Invariant Theory of Restricted Cartan Type Lie Algebras

PhD Thesis

Martin Mygind Jensen

Supervisor: Jens Carsten Jantzen

Department of Mathematics
Aarhus University
October 2015

Contents

Abstract

In this thesis we examine questions regarding group actions and invariants for a certain class of Lie algebras known as the *restricted Cartan types*. That these Lie algebras are *restricted* means that they are defined over a field of positive characteristic and possess a map with formal properties similar to those of the pth power map of an associative algebra. With some mild assumptions on the base field we determine orbit closures in the *Witt algebra* – the smallest of the Cartan types – and its dual space under the action of the automorphism group. Furthermore, we show that the symmetric algebra and universal enveloping algebra of *any* restricted Cartan type Lie algebra admit no nontrivial invariants under said action. Finally, we consider a version of Chevalley's Restriction Theorem for the restricted Cartan types, and prove that the restriction homomorphism is *not* an isomorphism whenever the torus involved is not generic.

Resumé

I denne afhandling undersøger vi spørgsmål vedrørende gruppevirkninger og invarianter for en bestemt klasse af Lie algebraer kendt som de *restringerede Lie algebraer af Cartan type*. At disse Lie algebraer er *restringerede* betyder at de er defineret over et legeme af positiv karakteristik og er udstyret med en afbildning med formelle egenskaber som minder om p'te potens afbildningen på en associativ algebra. Med milde betingelser på grundlegemet bestemmer vi banelukninger i *Witt algebraen* – den mindste af Cartan typerne – og dennes duale rum, under virkningen af automorfigruppen. Ydermere viser vi, at for en *vilkårlig* restringeret Lie algebra af Cartan type er der kun trivielle invarianter under samme gruppevirkning i den symmetriske algebra og den universelle indhyldningsalgebra. Endelig betragter vi en version af Chevalley's Restriction Theorem for de restringerede Cartan typer, og beviser at restringeringshomomorfien *ikke* er en isomorfi når den involverede torus ikke er generisk.

Introduction

It is safe to say that the theory of finite-dimensional complex semisimple Lie algebras, with its many beautiful theorems and all kinds of interesting applications, is by now a classical (but still evolving!) subject in mathematics. Such a position cannot exactly be claimed by the theory of Lie algebras over fields of *positive* characteristic. These Lie algebras are called *modular*, and their theory is younger, having been initiated by Jacobson in the 1930's, and less well developed. But even though the theory has spent its life outside the mathematical mainstream[1], there has still been made enormous progress, most notably seen in the full classification of finite-dimensional simple Lie algebras over an algebraically closed field of characteristic greater than three, which was recently completed by Strade and Premet. It is the combination of this solid foundation with the great number of natural questions yet to be answered (some of which are even quite easy to understand!) that is one of the most appealing features of the modular theory.

In this thesis we aim to further the understanding of an important class of finite-dimensional simple modular Lie algebras known as the *restricted Cartan types*. They are analogues of certain infinite-dimensional Lie algebras of complex vector fields studied by Cartan at the beginning of the previous century, and they often exhibit what could be considered 'pathological' behaviour, at least if one's definition of 'normal' is the complex semisimple case. We will study the invariant theory of the restricted Cartan types, or to be more precise, we will study certain group actions related to these Lie algebras, that are natural analogues of well known group actions from the semisimple complex world. The theorems we prove will, however, often be very different from their classical counterparts.

Before we get to work, let us briefly explain the structure of the thesis:

In Chapter 1 we introduce most of the required notation and terminology. Furthermore, we explain in detail the background for the questions to be studied. Topics include the notion of restrictedness, the KW1 conjecture and Veldkamp's Theorem.

In Chapter 2 we introduce the restricted Cartan types and determine orbit closures in the smallest of these – the *Witt algebra* – and its dual space, under the action of the automorphism group. Furthermore, we show that the symmetric algebra and the universal enveloping algebra of an arbitrary restricted Cartan type Lie algebra admit no non-trivial automorphism group invariants. Finally, we study semi-invariants, and prove that the center of the universal enveloping algebra of the

[1] One could perhaps consider the subtheory of Lie algebras of reductive algebraic groups defined over fields of positive characteristic *close* to mainstream.

Witt algebra is free over the so-called p-center. Most of the results of this chapter were published in the two papers [40], [41].

In Chapter 3 we consider an analogue of Chevalley's Restriction Theorem – a classical result in the complex semisimple theory – for the restricted Cartan types. We introduce the variety of tori of maximal dimension and the notion of *generic torus*, and we prove that the restriction homomorphism appearing in our version of Chevalley's Restriction Theorem *fails* to be an isomorphism whenever the torus considered is non-generic.

Chapter 1

Setting the Stage

1.1 Basic constructions and definitions

Let F denote any field. We start out by recalling three basic, but very important functors, while fixing some notation in the process (for more details, see [24] or [11]): Let V be a finite-dimensional vector space over F and denote by $T(V)$ the *tensor algebra* of V, defined as vector space by $T(V) = \bigoplus_{k=0}^{\infty} V^{\otimes k}$, and with multiplication given by concatenation of tensors. The tensor algebra is naturally a *graded* algebra, with the jth homogeneous piece $T(V)_j$ equal to $V^{\otimes j}$ for all $j \geq 0$. If $v_1, \ldots, v_j \in V$ we will often write $v_1 v_2 \cdots v_j$ for the element $v = v_1 \otimes v_2 \otimes \cdots \otimes v_j$ in $T(V)$ (and use similar notation for the image of v in any quotient of $T(V)$). Now we get the *symmetric algebra* of V by dividing out by the two-sided ideal of $T(V)$ generated by all $v \otimes w - w \otimes v$ with $v, w \in V$:

$$S(V) = T(V)/\langle v \otimes w - w \otimes v \mid v, w \in V \rangle.$$

The symmetric algebra is commutative and graded (being a quotient of $T(V)$ by a homogeneous ideal), and we write $S(V)_j$ for the jth homogeneous piece (we will use a similar notation for any graded algebra). Furthermore, $S(V)$ can be naturally identified, as we will often do, with the algebra $F[V^*]$ of polynomial functions on V^*. Any linear map $f : V \to W$ between vector spaces induces a graded homomorphism of algebras $S(f) : S(V) \to S(W)$ in an obvious way, so we can consider S as a functor between the category of F-vector spaces and the category of graded associative algebras over F.

Now let $\mathfrak{g}$ denote a finite-dimensional Lie algebra over F. The *universal enveloping algebra* $U(\mathfrak{g})$ of $\mathfrak{g}$ can be constructed by taking the tensor algebra $T(\mathfrak{g})$ and dividing out by the two-sided ideal generated by all $x \otimes y - y \otimes x - [x, y]$ with $x, y \in \mathfrak{g}$:

$$U(\mathfrak{g}) = T(\mathfrak{g})/\langle x \otimes y - y \otimes x - [x, y] \mid x, y \in \mathfrak{g} \rangle.$$

The universal enveloping algebra is a (generally noncommutative) noetherian domain with a standard filtration $\{U(\mathfrak{g})_{\leq k}\}_{k \in \mathbb{N}}$ given by:

$$U(\mathfrak{g})_{\leq k} = \mathrm{span}_F\{x_1 \cdots x_j \mid x_1, \ldots, x_j \in \mathfrak{g},\ j \leq k\}.$$

Any homomorphism of Lie algebras induces a filtered homomorphism of the corresponding universal enveloping algebras, so U is a functor from the category of Lie algebras to the category of filtered associative algebras. Furthermore, the category of modules over the Lie algebra $\mathfrak{g}$ is naturally equivalent to the category of modules over the algebra $U(\mathfrak{g})$, which is perhaps the main reason for our interest in the latter.

Finally, we define a functor Gr between the category of filtered associative algebras and the category of graded associative algebras in the following way: Consider an algebra A equipped with a filtration $\{A_{\leq k}\}_{k\in\mathbb{N}}$. The *associated graded algebra* $\mathrm{Gr}(A)$ of A is defined on vector space level as $\mathrm{Gr}(A) = \bigoplus_{k\in\mathbb{N}} A_{\leq k}/A_{\leq k-1}$, with $A_{\leq -1} = 0$ by definition. For $\tilde{a} \in A_{\leq i}/A_{\leq i-1}$, $\tilde{b} \in A_{\leq j}/A_{\leq j-1}$ we can define a product by first lifting $\tilde{a}, \tilde{b}$ to $a \in A_i$, $b \in A_j$ respectively, and then taking $\tilde{a}\tilde{b}$ to be the image of ab in $A_{\leq i+j}/A_{\leq i+j-1}$. One easily checks that this is well defined, and by expanding linearly we get a multiplication on $\mathrm{Gr}(A)$, making it into a graded algebra. Of course, if A is graded, then it is also canonically filtered, and we have $\mathrm{Gr}(A) \cong A$. For any $a \in A \setminus \{0\}$ we set $\deg(a) = \min\{j \in \mathbb{N} \mid a \in A_{\leq j}\}$ and define the *leading term map* $l : A \setminus \{0\} \to \mathrm{Gr}(A)$ (which is a priori only a map of sets) by letting $l(a)$ be the image of a in $A_{\leq \deg(a)}/A_{\leq \deg(a)-1} = \mathrm{Gr}(A)_{\deg(a)}$. The image of l is precisely the set of homogeneous elements of $\mathrm{Gr}(A)$. Note that we can apply the Gr-construction to any subspace (automatically filtered) V of A, in which case $\mathrm{Gr}(V)$ becomes a graded subspace of $\mathrm{Gr}(A)$. It is easy to show that if $V, W \subseteq A$ are subspaces such that $V \subseteq W$ and $\mathrm{Gr}(V) = \mathrm{Gr}(W)$, then $V = W$. This simple observation will prove extremely useful!

Returning to our Lie algebra $\mathfrak{g}$, we note that the image of $x_1 \otimes \cdots \otimes x_j \in T(\mathfrak{g})_j$ in $U(\mathfrak{g})$ is contained in $U(\mathfrak{g})_{\leq j}$, and thus we have a linear map $T(\mathfrak{g}) \to U(\mathfrak{g})_{\leq j}/U(\mathfrak{g})_{\leq j-1}$ which can be extended to an algebra homomorphism $\tilde{\psi} : T(\mathfrak{g}) \to \mathrm{Gr}(U(\mathfrak{g}))$. Since $\tilde{\psi}$ vanishes on the ideal defining $S(\mathfrak{g})$ we get an induced homomorphism $\psi : S(\mathfrak{g}) \to \mathrm{Gr}(U(\mathfrak{g}))$, which, by the PBW Theorem, is an isomorphism:

$$\mathrm{Gr}(U(\mathfrak{g})) \cong S(\mathfrak{g}).$$

So our three functors are related in the nicest possible way, and the universal enveloping algebra can be thought of as a *filtered deformation* of the symmetric algebra. The leading term map $l : U(\mathfrak{g}) \setminus \{0\} \to S(\mathfrak{g})$ is easily seen to be $\mathfrak{g}$-invariant, and also has a nice multiplicative property: $l(u_1u_2) = l(u_1)l(u_2)$ for all nonzero $u_1, u_2 \in U(\mathfrak{g})$. We are usually more interested in $U(\mathfrak{g})$ than in $S(\mathfrak{g})$ because of the former's closer relation to $\mathfrak{g}$ itself. However, the simpler structure of the symmetric algebra makes it a viable strategy in many situations to work in $S(\mathfrak{g})$ and then try to transfer the information to $U(\mathfrak{g})$. We will see plenty of examples of this later.

Now let M be any $\mathfrak{g}$-module. We have a natural homogeneous action of $\mathfrak{g}$ on $T(M)$ by derivations, given by

$$y.(m_1 \otimes \cdots \otimes m_j) = y.m_1 \otimes m_2 \otimes \cdots \otimes m_j + \cdots + m_1 \otimes \cdots \otimes m_{j-1} \otimes y.m_j$$

for $y \in \mathfrak{g}$, $m_1, \ldots, m_j \in M$. This action factors through the ideal defining $S(M)$, and thus $\mathfrak{g}$ also acts homogeneously by derivations on this algebra. If M is $\mathfrak{g}$ itself (with the adjoint action), then the action of $\mathfrak{g}$ on $T(\mathfrak{g})$ also factors through the ideal

defining $U(\mathfrak{g})$, and the resulting filtration preserving action turns out to be given ([11], 11.1) simply by

$$y.u = yu - uy$$

for $y \in \mathfrak{g}$, $u \in U(\mathfrak{g})$. In particular, the algebra of invariants $U(\mathfrak{g})^{\mathfrak{g}} = \{u \in U(\mathfrak{g}) \mid x.u = 0 \text{ for all } x \in \mathfrak{g}\}$ coincides with the center $Z(\mathfrak{g})$ of $U(\mathfrak{g})$.

If $M = \mathfrak{g}$ or $M = \mathfrak{g}^*$ (the cases we are primarily interested in) then M is also a rational module for the algebraic group $G = \mathrm{Aut}(\mathfrak{g})$ of Lie automorphisms of $\mathfrak{g}$, and we get an action of G on $T(M)$ by algebra automorphisms:

$$g.(m_1 \otimes \cdots \otimes m_j) = g(m_1) \otimes \cdots \otimes g(m_j)$$

for $g \in G$, $m_1, \ldots, m_j \in \mathfrak{g}$. Again we get induced actions on $S(\mathfrak{g})$, $S(\mathfrak{g}^*)$ and $U(\mathfrak{g})$, which are homogeneous in the first two cases, filtration preserving in the last. All this applies also if we start with an arbitrary algebraic F-group G and set $\mathfrak{g} = \mathrm{Lie}(G)$.[1]

A final notion, which will turn out to be very important, is that of *regular character*: For any $\chi \in \mathfrak{g}^*$ we let $\mathfrak{g}_\chi \subseteq \mathfrak{g}$ denote the stabiliser of χ in the coadjoint action:

$$\mathfrak{g}_\chi = \{x \in \mathfrak{g} \mid x.\chi = 0\} = \{x \in \mathfrak{g} \mid \chi([x, \mathfrak{g}]) = 0\}. \tag{1.1}$$

Note that $\mathfrak{g}_\chi$ is also the radical of the alternating bilinear form $(\cdot,\cdot)_\chi$ on $\mathfrak{g}$ defined by $(x, y)_\chi = \chi([x, y])$ for $x, y \in \mathfrak{g}$. The *index* of $\mathfrak{g}$ is the minimal dimension among all stabilisers:

$$\mathrm{ind}(\mathfrak{g}) = \min\{\dim(\mathfrak{g}_\chi) \mid \chi \in \mathfrak{g}^*\}.$$

Since $(\cdot,\cdot)_\chi$ induces a symplectic form on $\mathfrak{g}/\mathfrak{g}_\chi$ this vector space is even-dimensional for all χ. An element $\chi \in \mathfrak{g}^*$ with $\dim(\mathfrak{g}_\chi) = \mathrm{ind}(\mathfrak{g})$ is called *regular*, and we denote the set of regular characters $\mathfrak{g}^*_{\mathrm{reg}}$. This is a Zariski-open subset of $\mathfrak{g}^*$ by [16], 1.11.5.

We are interested in the invariants of the group and Lie algebra actions just described, along with some applications to representation theory, when F has positive characteristic and $\mathfrak{g}$ is *restricted* (to be defined). Let us first, however, recall the situation in characteristic zero, which will, particularly in the classical case where the Lie algebra is semisimple, serve as motivation and inspiration throughout:

1.2 Lie invariants in characteristic zero

Assume, unsurprisingly, that our ground field F has characteristic zero. Let furthermore $\{x_1, \ldots, x_n\}$ be an F-basis of $\mathfrak{g}$. We have a $\mathfrak{g}$-invariant isomorphism of vector spaces $\varphi : S(\mathfrak{g}) \to U(\mathfrak{g})$ given on basis monomials by

$$\varphi(x_{i_1} \cdots x_{i_k}) = \sum_{\sigma \in S_k} \frac{1}{k!} x_{i_{\sigma(1)}} \cdots x_{i_{\sigma(k)}} \tag{1.2}$$

for all k. Here S_k denotes the symmetric group on k letters, and the map is called the *symmetrization map*. Note that (1.2) only makes sense because of the restriction

[1] In this thesis we consider only the adjoint action of an algebraic group on its Lie algebra.

on the characteristic! While the symmetrization map is a very nice map (we miss it sorely in characteristic p!), which allows us to compare the $\mathfrak{g}$-module structure of $U(\mathfrak{g})$ and $S(\mathfrak{g})$, one could perhaps be bold and ask for an *even nicer* map. Namely, while $U(\mathfrak{g})$ and $S(\mathfrak{g})$ are clearly not isomorphic as algebras (one being commutative, the other generally noncommutative) it could still happen that the (commutative) invariant subalgebras $S(\mathfrak{g})^{\mathfrak{g}}$ and $Z(\mathfrak{g})$ were in fact isomorphic. It turns out that the symmetrization map *does not* induce an algebra isomorphism when restricted to $S(\mathfrak{g})^{\mathfrak{g}}$, *but* this can be remedied by twisting with a certain infinite order differential operator $J^{1/2}$ on $S(\mathfrak{g})$ (see [10], from where the notation is borrowed, or the original paper [17]). The resulting algebra isomorphism $\varphi \circ J^{1/2} : S(\mathfrak{g})^{\mathfrak{g}} \to Z(\mathfrak{g})$ is called the *Duflo isomorphism*. It should be mentioned that this is actually the degree zero part of a much more general theorem stating that the cohomology algebras $H^*(\mathfrak{g}, S(\mathfrak{g}))$ and $H^*(\mathfrak{g}, U(\mathfrak{g}))$ are graded isomorphic (see [10] for the full story).

Assume now furthermore that F is algebraically closed, and that $\mathfrak{g}$ is semisimple of rank r, with triangular decomposition $\mathfrak{g} = \mathfrak{n}_- \oplus \mathfrak{h} \oplus \mathfrak{n}_+$, group of inner automorphisms G, and Weyl group W. For any $\lambda \in \mathfrak{h}^*$, let $M(\lambda)$ denote the corresponding Verma module. The center of $U(\mathfrak{g})$ acts on $M(\lambda)$ by a central character $\chi_\lambda : Z(\mathfrak{g}) \to F$, and we define, for any $u \in Z(\mathfrak{g})$, a polynomial function $\Psi(u)$ on $\mathfrak{h}^*$ (that is, an element of $S(\mathfrak{h})$) by

$$\Psi(u)(\lambda) = \chi_{\lambda-\rho}(u),$$

where ρ is the half-sum of positive roots. It turns out that $\Psi(u)$ is W-invariant, and that we get an isomorphism of algebras

$$\Psi : Z(\mathfrak{g}) \xrightarrow{\sim} S(\mathfrak{h})^W$$

called the *twisted Harish-Chandra isomorphism* (where ρ obviously constitutes the 'twist'). In particular, the center is a polynomial algebra in $\dim(\mathfrak{h}) = r$ variables, by the Chevalley-Shephard-Todd Theorem.

Using the identifications $S(\mathfrak{g}^*) \cong F[\mathfrak{g}]$, $S(\mathfrak{h}^*) \cong F[\mathfrak{h}]$ we get a natural map $S(\mathfrak{g}^*) \to S(\mathfrak{h}^*)$ which is just restriction of polynomial functions. By *Chevalley's Restriction Theorem* this induces an isomorphism of algebras:

$$\mathrm{res} : S(\mathfrak{g}^*)^G \xrightarrow{\sim} S(\mathfrak{h}^*)^W.$$

Now the Killing form κ on $\mathfrak{g}$ gives us a G-module isomorphism $\mathfrak{g} \xrightarrow{\sim} \mathfrak{g}^*$, and similarly, the restriction of κ to $\mathfrak{h}$ induces a W-module isomorphism $\mathfrak{h} \xrightarrow{\sim} \mathfrak{h}^*$. These maps then yield isomorphisms of algebras $S(\mathfrak{g})^G \xrightarrow{\sim} S(\mathfrak{g}^*)^G$, $S(\mathfrak{h})^W \xrightarrow{\sim} S(\mathfrak{h}^*)^W$, and, composing with res, we finally get an algebra isomorphism

$$\tilde{\mathrm{res}} : S(\mathfrak{g})^G \xrightarrow{\sim} S(\mathfrak{h})^W$$

which, since we know that $S(\mathfrak{g})^G = S(\mathfrak{g})^{\mathfrak{g}}$, can be fitted into a diagram with our other two important isomorphisms, the Duflo map and the twisted Harish-Chandra map:

$$\begin{array}{ccc} S(\mathfrak{g})^{\mathfrak{g}} & \xrightarrow{\varphi \circ J^{1/2}} & Z(\mathfrak{g}) \\ & \searrow^{\tilde{\mathrm{res}}} & \downarrow \Psi \\ & & S(\mathfrak{h})^W. \end{array} \tag{1.3}$$

This diagram *commutes*, a fact which is not exactly trivial. Since it can be hard to track down a proof in the literature, we will sketch the idea here: The first thing one needs to know is that when F is algebraically closed (still of characteristic zero) and $\mathfrak{g}$ is *any* Lie algebra over F, it is possible to describe the inverse $(\varphi \circ J^{1/2})^{-1}$ of the Duflo map using representation theory (see [16], 10.4, and [17]): Start by taking any regular character $\lambda \in \mathfrak{g}^*_{\mathrm{reg}}$ and find a *solvable polarization* of λ, i.e., a solvable subalgebra $\mathfrak{p} \subseteq \mathfrak{g}$ such that $\lambda([\mathfrak{p},\mathfrak{p}]) = 0$ and $\dim(\mathfrak{p}) = \frac{1}{2}(\dim(\mathfrak{g}) + \dim(\mathfrak{g}_\lambda))$ (at least one such $\mathfrak{p}$ always exists when λ is regular). Now consider the twisted one-dimensional $\mathfrak{p}$-module $\tilde{F}_\lambda$ with action given by

$$x.1 = \lambda(x) + \tfrac{1}{2}\operatorname{tr}_{\mathfrak{g}/\mathfrak{p}}(\operatorname{ad} x)$$

for all $x \in \mathfrak{p}$. The last term is just half the trace of the linear operator on $\mathfrak{g}/\mathfrak{p}$ induced by $\operatorname{ad} x$. It turns out that it is always possible to find a solvable polarization such that the induced module $M_{\lambda,\mathfrak{p}} = \operatorname{ind}_{\mathfrak{p}}^{\mathfrak{g}} \tilde{F}_\lambda$ is *simple*. Furthermore, the primitive ideal $\operatorname{ann}(M_{\lambda,\mathfrak{p}})$ in $U(\mathfrak{g})$ is independent of $\mathfrak{p}$, so we can safely denote it by $I(\lambda)$. The intersection $I(\lambda) \cap Z(\mathfrak{g})$ is a maximal ideal of $Z(\mathfrak{g})$, i.e., it induces a central character $\psi_\lambda : Z(\mathfrak{g}) \to F$. For any $u \in Z(\mathfrak{g})$ we can now define a function $\tilde{\phi}(u) : \mathfrak{g}^*_{\mathrm{reg}} \to F$ by:

$$\tilde{\phi}(u)(\lambda) = \psi_\lambda(u).$$

Magically, it turns out that $\tilde{\phi}(u)$ can be uniquely extended to a polynomial function on $\mathfrak{g}^*$ which is *exactly* $(\varphi \circ J^{1/2})^{-1}(u)$!

By now, it should at least be clear*er* how to prove the commutativity of the diagram (1.3). First identify $\mathfrak{h}^*$ with the subset of $\mathfrak{g}^*$ consisting of characters λ satisfying $\lambda(\mathfrak{n}_- \oplus \mathfrak{n}_+) = 0$, then rẽs becomes the usual restriction of functions. For any nonzero $\lambda \in \mathfrak{h}^*$ the Borel subalgebra $\mathfrak{b} = \mathfrak{h} \oplus \mathfrak{n}_+$ is a solvable polarization of λ, and $\operatorname{ind}_{\mathfrak{b}}^{\mathfrak{g}} \tilde{F}_\lambda = M(\lambda - \rho)$ (with our two 'twists' $\frac{1}{2}\operatorname{tr}_{\mathfrak{g}/\mathfrak{p}}(\operatorname{ad} x)$ and ρ matching up). Thus we see, that for any $u \in Z(\mathfrak{g})$, the polynomial functions $(\tilde{\text{rẽs}} \circ (\varphi \circ J^{1/2})^{-1})(u)$ and $\Psi(u)$ coincide on the subset U of $\mathfrak{h}^*$ consisting of regular characters λ such that $M(\lambda - \rho)$ is simple. Luckily, U is nonempty and open in $\mathfrak{h}^*$, and we conclude that $(\tilde{\text{rẽs}} \circ (\varphi \circ J^{1/2})^{-1})(u) = \Psi(u)$ for all $u \in Z(\mathfrak{g})$.

So the natural question is how much of this carries over to the modular situation, to which the answer is: Not very much! First of all, there is *no* symmetrization map, and therefore *no* Duflo map.[2] Second, for a simple modular Lie algebra (the notion of 'semisimple' is not very workable in characteristic p) the Killing form is not necessarily nondegenerate, the Cartan subalgebras are not always conjugate under the action of the automorphism group and the representation theory is not nearly as well behaved, so pretty much everything breaks down! Nevertheless, we will see that in some cases it *is* possible to prove analogues of the characteristic zero results.

[2]In fact, Premet has provided an (unpublished) example to show that the algebras of $\mathfrak{g}$-invariants in $S(\mathfrak{g})$ and $U(\mathfrak{g})$ are not in general isomorphic in positive characteristic.

1.3 Restricted Lie algebras and representation theory

Assume now that our ground field F has characteristic $p > 0$. A *p-mapping* on $\mathfrak{g}$ is a map $.^{[p]} : \mathfrak{g} \to \mathfrak{g}$ satisfying

1. $(\operatorname{ad} x)^p = \operatorname{ad} x^{[p]}$ for all $x \in \mathfrak{g}$,
2. $(ax)^{[p]} = a^p x^{[p]}$ for all $a \in F$, $x \in \mathfrak{g}$,
3. $(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_i(x,y)$ for all $x, y \in \mathfrak{g}$,

where the $s_i(x,y) \in \mathfrak{g}$ are given by the expression

$$(\operatorname{ad}(x \otimes X + y \otimes 1))^{p-1}(x \otimes 1) = \sum_{i=1}^{p-1} i s_i(x,y) \otimes X^{i-1}$$

in $\mathfrak{g} \otimes F[X]$. While these properties, in particular the third one, might look weird at first, one should just think of the definition as extracting the essential properties of the operation of raising to the pth power in an associative algebra A over F (for a proof that $a \mapsto a^p$ does indeed define a p-mapping on A, see [26], V.7). The pair $(\mathfrak{g}, .^{[p]})$ is called a *restricted Lie algebra*, and a Lie homomorphism between restricted Lie algebras that respects the p-mappings is called a *restricted homomorphism*.

Why are the restricted Lie algebras important? Well, it turns out that many modular Lie algebras occurring 'in real life' have a natural p-mapping, typically induced from an embedding into an associative algebra. Examples include the Lie algebra of derivations $\operatorname{Der}(A)$ of an algebra A (for any derivation $D \in \operatorname{Der}(A)$, the associative pth power D^p taken in $\mathfrak{gl}(A)$ is again a derivation by Leibniz' formula) and the Lie algebra $\operatorname{Lie}(G)$ of any group scheme G over F (here the p-mapping is induced from the embedding of $\operatorname{Lie}(G)$ into the distribution algebra $\operatorname{Dist}(G)$, see [29], I.7.10). Furthermore, some of the tools of the theory of semisimple Lie algebras in characteristic zero – notably the unique decomposition of elements into semisimple and nilpotent parts – can be given meaningful analogues using the p-mapping. Finally, the theory in the nonrestricted case relies heavily on restricted theory through the use of so-called *p-envelopes* (see [58], 2.5).

