dimensions of the invariants in some of the A^r_s

3. Several matrices

In this section we study the invariants in the algebras $D_s((\mathfrak{g}^{\oplus m})^*)$.

3.1. **Conjugacy classes for the conjugation action of S_α on S_r.** We recall some notation and results from [5] about conjugacy classes of a Young subgroup in S_r. For a finite sequence $\underline{i} = (i_1, \dots, i_t)$ of elements of $\{1, \dots, m\}$ we define $\text{Content}(\underline{i})$ to be the m-tuple whose j-th component is the number of occurrences of j in $\underline{i}$. We say that sequences $\underline{i}$ and $\underline{j}$ as above are equivalent if one is a cyclic shift of the other, we denote the equivalence class of $\underline{i}$ by $[\underline{i}]$ and we put $|[\underline{i}]| = t$. We will call these equivalence classes *cycle patterns*. Clearly, equivalent sequences have the same content, so the content function is also defined on cycle patterns. For $l \geq 1$ we define the l-th power of $\underline{i}$ by

$$[\underline{i}]^l = [\underbrace{i_1, \dots, i_t, \dots, i_1, \dots, i_t}_{l \text{ copies of } \underline{i}}] \, .$$

We call a cycle pattern *primitive* if it is not the l-th power of another cycle pattern for some $l \geq 2$ and we denote the set of primitive cycle patterns by Φ. Let $\mathcal{P}$ be the set of partitions. For $\lambda = (\lambda_1, \lambda_2, \dots) \in \mathcal{P}$ we put $|\lambda| = \sum_{i \geq 1} \lambda_i$ and we denote the length of λ, i.e. the number of nonzero parts of λ, by $l(\lambda)$.

For a function $\boldsymbol{\lambda}:\Phi\to\mathcal{P}$ such that all but finitely many values are the empty partition we define the *content* of $\boldsymbol{\lambda}$ to be $\sum_{b\in\Phi}|\boldsymbol{\lambda}(b)|\mathrm{Content}(b)$ and we denote the set of such functions with content α by Θ_α.

Now fix a composition $\alpha=(\alpha_1,\dots,\alpha_m)$ of r. For $i\in\{1,\dots,m\}$ put $\Delta_i=\{j\in\mathbb{Z}\,|\,\sum_{l=1}^{i-1}\alpha_l<j\le\sum_{l=1}^{i}\alpha_l\}$. Define $\zeta:\{1,\dots,r\}\to\{1,\dots,m\}$ by $\zeta(j)=i$ when $j\in\Delta_i$. Let S_α be the simultaneous stabiliser of the Δ_i in S_r. Note that $S_\alpha\cong S_{\alpha_1}\times\cdots\times S_{\alpha_m}$. For a cycle $\sigma=(i_1,\dots,i_t)\in S_r$ we put $[\sigma]=[\zeta(i_1),\dots,\zeta(i_t)]$. We can associate to every π with disjoint cycle decomposition $\pi=\prod_{j\in J}\sigma_j$ the multiset of cycle patterns $\langle[\sigma_j]\,|\,j\in J\rangle$. This multiset is equal to $\langle b^{\boldsymbol{\lambda}(b)_i}\,|\,b\in\Phi,1\le i\le l(\boldsymbol{\lambda}(b))\rangle$ for a unique $\boldsymbol{\lambda}\in\Theta_\alpha$ which we call the S_α *cycle type* of π. Clearly, $\pi,\pi'\in S_r$ are S_α-conjugate if and only if they have the same S_α cycle type.