From now on we will assume that our Lie algebra $\mathfrak{g}$ is restricted, and that the ground field F is algebraically closed. Denote by $\operatorname{Mod}(\mathfrak{g})$ the category of $\mathfrak{g}$-modules and by $\operatorname{Mod}_{<\infty}(\mathfrak{g})$ the full subcategory of finite-dimensional modules. There are several features of the study of $\operatorname{Mod}(\mathfrak{g})$ that sets it apart from characteristic zero theory. One is the fact that the simple $\mathfrak{g}$-modules are of *finite bounded dimension*. This actually holds for any finite-dimensional modular Lie algebra (see [30], A.4), and is a consequence of the fact that the center of $U(\mathfrak{g})$ is much larger in positive characteristic, as we will see shortly. Another defining feature is the use of *p-characters*: Let M be any $\mathfrak{g}$-module. We say that M has p-character $\chi \in \mathfrak{g}^*$ if

$$(x^p - x^{[p]})m = \chi(x)^p m$$

for all $x \in \mathfrak{g}, m \in M$, where the product x^p is taken in the universal enveloping algebra $U(\mathfrak{g})$. Let $\mathrm{Mod}(\mathfrak{g}, \chi)$ denote the full subcategory of $\mathrm{Mod}(\mathfrak{g})$ consisting of $\mathfrak{g}$-modules having p-character χ. Not every module admits a p-character, but the *simple* modules always do, i.e., if M is a simple $\mathfrak{g}$-module, then there exists $\chi \in \mathfrak{g}^*$ such that $M \in \mathrm{Mod}(\mathfrak{g}, \chi)$ (a fact which was apparently first observed in [61]). Furthermore, the category $\mathrm{Mod}(\mathfrak{g}, \chi)$ is equivalent to the module category of the *χ-reduced enveloping algebra* $U(\mathfrak{g}, \chi)$, defined by:

$$U(\mathfrak{g}, \chi) = U(\mathfrak{g})/\langle x^p - x^{[p]} - \chi(x)^p 1 \mid x \in \mathfrak{g} \rangle.$$

This algebra is finite-dimensional for any χ: if $\{x_1, \ldots, x_n\}$ is a basis of $\mathfrak{g}$, then $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid 0 \leq \alpha_1, \ldots, \alpha_n < p\}$ is a basis of $U(\mathfrak{g}, \chi)$. So one can often use methods from the well-developed representation theory of finite-dimensional associative algebras in the study of simple $\mathfrak{g}$-modules. It should, however, be noted that Weyl's theorem *always* fails in positive characteristic, i.e., $\mathrm{Mod}_{<\infty}(\mathfrak{g})$ is not semisimple for *any* nonzero $\mathfrak{g}$ (see [20] for a nice cohomological proof). In other words, even if we knew everything there is to know about the simple modules, we would still not have complete knowledge of $\mathrm{Mod}_{<\infty}(\mathfrak{g})$.

The category $\mathrm{Mod}(\mathfrak{g}, 0)$ has special significance, and we call a $\mathfrak{g}$-module M *restricted* if $M \in \mathrm{Mod}(\mathfrak{g}, 0)$. Accordingly, the algebra $U(\mathfrak{g}, 0)$ will be referred to as the *restricted universal enveloping algebra* of $\mathfrak{g}$. Note that the ideal $\langle x^p - x^{[p]} \mid x \in \mathfrak{g} \rangle \subseteq U(\mathfrak{g})$ defining $U(\mathfrak{g}, 0)$ is a Hopf ideal, so that $U(\mathfrak{g}, 0)$ becomes a finite-dimensional cocommutative Hopf algebra. Using the equivalence of categories

$$\begin{array}{c} \{\text{finite-dimensional cocommutative Hopf algebras}\} \\ \updownarrow \\ \{\text{finite group schemes}\} \end{array}$$

we associate to $\mathfrak{g}$ the finite group scheme G over F having coordinate algebra $F[G] = U(\mathfrak{g}, 0)^*$. The assignment $\mathfrak{g} \mapsto G$ induces an equivalence of categories

$$\begin{array}{c} \{\text{finite-dimensional restricted Lie algebras}\} \\ \updownarrow \\ \{\text{finite group schemes of height} \leq 1\} \end{array}$$

with inverse functor given by $G \mapsto \mathrm{Lie}(G)$ ([12], II, §7, 4.1). This geometric reformulation can be very useful, but it should be noted that it only captures the *restricted* part of the representation theory of $\mathfrak{g}$: the category of G-modules (i.e., comodules of the coordinate algebra) is equivalent to the category of restricted $\mathfrak{g}$-modules.

When $\chi \neq 0$ the reduced enveloping algebra $U(\mathfrak{g}, \chi)$ does not inherit the Hopf algebra structure of $U(\mathfrak{g})$, so we have to settle for the weaker structure ([48], Corollary 8.4.3) of *Frobenius algebra*. A nondegenerate associative bilinear form $\langle \cdot, \cdot \rangle$ on $U(\mathfrak{g}, \chi)$ can be defined by choosing a basis $\{x_1, \ldots, x_n\}$ of $\mathfrak{g}$ and taking $\langle u, v \rangle$ to be the coefficient of $x_1^{p-1} \cdots x_n^{p-1}$ in uv for all $u, v \in U(\mathfrak{g}, \chi)$.

1.4 The center $Z(\mathfrak{g})$ of the universal enveloping algebra and the KW1 conjecture

One of the principal goals of most representation theories is to classify the simple modules (if possible) and find their dimensions. In the case of restricted Lie algebras, such a classification exists in a few special cases (a list is given in [20]), but in general we have to settle for less. As the simple $\mathfrak{g}$-modules are of finite, bounded dimension, a more modest (but, as it turns out, still very hard!) question would be to ask for the maximal dimension $M(\mathfrak{g})$ of such a module. In the fundamental paper [67] Zassenhaus gave a formula for $M(\mathfrak{g})$ in ring-theoretic terms. He worked in the general, i.e., not necessarily restricted, setting, but here we will translate his result to our setup (see also the account in [58], Chapter 6): Let $Z_0(\mathfrak{g}) \subseteq Z(\mathfrak{g})$ denote the *p-center* of $\mathfrak{g}$, defined as the subalgebra of $U(\mathfrak{g})$ generated by all $x^p - x^{[p]}$, $x \in \mathfrak{g}$. It follows directly from the axioms of the restriction map that the generators of $Z_0(\mathfrak{g})$ are indeed central. Also, let $Q(\mathfrak{g})$, $Q_0(\mathfrak{g})$ denote quotient fields of $Z(\mathfrak{g})$, $Z_0(\mathfrak{g})$ respectively. It is easy to see that $U(\mathfrak{g})$ is free of rank $p^{\dim(\mathfrak{g})}$ over $Z_0(\mathfrak{g})$, with any basis $\{x_1, \dots, x_n\}$ of $\mathfrak{g}$ over F giving a basis $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid 0 \leq \alpha_1, \dots, \alpha_n < p\}$ of $U(\mathfrak{g})$ over $Z_0(\mathfrak{g})$. In particular, $U(\mathfrak{g})$ is *finitely generated over* $Z(\mathfrak{g})$. Now $U(\mathfrak{g})$ is a noetherian domain, so it has a division ring of fractions $D(\mathfrak{g})$, which, since each nonzero $u \in U(\mathfrak{g})$ is integral over $Z_0(\mathfrak{g})$, can be realized as:

$$D(\mathfrak{g}) = U(\mathfrak{g}) \otimes_{Z_0(\mathfrak{g})} Q_0(\mathfrak{g}).$$

Our division ring $D(\mathfrak{g})$ contains $Q(\mathfrak{g})$ and $Q_0(\mathfrak{g})$ as subfields, and Zassenhaus proves that

$$M(\mathfrak{g})^2 = \dim_{Q(\mathfrak{g})} D(\mathfrak{g}) = \dim_{Q(\mathfrak{g})}(U(\mathfrak{g}) \otimes_{Z_0(\mathfrak{g})} Q_0(\mathfrak{g})).$$

Since $\dim_{Q_0(\mathfrak{g})}(U(\mathfrak{g}) \otimes_{Z_0(\mathfrak{g})} Q_0(\mathfrak{g})) = \operatorname{rank}_{Z_0(\mathfrak{g})}(U(\mathfrak{g})) = p^{\dim(\mathfrak{g})}$ we get

$$M(\mathfrak{g})^2 = \frac{p^{\dim(\mathfrak{g})}}{[Q(\mathfrak{g}) : Q_0(\mathfrak{g})]}. \tag{1.4}$$

While this is indeed a very pretty equation, it seems that it should be possible to give an *intrinsic* characterisation of $M(\mathfrak{g})$ not relying on the universal enveloping algebra. To that end, Kac and Weisfeiler gave the following conjecture in [61]:

Conjecture 1.

$$M(\mathfrak{g}) = p^{(\dim(\mathfrak{g}) - \operatorname{ind}(\mathfrak{g}))/2}. \tag{1.5}$$

We will refer to Conjecture 1 as the *first Kac-Weisfeiler conjecture*, or KW1 for short (as the name suggests, there was also a second Kac-Weisfeiler conjecture in the same paper, sometimes just called *the* Kac-Weisfeiler conjecture, which was proved in [43] by Premet). As for the motivation behind KW1, the authors write simply in [61] that "it seems plausible" (see, however, also Kac's review of [43] in [1])! We will provide some much needed further motivation in the next section. The conjecture has been verified – with certain minor restrictions on the characteristic – for:

- Lie algebras of reductive algebraic groups (essentially [50], see also [30], B.5),
- Solvable Lie algebras ([54], generalizing [61]),
- Lie algebras possessing a toral stabilizer ([45], generalizing [37]),
- The Poisson algebras B_{2n} ([53]).

In general, it is known that ([45], Remark 1)

$$p^{(\dim(\mathfrak{g})-\mathrm{ind}(\mathfrak{g}))/2} \mid M(\mathfrak{g}).$$

As for an upper bound, the best we have is $M(\mathfrak{g}) \leq p^{(\dim(\mathfrak{g})-\dim(C(\mathfrak{g})))/2}$, where $C(\mathfrak{g})$ is the center of $\mathfrak{g}$ (see [58], Exercise 1 in Section 6.6). It deserves mention that Mil'ner published a note ([38]) in 1980, in which he claimed to have a proof of KW1. He never published the details however, and his approach relied on a lemma which was later shown to be false (see [22]). So as of today, the conjecture still stands, though one can, unfortunately, still find otherwise reliable online sources where it is stated as a theorem.

Using (1.4) we can reformulate KW1:

Lemma 1.1. *The following statements are equivalent:*

1. *The KW1 conjecture is true.*
2. $\dim_{Q(\mathfrak{g})} D(\mathfrak{g}) = p^{\dim(\mathfrak{g})-\mathrm{ind}(\mathfrak{g})}$.
3. $[Q(\mathfrak{g}) : Q_0(\mathfrak{g})] = p^{\mathrm{ind}(\mathfrak{g})}$.

It is the last statement of this lemma which lends itself to the use of invariant theory, as we will see shortly. Let us first, however, consider finite group scheme actions, which turn out to be closely related to a non-deformed version of the second statement.

1.5 Invariants of finite group schemes and symmetrization

In this section we use the setup from [52], only slightly modified. Let G be a finite group scheme acting from the right on an irreducible affine algebraic variety X, i.e., a scheme $X = \mathrm{Spec}(A)$ with A a finitely generated F-algebra and an integral domain. By the notation $x \in X$ it will be understood that x is a *closed* point of X (we will not consider other kinds of points). Any closed subgroup scheme G' of G acts on G by right multiplication, and the quotient G/G' is an affine scheme with $F[G/G'] = F[G]^{G'}$ (here invariants are taken with respect to the right regular action of G' on $F[G]$). We define the *index* $(G : G')$ of G' in G by

$$(G : G') = \dim(F[G/G']).$$

Then one can show that we have $\dim(F[G]) = (G : G') \cdot \dim(F[G'])$, in analogy with Lagrange's Theorem for finite groups. Now, for any $x \in X$ the stabilizer G_x is a closed subgroup scheme of G. Let

$$M(X) = \max\{(G : G_x) \mid x \in X\}$$

and

$$X_{G-\mathrm{reg}} = \{x \in X \mid (G : G_x) = M(X)\}.$$

Skryabin proves in [52], among many other things, that $X_{G-\mathrm{reg}}$ is open in X, and that

$$[F(X) : F(X)^G] = M(X), \tag{1.6}$$

where $F(X)$ is the field of rational functions on X, i.e., the quotient field of $F[X] = A$ (he actually proves this in a more general situation, where X is not necessarily affine). But why is this result of interest to us? Well, assume that we have a restricted action of our Lie algebra $\mathfrak{g}$ on $F[X]$ by derivations (in other words, a restricted homomorphism $\mathfrak{g} \to \mathrm{Der}(F[X])$). Furthermore, for any $x \in X$ with corresponding maximal ideal $\mathfrak{m}_x \subseteq F[X]$, define

$$\mathfrak{g}_x = \{y \in \mathfrak{g} \mid y(\mathfrak{m}_x) \subseteq \mathfrak{m}_x\}, \tag{1.7}$$

$$m(X) = \max\{\mathrm{codim}_{\mathfrak{g}}(\mathfrak{g}_x) \mid x \in X\}, \tag{1.8}$$

$$X_{\mathfrak{g}-\mathrm{reg}} = \{x \in X \mid \mathrm{codim}_{\mathfrak{g}}(\mathfrak{g}_x) = m(X)\},$$

and note that $\mathfrak{g}_x$ is restricted for any $x \in X$. Let G denote the finite group scheme associated to $\mathfrak{g}$ (given by $F[G] = U(\mathfrak{g}, 0)^*$, as in Section 1.3) and $G(x)$ the finite group scheme associated to $\mathfrak{g}_x$. The action of $\mathfrak{g}$ on $F[X]$ induces an action of G on X such that $F(X)^G = F(X)^{\mathfrak{g}}$ and $G_x \cong G(x)$ for all x ([12], II, §7, 3.10), from which it follows that

$$(G : G_x) = \frac{\dim(F[G])}{\dim(F[G_x])} = p^{\mathrm{codim}_{\mathfrak{g}}(\mathfrak{g}_x)}.$$

But then $X_{G-\mathrm{reg}} = X_{\mathfrak{g}-\mathrm{reg}}$, and

$$[F(X) : F(X)^{\mathfrak{g}}] = p^{m(X)}. \tag{1.9}$$

Now consider the special case $X = \mathfrak{g}^*$ with the standard (restricted) action of $\mathfrak{g}$ by derivations on $F[\mathfrak{g}^*] \cong S(\mathfrak{g})$. One checks easily that, for any $y \in \mathfrak{g}$ and $\chi \in \mathfrak{g}^*$, we have $y(\mathfrak{m}_\chi) \subseteq \mathfrak{m}_\chi$ if and only if $\chi([y, \mathfrak{g}]) = 0$, so our two notions of stabilizer (definitions (1.1) and (1.7)) coincide. We get $m(X) = \dim(\mathfrak{g}) - \mathrm{ind}(\mathfrak{g})$ and finally, with $Q(S(\mathfrak{g}))$ denoting the field of fractions of $S(\mathfrak{g})$,

$$[Q(S(\mathfrak{g})) : Q(S(\mathfrak{g}))^{\mathfrak{g}}] = p^{\dim(\mathfrak{g}) - \mathrm{ind}(\mathfrak{g})}. \tag{1.10}$$

Looking at item 2 in Lemma 1.1, it becomes clear (since $Q(\mathfrak{g}) = D(\mathfrak{g})^{\mathfrak{g}}$) that the KW1 conjecture can be seen as a deformed version of a special case of the invariant-theoretic result (1.6). And of course, in view of (1.10), we are now *very* interested in finding ways to compare $S(\mathfrak{g})$ and $U(\mathfrak{g})$!

Let us for a moment consider the symmetrization map $\varphi : S(\mathfrak{l}) \to U(\mathfrak{l})$ (defined in Section 1.2) of a Lie algebra $\mathfrak{l}$ over a field of characteristic zero. Its inverse φ^{-1} (which we consider instead of φ only for technical and notational reasons) has several nice properties:[3]

1. φ^{-1} is an isomorphism of $\mathfrak{l}$-modules.
2. φ^{-1} is filtration-preserving (with the filtration on $S(\mathfrak{l})$ coming from the grading).
3. The map $\mathrm{Gr}(\varphi^{-1})$ from $\mathrm{Gr}(U(\mathfrak{l})) \cong S(\mathfrak{l})$ to $\mathrm{Gr}(S(\mathfrak{l})) \cong S(\mathfrak{l})$ is the identity.

Note that the identifications made in item 3 are canonical, so it makes sense to speak of 'the identity'. Sadly, the definition of φ does *not* make sense in prime characteristic, but by slight abuse of terminology, we will refer to any map $\psi : U(\mathfrak{g}) \to S(\mathfrak{g})$ satisfying items 1, 2 and 3 as a symmetrization map. The importance of this notion, from our perspective, comes from the fact that the KW1 conjecture is true for any Lie algebra admitting such a map! This follows essentially from results in [37], but we will work out some of the details here, for the sake of completeness. First, a little preparation is needed: If $x \in U(\mathfrak{g})$ and $z \in Z_0(\mathfrak{g})$ we write $\frac{x}{z}$ for the element $x \otimes z^{-1}$ in $D(\mathfrak{g}) = U(\mathfrak{g}) \otimes_{Z_0(\mathfrak{g})} Q_0(\mathfrak{g})$. Define a degree function on $D(\mathfrak{g})$ by setting

$$\deg\left(\frac{x}{z}\right) = \deg(x) - \deg(z).$$

One checks easily that this is well-defined. Now $D(\mathfrak{g})$ becomes a filtered algebra if we set $D(\mathfrak{g})_{\leq k} = \{y \in D(\mathfrak{g}) \mid \deg(y) \leq k\}$ for all $k \in \mathbb{Z}$. On the other hand, the localization $S(\mathfrak{g})_{l(Z_0(\mathfrak{g})\setminus\{0\})}$ (which makes sense since $l(Z_0(\mathfrak{g}) \setminus \{0\})$ is a multiplicative set) sitting inside $Q(S(\mathfrak{g}))$ becomes a $\mathbb{Z}$-graded algebra by defining

$$(S(\mathfrak{g})_{l(Z_0(\mathfrak{g})\setminus\{0\})})_k = \left\{ \frac{f}{g} \;\middle|\; f \text{ is homogeneous and } \deg(f) - \deg(g) = k \right\}$$

for all $k \in \mathbb{Z}$. Now we have:

Lemma 1.2.

$$\mathrm{Gr}(D(\mathfrak{g})) \cong S(\mathfrak{g})_{l(Z_0(\mathfrak{g})\setminus\{0\})}.$$

Proof. We have canonical linear maps $d_j : U(\mathfrak{g})_j \to U(\mathfrak{g})_j/U(\mathfrak{g})_{j-1} \cong S(\mathfrak{g})_j$ for all $j > 0$ and define $\bar{\psi}_k : D(\mathfrak{g})_{\leq k} \to S(\mathfrak{g})_{l(Z_0(\mathfrak{g})\setminus\{0\})}$ for all $k \in \mathbb{Z}$ by

$$\bar{\psi}_k\left(\frac{x}{z}\right) = \frac{d_{k+\deg(z)}(x)}{d_{\deg(z)}(z)}.$$

It is easy to check that these maps are well-defined and induce linear isomorphisms $\psi_k : D(\mathfrak{g})_{\leq k}/D(\mathfrak{g})_{\leq k-1} \xrightarrow{\sim} (S(\mathfrak{g})_{l(Z_0(\mathfrak{g})\setminus\{0\})})_k$. Finally, the map $\psi : \mathrm{Gr}(D(\mathfrak{g})) \to S(\mathfrak{g})_{l(Z_0(\mathfrak{g})\setminus\{0\})}$ defined by $\psi(\sum_k x_k) = \sum_k \psi_k(x_k)$, with $x_k \in D(\mathfrak{g})_{\leq k}/D(\mathfrak{g})_{\leq k-1}$ for all k, is an isomorphism of algebras. □

[3] Aside from the three listed, it is also an isomorphism of coalgebras

For any subspace V of $D(\mathfrak{g})$ we will identify $\mathrm{Gr}(V)$ with a subspace of $Q(S(\mathfrak{g}))$ via the map given in Lemma 1.2. Now we have:

Theorem 1.3. *Assume that $\mathfrak{g}$ admits a symmetrization map φ. Then*

$$[Q(\mathfrak{g}) : Q_0(\mathfrak{g})] = p^{\mathrm{ind}(\mathfrak{g})}$$

and the KW1 conjecture is true for $\mathfrak{g}$.

Proof. Set $\mathrm{ind}(\mathfrak{g}) = k$ and denote by $Q(S(\mathfrak{g})^{\mathfrak{g}})$, $Q(S(\mathfrak{g})^p)$ fields of fractions of $S(\mathfrak{g})^{\mathfrak{g}}$, $S(\mathfrak{g})^p$ respectively. By (1.10), and the fact that $S(\mathfrak{g})$ is free of rank $p^{\dim(\mathfrak{g})}$ over $S(\mathfrak{g})^p$, we get $[Q(S(\mathfrak{g})^{\mathfrak{g}}) : Q(S(\mathfrak{g})^p)] = p^k$. Choose a homogeneous basis $f_1, \dots, f_{p^k} \in S(\mathfrak{g})^{\mathfrak{g}}$ of $Q(S(\mathfrak{g})^{\mathfrak{g}})$ over $Q(S(\mathfrak{g})^p)$. We want to show that $f_1, \dots, f_{p^k}$ is also a basis of $S(\mathfrak{g})^{\mathfrak{g}}_{l(Z_0(\mathfrak{g})\setminus\{0\})}$ over $S(\mathfrak{g})^p_{l(Z_0(\mathfrak{g})\setminus\{0\})}$: The linear independence is clear, so assume $x \in S(\mathfrak{g})^{\mathfrak{g}}$ is homogeneous and write

$$x = \frac{g_1}{h_1} f_1 + \cdots + \frac{g_{p^k}}{h_{p^k}} f_{p^k}$$

for some $g_i, h_i \in S(\mathfrak{g})^p$. By clearing denominators we get $hx = g_1' f_1 + \cdots + g_{p^k}' f_{p^k}$, and since $x, f_1, \dots, f_{p^k}$ are homogeneous we can safely assume the same for $h, g_1, \dots, g_{p^k}$. But the set of homogeneous elements in $S(\mathfrak{g})^p$ is *precisely* $l(Z_0(\mathfrak{g}) \setminus \{0\})$, and so x belongs to the $S(\mathfrak{g})^p_{l(Z_0(\mathfrak{g})\setminus\{0\})}$-span of $f_1, \dots, f_{p^k}$, as was to be shown.

Since φ is $\mathfrak{g}$-invariant we have $\varphi^{-1}(f_1), \dots, \varphi^{-1}(f_{p^k}) \in Z(\mathfrak{g})$, and

$$\begin{aligned}\mathrm{Gr}(Q(\mathrm{g})) &\subseteq S(\mathfrak{g})^{\mathfrak{g}}_{l(Z_0(\mathfrak{g})\setminus\{0\})} = \mathrm{span}_{S(\mathfrak{g})^p_{l(Z_0(\mathfrak{g})\setminus\{0\})}}\{f_1, \dots, f_{p^k}\} \\ &= \mathrm{Gr}(\mathrm{span}_{Q_0(\mathfrak{g})}\{\varphi^{-1}(f_1), \dots, \varphi^{-1}(f_{p^k})\}) \subseteq \mathrm{Gr}(Q(\mathfrak{g})).\end{aligned}$$

For the second equality we use both that $\mathrm{Gr}(Z_0(\mathfrak{g})) = S(\mathfrak{g})^p$ and that $\mathrm{Gr}(\varphi)$ is the identity. It follows that $\mathrm{Gr}(\mathrm{span}_{Q_0(\mathfrak{g})}\{\varphi^{-1}(f_1), \dots, \varphi^{-1}(f_{p^k})\}) = \mathrm{Gr}(Q(\mathfrak{g}))$, which implies $\mathrm{span}_{Q_0(\mathfrak{g})}\{\varphi^{-1}(f_1), \dots, \varphi^{-1}(f_{p^k})\} = Q(\mathfrak{g})$. Linear independence of the set $\{\varphi^{-1}(f_1), \dots, \varphi^{-1}(f_{p^k})\}$ is easy to check, and the result follows. □

In his failed attempt [38] to resolve the KW1 conjecture in the positive, Mil'ner actually "proves" that every Lie algebra admits a symmetrization map. While some of his arguments were later shown to be flawed, it should be remarked that the author is not aware of a single example of a Lie algebra *not* admitting such a map. Thus the class $\mathfrak{S}$ of Lie algebras possessing symmetrization maps is still very much shrouded in mystery, but we do have the following characterization, which is based on a theorem by Friedlander and Parshall ([22]):

Theorem 1.4. *For a Lie algebra $\mathfrak{g}$, the following conditions are equivalent:*

1. *$\mathfrak{g}$ admits a symmetrization map.*
2. *The inclusion $\mathfrak{g} \hookrightarrow U(\mathfrak{g})$ splits as a map of $\mathfrak{g}$-modules.*
3. *There exists an associative F-algebra A and an injective Lie homomorphism $\rho : \mathfrak{g} \hookrightarrow A$ which splits as a map of $\mathfrak{g}$-modules.*

Note that the $\mathfrak{g}$-module structure on A in the third statement is given by $x.a = \rho(x)a - a\rho(x)$ for all $x \in \mathfrak{g}$, $a \in A$.

Proof. We prove that the first and second statements are equivalent first: Assume that there exists a symmetrization map $\psi : U(\mathfrak{g}) \to S(\mathfrak{g})$. Then we must have $\psi(U(\mathfrak{g})_{\leq 1}) = S(\mathfrak{g})_{\leq 1}$, and

$$U(\mathfrak{g}) = U(\mathfrak{g})_{\leq 1} \oplus \psi^{-1}\big(\bigoplus_{k=2}^{\infty} S(\mathfrak{g})_k\big) = F \oplus \mathfrak{g} \oplus \psi^{-1}\big(\bigoplus_{k=2}^{\infty} S(\mathfrak{g})_k\big).$$

These are direct sums *of* $\mathfrak{g}$*-modules* since ψ is $\mathfrak{g}$-invariant, so the $\mathfrak{g}$-module map $\mathfrak{g} \hookrightarrow U(\mathfrak{g})$ does indeed split.

As for the other implication, assume that there exists a $\mathfrak{g}$-invariant map $s : U(\mathfrak{g}) \to \mathfrak{g}$, which is the identity on $\mathfrak{g}$. By functoriality, s induces a map $S(s) : S(U(\mathfrak{g})) \to S(\mathfrak{g})$, which is also $\mathfrak{g}$-invariant. We will now introduce a rather strange map $M : U(\mathfrak{g}) \to S(U(\mathfrak{g}))$ known as *Mil'ner's map* (defined in [22], but inspired by [38]): Let $x_1, \ldots, x_n$ be a basis of $\mathfrak{g}$ and $x_{k_1} \cdots x_{k_j}$ a PBW basis element of $U(\mathfrak{g})$ (so we have $k_1 \leq \cdots \leq k_j$). For any ordered subset $I' = \{i_1, \ldots, i_s\}$ of $I = \{1, \ldots, j\}$ we write $x_{I'} = x_{k_{i_1}} \cdots x_{k_{i_s}}$ and define M by

$$M(x_{k_1} \cdots x_{k_j}) = \sum_{I = I_1 \cup \cdots \cup I_m} x_{I_1} \circ \cdots \circ x_{I_m},$$

where $\circ$ denotes the commutative product in $S(U(\mathfrak{g}))$, and the sum runs over all *disjoint* decompositions of I into ordered subsets (we do not care for the order of the subsets themselves). This definition begs for an example:

$$M(x_1x_2x_3) = x_1x_2x_3 + x_1x_2 \circ x_3 + x_1x_3 \circ x_2 + x_2x_3 \circ x_1 + x_1 \circ x_2 \circ x_3.$$

It turns out that M is $\mathfrak{g}$-invariant, and from there it is a simple matter to check that $\varphi = S(s) \circ M$ is the desired symmetrization map (it is even an isomorphism of coalgebras).

Now it is obvious that the second statement implies the third, and the proof of the opposite implication is a simple application of the universal property of $U(\mathfrak{g})$: Let an injective Lie homomorphism $\rho : \mathfrak{g} \to A$ and a $\mathfrak{g}$-module map $s : A \to \mathfrak{g}$ such that $s \circ \rho = \mathrm{id}_{\mathfrak{g}}$ be given. We get, by the aforementioned universal property, an algebra homomorphism $\hat{\rho} : U(\mathfrak{g}) \to A$ which extends ρ. But then the composition $s \circ \hat{\rho} : U(\mathfrak{g}) \to \mathfrak{g}$ is a $\mathfrak{g}$-module map which is the identity on $\mathfrak{g}$, and we are done. □

Theorem 1.4 enables us to prove, heavily inspired by Lemma 3.5 in [44], that $\mathfrak{S}$ is closed under taking centralizers:

Proposition 1.5. *Assume that* $\mathfrak{g}$ *admits a symmetrization map, and let* X *be any subset of* $\mathfrak{g}$*. Then the centralizer* $\mathfrak{c}_{\mathfrak{g}}(X) = \{y \in \mathfrak{g} \mid [y, X] = 0\}$ *also admits a symmetrization map.*

Proof. Identify $U(\mathfrak{c}_{\mathfrak{g}}(X))$ with a subalgebra of $U(\mathfrak{g})$ in the usual way. By Theorem 1.4, there exists a map of $\mathfrak{g}$-modules $s : U(\mathfrak{g}) \to \mathfrak{g}$ with $s_{|\mathfrak{g}} = \mathrm{id}_{\mathfrak{g}}$, and we only need to check that $s(U(\mathfrak{c}_{\mathfrak{g}}(X))) \subseteq \mathfrak{c}_{\mathfrak{g}}(X)$. But for all $u \in U(\mathfrak{c}_{\mathfrak{g}}(X))$ and $x \in X$ we clearly have $x.u = xu - ux = 0$, so the $\mathfrak{g}$-invariance of s gives us

$$[x, s(u)] = x.s(u) = s(x.u) = 0,$$

and $s(u) \in \mathfrak{c}_{\mathfrak{g}}(X)$. □

Let G be a connected reductive algebraic group over F satisfying the *standard hypotheses* (introduced in [28] to avoid some of the pathological behaviour inextricably linked to positive characteristic):

1. The derived group of G is simply connected.
2. p is good for G.
3. There exists a G-invariant non-degenerate bilinear form on $\mathrm{Lie}(G)$.

Then, by Proposition 1.4 in [59], $\mathrm{Lie}(G)$ admits a symmetrization map[4] (which can even be taken to be G-invariant) and thus satisfies the KW1 conjecture. By Proposition 1.5 the same is true for any centralizer in $\mathrm{Lie}(G)$.

1.6 Decomposition of $Z(\mathfrak{g})$ for Lie algebras of reductive groups

We now shift the perspective a little and consider the algebra extension $Z_0(\mathfrak{g}) \subseteq Z(\mathfrak{g})$, with item 3 of Lemma 1.1 as motivation. We know, of course, that this extension is finite, but other than that, it seems to be very hard to describe the structure of $Z(\mathfrak{g})$ as a $Z_0(\mathfrak{g})$-module in general. We do, however, have the following theorem:

Theorem 1.6. *Let G be a connected reductive algebraic F-group of rank n, let $\mathfrak{g} = \mathrm{Lie}(G)$, and assume that G satisfies the standard hypotheses of the previous section. Then we have:*

1. *$U(\mathfrak{g})^G$ is a polynomial algebra in n variables.*
2. *$Z(\mathfrak{g}) \cong Z_0(\mathfrak{g}) \otimes_{Z_0(\mathfrak{g})^G} U(\mathfrak{g})^G$.*
3. *$Z(\mathfrak{g})$ is free of rank p^n over $Z_0(\mathfrak{g})$.*
4. *The three previous statements are still true if we replace $U(\mathfrak{g})$ by $S(\mathfrak{g})$, $Z(\mathfrak{g})$ by $S(\mathfrak{g})^{\mathfrak{g}}$ and $Z_0(\mathfrak{g})$ by $S(\mathfrak{g})^p$.*

[4] One ingredient of the proof is the so-called *Richardson's property*, which appears several places in the literature (albeit with definitions varying slightly from the original one in [44]) and is essentially a linearized form of item 3 in Theorem 1.4.

Veldkamp proved a version of this theorem in [62], with much stronger conditions on G. His results were then generalized successively in [31], [39] and [9] (see also [59]), but Theorem 1.6 is still known as Veldkamp's Theorem (see [8] for some of the terrible things that can happen if we lessen the conditions on G further). We see that the center is in a natural way built from the p-center and the G-invariants, in contrast with the classical situation in Section 1.2, where we have (shifting to the notation from that section for a moment) $U(\mathfrak{g})^G = U(\mathfrak{g})^{\mathfrak{g}} = Z(\mathfrak{g})$. In both cases $U(\mathfrak{g})^G$ is a polynomial algebra in $\operatorname{rank}(G)$ variables, and in fact the first statement in Veldkamp's Theorem can be proved by constructing a map similar to the twisted Harish-Chandra isomorphism of Section 1.2 ([9]). Note also, that since the rank of G is equal to the index of $\mathfrak{g}$ (see [30], B.5), the third statement of the theorem confirms the KW1 conjecture for the Lie algebras considered.[5]

Later we will concern ourselves with the problem of finding an analogue of Veldkamp's Theorem for a very important class of Lie algebras known as the *restricted Cartan type Lie algebras* (to be defined in the next section). For now, let us remark that for a general finite-dimensional restricted $\mathfrak{g}$ there seems to be no canonical way of producing *non-trivial central elements*, i.e., elements $z \in Z(\mathfrak{g}) \setminus Z_0(\mathfrak{g})$, and the same can be said for elements in $S(\mathfrak{g})^{\mathfrak{g}} \setminus S(\mathfrak{g})^p$. In other words, we have no replacement for the G-invariants in Veldkamp's theorem. If we do, somehow, manage to overcome this problem in the symmetric case, then the following differential criterion by Skryabin (a shortened version of Theorem 5.4 in [52]) can be useful:

Theorem 1.7. *Let X be a smooth irreducible affine variety, and assume that we have a restricted action of $\mathfrak{g}$ on $F[X]$ by derivations. Recall the definition of $m(X)$ from section 1.5 and set $n = \dim(X) - m(X)$. For any $f_1, \dots f_n \in F[X]^{\mathfrak{g}}$ we denote by C the (closed) subset of X consisting of all $x \in X$ such that the differentials $d_x f_1, \dots, d_x f_n$ are linearly dependent. If $\operatorname{codim}_X(C) \geq 2$, then*

1. *$F[X]^{\mathfrak{g}} = F[X]^p[f_1, \dots f_n]$.*
2. *$F[X]^{\mathfrak{g}}$ is free of rank p^n over $F[X]^p$, with a basis given by*

$$\{f_1^{k_1} \dots f_n^{k_n} \mid 0 \leq k_1, \dots, k_n < p\}.$$

With $X = \mathfrak{g}^*$, as in Section 1.5, we have $n = \operatorname{ind}(\mathfrak{g})$ and $F[X] \cong S(\mathfrak{g})$, so we see that items 1 and 2 in Theorem 1.7 become analogues of the non-deformed versions of items 2 and 3 in Theorem 1.6. The big problem, as already mentioned, is to find f_i that satisfy the condition in Theorem 1.7! And if one then wants to transfer the results to the center, there is of course the issue of lacking symmetrization. Before exploring these complications further, we need, however, to introduce the class of Lie algebras which are at the center of most of our investigations.

[5] It deserves mention, that in [60] Topley uses a 'Veldkamp-like' theorem to prove KW1 for centralizers in Lie algebras of certain reductive groups. As we saw at the end of the last section, one can prove a more general result *without* such a theorem (though it is of course still of interest in its own right!).

Chapter 2

The restricted Cartan types: Invariants, semi-invariants and orbit closures

2.1 Restricted Cartan type Lie algebras

The restricted *simple* Lie algebras have been completely classified when the characteristic of the ground field is not too small:

Theorem 2.1. *Let $\mathfrak{g}$ be a finite-dimensional restricted simple Lie algebra over an algebraically closed field of characteristic $p > 5$. Then $\mathfrak{g}$ is either of classical or Cartan type.*

This theorem used to be known as the *Kostrikin-Shafarevich Conjecture* (stated in [33]). It was proved for $p > 7$ by Block and Strade in [4] and is now a special case of the classification of *all* simple modular Lie algebras over an algebraically closed field of characteristic $p > 3$:

Theorem 2.2. *Let $\mathfrak{g}$ be a finite-dimensional simple Lie algebra over an algebraically closed field of characteristic $p > 3$. Then $\mathfrak{g}$ is either classical, of filtered Cartan type or Melikian.*

Here the Melikian algebras (one of which is restricted) live only in characteristic 5. The proof of this monumental result, which spans many hundred pages spread out over several papers, was completed by Premet and Strade in [47].[1] The three volumes [55], [56] and [57] give a uniform treatment of the proof, along with the tools necessary to understand it (see also the survey [46]). For characteristics 2 and 3 the situation is significantly more complicated, and while progress is being made

[1] The classification theorem is only one of several examples of the modular theory placing itself at the halfway point between complex Lie algebras and finite groups: while it certainly possesses very little of the elegance and simplicity of the classification by Dynkin diagrams in the complex case, it does not quite match the enormous complexity of the classification of finite simple groups either.

(see for example [51] or the recent paper [7]), it still seems that we are nowhere near a full classification.

Returning to the restricted case, we proceed to explain the notions of 'classical' and 'Cartan type' in Theorem 2.1. Let F be a field of characteristic $p > 3$ and $\mathfrak{g}'$ a simple Lie algebra over the complex numbers. One can choose a special basis $\{x_1, \ldots, x_n\}$ of $\mathfrak{g}'$, called a *Chevalley basis* ([24], 25.2), such that the structure constants with respect to the Lie bracket are integers. Then $\mathfrak{g} = \sum_{i=1}^{n} \mathbb{Z}x_i \otimes_{\mathbb{Z}} F$ becomes a Lie algebra over F in an obvious way, and it turns out that $\mathfrak{g}$ is simple unless $\mathfrak{g}' \cong \mathfrak{sl}(m)$ with $p \mid m$, in which case the center $C(\mathfrak{g})$ is one-dimensional and $\mathfrak{g}/C(\mathfrak{g})$ is simple. The simple Lie algebras over F obtained by this method are called classical.

Moving on to the Cartan types, where we will go into significantly more detail. For the basic definitions and results we will follow 2.8–2.11 in [3] (which again refers to [58] for many proofs), but note that [3] takes a more general approach by using divided power algebras, whereas our approach is more concrete. The difference amounts to nothing more than a scaling of basis elements, so though some formulas might change, everything is essentially the same. In what follows, whenever we consider the Cartan types, we will assume that the characteristic of our ground field F is larger than 3. Let $A(n) = F[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$ denote the truncated polynomial ring in n variables over F. We write x_i for the image of X_i in $A(n)$ and also define $y_i = x_i + 1$ for later use. Note that $A(n)$ is a finite-dimensional local algebra, with maximal ideal $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$. The nth *Witt-Jacobson algebra* $W(n)$ is defined as the Lie algebra $\mathrm{Der}(A(n))$ of derivations of $A(n)$. It is restricted and simple, with the p-map being given by ordinary multiplication in $\mathrm{End}(A(n))$: $D^{[p]} = D^p$ for all $D \in W(n)$. Furthermore, it is an $A(n)$-module in an obvious way, and has a standard basis $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \partial_i \mid 0 \leq \alpha_j < p, 1 \leq i \leq n\}$ where ∂_i denotes partial differentiation with respect to x_i. The following useful formula is easy to prove:

$$D = \sum_{i=1}^{n} D(x_i)\partial_i \tag{2.1}$$

for all $D \in W(n)$. We will often use standard multi-index notation: For an n-tuple $\alpha = (\alpha_1, \ldots, \alpha_n)$ with $0 \leq \alpha_j < p$ for $1 \leq j \leq n$, we write x^α for $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and define the degree of x^α to be $|\alpha| = \alpha_1 + \cdots + \alpha_n$. We denote by ϵ_j the n-tuple $(0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in the j'th place, and by τ the n-tuple $(p-1, \ldots, p-1)$. The commutator in $W(n)$ is given by

$$[x^\alpha \partial_i, x^\beta \partial_j] = \beta_i x^{\alpha+\beta-\epsilon_i}\partial_j - \alpha_j x^{\alpha+\beta-\epsilon_j}\partial_i. \tag{2.2}$$

An important tool in the study of $W(n)$ is the standard grading $W(n) = \bigoplus_{i=-1}^{N} W(n)_i$, where $N = n(p-1) - 1$ and

$$W(n)_i = \sum_{j=1}^{n} \sum_{|\alpha|=i+1} Fx^\alpha \partial_j.$$

The module of Kähler differentials $\Omega_{A(n)/F}$ is easily seen to be free over $A(n)$, with a basis given by $\{dx_1, \ldots, dx_n\}$. Furthermore, every exterior power $\Omega^r_{A(n)/F}$ $(r \geq 0)$

is a $W(n)$-module in a natural way, which makes it possible to define the following (restricted) subalgebras:

$$S(n) = \{\partial \in W(n) \mid \partial(dx_1 \wedge dx_2 \wedge \cdots \wedge dx_n) = 0\}, \tag{2.3}$$

$$H(2m) = \{\partial \in W(2m) \mid \partial\Big(\sum_{i=1}^{m} dx_i \wedge dx_{2m+1-i}\Big) = 0\}, \tag{2.4}$$

$$K(2m+1) = \{\partial \in W(2m+1) \mid \partial(\omega_K) \in A(2m+1)\omega_K\}. \tag{2.5}$$

Here $\omega_K = \sum_{i=1}^{m}(x_i dx_{2m+1-i} - x_{2m+1-i}dx_i) + dx_{2m+1}$. It turns out, that in all three cases a certain higher derived algebra (to be elaborated on) is simple and restricted, and the three families of simple restricted Lie algebras obtained in this way are known respectively as the *special algebras*, the *Hamiltonian algebras* and the *contact algebras*. Together with the Witt-Jacobson algebras they constitute what is known as the *simple restricted Lie algebras of Cartan type*. We will, however, often omit the 'simple' in what follows.

Let us now gather some facts about $S(n)$. Define linear maps $\operatorname{div} : W(n) \to A(n)$ and $D_{ij} : A(n) \to W(n)$ $(1 \leq i, j \leq n)$ by

$$\operatorname{div}(\partial) = \sum_{i=1}^{n} \partial_i(\partial(x_i)),$$
$$D_{ij}(f) = \partial_j(f)\partial_i - \partial_i(f)\partial_j$$

for all $\partial \in W(n)$ and $f \in A(n)$. A direct calculation shows that

$$\partial(dx_1 \wedge \cdots \wedge dx_n) = \operatorname{div}(\partial)dx_1 \wedge \cdots \wedge dx_n$$

for all $\partial \in W(n)$, which implies $S(n) = \{\partial \in W(n) \mid \operatorname{div}(\partial) = 0\}$. Using this alternative definition it is easy to see that the images of the D_{ij} are contained in $S(n)$. In fact, it can be shown that

$$S(n) = \sum_{i,j} D_{ij}(A(n)) \oplus \bigoplus_{i=1}^{n} Fx^{\tau-(p-1)\epsilon_i}\partial_i.$$

Furthermore, it turns out that $\sum_{i,j} D_{ij}(A(n))$ is equal to the derived algebra $S(n)^{(1)}$ of $S(n)$. If $n \geq 3$, then $S(n)^{(1)}$ is restricted and simple, but for $n = 2$ the second derived algebra $S(n)^{(2)}$ is a proper ideal of $S(n)^{(1)}$, since the element $D_{12}(x_1^{p-1}x_2^{p-1})$ is not contained in the former. However, $S(n)^{(2)} = D_{12}(\sum_{|\alpha|<2p-2} Fx^{\alpha})$ is restricted and simple, and we define the nth *special algebra* to be $S(n)^{(1+\delta_{n2})}$. It is not hard to see that $S(1)$ is one-dimensional and therefore not terribly interesting, so in the following we will always assume $n \geq 2$ when looking at the special algebras.

Let us move on to the family $H(2m)$. Note first that $H(2) = S(2)$, so it makes no harm to assume $m \geq 2$. For a number $i \in \{1, \ldots, 2m\}$ we set $i' = 2m + 1 - i$ and

$$\sigma(i) = \begin{cases} 1 & \text{if } 1 \leq i \leq m, \\ -1 & \text{if } m+1 \leq i \leq 2m. \end{cases}$$

For $\partial = \sum_{i=1}^{2m} f_i \partial_i \in W(2m)$ the condition in (2.4) can be shown to be equivalent to

$$\sigma(i)\partial_j(f_i) = \sigma(j')\partial_{i'}(f_{j'}) \tag{2.6}$$

for all $1 \leq i, j \leq 2m$. Using this equation it is not hard to see that the image of the linear map $D_H : A(2m) \to W(2m)$ defined by

$$D_H(f) = \sum_{i=1}^{2m} \sigma(i)\partial_i(f)\partial_{i'}$$

is contained in $H(2m)$. It turns out that $H(2m)^{(1)} = D_H(\sum_{|\alpha|<2m(p-1)} Fx^\alpha)$. This subalgebra is simple and restricted, and we call it a *Hamiltonian algebra*.

The special and Hamiltonian algebras are easily seen to be *graded* subalgebras of the corresponding Witt-Jacobson algebra, but this is not true for the last family, the contact algebras: Define a linear map $D_K : A(2m+1) \to W(2m+1)$ by $D_K(f) = \sum_{i=1}^{2m+1} f_i \partial_i$, where

$$f_i = x_i \partial_{2m+1}(f) + \sigma(i')\partial_{i'}(f) \qquad \text{for } 1 \leq i \leq 2m,$$
$$f_{2m+1} = 2f - \sum_{j=1}^{2m} x_j \partial_j(f).$$

Furthermore, we define $\Delta(f) = 2f - \sum_{j=1}^{2m} x_j \partial_j(f)$ and

$$\langle f, g \rangle = \Delta(f)\partial_{2m+1}(g) - \Delta(g)\partial_{2m+1}(f) + \sum_{j=1}^{2m} \sigma(j)\partial_j(f)\partial_{j'}(g).$$

A basic calculation proves the commutation formula

$$[D_K(f), D_K(g)] = D_K(\langle f, g \rangle).$$

It turns out that the image of D_K is exactly $K(2m+1)$. Grading $A(2m+1)$ by $\deg(x^\alpha) = \|\alpha\| = |\alpha| + \alpha_{2m+1} - 2$ induces a grading on $K(2m+1)$ via

$$K(2m+1)_j = \text{span}\{D_K(x^\alpha) \mid \deg(x^\alpha) = j\}.$$

The derived algebra $K(2m+1)^{(1)}$ is restricted and simple, and we call it a *contact algebra*. It can be shown that $K(2m+1)^{(1)} = \text{span}\{D_K(x^\alpha) \mid \alpha \neq \tau\}$ if $2m+4 \equiv 0 \mod p$ and $K(2m+1)^{(1)} = K(2m+1)$ otherwise. We will need a few formulas regarding the product $\langle \cdot, \cdot \rangle$ (compare [3], p. 57, but note that formula (v) there is not correct as stated):

$$\langle 1, x^\alpha \rangle = \alpha_{2m+1} x^{\alpha - \epsilon_{2m+1}} \tag{2.7}$$
$$\langle x_i, x^\alpha \rangle = \sigma(i)\alpha_{i'} x^{\alpha - \epsilon_{i'}} + \alpha_{2m+1} x^{\alpha + \epsilon_i - \epsilon_{2m+1}} \qquad \text{for } 1 \leq i \leq 2m \tag{2.8}$$
$$\langle x_{2m+1}, x^\alpha \rangle = ||\alpha|| x^\alpha \tag{2.9}$$
$$\langle x_i x_j, x^\alpha \rangle = \sigma(i)\alpha_{i'} x^{\alpha + \epsilon_j - \epsilon_{i'}} + \sigma(j)\alpha_{j'} x^{\alpha + \epsilon_i - \epsilon_{j'}} \qquad \text{for } 1 \leq i, j \leq 2m \tag{2.10}$$
$$\langle x_i x_{i'}, x^\alpha \rangle = (\alpha_{i'} - \alpha_i) x^\alpha \qquad \text{for } 1 \leq i \leq m. \tag{2.11}$$

From now on we will (by abuse of notation) write $W(n)$, $S(n)$, $H(n)$ and $K(n)$ for the corresponding simple derived subalgebra, with the convention that $n = 2m$ for the Hamiltonian type and $n = 2m + 1$ for the contact type. If $\mathfrak{g}$ is an arbitrary simple restricted algebra of Cartan type, then we use the notation $\widehat{\mathfrak{g}}$ for the algebra from which it is derived (with the convention $\widehat{W(n)} = W(n)$). We have the following lemma, which sums up some of the most important information from the preceding discussion:

Lemma 2.3. *Let $A(n)$ be graded in the usual way if $\mathfrak{g} \in \{W, S, H\}$ and by $\deg(x^\beta) = ||\beta||$ if $\mathfrak{g} \in \{K\}$. Then there exists a finite family of graded linear maps $D_\alpha : A(n) \to \widehat{\mathfrak{g}}$ such that $\mathfrak{g}$ is spanned by elements of the form $D_\alpha(x^\beta)$. The maps $\{D_\alpha\}$ are said to be associated to $\mathfrak{g}$. Furthermore, if $\mathfrak{g} \in \{W, S, H\}$ we have*

$$(\operatorname{ad} \partial_s) \circ D_\alpha = D_\alpha \circ \partial_s \tag{2.12}$$

for $1 \leq s \leq n$ and all α.

Proof. For $W(n)$ we can use the maps D_i defined by $D_i(f) = f\partial_i$ for all $f \in A(n)$. For $S(n)$ we use the D_{ij} with $i \neq j$, and for $H(n)$, $K(n)$ we use D_H, D_K respectively. The identity (2.12) is an easy consequence of the formula $[\partial_s, x^\beta \partial_j] = \partial_s(x^\beta)\partial_j$, which follows from (2.2). For example, if $\mathfrak{g}$ is of type H, we get

$$[\partial_s, D_H(f)] = \sum_{i=1}^{2m} \sigma(i)\partial_s(\partial_i(f))\partial_{i'} = \sum_{i=1}^{2m} \sigma(i)\partial_i(\partial_s(f))\partial_{i'} = D_H(\partial_s(f)).$$

□

The sum $\mathfrak{g}_-$ of components of negative degree in $\mathfrak{g}$ turns up in several of our proofs, so it is nice to have a concrete description (which can be derived from the information above): If $\mathfrak{g} \in \{W, S, H\}$ then

$$\mathfrak{g}_- = \mathfrak{g}_{-1} = \operatorname{span}\{\partial_1, \ldots, \partial_n\},$$

and if $\mathfrak{g} \in \{K\}$ then

$$\mathfrak{g}_- = \mathfrak{g}_{-2} \oplus \mathfrak{g}_{-1} = \operatorname{span}\{D_K(1), D_K(x_1), \ldots, D_K(x_{2m})\}.$$

Let us now gather some facts on automorphisms: It is well known that we have an isomorphism $\operatorname{Aut}(A(n)) \xrightarrow{\sim} \operatorname{Aut}(W(n))$, $\varphi \mapsto \sigma_\varphi$, given by

$$\sigma_\varphi(D) = \varphi \circ D \circ \varphi^{-1}$$

for all $D \in W(n)$. Let G denote the automorphism group of $\mathfrak{g}$. This is a connected algebraic group, and we have

$$G \cong \{g \in \operatorname{Aut}(W(n)) \mid g(\mathfrak{g}) \subseteq \mathfrak{g}\}.$$

Furthermore, we know that ([36], Proposition 3.2)

$$\operatorname{Lie}(G) \cong \widehat{\mathfrak{c}\mathfrak{g}}_{\geq 0}, \tag{2.13}$$

where

$$\widehat{\mathfrak{cg}} = \begin{cases} \widehat{\mathfrak{g}} & \text{if } \mathfrak{g} \in \{W, K\} \\ \widehat{\mathfrak{g}} \oplus F \sum_i x_i \partial_i & \text{if } \mathfrak{g} \in \{S, H\} \end{cases}$$

The following subgroups of G will be very important:

$$G_0 = \{g \in G \mid g(\mathfrak{g}_i) = \mathfrak{g}_i \text{ for all } i\}$$
$$G_r = \{g \in G \mid g(x) - x \in \mathfrak{g}_{\geq r+i} \text{ for all } i \text{ and all } x \in \mathfrak{g}_i\}$$

Here $r \geq 1$ and $\mathfrak{g}_{\geq k} = \oplus_{j \geq k} \mathfrak{g}_j$ for all k. It is well known that

$$G = G_0 \ltimes G_1 \tag{2.14}$$

with G_0 reductive and G_1 the unipotent radical of G. Concretely, we have $G_0 \cong \mathrm{GL}_n$ if $\mathfrak{g} = W(n)$ or $\mathfrak{g} = S(n)$, and $G_0 \cong \mathrm{CSp}_{2m}$ if $\mathfrak{g} = H(2m)$ or $\mathfrak{g} = K(2m+1)$ ([65]). The normal series $G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq 1$ has abelian factor groups $G_j/G_{j+1} \cong \widehat{\mathfrak{g}}_j$, which implies

$$\dim(G) = \dim(G_0) + \dim(G_1) = \dim(G_0) + \dim(\widehat{\mathfrak{g}}_{\geq 1}). \tag{2.15}$$

So the dimension of G can be calculated from knowledge of $\widehat{\mathfrak{g}}$ and the (known) reductive part G_0. For example, if $\mathfrak{g} = W(n)$, we have $\dim(G) = np^n - n$. Note also, that it is a consequence of the semidirect product decomposition (2.14) that $g(\mathfrak{g}_{\geq i}) = \mathfrak{g}_{\geq i}$ for all $g \in G$ and all i. The grading on $\mathfrak{g}$ induces a grading $\mathfrak{g}^* = \bigoplus_i \mathfrak{g}_i^*$ by setting $\mathfrak{g}_i^* = \{\chi \in \mathfrak{g}^* \mid \chi(\mathfrak{g}_j) = 0 \text{ for all } j \neq i\}$. For any $\chi \in \mathfrak{g}^*$ we write χ_i for the component of χ of degree i and χ_- for the sum of components of negative degree. Set $\mathfrak{g}_{\leq i}^* = \bigoplus_{j \leq i} \mathfrak{g}_j^*$, then it follows from $g(\mathfrak{g}_{\geq i}) = \mathfrak{g}_{\geq i}$ and the definition of the coadjoint action, that $g(\mathfrak{g}_{\leq i}^*) = \mathfrak{g}_{\leq i}^*$ for all $g \in G$ and all i.