3.2. **Partial polarisation.** Let α, r, the Δ_i, S_α and ζ be as in the previous section and let V be a vector space over k. The algebra $S(V^{\oplus m})=S(V)^{\otimes m}$ is $\mathbb{Z}^m$-graded and we denote the piece of degree α by $S^\alpha(V^{\oplus m})$. We apply analogous notation to the algebras $S((V^{\oplus m})^*)$, $D(V^{\oplus m})$ and $D_s(V^{\oplus m})$. Note that $S^\alpha(V^{\oplus m})\cong S^{\alpha_1}(V)\otimes\cdots\otimes S^{\alpha_m}(V)$, so $S^\alpha(V^{\oplus m})^*$ can be regarded as the r-linear functions $V^{\oplus r}\to k$ which are symmetric in each of the sets of positions Δ_i, i.e. which are S_α-invariants. For an integer $t\ge0$ let $\underline{1}_t$ denotes the all-one vector of length t. The partial polarisation map $P_\alpha:S^\alpha((V^{\oplus m})^*)\to S^\alpha(V^{\oplus m})^*$ sends $f\in S^\alpha((V^{\oplus m})^*)$ to the multi-homogeneous component of degree $(\underline{1}_{\alpha_1},\dots,\underline{1}_{\alpha_m})$ of the r-variable polynomial function

$$(v_1^1,\dots,v_{\alpha_1}^1,\dots,v_1^m,\dots,v_{\alpha_m}^m)\mapsto f(v_1^1+\cdots+v_{\alpha_1}^1,\dots,v_1^m+\cdots+v_{\alpha_m}^m)\,.$$

If $F:V^{\oplus r}\to k$ is r-linear and $f=((v_1,\dots,v_m)\mapsto F(v_{\zeta(1)},\dots,v_{\zeta(r)}))$, then

$$P_\alpha(f)=((v_1,\dots,v_r)\mapsto\sum_{\sigma\in S_\alpha}F(v_{\sigma(1)},\dots,v_{\sigma(r)}))\,.$$

As in Section 1.4 we obtain isomorphisms $D^\alpha((V^{\oplus m})^*)\cong S^\alpha(V^{\oplus m})^*$. Under these isomorphisms $D_s^\alpha((V^{\oplus m})^*)$ can be regarded as the r-linear functions $V^{\oplus r}\to k$ which are symmetric in each of the sets of positions Δ_i and which vanish when the arguments in p^s positions within a Δ_i are the same. Furthermore, these isomorphisms are compatible with the isomorphism $D((V^{\oplus m})^*)\cong S(V^{\oplus m})^{*\mathrm{gr}}$ from Section 1.4.

3.3. **Invariants in the algebra $D((\mathfrak{g}^{\oplus m})^*)$.** We keep the notation of Section 3.1. For $f\in k[\mathfrak{g}]^G$ and $b=[i_1,\dots,i_t]$ a cycle pattern define $f_b\in k[\mathfrak{g}^{\oplus m}]^G$ by

$$f_b(x_1,\dots,x_m)=f(x_{i_1}\cdots x_{i_t})\,.$$

For $\boldsymbol{\lambda}\in\Theta_\alpha$ define $p_{\boldsymbol{\lambda}}=\prod_{b\in\Phi}p_{\boldsymbol{\lambda}(b),b}$, $e_{\boldsymbol{\lambda}}=\prod_{b\in\Phi}e_{\boldsymbol{\lambda}(b),b}$ and $h_{\boldsymbol{\lambda}}=\prod_{b\in\Phi}h_{\boldsymbol{\lambda}(b),b}$. Furthermore define $u_{\boldsymbol{\lambda}}=\prod_{b\in\Phi}u_{\lambda(b)}$ and $z_{\boldsymbol{\lambda}}=\prod_{b\in\Phi}z_{\lambda(b)}$, and call $\frac{1}{z_{\boldsymbol{\lambda}}}p_{\boldsymbol{\lambda}}$, $\frac{1}{u_{\boldsymbol{\lambda}}}h_{\boldsymbol{\lambda}}$, $\frac{1}{u_{\boldsymbol{\lambda}}}e_{\boldsymbol{\lambda}}\in S((\mathfrak{g}_{\mathbb{Q}}^{\oplus m})^*)$ *divided* $p_{\boldsymbol{\lambda}}$, $h_{\boldsymbol{\lambda}}$ and $e_{\boldsymbol{\lambda}}$. As shown in [5] $z_{\boldsymbol{\lambda}}$ is the order of the centraliser in S_α of an element in S_r of S_α cycle type λ. Clearly, the divided $h_{\boldsymbol{\lambda}}$ and $e_{\boldsymbol{\lambda}}$ can be considered as elements of $D^\alpha((\mathfrak{g}^{\oplus m})^*)^G$ by reduction mod p. We will now show that the same holds for the divided $p_{\boldsymbol{\lambda}}$ and that, for $n\ge r$, they form three bases of $D^\alpha((\mathfrak{g}^{\oplus m})^*)^G$. First we note that for $b\in\Phi$ the map $f\mapsto f_b$