Inside G_0 we have a one-dimensional torus $T \cong F^*$ corresponding to the nonzero scalar matrices, and this subgroup turns out to be of crucial importance. An easy calculation shows that the action of T on $\mathfrak{g}$ is given by $t.x = t^i x$ for all $t \in T$, $x \in \mathfrak{g}_i$, while the action on $\mathfrak{g}^*$ is given by $t.\chi = t^{-i}\chi$ for $\chi \in \mathfrak{g}_i^*$. Finally, if $\lambda : F^* \to G$ is a one-parameter subgroup of G, we will sometimes write $\lim_{t \to 0} \lambda(t).x = y$ to indicate that the morphism $F^* \to X$, $t \to \lambda(t).x$, extends to a morphism $\lambda' : F \to X$ such that $\lambda'(0) = y$. This implies in particular that $y \in \overline{G.x}$.

2.2 Orbit closures in the Witt algebra $\mathfrak{w}$

When considering the problem of finding an analogue of Veldkamp's Theorem for the restricted Cartan types, the first question is of course: what should we use as replacement for the reductive algebraic group in Theorem 1.6? Well, the natural choice is the automorphism group G (not to be confused with the G in the theorem), but then it is not even clear that $U(\mathfrak{g})^G$, $S(\mathfrak{g})^G$ are contained in $Z(\mathfrak{g})$, $S(\mathfrak{g})^{\mathfrak{g}}$ respectively (cf. the isomorphism (2.13)). However, if we instead consider the G- and $\mathfrak{g}$-action on $S(\mathfrak{g}^*)$, then Skryabin has shown (in an example at the very end of the paper [52]), that in the case $\mathfrak{g} = W(n)$ we do indeed have $S(W(n)^*)^G \subseteq S(W(n)^*)^{W(n)}$, and

$$S(W(n)^*)^{W(n)} \cong S(W(n)^*)^p \otimes_{(S(W(n)^*)^p)^G} S(W(n)^*)^G$$

with $S(W(n)^*)^{W(n)}$ free of rank p^n over $S(W(n)^*)^G$. Even though $\mathfrak{g}$ and $\mathfrak{g}^*$ are not isomorphic as $\mathfrak{g}$-modules (or G-modules), as in the setup of Theorem 1.6, one could perhaps see this result as a reason for cautious optimism. We will show in Section 2.4 that $U(\mathfrak{g})$ *is* contained in the center, and likewise $S(\mathfrak{g})^G \subseteq S(\mathfrak{g})^{\mathfrak{g}}$, but unfortunately in the most uninteresting way possible! As a prelude we determine orbit closures in the *Witt algebra* $\mathfrak{w} = W(1)$ and its dual space under the action of the automorphism group. These results, apart from being of independent interest, provided the inspiration for the more general invariant theoretic considerations in Section 2.4.

We simplify the notation a bit and write $\mathfrak{w} = \mathrm{Der}(F[X]/\langle X^p\rangle)$, with x denoting the class of X in $F[X]/\langle X^p\rangle$ and ∂ denoting differentiation with respect to x. We set $e_i = x^{i+1}\partial$ for $i \in \{-1, \dots, p-2\}$, so that $\{e_{-1}, \dots, e_{p-2}\}$ is an F-basis of $\mathfrak{w}$. Furthermore, we will say that a nonzero w in $\mathfrak{w}$ has degree i if $w \in \mathfrak{w}_{\geq i} \setminus \mathfrak{w}_{\geq i+1}$ (this of course determines the degree uniquely). Since $G = \mathrm{Aut}(\mathfrak{w})$ preserves degree, it also makes sense to speak of the degree of an orbit. Note finally that $G_0 = T$ in this particular case.

The starting point for our calculations is the following theorem, which gives a complete set of representatives for the nonzero orbits in $\mathfrak{w}$ under the action of G:

Theorem 2.4. *A set of representatives for the orbits of degree i is:*

1. $\{e_{-1} + ae_{p-2} \mid a \in F\}$ *if* $i = -1$.
2. $\{ae_0 \mid a \in F^*\}$ *if* $i = 0$.
3. $\{e_i + ae_{2i} \mid a \in F\}$ *if* $1 \leq i < \frac{p-1}{2}$.
4. $\{e_i\}$ *if* $\frac{p-1}{2} \leq i \leq p-2$.

The dimensions of the orbits are:

1'. dim $G.(e_{-1} + ae_{p-2}) = p-1$.

2'. dim $G.ae_0 = p-2$.

3'. dim $G.(e_i + ae_{2i}) = p-i-2$ *if* $1 \leq i < \frac{p-1}{2}$.

4'. dim $G.e_i = p-i-1$ *if* $\frac{p-1}{2} \leq i \leq p-2$.

Cases 3, 3', 4 and 4' were taken care of in [66] as these, along with $G.e_{-1}$ and 0, account for the nilpotent orbits. The proofs of 1 and 2, as well as the corresponding dimension statements, are very similar, but we include them here anyway for the sake of completeness. First, however, some general considerations (for more details, see [66]) that will be used throughout this section and the next: Let $\sigma_\varphi \in G_1$, with $\varphi(x) = x + b_2x^2 + \cdots + b_{p-1}x^{p-1}$ and $\varphi^{-1}(x) = x + c_2x^2 + \cdots + c_{p-1}x^{p-1}$. It is convenient to set $b_1 = c_1 = 1$ and $b_p = c_p = 0$. Using the definition of the isomorphism $\varphi \mapsto \sigma_\varphi$ we get

$$\sigma_\varphi(e_i)(x) = \varphi(x)^{i+1}(1 + 2c_2\varphi(x) + \cdots + (p-1)c_{p-1}\varphi(x)^{p-2}). \tag{2.16}$$

Write $\sigma_\varphi(e_i) = \sum_{j=i}^{p-2} a_j e_j$, then formulas (2.1) and (2.16) tell us that $a_i = 1$ and

$$a_j = (i+1)b_{j-i+1} + (j-i+1)c_{j-i+1} + g_j(b_2, \dots, b_{j-i}, c_2, \dots, c_{j-i}) \tag{2.17}$$

for certain polynomials g_j when $i < j \leq p-2$. We get another useful formula from looking at the coefficient of x^j on the left hand side of the equation $\varphi(\varphi^{-1}(x)) = x$:

$$c_j = -b_j + h_j(b_2, \dots, b_{j-1}, c_2, \dots, c_{j-1}). \tag{2.18}$$

Here the h_j are certain polynomials and $2 \leq j \leq p-1$. By induction we see that c_j can be expressed as a polynomial in $b_2, \dots, b_j$, and inserting into (2.17) yields

$$a_j = (2i-j)b_{j-i+1} + g'_j(b_2, \dots, b_{j-i}). \tag{2.19}$$

Now we are ready for the

Proof of Theorem 2.4. We start with case 2: Note first that $t.e_0 = e_0$ for all $t \in T$, and this easily implies that ae_0 and be_0 are in the same orbit if and only if $a = b$. Now let $w = w_0 e_0 + \cdots + w_{p-2}e_{p-2}$ with $w_0 \neq 0$. With notation as above, formula (2.19) shows that we can choose $b_2, \dots, b_{p-1} \in F$ recursively such that $\sigma_\varphi(e_0) = e_0 + \frac{w_1}{w_0}e_1 + \cdots + \frac{w_{p-2}}{w_0}e_{p-2}$. But then $\sigma_\varphi(w_0 e_0) = w$ and we are done. This argument actually shows that

$$G.ae_0 = \{ae_0 + a_1e_1 + \cdots + a_{p-2}e_{p-2} \mid a_1, \dots, a_{p-2} \in F\} \cong \mathbb{A}^{p-2}, \tag{2.20}$$

from which 2' follows. As for case 1, look at $y = y_{-1}e_{-1} + \cdots + y_{p-2}e_{p-2}$ with $y_{-1} \neq 0$. Again we can find $b_2, \dots, b_{p-1}$ such that $\sigma_\varphi(e_{-1}) = e_{-1} + y_0 e_0 + y_{-1}y_1 e_1 + \cdots + y_{-1}^{p-3}y_{p-3}e_{p-3} + g'_{p-2}(b_2, \dots, b_{p-1})e_{p-2}$. Choosing $a = y_{-1}^{p-2}y_{p-2} - g'_{p-2}(b_2, \dots, b_{p-1})$ we get

$$\sigma_\varphi(e_{-1} + ae_{p-2}) = e_{-1} + y_0 e_0 + y_{-1}y_1 e_1 + \cdots + y_{-1}^{p-2}y_{p-2}e_{p-2},$$

since $\sigma_\varphi(e_{p-2}) = e_{p-2}$. Now we apply the element $y_{-1}^{-1} \in T$ and get $y_{-1}^{-1}.\sigma_\varphi(e_{-1} + ae_{p-2}) = y$. Thus every element of degree -1 is in the orbit of $e_{-1} + ae_{p-2}$ for some a. It remains only to show that $e_{-1} + ae_{p-2}$ and $e_{-1} + be_{p-2}$ are in the same orbit if and only if $a = b$, and here one can use exactly the same method as in the proof of Proposition 3.4 in [66] (it is also a consequence of the proof of case 1 in the next theorem). Similarly, one can mimic the proof of Theorem 4.1 in said paper to show that $G.(e_{-1} + ae_{p-2})$ has trivial stabilizer in G, which implies

$$\dim(G.(e_{-1} + ae_{p-2})) = \dim(G) = p-1$$

□

The next theorem provides the full picture on orbit closures in the Witt algebra:

Theorem 2.5. *Let $a \in F$ and define $B = \{b \in F \mid b^{p-1} = -a\}$. We have*

1. $$\overline{G.(e_{-1} + ae_{p-2})} = \begin{cases} G.(e_{-1} + ae_{p-2}) \cup \left(\bigcup_{b \in B} G.be_0\right) & \text{if } a \neq 0 \\ G.e_{-1} \cup \mathfrak{w}_{\geq 1} & \text{if } a = 0 \end{cases}.$$

2. $\overline{G.ae_0} = G.ae_0$.

3. $\overline{G.(e_i + ae_{2i})} = G.(e_i + ae_{2i}) \cup \mathfrak{w}_{\geq i+2}$ *if* $1 \leq i < \frac{p-1}{2}$.

4. $\overline{G.e_i} = \mathfrak{w}_{\geq i}$ *if* $\frac{p-1}{2} \leq i \leq p-2$.

Cases 2 and 4 are more or less trivial: In the former case, equation (2.20) shows that $G.ae_0$ is a Zariski-closed subset of $\mathfrak{w}$ for all $a \in F$, and in the latter case we must have $G.e_i = \mathfrak{w}_{\geq i} \setminus \mathfrak{w}_{\geq i+1}$, which easily implies $\overline{G.e_i} = \mathfrak{w}_{\geq i}$. For orbits of type 1 or 3 we need to work considerably harder: Assume first that $1 \leq i < \frac{p-1}{2}$. The case $i = 1$ turns out to be degenerate, so we will save that for later and also assume $i \neq 1$. The following proposition provides further information about the action of G_1 on $e_i + ae_{2i}$. Note that we will sometimes represent an element $w \in \mathfrak{w}$ by its coordinates $(w_{-1}, \ldots, w_{p-2})$ with respect to the basis $\{e_i\}$.

Proposition 2.6.

$$G_1.(e_i + ae_{2i}) = \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ a_{i+1} \\ \vdots \\ a_{2i-1} \\ f(a_{i+1}, \ldots, a_{2i-1}) + a \\ a_{2i+1} \\ \vdots \\ a_{p-2} \end{pmatrix} \right\}.$$

Here $a_{i+1}, \ldots, \hat{a}_{2i}, \ldots, a_{p-2} \in F$, *and* $f \in F[X_{i+1}, \ldots, X_{2i-1}]$ *is a polynomial with the following properties:*

1. *If* $X_{i+1}^{\alpha_{i+1}} \cdots X_{2i-1}^{\alpha_{2i-1}}$ *is a monomial appearing in* f *with nonzero coefficient, then*

$$\sum_{j=i+1}^{2i-1} (j-i)\alpha_j = i.$$

2. *The (usual) degree of* f *is at most* i, *and the component in* f *of degree* i *is* cX_{i+1}^i *for some* $c \in F$.

Note that the proposition *does not* say that $c \neq 0$. This actually turns out to be the case – and of crucial importance – but we are not able to prove it yet.

Proof of Proposition 2.6. We use the notation from the discussion preceding the proof of Theorem 2.4. Because of the bijection $\varphi \mapsto \sigma_\varphi$ we can consider G_1 as a variety isomorphic to $\mathbb{A}^{p-2}$ with coordinate functions $b_2, \ldots b_{p-1}$. Grade the

polynomial ring $F[G_1]$ by setting $\deg(b_s) = s-1$ for $2 \leq s \leq p-1$. Looking closer at the equation $\varphi(\varphi^{-1}(x)) = x$ we can refine formula (2.18) a bit to get $c_2 = -b_2$ and

$$c_n = -b_n + \sum_{s=2}^{n-1} c_s \sum_{n_1+\cdots+n_s=n} b_{n_1} \cdots b_{n_s}$$

for $n > 2$. From this it follows easily by induction that $c_2, \ldots, c_{p-1} \in F[G_1]$, and that c_s is homogeneous of degree $s-1$. Equation (2.16) shows that a_j, $i < j \leq p-2$, can be written as a sum of terms $b_{s_1} \cdots b_{s_{i+1}} c_l b_{t_1} \cdots b_{t_{l-1}}$ where $s_1+\cdots+s_{i+1}+t_1+\cdots+t_{l-1} = j+1$. Since such a term has degree

$$\sum_{n=1}^{i+1}(s_n - 1) + (l-1) + \sum_{m=1}^{l-1}(t_m - 1) = j - i$$

we see that $a_j \in F[G_1]$ is homogeneous of degree $j-i$. Furthermore, changing the indices in (2.19) gives us $a_{s+i-1} = (i-s+1)b_s + h(b_2, \ldots, b_{s-1})$ for $2 \leq s \leq i$ and some polynomial h, from which it follows by induction that

$$F[a_{i+1}, \ldots, a_{s+i-1}] = F[b_2, \ldots, b_s]. \tag{2.21}$$

Now let $\sigma_\varphi(e_i + ae_{2i}) = (0, \ldots, 0, 1, a_{i+1}, \ldots, a_{p-2})$ (this is a slight abuse of notation, but notice that the new a_j agree with the old when $i < j < 2i$). Equation (2.19) shows that we can recursively choose $b_2, \ldots, b_i$ to make $a_{i+1}, \ldots, a_{2i-1}$ attain any set of values in F. But $a_{2i} = g'_{2i}(b_2, \ldots, b_i) + a$, and expressing $b_2, \ldots, b_i$ as polynomials in $a_{i+1}, \ldots, a_{2i-1}$ – which is possible because of (2.21) – we get $a_{2i} = f(a_{i+1}, \ldots, a_{2i-1}) + a$ for some polynomial $f \in F[X_{i+1}, \ldots, X_{2i-1}]$. The coordinates $a_{2i+1}, \ldots, a_{p-2}$ can again be assigned arbitrary values by choosing $b_{i+1}, \ldots, b_{p-1}$ accordingly. As for properties 1 and 2, we have shown that $f(a_{i+1}, \ldots, a_{2i-1})$ is homogeneous of degree $2i - i = i$ when considered as an element of $F[G_1]$. But since each of the a_j is homogeneous of degree $j-i$ we get 1, from which 2 follows directly. □

Write $f = f_0 + \cdots + f_i$, where f_j is the component in f of degree j. In particular we have $f_i = cX_{i+1}^i$. Now we are ready to describe the G-orbit of $e_i + ae_{2i}$:

Proposition 2.7.

$$G.(e_i + ae_{2i}) = \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ b_i \\ \vdots \\ b_{2i-1} \\ \sum_{j=0}^{i} \frac{f_j(b_{i+1},\ldots,b_{2i-1})}{b_i^{j-1}} + ab_i^2 \\ b_{2i+1} \\ \vdots \\ b_{p-2} \end{pmatrix} \right\}. \tag{2.22}$$

Here $b_i, \ldots, \hat{b}_{2i}, \ldots, b_{p-2} \in F$ *with* $b_i \neq 0$.

Proof. We have $G.(e_i + ae_{2i}) = T.(G_1.(e_i + ae_{2i}))$, so let us look at the action of $t \in T$ on $w \in G_1.(e_i + ae_{2i})$:

$$t.w = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ t^i \\ t^{i+1}a_{i+1} \\ \vdots \\ t^{2i}(f(a_{i+1}, \ldots, a_{2i-1}) + a) \\ \vdots \\ t^{p-2}a_{p-2} \end{pmatrix}$$

for some $a_{i+1}, \ldots, \hat{a}_{2i}, \ldots, a_{p-2} \in F$. It follows from property 1 in Proposition 2.6 that

$$t^i f(a_{i+1}, \ldots, a_{2i-1}) = f(ta_{i+1}, t^2 a_{i+2}, \ldots, t^{i-1}a_{2i-1}). \tag{2.23}$$

Writing $b_i = t^i, b_{i+1} = t^{i+1}a_{i+1}, \ldots, b_{p-2} = t^{p-2}a_{p-2}$ (skipping b_{2i}) and using (2.23), the $2i$th coordinate in $t.w$ becomes

$$\begin{aligned} &t^{2i}(f(a_{i+1}, \ldots, a_{2i-1}) + a) \\ &\quad = b_i f\left(\frac{b_{i+1}}{b_i}, \ldots, \frac{b_{2i-1}}{b_i}\right) + ab_i^2 = \sum_{j=0}^{i} \frac{f_j(b_{i+1}, \ldots, b_{2i-1})}{b_i^{j-1}} + ab_i^2. \end{aligned}$$

So we get a point like on the right hand side of (2.22). By simply reversing the process we see that every point of this kind is in $G.(e_i + ae_{2i})$. □

We will now ignore the first $i+1$ coordinates (since they are all zero anyway) and consider $G.(e_i + ae_{2i})$ as a subset of $\mathbb{A}^{p-i-1}$. A general remark: for any polynomial f in n variables, we write $V(f)$ for the zero set of f in $\mathbb{A}^n$. With this notation we have:

Corollary 2.8.

$$G.(e_i + ae_{2i}) = \{w \in V(X_{2i}X_i^{i-1} - cX_{i+1}^i - \sum_{j=0}^{i-1} X_i^{i-j} f_j - aX_i^{i+1}) \mid w_i \neq 0\}.$$

Proof. This follows directly from Proposition 2.7. □

We are almost ready to determine the orbit closure, but we need the following simple **algebraic geometric fact**: If $f \in F[X_1, \ldots, X_n]$ is a polynomial satisfying $X_j \nmid f$ for some $j \in \{1, \ldots, n\}$ and $A = \{x \in V(f) \mid x_j \neq 0\}$, then $\overline{A} = V(f)$. To prove this it is enough to show that A intersects every component of $V(f)$, so assume there is a component $V(f')$ of $V(f)$ (with f' an irreducible polynomial dividing f) such that $A \cap V(f') = \emptyset$. Then $x_j = 0$ for every $x \in V(f')$, and we must have $V(f') \subseteq V(X_j)$. But this means $(X_j) \subseteq (f')$ and so f' divides X_j, which can only happen if $f' = \alpha X_j$ for some $\alpha \neq 0$, a contradiction. The well known fact that the closure of an orbit is a union of the orbit itself and certain other orbits of strictly lower dimension will also be used several times.

Proposition 2.9.

$$\overline{G.(e_i + ae_{2i})} = V(X_{2i}X_i^{i-1} - cX_{i+1}^i - \sum_{j=0}^{i-1} X_i^{i-j} f_j - aX_i^{i+1})$$

and $c \neq 0$.

Proof. Let g denote the polynomial on the right hand side, and write $g = X_i^s g'$ with $X_i \nmid g'$. It follows easily from Corollary 2.8 and the aforementioned algebraic geometric fact that $\overline{G.(e_i + ae_{2i})} = V(g')$. We prove the proposition using descending induction in i: Assume first that $i = \frac{p-1}{2} - 1$. To reach a contradiction we also assume $c = 0$. Then g' cannot contain a term of the form βX_{i+1}^m (for some $\beta \neq 0, m > 0$) because of property 1 in Proposition 2.6, so we must have a point $w \in V(g')$ with $w_i = 0$, $w_{i+1} \neq 0$. It follows that $\overline{G.e_{(p-1)/2}} \subsetneq \overline{G.(e_i + ae_{2i})}$, but this is impossible since the dimension of the two varieties is the same (Theorem 2.4). Therefore $c \neq 0$ and $\overline{G.(e_i + ae_{2i})} = V(g') = V(g)$.

Assume now that the claim is true for $i+1$, and that $c = 0$ when we calculate $G.(e_i + ae_{2i})$. Exactly as before we can find a $w \in V(g')$ satisfying $w_i = 0$, $w_{i+1} \neq 0$. This means that there exists $a' \in F$ such that $\overline{G.(e_{i+1} + a'e_{2(i+1)})} \subseteq \overline{G.(e_i + ae_{2i})}$, and by induction we know

$$\overline{G.(e_{i+1} + a'e_{2(i+1)})} = V(X_{2(i+1)}X_{i+1}^i - c'X_{i+2}^{i+1} - \sum_{j=0}^{i} X_{i+1}^{i+1-j} f_j' - a'X_{i+1}^{i+2})$$

where the f'_j are certain homogeneous polynomials in $X_{i+2}, \ldots, X_{2i+1}$ and $c' \neq 0$. Let h denote the polynomial on the right hand side. Notice that h is irreducible: It is a first degree polynomial in $X_{2(i+1)}$, and the coefficients have no common factors, thanks to c' being different from zero. If we set $g'' = g'(0, X_{i+1}, \ldots, X_{2i})$, then $\overline{G.(e_{i+1} + a'e_{2(i+1)})} \subseteq \overline{G.(e_i + ae_{2i})}$ means that $V(h) \subseteq V(g'')$, so h divides g''. By looking at the degree of the two polynomials in the variable X_{i+1} this is seen to be impossible, and so $c \neq 0$ and we are done. □

Proof of case 3 in Theorem 2.5. Combining Corollary 2.8 and Proposition 2.9 we get

$$\overline{G.(e_i + ae_{2i})} = G.(e_i + ae_{2i}) \cup \{w \in V(g) \mid w_i = 0\}.$$

Since $g(0, X_{i+1}, \ldots, X_{2i}) = -cX_{i+1}^i$ we see that $\{w \in V(g) \mid w_i = 0\} = \mathfrak{w}_{\geq i+2}$, and so

$$\overline{G.(e_i + ae_{2i})} = G.(e_i + ae_{2i}) \cup \mathfrak{w}_{\geq i+2}.$$

This is true also for the degenerate case $i = 1$: Here we get $f = 0$ in the setup of Proposition 2.6, and inserting this in Proposition 2.7 gives us

$$G.(e_1 + ae_2) = \{w \in V(X_2 - aX_1^2) \mid w_1 \neq 0\}.$$

Using the remark preceding Proposition 2.9 we conclude that $\overline{G.(e_1 + ae_2)} = G.(e_1 + ae_2) \cup \mathfrak{w}_{\geq 3}$. □

The last case in Theorem 2.5 could be proved using a similar method, but there is an easier way:

Proof of case 1 in Theorem 2.5. The statement for $a = 0$ was proved in [66], so assume $a \neq 0$. For an arbitrary $\lambda \in F$ we define

$$\mathfrak{w}(\lambda) = \{w \in \mathfrak{w} \mid w^{[p]} = \lambda w\} \setminus \{0\}.$$

The idea of the proof is to describe the set $\mathfrak{w}(-a)$ in two different ways. First we claim that

$$\mathfrak{w}(-a) = G.(e_{-1} + ae_{p-2}) \cup \Big(\bigcup_{b \in B} G.be_0\Big). \tag{2.24}$$

To show this, note first that the sets $\mathfrak{w}(\lambda)$ are G-invariant: For $w \in \mathfrak{w}(\lambda)$ and $g \in G$ we have

$$g(w)^{[p]} = g(w^{[p]}) = g(\lambda w) = \lambda g(w).$$

Set $D = e_{-1} + ae_{p-2}$. By an easy induction in i we get

$$D^i(x) = a\frac{(p-1)!}{(p-i)!}x^{p-i}$$

for $2 \leq i \leq p-1$. In particular $D^{p-1}(x) = a(p-1)!x = -ax$ by Wilson's Theorem, so $D^p(x) = D(-ax) = -aD(x)$. Since elements in $\mathfrak{w}$ are uniquely determined by their value on x, we get $D^p = -aD$, which implies $G.D \subseteq \mathfrak{w}(-a)$. Now let $b \in F$

with $b^{p-1} = -a$. One easily checks that $e_0^{[p]} = e_0$, and from this it follows that $(be_0)^{[p]} = b^p e_0^{[p]} = -a(be_0)$. So $G.be_0 \subseteq \mathfrak{w}(-a)$ and we have shown:

$$\mathfrak{w}(-a) \supseteq G.(e_{-1} + ae_{p-2}) \cup \Big(\bigcup_{b \in B} G.be_0\Big). \tag{2.25}$$

Since $\mathfrak{w}(0) = (G.e_{-1} \cup \mathfrak{w}_{\geq 1}) \setminus \{0\}$ ([66], Lemma 3.1) we see that every nonzero element of $\mathfrak{w}$ is contained in some $\mathfrak{w}(\lambda)$. But $\mathfrak{w}(\lambda) \cap \mathfrak{w}(\mu) = \emptyset$ whenever $\lambda \neq \mu$, and this implies equality in (2.25).

Now consider $w \in \mathfrak{w}$ as an endomorphism of $A(1)$, and write $\mathrm{char}(w)$ for its characteristic polynomial. Corollary 1 in [42] gives us

$$\mathrm{char}(w) = X^p + \varphi(w_{-1}, \ldots, w_{p-2})X = X(X^{p-1} + \varphi(w_{-1}, \ldots, w_{p-2})),$$

where φ is a nonzero homogeneous polynomial of degree $p-1$. Our second claim is that

$$\mathfrak{w}(-a) = V(\varphi - a). \tag{2.26}$$

Assume first that $w \in \mathfrak{w}(-a)$. Then w is semisimple considered as an endomorphism of $A(1)$ ([58], Proposition 3.3). In particular w has a nonzero eigenvalue $\mu \in F^*$, and using the definition of $\mathfrak{w}(-a)$ one checks that $\mu^{p-1} = -a$. Inserting μ into the characteristic polynomial of w gives us $w \in V(\varphi - a)$. Next, assume this is true. Then w is not nilpotent, and therefore it is contained in $\mathfrak{w}(\lambda)$ for some $\lambda \neq 0$. But then any nonzero eigenvalue μ of w satisfies both $\mu^{p-1} = \lambda$ and $\mu^{p-1} = -a$. So $\lambda = -a$ and we have shown (2.26).