can be defined over $\mathbb{Q}$ and then it maps divided power $\mathbb{Z}$-form into divided power $\mathbb{Z}$-form. So for each $b \in \Phi$, the three families $(\frac{1}{u_\lambda} h_{\lambda,b})_{\lambda\in\mathcal{P}}$, $(\frac{1}{u_\lambda} e_{\lambda,b})_{\lambda\in\mathcal{P}}$ and $(\frac{1}{z_\lambda} p_{\lambda,b})_{\lambda\in\mathcal{P}}$ have the same $\mathbb{Z}$-span in $S((\mathfrak{g}_{\mathbb{Q}}^{\oplus m})^*)$. But then the same holds for the three families $(\frac{1}{u_{\boldsymbol\lambda}} h_{\boldsymbol\lambda})_{\boldsymbol\lambda\in\Theta_\alpha}$, $(\frac{1}{u_{\boldsymbol\lambda}} e_{\boldsymbol\lambda})_{\boldsymbol\lambda\in\Theta_\alpha}$ and $(\frac{1}{z_{\boldsymbol\lambda}} p_{\boldsymbol\lambda})_{\boldsymbol\lambda\in\Theta_\alpha}$. In particular, $\frac{1}{z_{\boldsymbol\lambda}} p_{\boldsymbol\lambda}$ belongs to $D((\mathfrak{g}_{\mathbb{Z}}^{\oplus m})^*)$.

Now let $\pi \in S_r$ be of S_α cycle type $\boldsymbol\lambda$. Then it is easy to see that $p_{\boldsymbol\lambda} = ((X_1, \cdots, X_m) \mapsto f_\pi(X_{\zeta(1)}, \ldots, X_{\zeta(r)}))$, f_π as in Section 1.5. So as an element of $S^\alpha(\mathfrak{g}_{\mathbb{Q}}^{\oplus m})^*$, via the partial polarisation map P_α, it is

$$((X_1, \cdots, X_r) \mapsto \sum_{\sigma\in S_\alpha} f_\pi(X_{\sigma(1)}, \ldots, X_{\sigma(r)})) = \sum_{\sigma\in S_\alpha} f_{\sigma\pi\sigma^{-1}}\,.$$

So under the S_r-equivariant isomorphism $\pi \mapsto f_\pi : kS_r \to ((\mathfrak{g}^{\otimes r})^*)^G$ the sum of the conjugacy class $[\pi]_{S_\alpha}$ corresponds to divided $p_{\boldsymbol\lambda}$. So the divided $p_{\boldsymbol\lambda}$, $\boldsymbol\lambda \in \Theta_\alpha$, form a basis of $D^\alpha((\mathfrak{g}^{\oplus m})^*)^G = ((\mathfrak{g}^{\otimes r})^*)^{G\times S_\alpha}$, and the same must then hold for the other two families.

3.4. **Invariants in the algebras $D_s((\mathfrak{g}^{\oplus m})^*)$.** We keep the notation of Section 3.1. Call $\boldsymbol\lambda \in \Theta_\alpha$ *s-reduced* if $\boldsymbol\lambda([j])$ has $< p^s$ ones for all $j \in \{1, \ldots, m\}$. To $\boldsymbol\lambda \in \Theta_\alpha$ we can associate its *s-reduced form* by repeatedly replacing p^s occurrences of 1 in a $\boldsymbol\lambda([j])$ by p^{s-1} occurrences of p. We will call two elements of Θ_α *s-equivalent* if they have the same s-reduced form. Call two elements of the symmetric group S_r *(s,α)-equivalent* if their S_α cycle types are s-equivalent.