We are now ready to complete the proof: Since the $\mathfrak{w}(\lambda)$ are closed, it follows from (2.24) that $\overline{G.(e_{-1} + ae_{p-2})} \subseteq \mathfrak{w}(-a)$. Assume for some $b \in F$ with $b^{p-1} = -a$ that $G.be_0$ is not in the closure of $G.(e_{-1} + ae_{p-2})$. Then we see from (2.24) that $G.be_0$ must be an irreducible component of $\mathfrak{w}(-a)$, of dimension $p-2$ (Theorem 2.4). But the description in (2.26) shows that every component of $\mathfrak{w}(-a)$ has dimension $p-1$ (see [25], Theorem 3.3). This contradiction implies $\overline{G.(e_{-1} + ae_{p-2})} = \mathfrak{w}(-a)$, and we are done. □

2.3 Orbit closures in $\mathfrak{w}^*$

Let $\{e'_{-1}, \ldots, e'_{p-2}\}$ denote the basis of $\mathfrak{w}^*$ dual to the basis $\{e_{-1}, \ldots, e_{p-2}\}$ of $\mathfrak{w}$. So $e'_i(e_j) = \delta_{ij}$ for $i, j \in \{-1, \ldots, p-2\}$. We define the *height* $r(\chi)$ of a character $\chi \in \mathfrak{w}^*$ by

$$r(\chi) = \begin{cases} \min\{i \in \{-1, \ldots, p-2\} \mid \chi_{|\mathfrak{w}_{\geq i}} = 0\} & \text{if } \chi(e_{p-2}) = 0 \\ p-1 & \text{if } \chi(e_{p-2}) \neq 0. \end{cases}$$

The notion of height has become standard in the literature on the Witt algebra and its representations, so we will use it in what follows, even though it would have been more in keeping with what we did for $\mathfrak{w}$ to use the height minus one. Of course,

since G preserves height, we have a well-defined notion of height for the orbits as well. Now recall the notation introduced right after Theorem 2.4: For $\sigma_\varphi \in G_1$ we write $\varphi(x) = x + b_2x^2 + \cdots + b_{p-1}x^{p-1}$ and $\varphi^{-1}(x) = x + c_2x^2 + \cdots + c_{p-1}x^{p-1}$. Using the definition of the action we get $\sigma_\varphi^{-1}(e'_i) = \sum_{j=-1}^{i} a_j e'_j$ where $a_i = 1$ and a_j $(-1 \leq j \leq i-1)$ is the coefficient of x^{i+1} in $\sigma_\varphi(e_j)(x)$. More precisely we have (see equation (2.16))

$$a_j = (j+1)b_{i-j+1} + (i-j+1)c_{i-j+1} + p_j(b_2, \ldots, b_{i-j}, c_2, \ldots, c_{i-j})$$

where $-1 \leq j \leq i-1$ and the p_j are certain polynomials. Applying formula (2.18) to express the c_k in terms of the b_k, we get

$$a_j = (2j-i)b_{i-j+1} + p'_j(b_2, \ldots, b_{i-j}) \tag{2.27}$$

It should also be noted that the action of the torus is now given by $t.e'_i = t^{-i}e'_i$ for $t \in T$.

A complete set of representatives for the nonzero orbits in $\mathfrak{w}^*$ is given by the following theorem, which is essentially due to Feldvoss and Nakano ([21]), but with some additions and corrections:

Theorem 2.10. *For any $j \in \mathbb{N}$, let $F^{(j)} \subseteq F$ denote a set of representatives for the equivalence classes of the equivalence relation on F given by: $x \sim y \Leftrightarrow x^j = y^j$. A set of representatives for the orbits of height i in $\mathfrak{w}^*$ is:*

1. $\{ae'_0 \mid a \in F^*\}$ *if* $i = 1$.
2. $\{e'_{i-1}\}$ *if* $0 \leq i \leq p-3$ *and i is even.*
3. $\{e'_{i-1} + ae'_{\frac{i-1}{2}} \mid a \in F^{(2)}\}$ *if* $3 \leq i \leq p-2$ *and i is odd.*
4. $\{e'_{p-2} + ae'_{-1} \mid a \in F^{(p-2)}\}$ *if* $i = p-1$.

Furthermore, the dimensions of the orbits are:

1'. dim $G.ae'_0 = 1$.

2'. dim $G.e'_{i-1} = i+1$ *if* $0 \leq i \leq p-3$ *and i is even.*

3'. dim $G.(e'_{i-1} + ae'_{\frac{i-1}{2}}) = i$ *if* $3 \leq i \leq p-2$ *and i is odd.*

4'. dim $G.(e'_{p-2} + ae'_{-1}) = p-1$.

Proof. Case 1 is analogous to 2 in Theorem 2.4 and proved in exactly the same way, while case 2 was proved in [21]. Here it was also shown that if $3 \leq i \leq p-2$ and i is odd, then every character of height i is in the orbit of some $e'_{i-1} + ae'_{(i-1)/2}$, but Feldvoss and Nakano actually gave incorrect results in cases 1 and 3, having seemingly overlooked the action of T (this was already remarked in [49]). Now assume $e'_{i-1} + ae'_{(i-1)/2}$ and $e'_{i-1} + a'e'_{(i-1)/2}$ are in the same orbit, for some $a, a' \in F$. So there exists

$g = t \circ \sigma_\varphi \in G$ (with $t \in T$, $\sigma_\varphi \in G_1$) such that $g.(e'_{i-1} + ae'_{(i-1)/2}) = e'_{i-1} + a'e'_{(i-1)/2}$, or equivalently,

$$\sigma_\varphi.(e'_{i-1} + ae'_{\frac{i-1}{2}}) = t^{i-1}e'_{i-1} + t^{\frac{i-1}{2}}a'e'_{\frac{i-1}{2}}.$$

If the coefficients of $e'_{i-2}, \ldots, e'_{(i-1)/2+1}$ in $\sigma_\varphi.(e'_{i-1} + ae'_{(i-1)/2})$ are all zero, then the coefficient of $e'_{(i-1)/2}$ must be a (look at equation (2.27)). So we get $t^{i-1} = 1$ and $a = t^{\frac{i-1}{2}}a'$. Raising this last equation to the second power yields $a^2 = (a')^2$. If on the other hand this is true, i.e., $a' = \pm a$, then it is easily seen that $e'_{i-1} + ae'_{(i-1)/2}$ and $e'_{i-1} + a'e'_{(i-1)/2}$ are in the same orbit (in the case $a' = -a$ just find $t \in T$ satisfying $t^{-\frac{i-1}{2}} = -1$ and let it act on $e'_{i-1} + ae'_{(i-1)/2}$). This proves case 3, and case 4 is proved in the same way. As for the dimension statements, the first two cases are straightforward, and one simply adapts the proof of Theorem 4.1 in [66] for the last two. We will give an outline of the steps needed in case 3': Write $\chi = e'_{i-1} + ae'_{(i-1)/2}$. Then we have

$$G_\chi = (G_\chi \cap T) \ltimes (G_\chi \cap G_1).$$

To prove this, it is enough to show that if $t^{-1} \in T$, $u \in G_1$ and $t^{-1} \circ u \in G_\chi$, then $t^{-1}, u \in G_\chi$. Let $u.\chi = e'_{i-1} + a_{i-2}e'_{i-2} + \cdots + a_{-1}e'_{-1}$. We get $(t^{-1} \circ u).\chi = t^{i-1}e'_{i-1} + t^{i-2}a_{i-2}e'_{i-2} + \cdots + t^{-1}a_{-1}e'_{-1}$, and since we assume $t^{-1} \circ u \in G_\chi$ we must have $a_{i-2}, \ldots, \hat{a}_{(i-1)/2}, \ldots, a_{-1} = 0$. It now follows from equation (2.28) on the next page that $a_{(i-1)/2} = a$. So $u \in G_\chi$, which easily implies that $t^{-1} \in G_\chi$ too.

Setting $G' = G_\chi \cap T$ and $G'' = G_\chi \cap G_1$, it can be shown that

$$\begin{aligned} G' &= \{t \in T \mid t^{\frac{i-1}{2}} = 1\}, \\ G'' &= \{\sigma_\varphi \in G_1 \mid \varphi(x) = x + b_{i+1}x^{i+1} + \cdots + b_{p-1}x^{p-1}\}. \end{aligned}$$

But then $\dim G_\chi = \dim G' + \dim G'' = p - i - 1$, which implies

$$\dim G.\chi = \dim G - \dim G_\chi = i. \qquad \square$$

Now we determine the closures in $\mathfrak{w}^*$ of orbits of all heights except $p - 1$:

Theorem 2.11. *Let $a \in F$. We have:*

1. $\overline{G.ae'_0} = G.ae'_0$.
2. $\overline{G.e'_{i-1}} = \{\chi \in \mathfrak{w}^* \mid r(\chi) \leq i\}$ *if* $0 \leq i \leq p-3$ *and i is even.*
3. $\overline{G.(e'_{i-1} + ae'_{\frac{i-1}{2}})} = G.(e'_{i-1} + ae'_{\frac{i-1}{2}}) \cup \{\chi \in \mathfrak{w}^* \mid r(\chi) \leq i-2\}$ *if* $3 \leq i \leq p-2$ *and i is odd.*

Proof. Cases 1 and 2 are trivial, so let us concentrate on case 3: Since the procedure is similar to the one we used to prove case 3 in Theorem 2.5 we will omit quite a few details. Write $s = \frac{i-1}{2}$ and $\sigma_\varphi^{-1}.e'_{i-1} = \sum_{j=-1}^{i-1} a_j e'_j$. We grade the polynomial ring $k[G_1] = k[b_2, \ldots, b_{p-1}]$ by setting $\deg(b_s) = s - 1$. Then it is easily shown that

$a_{-1}, \ldots, a_{i-2} \in F[G_1]$, and that a_j is homogeneous of degree $i-j-1$. Proceeding exactly as in the proof of Proposition 2.6, we get

$$G_1.(e'_{i-1} + ae'_s) = \left\{ \begin{pmatrix} a_{-1} \\ \vdots \\ a_{s-1} \\ f(a_{s+1}, \ldots, a_{i-2}) + a \\ a_{s+1} \\ \vdots \\ a_{i-2} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\} \tag{2.28}$$

where $a_{-1}, \ldots, \hat{a}_{2s}, \ldots, a_{i-2} \in F$ and $f \in F[X_{s+1}, \ldots, X_{i-2}]$ is a polynomial satisfying the following properties:

1. If $X_{s+1}^{\alpha_{s+1}} \cdots X_{i-2}^{\alpha_{i-2}}$ is a monomial appearing in f with nonzero coefficient, then

$$\sum_{j=s+1}^{i-2} (i-j-1)\alpha_j = s.$$

2. The (usual) degree of f is at most s, and the component in f of degree s is cX_{i-2}^s for some $c \in F$.

One can now write $f = f_0 + \cdots + f_s$ (f_j being the component in f of degree j) and repeat the proof of Proposition 2.7 to get

$$G.(e'_{i-1} + ae'_s) = \left\{ \begin{pmatrix} b_{-1} \\ \vdots \\ b_{s-1} \\ \sum_{j=0}^{s} \frac{f_j(b_{s+1}, \ldots, b_{i-2})}{b_{i-1}^{j-1}} \pm a\sqrt{b_{i-1}} \\ b_{s+1} \\ \vdots \\ b_{i-1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\}$$

where $b_{-1}, \ldots, \hat{b}_s, \ldots, b_{i-1} \in F$ and $b_{i-1} \neq 0$. It follows directly that

$$G.(e'_{i-1} + ae'_s)$$
$$= \{x \in V((X_s X_{i-1}^{s-1} - cX_{i-2}^s - \sum_{j=0}^{s-1} X_{i-1}^{s-j} f_j)^2 - a^2 X_{i-1}^{2s-1}) \mid x_{i-1} \neq 0\}.$$

If $c = 0$ then $\overline{G.e'_{i-2}} \subsetneq \overline{G.(e'_{i-1} + ae'_s)}$, just as in the proof of Proposition 2.9, but this is a contradiction since the dimension of the two varieties is the same. So $c \neq 0$ and the theorem follows easily. □

It remains only to determine the orbit closures of characters of height $p-1$. This case turns out to be the hardest, and the strongest statement we can prove is:

Proposition 2.12. *Either* $\overline{G.e'_{p-2}} = G.e'_{p-2} \cup \{\chi \in \mathfrak{w}^* \mid r(\chi) \leq p-3\}$ *or* $\overline{G.e'_{p-2}} = G.e'_{p-2} \cup G.e'_{p-3} \cup \{\chi \in \mathfrak{w}^* \mid r(\chi) \leq p-3\}$. *If the former is true, then*

$$\overline{G.(e'_{p-2} + ae'_{-1})} = G.(e'_{p-2} + ae'_{-1}) \cup \{\chi \in \mathfrak{w}^* \mid r(\chi) \leq p-3\} \tag{2.29}$$

for all $a \in F$.

Proof. Applying the usual method, we get

$$G.(e'_{p-2} + ae'_{-1})$$
$$= \{x \in V((X_{-1} X_{p-2}^{p-2} - cX_{p-3}^{p-1} - q)^{p-2} - a^{p-2} X_{p-2}^{(p-2)(p-2)-1}) \mid x_{p-2} \neq 0\},$$

where $q = \sum_{j=1}^{p-2} X_{p-2}^{p-1-j} f_j$ and f_j is a homogeneous polynomial of degree j. Furthermore, if $X_0^{\alpha_0} \cdots X_{p-3}^{\alpha_{p-3}}$ is a monomial appearing in any of the f_j with non-zero coefficient, then

$$\sum_{k=0}^{p-3} (p-2-k)\alpha_k = p-1. \tag{2.30}$$

We would like to prove $c \neq 0$, but this time we cannot use a dimension argument (notice that the dimension of an orbit of height $p-2$ is *one less* than the dimension of $\overline{G.(e'_{p-2} + ae'_{-1})}$), nor look at the degree of the polynomials defining the orbits (as in Proposition 2.9), to derive a contradiction. It is, however, possible to say something meaningful when $a = 0$. In this case we have

$$G.e'_{p-2} = \{x \in V(X_{-1} X_{p-2}^{p-2} - cX_{p-3}^{p-1} - \sum_{j=1}^{p-2} X_{p-2}^{p-1-j} f_j) \mid x_{p-2} \neq 0\}.$$

If $c \neq 0$, then the orbit closure is equal to the zero set of the polynomial on the right hand side, which is exactly $G.e'_{p-2} \cup \{\chi \in \mathfrak{w}^* \mid r(\chi) \leq p-3\}$, and the same argument for arbitrary a gives us (2.29). Now assume $c = 0$ and let l be the maximal number satisfying $f_l \neq 0$. Then we get

$$\overline{G.e'_{p-2}} = V(X_{-1} X_{p-2}^{l-1} - \sum_{j=1}^{l} X_{p-2}^{l-j} f_j).$$

The polynomial on the right hand side will be denoted by f'. It follows, as in the proof of Proposition 2.9, that an orbit $G.(e'_{p-3} + a'e_{(p-3)/2})$ is contained in $\overline{G.e'_{p-2}}$. Assume $a' \neq 0$. Note that $G.e_{p-2}$ is invariant under multiplication by scalars different from zero, and the same is then true for the closure. Since $b(G.(e'_{p-3} + a'e_{(p-3)/2})) = G.(e'_{p-3} + \sqrt{b}a'e_{(p-3)/2})$ for any $b \neq 0$ we infer that

$$\bigcup_{b\neq 0} G.(e'_{p-3} + be_{\frac{p-3}{2}}) \subseteq \overline{G.e'_{p-2}}.$$

But the set on the left hand side is open in $\{\chi \in \mathfrak{w}^* \mid r(\chi) \leq p-2\}$, and since this set is irreducible we have

$$\{\chi \in \mathfrak{w}^* \mid r(\chi) \leq p-2\} \subsetneq \overline{G.e'_{p-2}}.$$

But the dimension of both these varieties is $p-1$, which is a contradiction. This means that a' cannot be zero, and so $G.e'_{p-3} \subseteq \overline{G.e'_{p-2}}$. From the proof of Theorem 2.11 we get

$$\overline{G.e'_{p-3}} = V(X_s X_{p-3}^{s-1} - c'X_{p-4}^s - \sum_{j=1}^{s-1} X_{p-3}^{s-j} g_j),$$

where $s = (p-3)/2$, $c' \neq 0$ and the polynomial on the right hand side – let us call it g – is irreducible. Also, every monomial $X_0^{\alpha_0} \cdots X_{p-3}^{\alpha_{p-3}}$ appearing in g with non-zero coefficient satisfies $\sum_{k=0}^{p-3}(p-3-k)\alpha_k = s$. The inclusion $\overline{G.e'_{p-3}} \subseteq \overline{G.e'_{p-2}}$ implies that g divides $f'(X_0, \ldots, X_{p-3}, 0) = f_l$, so we can write $f_l = gh$ for some polynomial h. Now grade the polynomial ring in the X_j by letting the degree of X_j be $p-2-j$. Then f_l is homogeneous of degree $p-1$, and for a monomial $X_0^{\alpha_0} \cdots X_{p-3}^{\alpha_{p-3}}$ appearing in g we have

$$\sum_{j=0}^{p-3}(p-2-j)\alpha_j = \sum_{j=0}^{p-3}(p-3-j)\alpha_j + \sum_{j=0}^{p-3}\alpha_j = 2s = p-3,$$

so g is homogeneous of degree $p-3$ (note that we use the fact that g is homogeneous of degree s in the usual sense for the second equality). It follows that h is homogeneous of degree 2, which leaves only two possibilities: either $h = dX_{p-3}^2$ or $h = d'X_{p-4}$. In the second case we get $f_l = d'X_{p-4}g$ and

$$\begin{aligned}\overline{G.e'_{p-2}} &= G.e'_{p-2} \cup \{x \in \mathfrak{w}^* \mid x_{p-2} = 0, f_q(x_{-1}, \ldots, x_{p-3}) = 0\} \\ &= G.e'_{p-2} \cup \overline{G.e'_{p-3}} \cup \{x \in \mathfrak{w}^* \mid x_{p-2} = x_{p-4} = 0\}.\end{aligned}$$

But this is impossible: Consider the set $B = \{x \in \mathfrak{w}^* \mid x_{p-2} = 0, x_{p-3} = b, x_{p-4} = 0\}$ for some $b \neq 0$. This set would then be contained in $\overline{G.e'_{p-2}}$, and since characters of height $p-2$ in $\overline{G.e'_{p-2}}$ must be contained in $\overline{G.e'_{p-3}}$ we get $B \subseteq \overline{G.e'_{p-3}}$. But this means that g becomes zero when inserting b for X_{p-3} and 0 for X_{p-4}, and this is clearly untrue. So we must have $f_l = dX_{p-3}^2 g$, and a calculation similar to the previous one gives us

$$\overline{G.e'_{p-2}} = G.e'_{p-2} \cup G.e'_{p-3} \cup \{\chi \in \mathfrak{w}^* \mid r(\chi) \leq p-3\}. \qquad \square$$

Although the description of the coadjoint orbit closures in Theorem 2.11 is not quite complete, it only takes a little more work to show that every character $\chi \in \mathfrak{w}^*$ is contained in an orbit closure that also contains 0 (for details, see [40]). It follows immediately that any invariant polynomial on $\mathfrak{w}^*$ must be constant, i.e., $F[\mathfrak{w}^*]^G = F$. We generalize this result in the next section.

2.4 Invariants of the automorphism group

Throughout this section $\mathfrak{g}$ denotes a restricted Cartan type Lie algebra with automorphism group G. Assume that the characteristic p of our ground field F is larger than 3. We will show that both $S(\mathfrak{g}) \cong F[\mathfrak{g}^*]$ and $U(\mathfrak{g})$ possess *no non-trivial G-invariants*. The following set is an important ingredient in the proof:

$$Y = \{\chi \in \mathfrak{g}^* \mid \text{there exists } g \in G \text{ such that } (g.\chi)_- = 0\}.$$

For the proof of the first lemma we will need an alternate grading on $\mathfrak{g}$, defined as follows: Grade $A(n)$ and $W(n)$ by $\deg(x^\alpha) = \sum_{i=1}^n i\alpha_i$ and $\deg(x^\alpha \partial_j) = \sum_{i=1}^n i\alpha_i - j$. Formula (2.2) shows that this grades $W(n)$ as a Lie algebra, and we write $W(n)_{[s]}$ for the sth graded component. Looking at the definitions, we see that the associated maps $\{D_\alpha\}$ are all graded (D_i of degree $-i$, D_{ij} of degree $-i-j$ and D_H, D_K of degree $-n$), which implies that we get a Lie algebra grading on $\mathfrak{g}$ by setting $\mathfrak{g}_{[s]} = \mathfrak{g} \cap W(n)_{[s]}$. Furthermore, each $\mathfrak{g}_i$ is graded, i.e., $\mathfrak{g}_i = \bigoplus_s (\mathfrak{g}_i \cap \mathfrak{g}_{[s]})$.

Lemma 2.13. *For every $\chi \in \mathfrak{g}^*_{\leq 1} \setminus \mathfrak{g}^*_{\leq 0}$ there exists $g \in G_2$ such that $g.\chi = \chi_0 + \chi_1$.*

Proof. Let $\{D_\alpha\}$ be the maps associated to $\mathfrak{g}$. The core of the proof is an adaptation (and simplification) of Theorem 4.1(3) in [23]. Assume $\chi \in \mathfrak{g}^*_{\leq 1} \setminus \mathfrak{g}^*_{\leq 0}$ and note that it is enough to find $g \in G_2$ such that $(g.\chi)_- = 0$. For if $y \in \mathfrak{g}_{\geq 0}$ then $g^{-1}(y) - y \in \mathfrak{g}_{\geq 2}$, which implies that $g.\chi$ and χ agree on $\mathfrak{g}_{\geq 0}$, i.e., $g.\chi = \chi_0 + \chi_1$.

Choose t minimal such that $\chi(\mathfrak{g}_1 \cap \mathfrak{g}_{[t]}) \neq 0$, then we can find an associated map D and some $x^\beta \in A(n)$ such that $x = D(x^\beta) \in \mathfrak{g}_1 \cap \mathfrak{g}_{[t]}$ and $\chi(x) \neq 0$. We deal first with the case $\mathfrak{g} \in \{W, S, H\}$: If $\chi_- = 0$ there is nothing to show, so assume otherwise and choose l maximal with the property $\chi(\partial_l) \neq 0$. Define $E = D(x^{\beta+\epsilon_l})$, then we have $E \in \mathfrak{g}_2 \cap \mathfrak{g}_{[t+l]}$, and according to Theorem 1 in [65] we can find, for any $c \in F$, a $g \in G_2$ such that

$$g^{-1}(\partial_s) - \partial_s - [cE, \partial_s] \in \mathfrak{g}_{\geq 2} \tag{2.31}$$

for all s, $1 \leq s \leq n$. This implies $g.\chi(\partial_s) = \chi(\partial_s) + c\chi([E, \partial_s])$. Since $[E, \partial_s] \in \mathfrak{g}_1 \cap \mathfrak{g}_{[t+l-s]}$ we get $g.\chi(\partial_s) = \chi(\partial_s) = 0$ if $s > l$, by minimality of t and maximality of l. Notice also that

$$[E, \partial_l] = [D(x^{\beta+\epsilon_l}), \partial_l] = -D(\partial_l(x^{\beta+\epsilon_l})) = -(\beta_l + 1)x. \tag{2.32}$$

Here the second equality follows from (2.12). Note that $\beta_l + 1 \neq 0$ because $\beta_l \leq 3$ (here the assumption $p > 3$ comes into play), so the calculation implies $\chi([E, \partial_l]) \neq 0$,

which again implies that we can choose c such that $g.\chi(\partial_l) = 0$. Applying this process at most n times and composing the g's, we end up with a $g' \in G_2$ such that $(g'.\chi)_- = 0$.

Now assume $\mathfrak{g}$ is a contact algebra, in which case $\bigoplus_{i<0} \mathfrak{g}_i = \mathfrak{g}_{-2} \oplus \mathfrak{g}_{-1} = \operatorname{span}\{D_K(1), D_K(x_1), \ldots, D_K(x_{2m})\}$. If $\chi(\mathfrak{g}_{-1}) \neq 0$ we choose l *minimal* such that $\chi(D_K(x_l)) \neq 0$ and define $E = D_K(x^{\beta+\epsilon_{l'}}) \in \mathfrak{g}_2 \cap \mathfrak{g}_{[t+l']}$. Again we can find $g \in G_2$ such that (2.31) holds with $D_K(x_s)$ in place of ∂_s, and it follows that $g.\chi(D_K(x_s)) = \chi(D_K(x_s)) + c\chi([E, D_K(x_s)])$. Since $[E, D_K(x_s)] \in \mathfrak{g}_1 \cap \mathfrak{g}_{[t+l'-s']}$ we get $\chi(D_K(x_s)) = 0$ for $s < l$ because of the choice of t. Furthermore,

$$[E, D_K(x_l)] = D_K(\langle x^{\beta+\epsilon_{l'}}, x_l\rangle) = -\sigma(l)(\beta_{l'}+1)D_K(x^\beta) - \beta_n D_K(x^{\beta+\epsilon_l+\epsilon_{l'}-\epsilon_n}). \quad (2.33)$$

If $\chi(D_K(x^{\beta+\epsilon_l+\epsilon_{l'}-\epsilon_n})) = 0$ the proof proceeds as in the first case. Otherwise we can replace x^β by $x^{\beta+\epsilon_l+\epsilon_{l'}-\epsilon_n} \in \mathfrak{g}_1 \cap \mathfrak{g}_{[t]}$ and repeat the process. The new x^β satisfies $\beta_n = 0$, so the last term in (2.33) disappears and we can again proceed as in the first case. Now induction yields a $g' \in G_2$ such that $(g'.\chi)_{-1} = 0$. Finally, let $E' = D_K(x^{\beta+\epsilon_n}) \in \mathfrak{g}_3$. Then we can find $g'' \in G_3$ such that

$$\begin{aligned}&(g''g').\chi(D_K(1))\\ &\quad = g'.\chi(D_K(1)) + cg'.\chi([E', D_K(1)]) = g'.\chi(D_K(1)) - (\beta_n+1)cg'.\chi(D_K(x^\beta)).\end{aligned}$$

It is clear that we can again choose c such that $(g''g').\chi(D_K(1)) = 0$, and since $((g''g').\chi)_{-1} = (g'.\chi)_{-1} = 0$ (because $g'' \in G_3$) we are done. □

Lemma 2.14. *For every $\chi \in \mathfrak{g}^*_{\leq 1} \setminus \mathfrak{g}^*_{\leq 0}$ we have $\{\chi_0 + t\chi_1 \mid t \in F^*\} \subseteq G.\chi$ and $\chi_0 \in \overline{G.\chi}$.*

Proof. Use the action of T on $\chi_0 + \chi_1$ and take the limit as t approaches zero. □

Lemma 2.15. *The set Y is dense in $\mathfrak{g}^*$.*

Proof. Consider an element $w = \sum_{i=1}^n a_i D(x^{\tau-\epsilon_i}) \in \mathfrak{g}$ with $D = D_1$ if $\mathfrak{g} = W(n)$, $D = D_{12}$ if $\mathfrak{g} = S(n)$, $D = D_H$ if $\mathfrak{g} = H(n)$ and $D = D_K$ if $\mathfrak{g} = K(n)$ (the $a_i \in F$ are arbitrary). Using the grading on $\mathfrak{g}$ and the assumption $p \geq 5$ one checks that, with the exception of the case $\mathfrak{g} = W(1)$, $p = 5$, we have $(\operatorname{ad} w)^2 = 0$ and $[(\operatorname{ad} w)(x_1), (\operatorname{ad} w)(x_2)] = 0$ for all $x_1, x_2 \in \mathfrak{g}$, which implies that $g = \exp(\operatorname{ad} w) = \operatorname{id} + \operatorname{ad} w$ is an automorphism of $\mathfrak{g}$ (if $\mathfrak{g} = W(1)$ one can use our results on orbit representatives to prove $Y = \mathfrak{g}^*$). We treat the case $\mathfrak{g} \in \{W, S, H\}$ first. Here we can use (2.12) to get

$$g(\partial_s) = \partial_s + [w, \partial_s] = \partial_s - \sum_{i=1}^n a_i D(\partial_s(x^{\tau-\epsilon_i})).$$

For any $\chi \in \mathfrak{g}^*$ we set $\chi(D(\partial_s(x^{\tau-\epsilon_i}))) = b_{si}$. So we have

$$g^{-1}.\chi(\partial_s) = \chi(\partial_s) - \sum_{i=1}^n a_i b_{si}.$$

If the $n \times n$ matrix $B = (b_{si})$ is invertible, then we can choose the a_i such that $g^{-1}.\chi(\partial_s) = 0$ for all s. The set $Y' \subseteq Y$ of all $\chi \in \mathfrak{g}^*$ that satisfies this condition is open, so we just have to show that it is nonempty: Define matrices $C = (\partial_s(x^{\tau-\epsilon_i}))_{s,i}$ and $B' = (D(\partial_s(x^{\tau-\epsilon_i})))_{s,i}$. Explicitly, we have

$$c_{si} = \begin{cases} (p-2)x^{\tau-2\epsilon_i} & \text{if } s = i \\ (p-1)x^{\tau-\epsilon_i-\epsilon_s} & \text{if } s \neq i. \end{cases}$$

We see that C, and therefore also B', is symmetric. Furthermore, the c_{si} with $s \geq i$ are linearly independent, and since D is injective on the ideal generated by $x_1x_2\cdots x_n$ (can easily be checked case by case) which contains all the c_{si}, the elements on and below the diagonal of B' must also be linearly independent. But then we can choose χ such that (say) $B = I$, and we are done.