As in Section 2 we can now show that the sums of the E_π over the (s,α)-equivalence classes belong to $D_s(\mathfrak{g}^{\oplus m})^G$, and when $n \geq r$ they form a basis of $D_s^\alpha(\mathfrak{g}^{\oplus m})^G$. We only need the lemma in the proof of Theorem 2.1 for sets Λ that are contained in one of the Δ_i. The proof of the theorem below is completely analogous to that of Theorem 2.2 and we leave this to the reader as well.

Theorem 3.1.

(i) *The sums of the divided $p_{\boldsymbol\lambda}$'s over the s-equivalence classes in Θ_α belong to $D_s^\alpha((\mathfrak{g}^{\oplus m})^*)^G$, and when $n \geq r$ they form a basis of $D_s^\alpha((\mathfrak{g}^{\oplus m})^*)^G$.*

(ii) *The divided $h_{\boldsymbol\lambda}$'s and the divided $e_{\boldsymbol\lambda}$'s, both with $\boldsymbol\lambda \in \Theta_\alpha$ such that $\boldsymbol\lambda([j])$ has $< p^s$ ones for all $j \in \{1, \ldots, m\}$, belong to $D_s^\alpha((\mathfrak{g}^{\oplus m})^*)^G$, and when $n \geq r$ they form two bases of $D_s^\alpha((\mathfrak{g}^{\oplus m})^*)^G$.*

Corollary 1. *The monomials $\prod_{1\leq i\leq n, b\in\Phi} e_{i,b}^{(m_{i,b})}$, $m_{1,[j]} < p^s$ for $j \in \{1, \ldots, m\}$, belong to $D_s^r((\mathfrak{g}^{\oplus m})^*)^G$. Furthermore, for $r \leq n$, those with $\sum_{1\leq i\leq n, b\in\Phi} m_{i,b}|b| = r$ form a basis of $D_s^r((\mathfrak{g}^{\oplus m})^*)^G$.*

Proof. Given that $D_s^r((\mathfrak{g}^{\oplus m})^*)$ is the direct sum of the $D_s^\alpha((\mathfrak{g}^{\oplus m})^*)$, $\alpha \in \mathbb{Z}^m$ a composition of r, this is just a reformulation of the statement about the e_λ's in Theorem 3.1. □

Proposition 3.1. *Assume $r \leq n$. Then $D_s^r((\mathfrak{g}^{\oplus m})^*)^{\mathfrak{g}} = D_s^r((\mathfrak{g}^{\oplus m})^*)^G$.*

Proof. For α a composition of r we have $D_s^\alpha((\mathfrak{g}^{\oplus m})^*)$ is a G-submodule of $(\mathfrak{g}^{\otimes r})^*$, so this follows as in the proof of Proposition 2.1. □

Corollary 2.

$$\varprojlim_n D_s((\mathfrak{gl}_n^{\oplus m})^*)^{\mathfrak{gl}_n} = \varprojlim_n D_s((\mathfrak{gl}_n^{\oplus m})^*)^{\mathrm{GL}_n} = D_s((e_{1,[j]})_{1\le j\le m}) \otimes D((e_{i,b})_{i\,or\,|b|\ge 2}),$$

where $D((e_{i,b})_{i\,or\,|b|\ge 2})$ is graded such that $e_{i,b}^{(t)}$ has degree $ti|b|$, and the limit is in the category of graded k-algebras.

Proof. This follows from Proposition 3.1 and Corollary 1 to Theorem 3.1. □

4. Vectors and covectors

Let $V = V_n = k^n$ be the natural module for G, let $m_1, m_2 \ge 0$ be integers and put $W = W_n = V^{\oplus m_1} \oplus (V^*)^{\oplus m_2}$. In this section we study the invariants in the algebras $D_s(W^*)$. For $i \in \{1, \dots, m_1\}$ and $j \in \{1, \dots, m_2\}$ let $x_i : W \to V$ and $y_j : W \to V^*$ be the i-th vector component and j-th covector component function and $\langle x_i, y_j\rangle = ((v, w) \mapsto w_j(v_i)) \in k[W]^G$ be the bracket function. By Section 1.4 these bracket functions can also be considered as elements of $D(W^*)^G$. The algebra $S(W)$ is $\mathbb{Z}^m \times \mathbb{Z}^m$-graded and $\mathbb{Z} \times \mathbb{Z}$-graded and we denote the piece of multidegree (α^1, α^2) by $S^{\alpha^1,\alpha^2}(W)$ and the piece of bidegree (r_1, r_2) by $S^{r_1,r_2}(W)$. We apply analogous notation to the algebras $S(W^*)$, $D(W^*)$ and $D_s(W^*)$.