Now let $\mathfrak{g}$ be of type K and write $z_s = D_K(x_{s'})$ for $1 \leq s \leq 2m$, $z_n = D_K(1)$. As before, we calculate (with the convention $x_{n'} = 1$):

$$\begin{aligned} g(z_s) &= z_s + [w, z_s] \\ &= z_s - \sum_{i=1}^{n} a_i[D_K(x_{s'}), D_K(x^{\tau-\epsilon_i})] = z_s - \sum_{i=1}^{n} a_i D_K(\langle x_{s'}, x^{\tau-\epsilon_i}\rangle). \end{aligned}$$

We set $b_{si} = \chi(D_K(\langle x_{s'}, x^{\tau-\epsilon_i}\rangle))$ for all $\chi \in \mathfrak{g}^*$, then it is again enough to find χ such that $B = (b_{si})$ is invertible: Consider first the matrix $C = (\langle x_{s'}, x^{\tau-\epsilon_i}\rangle)_{s,i}$. Using (2.7), (2.8) and (2.9) we get, for $1 \leq s, i \leq 2m$,

$$c_{si} = \begin{cases} \sigma(i')(p-2)x^{\tau-2\epsilon_i} & \text{if } s = i \\ \sigma(s')(p-1)x^{\tau-\epsilon_i-\epsilon_s} + \delta_{si'}(p-1)x^{\tau-\epsilon_n} & \text{if } s \neq i \end{cases}$$

and

$$\begin{aligned} c_{sn} &= \sigma(s')(p-1)x^{\tau-\epsilon_s-\epsilon_n} \\ c_{ns} &= (p-1)x^{\tau-\epsilon_s-\epsilon_n} \\ c_{nn} &= (p-2)x^{\tau-2\epsilon_n} \end{aligned}$$

It is easy to see from these formulas that the c_{si} with $s \geq i$ are linearly independent. But D_K is injective (can be derived from [58], Lemma 5.1), so the entries on and below the diagonal in the matrix $B' = (D_K(\langle x_{s'}, x^{\tau-\epsilon_i}\rangle))_{s,i}$ are also linearly independent. Then we can choose χ such that B has the form

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

This matrix is clearly invertible. □

Lemma 2.16. *There exists $x \in \mathfrak{g}_1$ such that the map $(\operatorname{ad} x)_{|\mathfrak{g}_0} : \mathfrak{g}_0 \to \mathfrak{g}_1$ is injective.*

Proof. Assume first that $\mathfrak{g} \in \{W, S\}$. We set $x = \sum_{i=1}^{n-1} x_i^2 \partial_i - \sum_{i=1}^{n-1} 2x_n x_i \partial_n \in \mathfrak{g}_1$. If $y = \sum_{i,j} b_{ij} x_i \partial_j$ is an arbitrary element of $\mathfrak{g}_0$ and $[x, y] = 0$, then we have, for $1 \leq s \leq n-1$,

$$y \circ x(x_s) = \sum_{i=1}^{n} 2b_{is} x_i x_s,$$
$$x \circ y(x_s) = \sum_{i=1}^{n-1} b_{is} x_i^2 - \sum_{i=1}^{n-1} 2b_{ns} x_i x_n.$$

It follows (since we assume $[x, y] = 0$) that $b_{ij} = 0$ if $j \neq n$. So $y = \sum_{i=1}^{n} b_{in} x_i \partial_n$ and

$$y \circ x(x_n) = \sum_{i=1}^{n-1} \sum_{j=1}^{n} 2b_{jn} x_i x_j,$$
$$x \circ y(x_n) = \sum_{j=1}^{n-1} b_{jn} x_j^2 - \sum_{i=1}^{n-1} 2b_{nn} x_i x_n.$$

Equating these expressions, we get $b_{jn} = 0$ for $1 \leq j \leq n$, so $y = 0$ and x works like it should.

If $\mathfrak{g}$ is of type H we set $x = \sum_{i=1}^{2n} \sigma(i) x_i^2 \partial_{i'} \in \mathfrak{g}_1$. Note first that the condition (2.6) with $i = j$ implies that if $y = \sum_{i,j} b_{ij} x_i \partial_j \in \mathfrak{g}$, then $b_{ii} = -b_{i'i'}$. Again we calculate, for $1 \leq s \leq 2n$,

$$y \circ x(x_s) = \sum_{i=1}^{2n} 2\sigma(s') b_{is'} x_i x_{s'}$$
$$x \circ y(x_s) = \sum_{i=1}^{2n} \sigma(i') b_{is} x_{i'}^2$$

If $[x, y] = 0$ then these equations show that all $b_{ij} = 0$ (using that $b_{ss} = -b_{s's'}$), so $(\operatorname{ad} x)_{|\mathfrak{g}_0}$ is injective, and we are done.

Finally, assume $\mathfrak{g}$ is of type K and set $x = D_K(\sum_{s=1}^{2m} x_s^3) \in \mathfrak{g}_1$. An arbitrary element y of $\mathfrak{g}_0$ has the form $D_K(\sum_{1 \leq i \leq j \leq 2m} b_{ij} x_i x_j + c x_n)$. Using formulas (2.9), (2.10) and (2.11) we get

$$\Big\langle \sum_{1 \leq i \leq j \leq 2m} b_{ij} x_i x_j + c x_n, \sum_{s=1}^{2m} x_s^3 \Big\rangle$$
$$= \sum_{\substack{1 \leq i \leq j \leq 2m \\ j \neq i'}} 3b_{ij} (\sigma(i) x_j x_{i'}^2 + \sigma(j) x_i x_{j'}^2) + \sum_{i=1}^{m} 3b_{ii'} (x_{i'}^3 - x_i^3) + c \sum_{i=1}^{2m} x_i^3.$$

Each term in the first sum contains standard basis elements which do not appear anywhere else, so if $[x, y] = 0$ all the b_{ij} in the first sum must also be zero (recall that D_K is injective). Then we can look at the last two sums to get $3b_{ii'} = -c = -3b_{ii'}$ for $1 \leq i \leq m$, which implies $b_{ii'} = 0$. Finally c must also be zero, and we are done. $\square$

Now we are ready for the main theorem:

Theorem 2.17. *$S(\mathfrak{g})^G = F$ and $U(\mathfrak{g})^G = F$.*

Proof. Let $f \in F[\mathfrak{g}^*]^G \cong S(\mathfrak{g})^G$. We show first that f is constant on $\mathfrak{g}_0^*$: For any $\chi \in \mathfrak{g}_1^*$ and $g \in G$, we use Corollary 2.14 to write

$$f(0) = f(\chi_0) = f(\chi) = f(g.\chi) = f((g.\chi)_0). \tag{2.34}$$

Let $\chi' \in \mathfrak{g}_0^*$ be arbitrary and fix a basis $\{y_s\}$ of $\mathfrak{g}_0$. Theorem 1 in [65] ensures the existence of a $g \in G_1$ that satisfies

$$g^{-1}(y_s) - y_s - [x, y_s] \in \mathfrak{g}_{\geq 2}$$

for all s, where x is the one from Lemma 2.16. But the $[x, y_s]$ are linearly independent, so we can choose $\chi \in \mathfrak{g}_1^*$ that satisfies $\chi([x, y_s]) = \chi'(y_s)$ for all s. This means that

$$g.\chi(y_s) = \chi(y_s) + \chi([x, y_s]) = \chi'(y_s)$$

and $(g.\chi)_0 = \chi'$. Now (2.34) gives $f(\chi') = f(0)$.

For any $\chi \in Y$, we can find $g \in G$ such that $(g.\chi)_- = 0$ and use the action of T to get

$$\{(g.\chi)_0 + t(g.\chi)_1 + \cdots + t^N(g.\chi)_N \mid t \in F^*\} \subseteq G.\chi.$$

It follows, by taking the limit as t approaches zero, that $(g.\chi)_0 \in \overline{G.\chi}$, and so $f(\chi) = f((g.\chi)_0) = f(0)$. We have shown that f is constant on Y, and as a consequence of Lemma 2.15 we get $F[\mathfrak{g}^*]^G = F$.

Finally, let $z \in U(\mathfrak{g})^G$. One checks easily that the leading term map l from section 1.1 is G-invariant, which implies $l(z) \in S(\mathfrak{g})^G \cap S(\mathfrak{g})_{\deg(z)}$. But then we must have $\deg(z) = 0$, and thus $z \in F$. □

2.5 Semi-invariants

The results of the previous section are of course rather discouraging, but the automorphism group could still play a part in our search for non-trivial central elements and an analogue of Veldkamp's Theorem for the restricted Cartan type Lie algebras. To explain how, we need a couple of definitions: Let H be an arbitrary algebraic F-group with Lie algebra $\mathfrak{h} = \mathrm{Lie}(H)$, and let A be an associative F-algebra on which H acts rationally by algebra automorphisms. We denote by $X(H)$ the character group of H and by $X(\mathfrak{h}) = \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{h}, F)$ the character group of $\mathfrak{h}$. For any $\chi \in X(H)$ we set

$$A_\chi = \{x \in A \mid h.x = \chi(h)x \text{ for all } h \in H\}$$

and call χ a *weight* if $A_\chi \neq \{0\}$. The nonzero $x \in A_\chi$ are called *semi-invariants* of weight χ, and the monoid of weights is denoted by $\Lambda(H, A)$. If we even have $\chi \in \Lambda(H, A) \cap \ker d$, where $d : X(H) \to X(\mathfrak{h})$ is the group homomorphism given by the usual differential, then we call χ a *p-weight* and x a *p-semi-invariant*. As

motivation for this name, note that we always get $pX(H) \in \ker d$. Now the sum of weight spaces is easily seen to be direct, and we define the *algebra of semi-invariants* $A^{H\text{-si}}$ and the *algebra of p-semi-invariants* $A^{H\text{-psi}}$ by

$$A^{H\text{-si}} = \bigoplus_{\chi \in \Lambda(H,A)} A_\chi,$$
$$A^{H\text{-psi}} = \bigoplus_{\chi \in \Lambda(H,A) \cap \ker\, d} A_\chi.$$

So, strictly speaking, the algebra of semi-invariants consists not only of semi-invariants, but of all linear combinations of these, and similarly for the algebra of p-semi-invariants. Clearly, we have

$$A^H \subseteq A^{H\text{-psi}} \subseteq A^{H\text{-si}} \subseteq A^{[H,H]} \tag{2.35}$$

and also $A^{H\text{-psi}} \subseteq A^{\mathfrak{h}}$, which is the main reason for our interest in $A^{H\text{-psi}}$. The following standard result (which we give without proof) is often useful:

Proposition 2.18. *Assume that $H/[H,H]$ is diagonalizable. Then*

$$A^{H\text{-si}} = A^{[H,H]}.$$

Now if $H = [H,H]$ (which holds, for example, when H is semisimple) we get $A^H = A^{H\text{-si}}$ by (2.35), so there are no semi-invariants except for the 'real' invariants. If H is reductive, then $H = Z(H)[H,H]$ and the adjoint action of $Z(H)$ on $\mathfrak{h}$ and $\mathfrak{h}^*$ is trivial, which implies $S(\mathfrak{h})^H = S(\mathfrak{h})^{[H,H]}$ and $S(\mathfrak{h}^*)^H = S(\mathfrak{h}^*)^{[H,H]}$. So also in these cases we have only the trivial weight, and if furthermore H satisfies the standard hypotheses (so that $\mathfrak{h}$ admits an H-invariant symmetrization map), then $\Lambda(H, U(\mathfrak{h}))$ is trivial as well.

We return now to the setup of the previous section, so that $\mathfrak{g}$ denotes a Lie algebra of restricted Cartan type, with automorphism group G. Then we have:

Lemma 2.19.

$$[G,G] = [G_0,G_0] \ltimes G_1 \cong \begin{cases} \mathrm{SL}_n \ltimes G_1 & \text{if } \mathfrak{g} = W(n), S(n) \\ \mathrm{Sp}_{2m} \ltimes G_1 & \text{if } \mathfrak{g} = H(2m), K(2m+1). \end{cases}$$

Proof. The inclusion $[G,G] \subseteq [G_0,G_0] \ltimes G_1$ follows from general facts, so to prove the equality it is enough to show $G_1 \subseteq [G,G]$. We will actually show the stronger statement that $G_r = [T, G_r]$ for all $r \geq 1$ by induction on r. It is well known that we have surjective group homomorphisms $f_r : G_r \to \widehat{\mathfrak{g}}_r$ (with $\widehat{\mathfrak{g}}_r$ considered as an additive group) defined by

$$f_r(\sigma_\varphi) = \sum_{i=1}^{n} \varphi(x_i)_{r+1} \partial_i$$

for $\sigma_\varphi \in G_r$. A straightforward calculation shows that

$$f_r([t,g]) = (t^r - 1) f_r(g)$$

for all $g \in G_r$, $t \in T$. So we can always choose t such that $f_r([t,g]) = f_r(g)$, and since the kernel of f_r is G_{r+1} we get $[t,g] \equiv g \bmod G_{r+1}$, which implies $g \in [T, G_r]$ by induction. □

We see that $G/[G,G]$ is a one-dimensional torus, so in particular Proposition 2.18 applies. Furthermore, $X(G) \cong X(T) \cong \mathbb{Z}$ so we can, and will, identify weights with integers. A priori we could have both positive and negative weights for the action of G on $U(\mathfrak{g})$ and $S(\mathfrak{g})$, but a simple application of Theorem 2.17 shows that we actually only get one or the other:

Proposition 2.20. *We have $\Lambda(G, U(\mathfrak{g})) \subseteq \mathbb{N}$ or $\Lambda(G, U(\mathfrak{g})) \subseteq -\mathbb{N}$, and the same is true with $S(\mathfrak{g})$ in place of $U(\mathfrak{g})$.*

Proof. Assume that there exist both positive and and negative weights in $\Lambda(G, U(\mathfrak{g}))$, and let ψ_1, ψ_2 be the largest negative, resp. least positive, weight. Since $\Lambda(G, U(\mathfrak{g}))$ is a monoid we must have $\psi_1 = -\psi_2$. If we choose nonzero elements $x_1 \in U(\mathfrak{g})_{\psi_1}, x_2 \in U(\mathfrak{g})_{\psi_2}$, then $x_1 x_2 \in U(\mathfrak{g})_0 = U(\mathfrak{g})^G$. But $U(\mathfrak{g})^G = F$ by Theorem 2.17, so x_1 and x_2 are units, which is a contradiction since the set of units in $U(\mathfrak{g})$ is precisely F. The proof for $S(\mathfrak{g})$ is exactly the same. □

It follows from (2.13) that p-semi-invariants in $U(\mathfrak{g})$ are not automatically central, and neither are p-semi-invariants in $S(\mathfrak{g})$ automatically contained in $S(\mathfrak{g})^{\mathfrak{g}}$. When investigating the latter problem, the following lemma (which is essentially a consequence of (1.9) and proved in [52])[2] often comes in handy:

Lemma 2.21. *Let $\mathfrak{h}$ be an arbitrary restricted Lie algebra, and let X be an irreducible affine variety, such that there is a restricted action of $\mathfrak{h}$ on $F[X]$ by derivations. If $\mathfrak{h}'$ is any restricted subalgebra of $\mathfrak{h}$, then $F[X]^{\mathfrak{h}} = F[X]^{\mathfrak{h}'}$ if and only if there exists $x \in X_{\mathfrak{g}-\mathrm{reg}}$ such that $\mathfrak{h} = \mathfrak{h}_x + \mathfrak{h}'$.*

As an example of what we *hope* to be true in general, we now prove the following theorem:

Theorem 2.22. *Set $\mathfrak{w} = W(1)$ and $G = \mathrm{Aut}(\mathfrak{w})$. Then we have*

1. *$U(\mathfrak{w})^{G\text{-psi}} \subseteq Z(\mathfrak{w})$.*
2. *$Z(\mathfrak{w})$ is free of rank p over $Z_0(\mathfrak{w})$ and there exists a $Z_0(\mathfrak{w})$-basis of $Z(\mathfrak{w})$ consisting of p-semi-invariants.*
3. *The two previous statements are still true if we replace $U(\mathfrak{w})$ by $S(\mathfrak{w})$, $Z(\mathfrak{w})$ by $S(\mathfrak{w})^{\mathfrak{w}}$ and $Z_0(\mathfrak{w})$ by $S(\mathfrak{w})^p$.*

Proof. Our approach relies heavily on Jakovlev's short paper [27], and we prove the third statement first. Recall the notation from the start of section 2.2 and define a character $\chi \in \mathfrak{w}^*$ by $\chi(x^{p-1}\partial) = 1$ and $\chi(x^i\partial) = 0$ for $0 \leq i \leq p-2$. One checks easily that $\mathfrak{w}_\chi = F\partial$ and $\mathrm{ind}(\mathfrak{w}) = 1$ (in fact, the index has been calculated for all

[2] To be precise, Skryabin only proves one implication of the lemma, but the other one is easy.

the restricted Cartan type algebras, with certain restrictions on the characteristic, by Krylyuk in [34] and [35]), so $\chi \in \mathfrak{w}^*_{\mathrm{reg}}$ and $\mathfrak{w} = \mathfrak{w}_\chi + \mathfrak{w}_{\geq 0}$. But then, by Lemma 2.21, we get $S(\mathfrak{w})^{\mathrm{Lie}(G)} = S(\mathfrak{w})^{\mathfrak{w}_{\geq 0}} = S(\mathfrak{w})^{\mathfrak{w}}$ and thus $S(\mathfrak{w})^{G\text{-psi}} \subseteq S(\mathfrak{w})^{\mathfrak{w}}$.

Now we define a basis $\{d_0, \ldots, d_{p-1}\}$ of $\mathfrak{w}$ by $d_i = y^{i+1}\partial$, where $y = x + 1$, and set

$$f = \sum_{|\alpha| = \frac{p+1}{2}} c_\alpha d_0^{\alpha_0} \cdots d_{p-1}^{\alpha_{p-1}} \tag{2.36}$$

with $c_\alpha = \frac{1}{\alpha_0! \ldots \alpha_{p-1}!}$ if $\sum i\alpha_i = 0$ and $c_\alpha = 0$ otherwise. It takes only a straightforward calculation to get $d_i.f = 0$ for all i, so that $f \in S(\mathfrak{w})^{\mathfrak{w}}$. We want to show that $\{1, f, \ldots, f^{p-1}\}$ is an $S(\mathfrak{w})^p$-basis of $S(\mathfrak{w})^{\mathfrak{w}}$, and by Theorem 1.7 it is enough to show that the closed subset $C \subset \mathfrak{w}^*$, consisting of all $\chi \in \mathfrak{w}^*$ where the differential $d_\chi f$ vanishes, has codimension at least 2 in $\mathfrak{w}^*$. Let D_i denote partial differentiation with respect to d_i. Then

$$C = \bigcap_{i=0}^{p-1} V(D_i(f)).$$

Notice that the term $d_{p-2}^{(p-1)/2}$ appears in $D_{p-1}(f)$ with nonzero coefficient. No other $D_i(f)$ contains a "pure" d_{p-2}-term, and this implies that $D_{p-1}(f)$ cannot be contained in the radical of any other $D_i(f)$. But then the codimension of C must be at least 2. To finish the proof of the third statement, we need only to show that f is a p-semi-invariant, which is now easy. For arbitrary $g \in G$ we can write

$$g(f) = h_0 + h_1 f + \cdots + h_{p-1} f^{p-1} \tag{2.37}$$

for some unique $h_0 \ldots, h_{p-1} \in S(\mathfrak{w})^p$, since G preserves $S(\mathfrak{w})^{\mathfrak{w}}$. But G also preserves the grading of $S(\mathfrak{w})$, so (2.37) can only be true if $h_1 \in F^*$ and $h_i = 0$ for all $i \neq 1$.[3]

To prove the statements for $U(\mathfrak{w})$, we note first, that even though the definition of the standard symmetrization map in characteristic zero does not make sense in our world, we still have 'symmetrization in degrees less than p', i.e., there is a G- and $\mathfrak{w}$-module isomorphism $\phi : S(\mathfrak{w})_{\leq p-1} \to U(\mathfrak{w})_{\leq p-1}$ given by

$$\phi(d_{i_1} \ldots d_{i_k}) = \sum_{\sigma \in S_k} \frac{1}{k!} d_{i_{\sigma(1)}} \cdots d_{i_{\sigma(k)}}$$

for $k < p$. With $\hat{f} = \phi(f)$ we have $Z(\mathfrak{w}) = Z_0(\mathfrak{w})[\hat{f}]$ by [27]. Denote by Z' the $Z_0(\mathfrak{w})$-module generated by $1, \hat{f}, \ldots, \hat{f}^{p-1}$, then we can write

$$S(\mathfrak{w})^{\mathfrak{w}} = \mathrm{Gr}(Z') \subseteq \mathrm{Gr}(Z(\mathfrak{w})) \subseteq S(\mathfrak{w})^{\mathfrak{w}}.$$

It follows that $\mathrm{Gr}(Z') = \mathrm{Gr}(Z(\mathfrak{w}))$ and therefore $Z' = Z(\mathfrak{w})$. A standard argument shows that $1, \hat{f}, \ldots, \hat{f}^{p-1}$ are linearly independent, and thus we have proved the second statement of the theorem. To prove the first, note simply that $Z(\mathfrak{w}) \subseteq U(\mathfrak{w})^{\mathfrak{w}_{\geq 0}}$, while at the same time,

$$\mathrm{Gr}(U(\mathfrak{w})^{\mathfrak{w}_{\geq 0}}) \subseteq S(\mathfrak{w})^{\mathfrak{w}_{\geq 0}} = S(\mathfrak{w})^{\mathfrak{w}} = \mathrm{Gr}(Z(\mathfrak{w})).$$

So $Z(\mathfrak{w}) = U(\mathfrak{w})^{\mathfrak{w}_{\geq 0}} \supseteq U(\mathfrak{w})^{G\text{-psi}}$ and we are done. □

[3] It is not too hard to show that the weight of f is in fact $\frac{p(p-3)}{2}$

It should be painfully clear, that the rather ad hoc definition of the all-important $f \in S(\mathfrak{w})$ makes it hard to generalize this proof to bigger Lie algebras of restricted Cartan type (see, however, [5]), and even though f *is* a p-semi-invariant, we arrive at this fact in a sort of 'backwards' way. Thus the theorem might not might convince the reader (it has not totally convinced the author!) that the study of p-semi-invariants will make it any easier to find non-trivial central elements. Of course, a first step in the right direction would be to prove that $U(\mathfrak{g})^{G\text{-psi}} \subseteq Z(\mathfrak{g})$ for *any* restricted Cartan type Lie algebra $\mathfrak{g}$ with automorphism group G, which is equivalent to $U(\mathfrak{g})^{G\text{-psi}} \subseteq U(\mathfrak{g})^{\mathfrak{g}-}$. In the symmetric case we actually have a description of $S(\mathfrak{g})^{\mathfrak{g}-}$ for $\mathfrak{g} \in \{W, S, H\}$ in [2] by Bedratyuk. Note also, that if we consider the *second* Witt-Jacobson algebra $W(2)$, then an example in section 6.4 of [45] provides a character $\chi \in W(2)^*_{\text{reg}}$ satisfying $W(2) = W(2)_\chi + W(2)_{\geq 0}$. By Lemma 2.21 the p-semi-invariants in $S(W(2))$ are then $W(2)$-invariant. For further results concerning non-trivial central elements in special cases, see [18] and [32].

Chapter 3

An analogue of Chevalley's Restriction Theorem

3.1 The variety of tori of maximal dimension

Chevalley's Restriction Theorem (CRT for short) was already briefly explained in Section 1.2, but let us restate it here for reference:

Theorem 3.1. *Let $\mathfrak{g}$ be a semisimple Lie algebra over an algebraically closed field of characteristic zero, with Cartan subalgebra $\mathfrak{h} \subseteq \mathfrak{g}$, Weyl group W and group of inner automorphisms G. Then the natural restriction map $F[\mathfrak{g}] \to F[\mathfrak{h}]$ induces an algebra isomorphism*

$$\mathrm{res} : F[\mathfrak{g}]^G \xrightarrow{\sim} F[\mathfrak{h}]^W.$$

In particular, $F[\mathfrak{g}]^G$ is a polynomial algebra in $\dim(\mathfrak{h})$ variables.