Let $r_1, r_2 \ge 0$ be integers and let $\alpha^1 = (\alpha^1_1, \dots, \alpha^1_{m_1})$ and $\alpha^2 = (\alpha^2_1, \dots, \alpha^2_{m_2})$ be compositions of r_1 and r_2. As in Section 3.1 we associate to these Δ^1_i, $i \in \{1, \dots, m_1\}$, Δ^2_j, $j \in \{1, \dots, m_2\}$, $\zeta_1 : \{1, \dots, r_1\} \to \{1, \dots, m_1\}$, $\zeta_2 : \{1, \dots, r_2\} \to \{1, \dots, m_2\}$, and $S_{\alpha^1}, S_{\alpha^2} \le S_r$. We have a partial polarisation map

$$P_{\alpha^1,\alpha^2} : S^{\alpha^1,\alpha^2}(W^*) \to S^{\alpha^1,\alpha^2}(W)^* = \Big(\big(V^{\otimes r_1} \otimes (V^*)^{\otimes r_2}\big)^*\Big)^{S_{\alpha^1}\times S_{\alpha^2}}.$$

If $F : V^{\oplus r_1} \oplus (V^*)^{\oplus r_2} \to k$ is multilinear and f equals

$$((v_1, \dots, v_{m_1}, w_1, \dots, w_{m_2}) \mapsto F(v_{\zeta_1(1)}, \dots, v_{\zeta_1(r_1)}, w_{\zeta_2(1)}, \dots, w_{\zeta_2(r_2)}))\,,$$

then $P_{\alpha^1,\alpha^2}(f)$ equals

$$\big((v_1, \dots, v_{r_1}, w_1, \dots, w_{r_2}) \mapsto \sum_{\sigma\in S_{\alpha^1}, \tau\in S_{\alpha^2}} F(v_{\sigma(1)}, \dots, v_{\sigma(r_1)}, w_{\tau(1)}, \dots, w_{\tau(r_2)})\big)\,.$$

As in Section 1.4 we obtain isomorphisms $D^{\alpha^1,\alpha^2}(W^*) \cong S^{\alpha^1,\alpha^2}(W)^*$. Under these isomorphisms $D_s^{\alpha^1,\alpha^2}(W^*)$ can be regarded as the multilinear functions $V^{\oplus r_1} \oplus (V^*)^{\oplus r_2} \to k$ which are symmetric in each of the sets of vector positions Δ^1_i and in each of the sets of covector positions Δ^2_i, and which vanish when the arguments in p^s positions within a Δ^ι_i, $\iota \in \{1, 2\}$, are the same. Furthermore, these isomorphisms are compatible with the isomorphism $D(W^*) \cong S(W)^{*\mathrm{gr}}$ from Section 1.4.

Assume now that α^1 and α^2 above are compositions of r. The group $S_r \times S_r$ acts on S_r via $(\sigma, \tau)\cdot\pi = \sigma\pi\tau^{-1}$. Each $S_{\alpha^1} \times S_{\alpha^2}$-orbit has a unique representant π such that π is increasing on each Δ^2_j and π^{-1} is increasing on each Δ^1_i. Let

$\pi \in S_r$. Put $\Delta^1_{ij} = \Delta^1_i \cap \pi(\Delta^2_j)$ and $m_{ij} = |\Delta^1_{ij}|$ for $1 \leq i \leq m_1, 1 \leq j \leq m_2$. Then

$$\alpha^1_i = \sum_{j=1}^{m_2} m_{ij} \text{ and } \alpha^2_j = \sum_{i=1}^{m_1} m_{ij}\,. \tag{3}$$

For $\sigma, \tau \in S_r$ we have $(\sigma, \tau) \in S_{\alpha^1} \times S_{\alpha^2}$ and $\sigma\pi\tau^{-1} = \pi$ if and only if $\sigma \in S_{\alpha^1} \cap \pi S_{\alpha^2}\pi^{-1}$ and $\tau = \pi^{-1}\sigma\pi$. So the $S_{\alpha^1} \times S_{\alpha^2}$-centraliser of π has size $|S_{\alpha^1} \cap \pi S_{\alpha^2}\pi^{-1}| = \prod_{1\leq i\leq m_1, 1\leq j\leq m_2} m_{ij}!$.

Conversely, if we are given integers $m_{i,j} \geq 0$, $1 \leq i \leq m_1, 1 \leq j \leq m_2$, which sum to r, then we can define α^1 and α^2 by (3) and we can define the Δ^1_i and Δ^2_j as before. We divide each Δ^1_i into m_2 consecutive intervals $\Delta^1_{i1}, \ldots, \Delta^1_{im_2}$ and we divide each Δ^2_j into m_1 consecutive intervals $\Delta^2_{1j}, \ldots, \Delta^2_{m_1 j}$ such that Δ^1_{ij} and Δ^2_{ij} have length m_{ij}. Now we define $\pi \in S_r$ by requiring that $\pi : \Delta^2_{ij} \to \Delta^1_{ij}$ is increasing. Then π is increasing on each Δ^2_j and π^{-1} is increasing on each Δ^1_i.

Proposition 4.1. *Let $r_1, r_2 \geq 0$ be integers.*

(i) *If $r_1 \neq r_2$, then $D^{r_1,r_2}(W^*) = 0$. If $r_1 = r_2 = r$, then the divided power monomials in the $\langle x_i, y_j\rangle$ of bidegree (r, r) belong to $D^{r,r}_1(W^*)^G$, and when $n \geq r$ they form a basis of $D^{r,r}(W^*)^G = D^{r,r}_1(W^*)^G$.*

(ii) *If $n \geq r_1, r_2$, then $D^{r_1,r_2}(W^*)^{\mathfrak{g}} = D^{r_1,r_2}(W^*)^G$.*

Proof. (i). By considering the action of the centre of G it follows that if $r_1 \neq r_2$, then $D^{r_1,r_2}(W^*)^G = 0$, so we assume now that $r_1 = r_2 = r$. By Lemma 1.1 the given monomials belong to $D^{r,r}_1(W^*)$. Denote the vector and covector component functions of $V^{\oplus r} \oplus (V^*)^{\oplus r}$ by $\overline{x}_i$ and $\overline{y}_i$, $i \in \{1, \ldots, r\}$. The function $f_\pi \in (\mathfrak{g}^{\otimes r})^*$ from Section 1.5 can also be seen as an element of $(V^{\otimes r} \otimes (V^*)^{\otimes r})^*$. Then we have $f_\pi = \prod_{i=1}^r \langle \overline{x}_{\pi(i)}, \overline{y}_i\rangle$ and we see that the map $\pi \mapsto f_\pi$ is $S_r \times S_r$-equivariant.

Let $m_{i,j} \geq 0$, $1 \leq i \leq m_1, 1 \leq j \leq m_2$, be integers which sum to r. Define α^1 and α^2 by (3) and then define Δ^1_i, Δ^2_j, ζ_1, ζ_2, S_{α^1}, S_{α^2} as in Section 3.2, and define π as before the proposition. It is easy to see that $\prod_{1\leq i\leq m_1, 1\leq j\leq m_2} \langle x_i, y_j\rangle^{m_{ij}} = \prod_{i=1}^r \langle x_{\zeta_1(\pi(i))}, y_{\zeta_2(i)}\rangle$. So as an element of $S^{r,r}(W_{\mathbb{Q}})^*$, via the partial polarisation map P_{α^1,α^2}, it is $\sum_{\sigma\in S_{\alpha^1}, \tau\in S_{\alpha^2}} \prod_{i=1}^r \langle \overline{x}_{\sigma(\pi(i))}, \overline{y}_{\tau(i)}\rangle = \sum_{\sigma\in S_{\alpha^1}, \tau\in S_{\alpha^2}} f_{\sigma\pi\tau^{-1}}$. So under the $S_r \times S_r$-equivariant isomorphism $\pi \mapsto f_\pi : kS_r \to \big((V^{\otimes r} \otimes (V^*)^{\otimes r})^*\big)^G$ the sum of the orbit $[\pi]_{S_{\alpha^1}\times S_{\alpha^2}}$ corresponds to $\prod_{1\leq i\leq m_1, 1\leq j\leq m_2} \langle x_i, y_j\rangle^{(m_{ij})}$. So these divided power monomials form a basis of $D^{r,r}(W^*)^G = \bigoplus_{\alpha^1,\alpha^2} D^{\alpha^1,\alpha^2}(W^*)^G$.