A couple of remarks: In the setup of this theorem the notions of Cartan subalgebra and *maximal toral subalgebra* (as in [24]) coincide. Corresponding to the latter kind of subalgebra we have *maximal tori* in the restricted theory (we will elaborate on this concept in a moment), but these need not be Cartan subalgebras, even when the Lie algebra considered is simple. It turns out, that to get an analogue of CRT for the restricted Cartan types we will have to replace the Cartan subalgebra by a maximal torus. Furthermore, it is well known, that (with the notation of Theorem 3.1) we have

$$W \cong N_G(\mathfrak{h})/C_G(\mathfrak{h}) \tag{3.1}$$

where $N_G(\mathfrak{h}) = \{g \in G \mid g(\mathfrak{h}) \subseteq \mathfrak{h}\}$ is the normalizer of $\mathfrak{h}$ in G and $C_G(\mathfrak{h}) = \{g \in G \mid g(h) = h \text{ for all } h \in \mathfrak{h}\}$ is the centralizer of $\mathfrak{h}$ in G. It is the right hand side of (3.1) which we will adapt to our setup. Finally, in characteristic zero any two Cartan subalgebras of a Lie algebra are conjugate under the action of the group of inner automorphisms, so in particular, the choice of $\mathfrak{h}$ in Theorem 3.1 does not matter. For the restricted Cartan types, the maximal tori are *not* all conjugate under the action of the automorphism group, and the choice of maximal torus matters very much, as we will see! Before we dive deeper into this problem, we will briefly recall the basics:

Return to the general setup of an arbitrary restricted Lie algebra $\mathfrak{g}$ over an algebraically closed field F of positive characteristic. As mentioned previously, one of the advantages of working in the restricted setting is that we have an analogue of the Jordan decomposition in nonmodular semisimple Lie algebras: For any $x \in \mathfrak{g}$ we denote by $\langle x \rangle_{[p]}$ the smallest restricted subalgebra of $\mathfrak{g}$ containing x. We say that x is *semisimple* if $x \in \langle x^{[p]} \rangle_{[p]}$, and we say that x is *p-nilpotent* if $x^{[p]^n} = 0$ for some n. It can easily be shown ([58], proposition 3.3) that a semisimple x acts semisimply on any finite-dimensional restricted $\mathfrak{g}$-module M, while a p-nilpotent x acts nilpotently on M. The point now is that for any $y \in \mathfrak{g}$ we can find uniquely determined y_s, y_n such that y_s is semisimple, y_n is p-nilpotent, $[y_s, y_n] = 0$, and

$$y = y_s + y_n.$$

This version of the Jordan decomposition is useful in many situations. A restricted abelian subalgebra $\mathfrak{t}$ of $\mathfrak{g}$ consisting only of semisimple elements is called a *torus*. It is well known that a restricted subalgebra $\mathfrak{t}'$ is a torus if and only if the p-mapping is invertible on $\mathfrak{t}'$. Furthermore, any torus admits a vector space basis consisting of *toral* elements, i.e., elements $y \in \mathfrak{g}$ satisfying $y^{[p]} = y$. If $\{y_1, \ldots, y_n\}$ is a toral basis of the torus $\mathfrak{t}$, then the set $\mathrm{tor}(\mathfrak{t})$ of toral elements in $\mathfrak{t}$ is given explicitly by

$$\mathrm{tor}(\mathfrak{t}) = \sum_{i=1}^{n} \mathbb{F}_p y_i.$$

In particular, $\mathrm{tor}(\mathfrak{t})$ is a vector space over $\mathbb{F}_p$. If we denote by $\mathrm{Aut}_p(\mathfrak{t})$ the group of restricted automorphisms of $\mathfrak{t}$, then it is easily seen that any $\mathbb{F}_p$-linear automorphism of $\mathrm{tor}(\mathfrak{t})$ induces canonically an element of $\mathrm{Aut}_p(\mathfrak{t})$ and vice versa. It follows that $\mathrm{Aut}_p(\mathfrak{t}) \cong \mathrm{GL}_n(\mathbb{F}_p)$. Now let $\mathfrak{G} = \mathrm{Aut}_p(\mathfrak{g})^\circ$ denote the identity component of the (algebraic) group of restricted automorphisms of $\mathfrak{g}$. We define

$$W(\mathfrak{g}, \mathfrak{t}) = N_{\mathfrak{G}}(\mathfrak{t}) / C_{\mathfrak{G}}(\mathfrak{t})$$

and call $W(\mathfrak{g}, \mathfrak{t})$ the *Weyl group of* $\mathfrak{g}$ *relative to* $\mathfrak{t}$. We clearly have an injective homomorphism $W(\mathfrak{g}, \mathfrak{t}) \hookrightarrow \mathrm{Aut}_p(\mathfrak{t})$. In particular, $W(\mathfrak{g}, \mathfrak{t})$ is *finite*.

Let $\mu(\mathfrak{g})$ denote the maximal dimension of a torus in $\mathfrak{g}$ and $\mathrm{rk}(\mathfrak{g})$ the minimal dimension of a Cartan subalgebra in $\mathfrak{g}$. The notions of *maximal torus* (that is, a torus not properly contained in any other torus) and torus of maximal dimension need not coincide, but in the case of restricted Cartan type Lie algebras, they do ([55], Section 7.5). The set $\mathcal{T}$ of tori of dimension $\mu(\mathfrak{g})$ can be given the structure of a variety in two different ways, which ultimately turn out to be equivalent: first consider $\mathcal{T}$ as a subset of the Grassmannian $\mathrm{Gr}_{\mu(\mathfrak{g})}(\mathfrak{g})$. It can be shown ([19], Lemma 7.4) that $\mathcal{T}$ is locally closed in $\mathrm{Gr}_{\mu(\mathfrak{g})}(\mathfrak{g})$ and thereby a quasi-projective variety. Second, let $\mathfrak{t} \subseteq \mathfrak{g}$ be any torus of dimension $\mu(\mathfrak{g})$ and consider the variety $E_{\mathfrak{t}}$ of embeddings $\mathfrak{t} \hookrightarrow \mathfrak{g}$ of restricted lie algebras. There is a natural free action of the finite group $\mathrm{Aut}_p(\mathfrak{t})$ on $E_{\mathfrak{t}}$, and the geometric quotient $E_{\mathfrak{t}}/\mathrm{Aut}_p(\mathfrak{t})$ turns out to be an affine smooth irreducible variety of dimension $\dim(\mathfrak{g}) - \mathrm{rk}(\mathfrak{g})$. The map $\varphi \mapsto \varphi(\mathfrak{t})$ clearly induces a bijection ψ between $E_{\mathfrak{t}}/\mathrm{Aut}_p(\mathfrak{t})$ and $\mathcal{T}$, and thus we have another way of realizing the set of

tori of maximal dimension as a variety. Luckily, ψ is actually an isomorphism of varieties ([19], Theorem 9.3). In particular, $\mathcal{T}$ is affine. Note furthermore, that we have a natural $\mathfrak{G}$-action on $\mathcal{T}$. A torus $\mathfrak{t} \in \mathcal{T}$ such that

$$\overline{\mathfrak{G}.\mathfrak{t}} = \mathcal{T}$$

is said to be *generic*.

Let $\mathcal{C}$ denote the set of all Cartan subalgebras of dimension $\mathrm{rk}(\mathfrak{g})$ in $\mathfrak{g}$. As a subset of $\mathrm{Gr}_{\mathrm{rk}(\mathfrak{g})}(\mathfrak{g})$, $\mathcal{C}$ is locally closed and thus a quasi-projective variety. We have a morphism $\mathcal{E} : \mathcal{T} \to \mathcal{C}$, defined by $\mathcal{E}(\mathfrak{t}) = \mathfrak{c}_{\mathfrak{g}}(\mathfrak{t})$, where

$$\mathfrak{c}_{\mathfrak{g}}(\mathfrak{t}) = \{x \in \mathfrak{g} \mid [x, t] = 0 \text{ for all } t \in \mathfrak{t}\}.$$

This morphism is injective, dominant, étale and equivariant with respect to the canonical $\mathfrak{G}$-action on $\mathcal{T}$ and $\mathcal{C}$. If all maximal tori in $\mathfrak{g}$ have dimension $\mu(\mathfrak{g})$, then $\mathcal{E}$ is even bijective (an inverse map is given by $\mathfrak{h} \to \{t \in \mathfrak{c}_{\mathfrak{h}}(\mathfrak{h}) \mid t \text{ is semisimple}\}$, see [58], Theorem 2.4.1 and Corollary 2.4.2) and thereby a $\mathfrak{G}$-equivariant isomorphism of varieties. Since this is the case for the Lie algebras we consider, the results we prove for $\mathcal{T}$ can be transferred to $\mathcal{C}$ via $\mathcal{E}$.

We specialize now to our favourite setup of a restricted Cartan type Lie algebra $\mathfrak{g}$ with automorphism group G. Note that we have $G = \mathfrak{G}$ since G is connected. Let $\mathcal{T}'$ be the subset of $\mathcal{T}$ consisting of all tori contained in $\mathfrak{g}_{\geq -1}$. Of course $\mathcal{T} = \mathcal{T}'$ if $\mathfrak{g} \in \{W, S, H\}$, but if $\mathfrak{g}$ is of type K then $\mathcal{T}'$ is a proper closed subvariety of $\mathcal{T}$.[1] From the fact that G respects the standard filtration of $\mathfrak{g}$ it follows that $\mathcal{T}'$ is G-invariant. As shown by Demushkin in [13], [14] (with corrections by Strade in [55], Section 7.5) there are exactly $\mu(\mathfrak{g}) + 1 - \delta_{\mathfrak{g}K}$ orbits $\mathcal{O}_{0+\delta_{\mathfrak{g}K}}, \ldots, \mathcal{O}_{\mu(\mathfrak{g})}$ in $\mathcal{T}'$ under the G-action, and these have the following simple description:

$$\mathcal{O}_k = \{\mathfrak{t} \in \mathcal{T} \mid \dim(\mathfrak{t} \cap \mathfrak{g}_{\geq 0}) = k\}.$$

For each of the four Cartan types we have canonical orbit representatives $\mathfrak{t}_k$ of $\mathcal{O}_k$ given by

$$\mathfrak{t}_k = \sum_{i=1}^{k} Fx_i\partial_i \oplus \sum_{i=k+1}^{n} F(1 + x_i)\partial_i \qquad \text{if } \mathfrak{g} = W(n) \tag{3.2}$$

$$\mathfrak{t}_k = \sum_{i=1}^{k} F(x_i\partial_i - x_n\partial_n) \oplus \sum_{i=k+1}^{n-1} F((1 + x_i)\partial_i - x_n\partial_n) \qquad \text{if } \mathfrak{g} = S(n) \tag{3.3}$$

$$\mathfrak{t}_k = \sum_{i=1}^{k} F(x_i\partial_i - x_{i'}\partial_{i'}) \oplus \sum_{i=k+1}^{m} F((1 + x_i)\partial_i - x_{i'}\partial_{i'}) \qquad \text{if } \mathfrak{g} = H(2m) \tag{3.4}$$

$$\mathfrak{t}_k = \sum_{i=1}^{k-1} Fx_ix_{i'} \oplus \sum_{i=k}^{m} F(1 + x_i)x_{i'} \oplus F\Big(\sum_{i=1}^{m} x_ix_{i'} + x_{2m+1}\Big) \qquad \text{if } \mathfrak{g} = K(2m+1) \tag{3.5}$$

[1] For results on tori not contained in $\mathcal{T}'$ for type K, see [55], Theorem 7.5.15.

In type K we have identified $K(2m+1)$ with $A(2m+1)$ via D_K and also modified the $\mathfrak{t}_k$ used in [55], Theorem 7.5.13, slightly. Note that the standard bases of the tori $\mathfrak{t}_k$ exhibited here are all *toral* bases.

The closure relations in $\mathcal{T}'$ are not too hard to determine:

Proposition 3.2. *We have*

$$\overline{G.\mathfrak{t}_k} = G.\mathfrak{t}_k \cup G.\mathfrak{t}_{k+1} \cup \cdots \cup G.\mathfrak{t}_{\mu(\mathfrak{g})}$$

for $k = 0 + \delta_{\mathfrak{g}K}, \ldots, \mu(\mathfrak{g})$.

Proof. Note first that the result follows by induction if we can prove $\mathfrak{t}_k \in \overline{G.\mathfrak{t}_{k-1}}$. Assume first that $\mathfrak{g}$ is of type W and define a one-parameter subgroup $t \to \varphi_t$ of $\mathrm{Aut}(A(n))$ by $\varphi_t(x_i) = x_i$ if $i \neq k$ and $\varphi_t(x_k) = t^{-1}x_k$. This induces a one-parameter subgroup $t \to \sigma_{\varphi_t}$ of G, and an easy calculation shows that

$$\begin{aligned} \sigma_{\varphi_t}(x_i\partial_i) &= x_i\partial_i && \text{for } 1 \leq i < k \\ \sigma_{\varphi_t}((1+x_k)\partial_k) &= (t+x_k)\partial_k \\ \sigma_{\varphi_t}((1+x_i)\partial_i) &= (1+x_i)\partial_i && \text{for } k < i \leq n \end{aligned}$$

Now for any point $y \in \bigwedge W(n)$ we write (y) for the line through it (recall that $\mathcal{T}$ is a subset of $\mathbb{P}(\bigwedge W(n))$). Then $\mathfrak{t}_{k-1}$ identifies with $(x_1\partial_1 \wedge \cdots \wedge x_{k-1}\partial_{k-1} \wedge (1+x_k)\partial_k \wedge \cdots \wedge (1+x_n)\partial_n)$ and we get

$$\begin{aligned} &\sigma_{\varphi_t}.(x_1\partial_1 \wedge \cdots \wedge x_{k-1}\partial_{k-1} \wedge (1+x_k)\partial_k \wedge \cdots \wedge (1+x_n)\partial_n) \\ &\quad = (x_1\partial_1 \wedge \cdots \wedge x_{k-1}\partial_{k-1} \wedge (t+x_k)\partial_k \wedge \cdots \wedge (1+x_n)\partial_n). \end{aligned}$$

Taking the limit as t approaches zero, we get $\lim_{t\to 0} \sigma_{\varphi_t}.\mathfrak{t}_{k-1} = (x_1\partial_1 \wedge \cdots \wedge x_k\partial_k \wedge (1+x_{k+1})\partial_{k+1} \wedge \cdots \wedge (1+x_n)\partial_n) = \mathfrak{t}_k \in \overline{G.\mathfrak{t}_{k-1}}$. If $\mathfrak{g}$ is of type S, then the automorphisms σ_{φ_t} restrict to $\mathfrak{g}$, and we get $\lim_{t\to 0} \sigma_{\varphi_t}.\mathfrak{t}_{k-1} = \mathfrak{t}_k$ in exactly the same way. For $\mathfrak{g}$ of type H or K we only have to modify the approach slightly: Define a one-parameter subgroup $t \to \mu_t$ of $\mathrm{Aut}(A(n))$ by $\mu_t(x_{k-\delta_{\mathfrak{g}K}}) = t^{-1}x_{k-\delta_{\mathfrak{g}K}}$, $\mu_t(x_{(k-\delta_{\mathfrak{g}K})'}) = tx_{(k-\delta_{\mathfrak{g}K})'}$ and $\mu_t(x_i) = x_i$ for all other i. One checks easily, using Theorems 7.3.6 and 7.3.8 in [55], that the automorphisms σ_{μ_t} restrict to $\mathfrak{g}$, and calculations similar to those we did for type W show that $\lim_{t\to 0} \sigma_{\mu_t}.\mathfrak{t}_{k-1} = \mathfrak{t}_k$ in these cases also. □

In particular we recover the result (from [6]) that when $\mathfrak{g} \in \{W, S, H\}$ we have $\overline{G.\mathfrak{t}_0} = \mathcal{T}$, i.e., $\mathfrak{t}_0$ is a generic tori of $\mathfrak{g}$. If $\mathfrak{g} = K(2m+1)$, then there are *no* generic tori, a fact which was proved in [6] using detailed information on an associated Poisson algebra. It can, however, also be done directly: Using the formulas (2.7)–(2.11) one can easily show that the tori $\mathfrak{t}_k$ are in fact self-centralizing, which implies

$$\dim(\mathcal{T}) = \dim(\mathfrak{g}) - \mathrm{rk}(\mathfrak{g}) = \dim(\mathfrak{g}) - \mu(\mathfrak{g}) = \dim(\mathfrak{g}) - (m+1).$$

But then it quickly follows from (2.15) that

$$\dim(G) < \dim(\mathcal{T}),$$

and thus there can be no generic tori in $K(2m+1)$.

3.2 CRT and non-generic tori

The following analogue of CRT can be pieced together from the results of [42], [64], [63] and [6]:

Theorem 3.3. *Assume that* $\mathfrak{g} \in \{W, S, H\}$. *Then* $W(\mathfrak{g}, \mathfrak{t}_0) \cong \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$ *and the natural restriction map*

$$\mathrm{res} : F[\mathfrak{g}]^G \to F[\mathfrak{t}_0]^{W(\mathfrak{g},\mathfrak{t}_0)}$$

is an algebra isomorphism. Furthermore, $F[\mathfrak{g}]^G$ *is a polynomial algebra in* $\mu(\mathfrak{g})$ *variables.*

Of course, all the statements of this theorem remain true with $\mathfrak{t}_0$ replaced by any $\mathfrak{t} \in G.\mathfrak{t}_0$, or, to put it in other words, with $\mathfrak{t}_0$ replaced by any other generic torus. We are interested in what happens for the *non-generic* tori. In order to calculate the Weyl groups with respects to these it will be necessary to decompose the standard tori given in (3.2), (3.3), (3.4), so define for the three Cartan types W, S and H, tori $\mathfrak{t}'_k$ and $\mathfrak{t}''_k$ for $1 \leq k \leq \mu(\mathfrak{g})$ by

$$\mathfrak{t}'_k = \sum_{i=1}^{k} Fx_i\partial_i \qquad \text{if } \mathfrak{g} = W(n)$$

$$\mathfrak{t}'_k = \sum_{i=1}^{k} F(x_i\partial_i - x_n\partial_n) \qquad \text{if } \mathfrak{g} = S(n)$$

$$\mathfrak{t}'_k = \sum_{i=1}^{k} F(x_i\partial_i - x_{i'}\partial_{i'}) \qquad \text{if } \mathfrak{g} = H(2m)$$

and

$$\mathfrak{t}''_k = \sum_{i=k+1}^{n} F(1 + x_i)\partial_i \qquad \text{if } \mathfrak{g} = W(n)$$

$$\mathfrak{t}''_k = \sum_{i=k+1}^{n-1} F((1 + x_i)\partial_i - x_n\partial_n) \qquad \text{if } \mathfrak{g} = S(n)$$

$$\mathfrak{t}''_k = \sum_{i=k+1}^{m} F((1 + x_i)\partial_i - x_{i'}\partial_{i'}) \qquad \text{if } \mathfrak{g} = H(2m)$$

So we have $\mathfrak{t}_k = \mathfrak{t}'_k \oplus \mathfrak{t}''_k$. Let $\pi : \mathfrak{g} \to \mathfrak{g}/\mathfrak{g}_{\geq 0}$ denote the canonical quotient map. Since G preserves $\mathfrak{g}_{\geq 0}$ and $\mathfrak{t}'_k = \mathfrak{t}_k \cap \mathfrak{g}_{\geq 0}$ we have a group homomorphism

$$\Psi : W(\mathfrak{g}, \mathfrak{t}_k) \to GL(\mathfrak{t}'_k) \times GL(\pi(\mathfrak{t}_k)).$$

In the extremal cases we already know $W(\mathfrak{g}, \mathfrak{t}_0)$ from Theorem 3.3, while it is relatively easy to show that

$$W(\mathfrak{g}, \mathfrak{t}_{\mu(\mathfrak{g})}) \cong N_{G_0}(\mathfrak{t}_{\mu(\mathfrak{g})})/C_{G_0}(\mathfrak{t}_{\mu(\mathfrak{g})})$$

which is more or less the 'usual' Weyl group of the reductive group G_0. It turns out that $W(\mathfrak{g}, \mathfrak{t}_k)$ is built out of smaller Weyl groups of these two types, along with the kernel of Ψ. To prove this we need a couple of lemmas, the first of which can be proved in a very general setup. Let A be any finite-dimensional commutative F-algebra, and note that we can define a group homomorphism $\mathrm{Aut}(A) \to \mathrm{Aut}(\mathrm{Der}(A))$, $\varphi \mapsto \sigma_\varphi$, by $\sigma_\varphi(D) = \varphi \circ D \circ \varphi^{-1}$ for $D \in \mathrm{Der}(A)$, just as we did for the case $A = A(n)$. Now we have:

Lemma 3.4. *Assume that the module of Kähler differentials $\Omega_{A/F}$ is a free A-module. Let $\mathfrak{l}$ be any restricted subalgebra of $\mathrm{Der}(A)$, with maximal torus $\mathfrak{t}$, let $a_1, \dots, a_n \in A$ be weight vectors with respect to the $\mathfrak{t}$-action such that $\{da_1, \dots, da_n\}$ is an A-basis of $\Omega_{A/F}$, and let φ be an F-algebra automorphism of A such that σ_φ restricts to a Lie automorphism of $\mathfrak{l}$. Then the following are equivalent:*

1. *σ_φ normalizes $\mathfrak{t}$.*
2. *$\varphi(a_1), \dots, \varphi(a_n)$ are weight vectors with respect to the $\mathfrak{t}$-action.*

Furthermore, σ_φ centralises $\mathfrak{t}$ if and only if the weights of a_i and $\varphi(a_i)$ are the same for $1 \leq i \leq n$.

Proof. $1 \Rightarrow 2$: For any $D \in \mathfrak{t}$ we have

$$(\varphi^{-1} \circ D \circ \varphi)(a_i) = \sigma_{\varphi^{-1}}(D)(a_i) = \lambda(\sigma_{\varphi^{-1}}(D))a_i$$

for some weight $\lambda \in \mathfrak{t}^*$. So $D(\varphi(a_i)) = \lambda(\sigma_{\varphi^{-1}}(D))\varphi(a_i)$ and $\varphi(a_i)$ is a weight vector, with weight λ' defined by $\lambda'(D') = \lambda(\sigma_{\varphi^{-1}}(D'))$ for all $D' \in \mathfrak{t}$.

$2 \Rightarrow 1$: Let $\{f_i\}_{1 \leq i \leq n}$ be the A-basis of $\mathrm{Hom}_A(\Omega_{A/F}, A)$ dual to the basis $\{da_i\}$ of $\Omega_{A/F}$. The preimage D_i of f_i under the canonical isomorphism $\mathrm{Der}(A) \xrightarrow{\sim} \mathrm{Hom}_A(\Omega_{A/F}, A)$ satisfies $D_i(a_j) = \delta_{ij}$, and $\{D_i\}_{1 \leq i \leq n}$ is an A-basis of $\mathrm{Der}(A)$. We have

$$D = \sum_{i=1}^{n} D(a_i) D_i \tag{3.6}$$

for all $D \in \mathrm{Der}(A)$. Now define $\mathfrak{t}' = \sum_{i=1}^{n} F a_i D_i$. The $a_i D_i$ are commuting toral elements of $\mathrm{Der}(A)$, and so $\mathfrak{t}'$ is a torus. Since the a_i are weight vectors, it follows from (3.6) that $\mathfrak{t} \subseteq \mathfrak{t}' \cap \mathfrak{l}$, and by maximality of $\mathfrak{t}$ we must have $\mathfrak{t} = \mathfrak{t}' \cap \mathfrak{l}$. For any $D \in \mathfrak{t}$ we get now

$$\sigma_{\varphi^{-1}}(D) = \sum_{i=1}^{n} \sigma_{\varphi^{-1}}(D)(a_i) D_i = \sum_{i=1}^{n} \lambda_i(D) a_i D_i$$

for certain weights $\lambda_i \in \mathfrak{t}^*$. So $\sigma_{\varphi^{-1}}(D) \in \mathfrak{t}' \cap \mathfrak{l} = \mathfrak{t}$ and $\sigma_{\varphi^{-1}}$ normalises $\mathfrak{t}$. The proof of the last statement is now easy, and will be left to the reader. □

We intend, of course, to use this lemma with $A = A(n)$, $\mathfrak{l} = \mathfrak{g}$ and $\mathfrak{t} = \mathfrak{t}_k$. Define

$$z_i = \begin{cases} x_i & \text{if } 1 \leq i \leq k \text{ or } \mu(\mathfrak{g}) < i \leq n \\ y_i & \text{if } k+1 \leq i \leq \mu(\mathfrak{g}) \end{cases}$$

Then one checks easily that $z_1, \dots, z_n$ are weight vectors with respect to the action of $\mathfrak{t}_k$ on $A(n)$, and that $\{dz_1, \dots, dz_n\}$ is an $A(n)$-basis of $\Omega_{A(n)/F}$. Furthermore, $\{z_1^{\alpha_1} \cdots z_n^{\alpha_n} \mid 0 \leq \alpha_1, \dots, \alpha_n < p\}$ is an F-basis of $A(n)$ consisting of weight vectors. Using this basis one can easily determine the weight spaces of $A(n)$ with respect to the $\mathfrak{t}_k$-action. In fact, if $\{\beta_1 \dots, \beta_{\mu(\mathfrak{g})}\}$ is the basis of $\mathfrak{t}_k^*$ dual to the standard basis of $\mathfrak{t}_k$ given in (3.2), (3.3). (3.4), then the weight lattice is $\sum_{i=1}^{\mu(\mathfrak{g})} \mathbb{F}_p \beta_i$ and the weight spaces are

$$A(n)_{b_1\beta_1 + \cdots + b_n\beta_n} = F z_1^{b_1} \cdots z_n^{b_n}$$

for $\mathfrak{g} = W(n)$,

$$A(n)_{b_1\beta_1 + \cdots + b_{n-1}\beta_{n-1}} = \sum_{j=0,\dots,p-1} F z_1^{b_1+j} \cdots z_{n-1}^{b_{n-1}+j} z_n^j \tag{3.7}$$

for $\mathfrak{g} = S(n)$, and

$$A(2m)_{b_1\beta_1 + \cdots + b_m\beta_m} = \sum_{0 \leq c_1, \dots, c_m < p} F z_1^{b_1+c_1} \cdots z_m^{b_m+c_m} z_{m+1}^{c_1} \cdots z_{2m}^{c_m} \tag{3.8}$$

for $\mathfrak{g} = H(2m)$. The notation used here is not quite precise: The b_i are elements in $\mathbb{F}_p$ on the left hand sides, while we use their integer representatives in the interval $I = [0, \dots, p-1]$ on the right hand sides. Furthermore, all exponents on the right should be thought of as reduced mod p to an integer in I.

Lemma 3.4 and the preceding discussion shows that we have an injective homomorphism $W(\mathfrak{g}, \mathfrak{t}_k) \hookrightarrow (\sum_{i=1}^{\mu(\mathfrak{g})} \mathbb{F}_p \beta_i)^n$. To determine for which sets of weights $\{\lambda_1, \dots, \lambda_n\}$ there exists $\sigma_\varphi \in G$ such that $\varphi(z_i)$ has weight λ_i, we need only a couple of well known results on automorphisms of $A(n)$, which we put together in a lemma:

Lemma 3.5. *Let $f_1, \dots, f_n \in A(n)$. There exists an automorphism $\varphi \in A(n)$ satisfying $\varphi(z_i) = f_i$ if and only if the following two conditions are satisfied:*

$$f(z_i) - z_i \in \mathfrak{m} \qquad \text{for all } i \tag{3.9}$$

$$\det\big(\big(\partial_i((f_j)_1)\big)_{i,j=1}^n\big) \neq 0. \tag{3.10}$$

Assume these conditions hold. Then σ_φ induces an automorphism of $S(n)$ if and only if

$$\det\big(\big(\partial_i(f_j)\big)_{i,j=1}^n\big) \in F, \tag{3.11}$$

and σ_φ induces an automorphism of $H(n)$ (assuming $n = 2m$ is even) if and only if

$$\{f_i, f_j\} = c\sigma(i)\delta_{i'j} \tag{3.12}$$

for some $c \in F^*$ and all i, j.