(ii). As $D^{\alpha^1,\alpha^2}(W)^* = \Big(\big(V^{\otimes r_1} \otimes (V^*)^{\otimes r_2}\big)^*\Big)^{S_{\alpha^1}\times S_{\alpha^2}}$, this follows from Lemma 2.1(ii). □

Note that we have a natural embedding $V_{n-1} \hookrightarrow V_n$ by adding a zero component in the n-th position, and a natural embedding $V^*_{n-1} \hookrightarrow V^*_n$ by extending a function $f \in V^*_{n-1}$ by sending the n-th standard basis vector to 0. This gives us a natural embedding $W_{n-1} \hookrightarrow W_n$, and we get restriction maps for the algebras

$(k[W_n])_{n\geq 1}$, $(D(W_n^*))_{n\geq 1}$ and $(D_s(W_n^*))_{n\geq 1}$. From the previous proposition we immediately obtain the following corollary, where we may omit the subscript s.

Corollary.

$$\varprojlim_n (D_s(W_n^*))^{\mathfrak{gl}_n} = \varprojlim_n (D_s(W_n^*))^{\mathrm{GL}_n} = D(\langle x_i, y_j\rangle_{1\leq i\leq m_1, 1\leq j\leq m_2}),$$

where the grading is such that $\langle x_i, y_j\rangle^{(t)}$ has degree $2t$, and the limit is in the category of graded k-algebras.

Remarks 4.1. 1. It is immediate from classical invariant theory, see [4], that the algebras $(k[W_n])_{n\geq 1}$ have the restriction property.
2. Since $W_n \cong (V_n^{\oplus m_2} \oplus (V_n^*)^{\oplus m_1})^*$, we get restriction maps $W_n \to W_{n-1}$. From the description of $\bigwedge(W_n)^G$ in [1, Sect 5] it is clear that the algebras $\bigwedge(W_n)_{n\geq 1}$ have the restriction property. This implies that when $p = 2$, the algebras $(A_1(W_n))_{n\geq 1}$ have the restriction property.
3. For $p = 3$ the algebras $(D(W_n^*))_{n\geq 1}$ and $(D_s(W_n^*))_{n\geq 1}$ don't have the restriction property. I checked with the computer for $p = 3, n = 2, m_1 = 1, m_2 = 3$ that $\dim D_1^r(W_n^*) = 1, 0, 3, 0, 6, 0, 11, 0, 15$ for $r = 0, \ldots, 8$ and 0 for $r > 8$, and that the dimensions of the span of the invariants from Proposition 4.1 in degrees $= 0, \ldots, 8$ are $1, 0, 3, 0, 6, 0, 10, 0, 15$. In degree 6 the invariant $x_1x_2(x_1y_{21} - x_2y_{22})(y_{12}y_{31} - y_{11}y_{32})$ is outside this span, where y_{ji} denotes the i-th component of the j-th covector.
4. Similar to [1, Sect 5] one could try to determine the invariants in $A_1(W_n) = D_1(W_n^*)$ by using the isomorphism $A_1(W_n) \cong A_1((V_n^*)^{\oplus m}) \otimes \det^{m_1(1-p)}$, $m = m_1 + m_2$, of GL_n-modules, and then use the commuting GL_m-action. Let $U_n \leq \mathrm{GL}_n$ be the subgroup of upper uni-triangular matrices. Then we get $A_1(W_n)^{\mathrm{GL}_n} \cong A_1((V_n^*)^{\oplus m})^{U_n}_{m_1(p-1)\underline{1}_n}$, where $\underline{1}_n$ is the all-one vector of length n. Now one could hope that $A_1((V_n^*)^{\oplus m})^{U_n}_{(p-1)\nu} \cong \Delta_{\mathrm{GL}_m}((p-1)\nu^T)$, $\Delta_{\mathrm{GL}_m}(\mu)$ the Weyl module of highest weight μ and ν^T the transpose of ν, at least for ν a multiple of $\underline{1}_n$. Indeed the analogue for the exterior algebra holds by [2] or [1]. However, in the case $p = 3, n = 2, m_1 = 1, m_2 = 3$, $A_1((V_2^*)^{\oplus 4})^{U_2}_{(2,2)}$ is not even a quotient of some Weyl module. Indeed its socle and ascending radical series both have two layers: the first one is the irreducible $L_{\mathrm{GL}_4}(2,2,0,0)$ of dimension 19 and the second layer is $L_{\mathrm{GL}_4}(1,1,1,1) \oplus L_{\mathrm{GL}_4}(4,0,0,0)$ of dimension $1 + 16 = 17$. The Weyl module $\Delta_{\mathrm{GL}_4}(4,0,0,0)$ has dimension 35 and the two layers of its socle and ascending radical series are $L_{\mathrm{GL}_4}(2,2,0,0)$ and $L_{\mathrm{GL}_4}(4,0,0,0)$.