We are almost ready to determine the Weyl group of $\mathfrak{g}$ relative to $\mathfrak{t}_k$. Let us first define three subgroups of $W(\mathfrak{g}, \mathfrak{t}_k)$:

$$W_1 = \{w \in W(\mathfrak{g}, \mathfrak{t}_k) \mid w_{|\mathfrak{t}_k''} = \mathrm{id}\}$$

$$W_2 = \{w \in W(\mathfrak{g}, \mathfrak{t}_k) \mid w_{|\mathfrak{t}'_k} = id \text{ and } w(\mathfrak{t}''_k) \subseteq \mathfrak{t}''_k\}$$
$$W_3 = \ker(\Psi)$$

Now we have:

Proposition 3.6. *Assume* $\mathfrak{g} \in \{W, S, H\}$ *and* $k \geq 1$. *Then*

$$W(\mathfrak{g}, \mathfrak{t}_k) \cong (W_1 \times W_2) \ltimes W_3,$$

with

$$W_1 \cong \begin{cases} S_k & \text{if } \mathfrak{g} = W(n) \\ S_{k+1} & \text{if } \mathfrak{g} = S(n) \\ S_k \ltimes (\mathbb{Z}/2\mathbb{Z})^k & \text{if } \mathfrak{g} = H(n) \end{cases} \tag{3.13}$$
$$W_2 \cong \mathrm{GL}_{\mu(\mathfrak{g})-k}(\mathbb{F}_p) \tag{3.14}$$
$$W_3 \cong \mathrm{M}_{\mu(\mathfrak{g})-k,k}(\mathbb{F}_p) \tag{3.15}$$

Proof. It is easy to see that the product of W_2 and W_3 must be direct, and that the intersection $(W_1 \times W_2) \cap W_3$ is trivial. Our approach is to construct 'by hand' three subgroups W'_1, W'_2, W'_3 isomorphic to the right hand sides of (3.13), (3.14), (3.15), such that $W'_j \subseteq W_j$ for $j = 1, 2, 3$ and $W(\mathfrak{g}, \mathfrak{t}_k) = W'_1 W'_2 W'_3$. From this it follows automatically that $W'_j = W_j$ and we will be done. Note that we will sometimes define elements of $W(\mathfrak{g}, \mathfrak{t}_k)$ simply by giving weight vectors satisfying the requirements of Lemma 3.5.

Assume first that $\mathfrak{g} = W(n)$. A moment's thought reveals that weight vectors $f_j = c_j z_1^{c_{j1}} \cdots z_n^{c_{jn}}$, $1 \leq j \leq n$, satisfy (3.9), (3.10) if and only if

$$f_j = c_j x_{\tau(j)} y_{i+1}^{c_{j(i+1)}} \cdots y_n^{c_{jn}} \qquad 1 \leq j \leq k \tag{3.16}$$
$$f_j = y_{k+1}^{c_{j(k+1)}} \cdots y_n^{c_{jn}} \qquad k+1 \leq j \leq n \tag{3.17}$$

where $\tau \in S_k$ and $(c_{ji})_{k<j,i\leq n} \in \mathrm{GL}_{n-k}(\mathbb{F}_p)$. Inspired by this we define the subgroup W'_1 of $W(\mathfrak{g}, \mathfrak{t}_k)$ by

$$\varphi(x_j) = x_{\tau(j)} \qquad 1 \leq j \leq k$$
$$\varphi(y_j) = y_j \qquad k+1 \leq j \leq n$$

for any $\tau \in S_k$, the subgroup W'_2 by

$$\varphi(x_j) = x_j \qquad 1 \leq j \leq k$$
$$\varphi(y_j) = y_{k+1}^{c_{j(k+1)}} \cdots y_n^{c_{jn}} \qquad k+1 \leq j \leq n$$

for any $(c_{ji})_{k<j,i\leq n} \in \mathrm{GL}_{n-k}(\mathbb{F}_p)$, and finally the subgroup W'_3 by

$$\varphi(x_j) = x_j y_{k+1}^{c_{j(k+1)}} \cdots y_n^{c_{jn}} \qquad 1 \leq j \leq k$$
$$\varphi(y_j) = y_j \qquad k+1 \leq j \leq n$$

with the c_{ji} arbitrary. It follows from (3.16) and (3.17) that any element of $W(\mathfrak{g}, \mathfrak{t}_k)$ is a product of elements from W_1', W_2', W_3'. Now it is a routine matter to check that $W_j' \subseteq W_j$ for $j = 1, 2, 3$, and that $W_1' \cong S_k$, $W_2' \cong \mathrm{GL}_{n-k}(\mathbb{F}_p)$, $W_3' \cong \mathrm{M}_{n-k,k}(\mathbb{F}_p)$.

Assume now $\mathfrak{g} = S(n)$. Using the weight space decomposition (3.7) we see that weight vectors $f_1, \ldots, f_n$ satisfy (3.9), (3.10) if and only if they have the following form, modulo the corresponding weight spaces:

$$f_j = x_{\tau(j)} y_{k+1}^{c_{j(k+1)}} \cdots y_{n-1}^{c_{j(n-1)}} \qquad 1 \leq j \leq k \text{ and } j = n \tag{3.18}$$

$$f_j = y_{k+1}^{c_{j(k+1)}} \cdots y_{n-1}^{c_{j(n-1)}} \qquad k+1 \leq j \leq n-1 \tag{3.19}$$

Now $\tau \in S_{k+1}$ is a permutation on $\{1, \ldots, k, n\}$ and $(c_{ji})_{k<j,i<n}$ is a matrix in $\mathrm{GL}_{n-1-k}(\mathbb{F}_p)$. Define $\varphi \in \mathrm{Aut}(A(n))$ by $\varphi(z_j) = f_j$ and let

$$\begin{aligned} w_i = \sigma_{\varphi^{-1}}(y_i\partial_i - x_n\partial_n) &= \sum_{j=1}^{n} \sigma_{\varphi^{-1}}(y_i\partial_i - x_n\partial_n)(z_j)\partial_j \\ &= \sum_{j=1}^{n} (c_{ji} - \delta_{j\tau^{-1}(n)}) z_j \partial_j \end{aligned}$$

for $k < i < n$. To get $\mathrm{div}(w_i) = 0$ we must have

$$c_{ni} = \sum_{j=1}^{n-1} c_{ji} + 1 \tag{3.20}$$

for $k < i < n$. Assume that f_n satisfies this, then it is a simple exercise in linear algebra to show

$$\det\big(\big(\partial_i(f_j)\big)_{j,i}\big) = \det\big((c_{sr})_{k<s,r<n}\big) \in F.$$

It follows that any φ defined by $\varphi(z_j) = f_j$ subject to the condition (3.20) induces an element of $W(\mathfrak{g}, \mathfrak{t}_k)$, and that all elements of $W(\mathfrak{g}, \mathfrak{t}_k)$ can be obtained in this way. It is now easy to see how to define the three subgroups W_1', W_2', W_3' to get the desired result.

Finally the case $\mathfrak{g} = H(n)$, with $n = 2m$ for some $m \geq 1$. Assume $\sigma_\varphi \in N_G(\mathfrak{t}_k)$. For any $D \in \mathfrak{t}_k$ we have

$$\sigma_\varphi(D) = \sum_{j=1}^{n} \sigma_\varphi(D)(z_j)\partial_j = \sum_{j=1}^{n} \lambda_j(D) z_j \partial_j \in \mathfrak{t}_k$$

for certain weights λ_j, from which it follows that $\lambda_{j'} = -\lambda_j$. In other words, σ_φ is completely determined by the weights of $\varphi(z_1), \ldots, \varphi(z_m)$. The conditions (3.9) and (3.10) together with the weight space decomposition (3.8) imply that $\varphi(x_j)$, $1 \leq j \leq k$, is a weight vector belonging to a weight of the form $\sum_{i=k+1}^{m} c_{ji}\beta_i$ or $\pm\beta_{i_j} + \sum_{i=k+1}^{m} c_{ji}\beta_i$ for an integer $i_j \in \{1, \ldots, k\}$, while the $\varphi(y_j)$, $k < j \leq m$, belong to weight spaces of the former type. Since φ must satisfy (3.12) we can rule out the first possible kind of weight space for the $\varphi(x_j)$: For if $\varphi(x_j) \in A(n)_{\sum_{i=k+1}^{m} c_{ji}\beta_i}$,

$1 \leq j \leq k$, then $\varphi(x_{j'}) \in A(n)_{-\sum_{i=k+1}^{m} c_{ji}\beta_i}$, and the first degree terms of $\varphi(x_j), \varphi(x_{j'})$ must be of the form $\sum_{i=m+k+1}^{n} a_i x_i$, $\sum_{i=m+k+1}^{n} b_i x_i$ respectively, for some $a_i, b_i \in F$. But then

$$\{\varphi(x_j), \varphi(x_{j'})\}_0 = \Big\{ \sum_{i=m+k+1}^{n} a_i x_i, \sum_{i=m+k+1}^{n} b_i x_i \Big\} = 0$$

which contradicts (3.12). So $\varphi(x_j) \in A_{\pm\beta_{i_j} + \sum_{i=k+1}^{m} c_{ji}\beta_i}$, and the first degree term of $\varphi(x_j)$ is $a_j x_{i_j}$ if the sign is positive and $a_j x_{i'_j}$ if the sign is negative. For $\varphi(x_{j'})$ it is the other way around. Define a map $\tau : \{1, \ldots, k, 1', \ldots, k'\} \to \{1, \ldots, k, 1', \ldots, k'\}$ by sending j to the index of the first degree term in $\varphi(x_j)$. From the condition $\{\varphi(x_j), \varphi(x_i)\}_0 = \alpha\delta_{j'i}$, $1 \leq j, i \leq k$, it follows that τ can be identified with an element of $S_k \ltimes (\mathbb{Z}/2\mathbb{Z})^k$ (where the copies of $\mathbb{Z}/2\mathbb{Z}$ act coordinate-wise by $'$).

By now we know that

$$\begin{aligned}
\varphi(x_j)_1 &= a_j x_{\tau(j)} && \text{if } 1 \leq j \leq k \text{ or } m < j \leq k+m \\
\varphi(y_j)_1 &= \sum_{i=k+1}^{m} (c_{ji} x_i + d_{ji} x_{i'}) && \text{if } k < j \leq m \\
\varphi(x_j)_1 &= \sum_{i=k+1}^{m} d_{ji} x_{i'} && \text{if } k+m < j \leq 2m
\end{aligned}$$

and by imposing the condition (3.10) on these terms, we see that the matrix $(c_{ji})_{k<j,i\leq m}$ must be invertible. Define the subgroup W_1' of $W(\mathfrak{g}, \mathfrak{t}_k)$ by

$$\begin{aligned}
\varphi(x_j) &= \sigma(\tau(j)) x_{\tau(j)} && \text{for } 1 \leq j \leq k \text{ and } m < j \leq m+k \\
\varphi(y_j) &= y_j && \text{for } k < j \leq m \\
\varphi(x_j) &= x_j && \text{for } m+k < j \leq 2m
\end{aligned}$$

for any $\tau \in S_k \ltimes (\mathbb{Z}/2\mathbb{Z})^k$, the subgroup W_2' by

$$\begin{aligned}
\varphi(x_j) &= x_j && \text{for } 1 \leq j \leq k \text{ and } m < j \leq m+k \\
\varphi(y_j) &= y_{i+1}^{c_{j(k+1)}} \cdots y_m^{c_{jm}} && \text{for } k < j \leq m \\
\varphi(x_j) &= \sum_{i=k+1}^{m} d_{ij'} x_{i'} y_{k+1}^{-c_{j'(k+1)}} \cdots y_i^{-c_{j'i}+1} \cdots y_m^{-c_{j'm}} && \text{for } m+k < j \leq 2m
\end{aligned}$$

where $(c_{ji})_{k<j,i\leq m} \in \mathrm{GL}_{m-k}(\mathbb{F}_p)$ and $(d_{ij'})_{k<j',i\leq m} = (c_{j'i})^{-1}$, and finally the subgroup W_3' of $W(\mathfrak{g}, \mathfrak{t}_i)$ by

$$\begin{aligned}
\varphi(x_j) &= x_j y_{k+1}^{c_{j(k+1)}} \cdots y_m^{c_{jm}} && \text{for } 1 \leq j \leq k \\
\varphi(y_j) &= y_j && \text{for } k < j \leq m \\
\varphi(x_j) &= x_j y_{k+1}^{-c_{j'(k+1)}} \cdots y_m^{-c_{j'm}} && \text{for } m < j \leq m+k \\
\varphi(x_j) &= x_j - \Big(\sum_{i=1}^{k} c_{ij'} x_i x_{i'} \Big) y_{j'}^{p-1} && \text{for } m+k < j \leq 2m.
\end{aligned}$$

One checks easily that these automorphisms are actually well defined, i.e., that they satisfy (3.9), (3.10) and (3.12). The preceding discussion shows that every element of $W(\mathfrak{g}, \mathfrak{t}_k)$ must be a product of elements from W_1', W_2', W_3', and the result follows. $\square$

Armed with this detailed understanding of the Weyl groups associated to non-generic tori, we are able to prove an extension of Theorem 3.3:

Theorem 3.7. *Assume $\mathfrak{g} \in \{W, S, H\}$ and let $\mathfrak{t} \subseteq \mathfrak{g}$ be any torus of dimension $\mu(\mathfrak{g})$. The canonical restriction homomorphism*

$$\mathrm{res} : F[\mathfrak{g}]^G \to F[\mathfrak{t}]^{W(\mathfrak{g},\mathfrak{t})}.$$

is an isomorphism if and only if $\mathfrak{t}$ is generic.

Proof. Because of Theorem 3.3 it is enough to show that res is *not* an isomorphism if $\mathfrak{t}$ is not generic. More precisely, we will show that res is not surjective in this case. Assume first $\mathfrak{t} = \mathfrak{t}_k$ for some $k \in \{1, \dots, \mu(\mathfrak{g}) - 1\}$ and write $F[\mathfrak{t}_k] = F[X_1, \dots, X_k, Y_{k+1}, \dots, Y_{\mu(\mathfrak{g})}]$, where $\{X_1, \dots, X_k\}$ is a basis of $(\mathfrak{t}_k')^*$ dual to the standard basis of $(\mathfrak{t}_k')$ and $\{Y_{k+1}, \dots, Y_{\mu(\mathfrak{g})}\}$ is a basis of $(\mathfrak{t}_k'')^*$ dual to the standard basis of $(\mathfrak{t}_k'')$. It follows directly from the definition of the subgroups W_1 and W_3 that these act trivially on $F[Y_{k+1}, \dots, Y_{\mu(\mathfrak{g})}] \cong F[\mathfrak{t}_k'']$, so

$$F[Y_{k+1}, \dots, Y_{\mu(\mathfrak{g})}]^{W_2} \subseteq F[\mathfrak{t}_k]^{W(\mathfrak{g},\mathfrak{t}_k)}.$$

Let us now identify the action of W_2 on $F[Y_{k+1}, \dots, Y_{\mu(\mathfrak{g})}]$ with the action of $\mathrm{GL}_{\mu(\mathfrak{g})-k}(\mathbb{F}_p)$ on $S(\mathrm{tor}(\mathfrak{t}_k'')^* \otimes F)$ induced from the natural action of $\mathrm{GL}_{\mu(\mathfrak{g})-k}(\mathbb{F}_p)$ on $\mathrm{tor}(\mathfrak{t}_k'')$. Then, by a classical invariant theoretic result by Dickson ([15], see also the proof of Theorem 1 in [42]) we have a homogeneous invariant $f \in F[Y_{k+1}, \dots, Y_{\mu(\mathfrak{g})}]$ of degree $p^{\mu(\mathfrak{g})-k} - p^{\mu(\mathfrak{g})-k-1}$. We also know, however, that $F[\mathfrak{g}]^G$ is generated by algebraically independent polynomials of degree at least $p^{\mu(\mathfrak{g})} - p^{\mu(\mathfrak{g})-1}$ ([42], [64], [63]), and since res is a graded homomorphism it cannot be surjective.

Assume now $\mathfrak{t} = \mathfrak{t}_{\mu(\mathfrak{g})}$. Then we have

$$W(\mathfrak{g}, \mathfrak{t}_{\mu(\mathfrak{g})}) = W_1 \cong N_{G_0}(\mathfrak{t}_{\mu(\mathfrak{g})})/C_{G_0}(\mathfrak{t}_{\mu(\mathfrak{g})}).$$

By standard reductive group theory there exists an invariant f of degree at most 2 (one can also easily find such an f manually, take for example $f = X_1 + \cdots + X_n$ for $\mathfrak{g} = W(n)$, with the notation from the previous case). By the same argument as before, res cannot be surjective, and we are done. $\square$

The natural next question to adress is of course: what happens when $\mathfrak{g} = K(2m+1)$? It is not at all clear how to determine the structure of $F[\mathfrak{g}]^G$ in this case. Even though there are no generic tori, it is still entirely possible that one could find a torus such that restriction induces an isomorphism of invariants. This is the same as saying that Theorem 3.7 cannot be extended to type K. On the other, if the theorem *does* extend, then one will have to find some other way to describe $F[\mathfrak{g}]^G$. Either way, it is certainly an interesting problem, that deserves further study!

Bibliography

[1] Donald G. Babbitt and Jane E. Kister (eds.), *Featured reviews in Mathematical Reviews 1995–1996*, Featured Reviews in Mathematical Reviews, American Mathematical Society, Providence, RI, 1998.

[2] L. P. Bedratyuk, *Symmetric invariants of some modular Lie algebras*, Mat. Sb. **184** (1993), no. 9, 149–160.

[3] Georgia Benkart, Thomas Gregory, and Alexander Premet, *The recognition theorem for graded Lie algebras in prime characteristic*, Mem. Amer. Math. Soc. **197** (2009), no. 920, xii+145.

[4] Richard E. Block and Robert Lee Wilson, *Classification of the restricted simple Lie algebras*, J. Algebra **114** (1988), no. 1, 115–259.

[5] Jean-Marie Bois, *Gelfand-Kirillov conjecture in positive characteristics*, J. Algebra **305** (2006), no. 2, 820–844.

[6] Jean-Marie Bois, Rolf Farnsteiner, and Bin Shu, *Weyl groups for non-classical restricted Lie algebras and the Chevalley Restriction Theorem*, Forum Math. **26** (2014), no. 5, 1333–1379.

[7] Sofiane Bouarroudj, Alexei Lebedev, Dimitry Leites, and Irina Shchepochkina, *Lie algebra deformations in characteristic 2*, Math. Res. Lett. **22** (2015), no. 2, 353–402.

[8] Amiram Braun, *The center of the enveloping algebra of the p-lie algebras* $\mathfrak{sl}_n$, $\mathfrak{pgl}_n$, $\mathfrak{psl}_n$, *when p divides n*, 2015. Preprint.

[9] Kenneth A. Brown and Iain Gordon, *The ramification of centres: Lie algebras in positive characteristic and quantised enveloping algebras*, Math. Z. **238** (2001), no. 4, 733–779.

[10] Damien Calaque and Carlo A. Rossi, *Lectures on Duflo isomorphisms in Lie algebra and complex geometry*, EMS Series of Lectures in Mathematics, European Mathematical Society (EMS), Zürich, 2011.

[11] R. W. Carter, *Lie algebras of finite and affine type*, Cambridge Studies in Advanced Mathematics, vol. 96, Cambridge University Press, Cambridge, 2005.

[12] Michel Demazure and Pierre Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970. Avec un appendice ıt Corps de classes local par Michiel Hazewinkel.

[13] S. P. Demuškin, *Cartan subalgebras of the simple Lie p-algebras* W_n *and* S_n, Sibirsk. Mat. Ž. **11** (1970), 310–325.

[14] ———, *Cartan subalgebras of simple non-classical Lie p-algebras*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 915–932.

[15] Leonard Eugene Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. Amer. Math. Soc. **12** (1911), no. 1, 75–98.

[16] Jacques Dixmier, *Algèbres enveloppantes*, Gauthier-Villars Éditeur, Paris-Brussels-Montreal, Que., 1974. Cahiers Scientifiques, Fasc. XXXVII.

[17] Michel Duflo, *Opérateurs différentiels bi-invariants sur un groupe de Lie*, Ann. Sci. École Norm. Sup. (4) **10** (1977), no. 2, 265–288.

[18] A. S. Dzhumadil′daev, *Generalized Casimir elements*, Izv. Akad. Nauk SSSR Ser. Mat. **49** (1985), no. 5, 1107–1117, 1120.

[19] Rolf Farnsteiner, *Varieties of tori and Cartan subalgebras of restricted Lie algebras*, Trans. Amer. Math. Soc. **356** (2004), no. 10, 4181–4236 (electronic).

[20] Jörg Feldvoss, *Homological topics in the representation theory of restricted Lie algebras*, Lie algebras and their representations (Seoul, 1995), 1996, pp. 69–119.

[21] Jörg Feldvoss and Daniel K. Nakano, *Representation theory of the Witt algebra*, J. Algebra **203** (1998), no. 2, 447–469.

[22] Eric M. Friedlander and Brian J. Parshall, *Rational actions associated to the adjoint representation*, Ann. Sci. École Norm. Sup. (4) **20** (1987), no. 2, 215–226.

[23] Randall R. Holmes and Chaowen Zhang, *Some simple modules for the restricted Cartan-type Lie algebras*, J. Pure Appl. Algebra **173** (2002), no. 2, 135–165.

[24] James E. Humphreys, *Introduction to Lie algebras and representation theory*, Springer-Verlag, New York-Berlin, 1972. Graduate Texts in Mathematics, Vol. 9.

[25] ———, *Linear algebraic groups*, Springer-Verlag, New York-Heidelberg, 1975. Graduate Texts in Mathematics, No. 21.

[26] Nathan Jacobson, *Lie algebras*, Interscience Tracts in Pure and Applied Mathematics, No. 10, Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962.

[27] N. N. Jakovlev, *The center of the enveloping algebra of a Witt algebra*, Funkcional. Anal. i Priložen. **6** (1972), no. 2, 99–100.

[28] Jens Carsten Jantzen, *Representations of Lie algebras in prime characteristic*, Representation theories and algebraic geometry (Montreal, PQ, 1997), 1998, pp. 185–235. Notes by Iain Gordon.

[29] ———, *Representations of algebraic groups*, Second, Mathematical Surveys and Monographs, vol. 107, American Mathematical Society, Providence, RI, 2003.

[30] ———, *Representations of Lie algebras in positive characteristic*, Representation theory of algebraic groups and quantum groups, 2004, pp. 175–218.

[31] V. Kac and B. Weisfeiler, *Coadjoint action of a semi-simple algebraic group and the center of the enveloping algebra in characteristic p*, Nederl. Akad. Wetensch. Proc. Ser. A **79**=Indag. Math. **38** (1976), no. 2, 136–151.

[32] N. A. Koreshkov, *Central elements in the algebra $U(K_m)$*, Izv. Vyssh. Uchebn. Zaved. Mat. **5** (1991), 16–22.

[33] A. I. Kostrikin and I. R. Šafarevič, *Cartan's pseudogroups and the p-algebras of Lie*, Dokl. Akad. Nauk SSSR **168** (1966), 740–742.

[34] Ya. S. Krylyuk, *Maximum dimension of irreducible representations of simple Lie p-algebras of Cartan series S and H*, Mat. Sb. (N.S.) **123(165)** (1984), no. 1, 108–119.

[35] ———, *The index of algebras of Cartan type in finite characteristic*, Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986), no. 2, 393–412.

[36] Zongzhu Lin and Daniel K. Nakano, *Algebraic group actions in the cohomology theory of Lie algebras of Cartan type*, J. Algebra **179** (1996), no. 3, 852–888.

[37] A. A. Mil′ner, *Irreducible representations of modular Lie algebras*, Izv. Akad. Nauk SSSR Ser. Mat. **39** (1975), no. 6, 1240–1259, 1437.

[38] ———, *The maximal degree of irreducible representations of a Lie algebra over a field of positive characteristic*, Funktsional. Anal. i Prilozhen. **14** (1980), no. 2, 67–68.

[39] Ivan Mirković and Dmitriy Rumynin, *Centers of reduced enveloping algebras*, Math. Z. **231** (1999), no. 1, 123–132.

[40] Martin Mygind, *Orbit closures in the Witt algebra and its dual space*, J. Algebra Appl. **13** (2014), no. 5, 1350146, 18.

[41] ———, *Restricted cartan type lie algebras and the coadjoint representation*, Transformation Groups **20** (2015), no. 2, 495–505.

[42] Alexander Premet, *A theorem on the restriction of invariants, and nilpotent elements in W_n*, Mat. Sb. **182** (1991), no. 5, 746–773.

[43] ———, *Irreducible representations of Lie algebras of reductive groups and the Kac-Weisfeiler conjecture*, Invent. Math. **121** (1995), no. 1, 79–117.

[44] ———, *Complexity of Lie algebra representations and nilpotent elements of the stabilizers of linear forms*, Math. Z. **228** (1998), no. 2, 255–282.

[45] Alexander Premet and Serge Skryabin, *Representations of restricted Lie algebras and families of associative $\mathcal{L}$-algebras*, J. Reine Angew. Math. **507** (1999), 189–218.

[46] Alexander Premet and Helmut Strade, *Classification of finite dimensional simple Lie algebras in prime characteristics*, Representations of algebraic groups, quantum groups, and Lie algebras, 2006, pp. 185–214.

[47] ———, *Simple Lie algebras of small characteristic. VI. Completion of the classification*, J. Algebra **320** (2008), no. 9, 3559–3604.

[48] David E. Radford, *Hopf algebras*, Series on Knots and Everything, vol. 49, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.

[49] Khalid Rian, *Extensions of the Witt algebra and applications*, J. Algebra Appl. **10** (2011), no. 6, 1233–1259.

[50] A. N. Rudakov, *The representations of classical semisimple Lie algebras in characteristic p*, Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 735–743.

[51] Serge Skryabin, *Toral rank one simple Lie algebras of low characteristics*, J. Algebra **200** (1998), no. 2, 650–700.

[52] ———, *Invariants of finite group schemes*, J. London Math. Soc. (2) **65** (2002), no. 2, 339–360.

[53] ———, *Representations of the Poisson algebra in prime characteristic*, Math. Z. **243** (2003), no. 3, 563–597.

[54] Helmut Strade, *Darstellungen auflösbarer Lie-p-Algebren*, Math. Ann. **232** (1978), no. 1, 15–32.

[55] ———, *Simple Lie algebras over fields of positive characteristic. I*, de Gruyter Expositions in Mathematics, vol. 38, Walter de Gruyter & Co., Berlin, 2004. Structure theory.

[56] ———, *Simple Lie algebras over fields of positive characteristic. II*, de Gruyter Expositions in Mathematics, vol. 42, Walter de Gruyter & Co., Berlin, 2009. Classifying the absolute toral rank two case.

[57] ———, *Simple Lie algebras over fields of positive characteristic. III*, de Gruyter Expositions in Mathematics, vol. 57, Walter de Gruyter GmbH & Co. KG, Berlin, 2013. Completion of the classification.

[58] Helmut Strade and Rolf Farnsteiner, *Modular Lie algebras and their representations*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 116, Marcel Dekker, Inc., New York, 1988.

[59] Rudolf Tange, *The Zassenhaus variety of a reductive Lie algebra in positive characteristic*, Adv. Math. **224** (2010), no. 1, 340–354.

[60] Lewis W. Topley, *Invariants of centralisers in positive characteristic*, J. Algebra **399** (2014), 1021–1050.

[61] B. Ju. Veĭsfeĭler and V. G. Kac, *The irreducible representations of Lie p-algebras*, Funkcional. Anal. i Priložen. **5** (1971), no. 2, 28–36.

[62] F. D. Veldkamp, *The center of the universal enveloping algebra of a Lie algebra in characteristic p*, Ann. Sci. École Norm. Sup. (4) **5** (1972), 217–240.

[63] Junyan Wei, *The nilpotent variety and invariant polynomial functions in the hamiltonian algebra*, 2014. Preprint.

[64] Junyan Wei, Hao Chang, and Xin Lu, *The variety of nilpotent elements and invariant polynomial functions on the special algebra S_n*, Forum Math. **27** (2015), no. 3, 1689–1715.

[65] Robert Lee Wilson, *Automorphisms of graded Lie algebras of Cartan type*, Comm. Algebra **3** (1975), no. 7, 591–613.

[66] Yu-Feng Yao and Bin Shu, *Nilpotent orbits in the Witt algebra W_1*, Comm. Algebra **39** (2011), no. 9, 3232–3241.

[67] Hans Zassenhaus, *The representations of Lie algebras of prime characteristic*, Proc. Glasgow Math. Assoc. **2** (1954), 1–36.