References

[1] A. M. Adamovich, G. L. Rybnikov, *Tilting modules for classical groups and Howe duality in positive characteristic*, Transform. Groups **1** (1996), no. 1-2, 1-34.

[2] K. Akin, D. A. Buchsbaum, J. Weyman, *Schur functors and Schur complexes*, Adv. in Math. **44** (1982), no. 3, 207-278.

[3] N. Bourbaki, *Algèbre*, Chaps. 1, 2 et 3, Hermann, Paris, 1970.

[4] C. De Concini, C. Procesi, *A characteristic free approach to invariant theory*, Advances in Math. **21** (1976), no. 3, 330-354.

[5] S. Donkin, *Invariant functions on matrices*, Math. Proc. Cambridge Philos. Soc. **113** (1993), no. 1, 23-43.

[6] E. M. Friedlander and B. J. Parshall, *Rational actions associated to the adjoint representation*, Ann. Sci. École Norm. Sup. (4) **20** (1987), no. 2, 215-226.

[7] J. A. Green, *Polynomial representations of* GL_n, Lecture Notes in Mathematics, **830**, Springer-Verlag, Berlin-New York, 1980.

[8] W. J. Haboush, *Central differential operators on split semisimple groups over fields of positive characteristic*, Séminaire d'Algèbre Paul Dubreil et Marie-Paule Malliavin, 32ème année (Paris, 1979), pp. 35-85, Lecture Notes in Math. **795**, Springer, Berlin, 1980.

[9] J. C. Jantzen, *Representations of algebraic groups*, Pure and Applied Math., vol. 131. Academic Press, Boston, 1987.

[10] I. G. Macdonald, *Symmetric functions and Hall polynomials*, Second edition, Oxford University Press, New York, 1995.

[11] A. Yu. Okounkov and G. I. Olshanskii, *Shifted Schur functions* (Russian), Algebra i Analiz **9** (1997), no.2, 73-146; translation in St. Petersburg Math. J. **9** (1998), no.2, 239-300.

[12] A. Premet, *Special transverse slices and their enveloping algebras*, Adv. Math. **170** (2002), no. 1, 1–55.

[13] A. A. Premet and R. H. Tange, *Zassenhaus varieties of general linear Lie algebras*, J. Algebra **294** (2005), no. 1, 177-195.

[14] S. Skryabin, *Invariants of finite group schemes*, J. London Math. Soc. (2) **65** (2002), no. 2, 339-360.

[15] R. Tange, *On the first restricted cohomology of a reductive Lie algebra and its Borel subalgebras*, Ann. Inst. Fourier (Grenoble) **69** (2019), no. 3, 1295-1308.

School of Mathematics, University of Leeds, LS2 9JT, Leeds, UK
Email address: `R.H.Tange@leeds.ac.uk`