WEYL GROUPS FOR NON-CLASSICAL RESTRICTED LIE ALGEBRAS AND THE CHEVALLEY RESTRICTION THEOREM

JEAN-MARIE BOIS, ROLF FARNSTEINER and BIN SHU

ABSTRACT. Let $(\mathfrak{g}, [p])$ be a finite-dimensional restricted Lie algebra, defined over an algebraically closed field k of characteristic $p > 0$. The scheme of tori of maximal dimension of $\mathfrak{g}$ gives rise to a finite group $S(\mathfrak{g})$ that coincides with the Weyl group of $\mathfrak{g}$ in case $\mathfrak{g}$ is a Lie algebra of classical type. In this paper, we compute the group $S(\mathfrak{g})$ for Lie algebras of Cartan type and provide applications concerning weight space decompositions, the existence of generic tori and polynomial invariants.

INTRODUCTION

In the structure- and representation theory of complex semi-simple Lie algebras, root systems and their Weyl groups play a fundamental rôle. For fields of positive characteristic the situation is similar, provided one studies Lie algebras $\mathfrak{g} = \mathrm{Lie}(G)$ that are associated with a reductive group G. By contrast, the maximal tori of arbitrary restricted Lie algebras usually are no longer conjugate, so there are many root systems available, whose structure and utility crucially depend on the initially chosen maximal tori. Accordingly, it is not clear which maximal tori are appropriate for defining finite groups that take on the rôle of Weyl groups. In his article [19], Premet studied this problem for the Jacobson-Witt algebras $W(n)$. He identified a maximal torus $\mathfrak{t}_0 \subseteq W(n)$, whose automorphism group allowed to establish an analogue of the Chevalley restriction theorem on polynomial invariants.

One way to address the problem of choosing tori is the systematic study of schemes of tori. Roughly speaking, this geometric approach seeks to identify generic properties of tori and their root systems. In the context of Lie algebras of complexity ≤ 2, that naturally arise in the study of restricted enveloping algebras of tame representation type, this method has produced satisfactory results, cf. [8, 9]. A detailed investigation of the scheme of tori of maximal dimension $\mu(\mathfrak{g})$ of a restricted Lie algebra $\mathfrak{g}$ in [7] led to the definition of a group $S(\mathfrak{g})$ that turned out to coincide with the Weyl group in case $\mathfrak{g}$ is of classical type.

Aside from the analogues of the complex simple Lie algebras there are usually four additional classes of simple restricte Lie algebras, the so-called restricted Lie algebras of Cartan type. These Lie algebras, which include the abovementioned Jacobson-Witt algebras, already differ significantly from their classical precursors in that their maximal tori are no longer conjugate. The main object of the present paper is to identify the corresponding finite groups along with providing applications.

Our paper is organized as follows. After recalling basic results on the scheme $\mathcal{T}_{\mathfrak{g}}$ of tori of a restricted Lie algebra $\mathfrak{g}$, we show in Section 1 that the toral stabilizer $S(\mathfrak{g})$ of $\mathfrak{g}$ is isomorphic to the "Weyl group" associated with any generic torus of $\mathfrak{g}$. For future reference, we also provide criteria for a given torus or Cartan subalgebra to be generic. Section 2 is concerned with the behavior of toral stabilizers under passage to subalgebras and factor algebras. In particular, we show that

the toral stabilizer of a product of restricted Lie algebras is the product of the toral stabilizers of the factors. Using basic results on tori and automorphism groups, due to Demuškin [3, 4] and Wilson [24, 25], respectively, we identify in Section 3 the generic tori of the restricted Lie algebras of Cartan types types W, S and H. Accordingly, the Weyl groups of these tori coincide with the toral stabilizers, whose computation relies on embeddings of certain subalgebras, particularly those of the form $W(\mu(\mathfrak{g})) \hookrightarrow \mathfrak{g}$. Section 5 is devoted to the proof of our main result:

Theorem A. *Suppose that $p \geq 3$ and let $\mathfrak{g}$ be a restricted Lie algebra of Cartan type. Then there is an isomorphism*

$$S(\mathfrak{g}) \cong \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$$

and the scheme $\mathfrak{T}_{\mathfrak{g}}$ of embeddings of tori of maximal dimension is irreducible.

Along the way, a few other toral stabilizers need to be computed, notably those of the Poisson algebras $\mathcal{P}(2r)$ with toral center.

The final section presents applications of our methods and results. With regard to weight space decompositions defined by tori of maximal dimension, the group $S(\mathfrak{g})$ exhibits features analogous to those of Weyl groups: There is an action of $S(\mathfrak{g})$ on the set of weights such that the dimensions of weight spaces are constant on the orbits. As a result, only three types of weight sets can occur for Lie algebras $\mathfrak{g}$ with $S(\mathfrak{g}) \cong \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$. In particular, all root spaces of such Lie algebras have the same dimension.

In [22, Chap.7] Strade shows that the contact algebras $K(2r+1)$ possess infinitely many conjugacy classes of tori of dimension $\mu(K(2r+1)) = r+1$. Using explicit information on Weyl groups and toral stabilizers of the aforementioned Poisson algebras, we prove that $K(2r+1)$ does not possess any generic tori.

Given a restricted Lie algebra $(\mathfrak{g}, [p])$, we denote by $S_{\mathfrak{g}}$ the variety of semi-simple elements. By modifying Premet's approach concerning $W(n)$, we finally establish the following analogue of the Chevalley restriction theorem:

Theorem B. *Suppose that $p \geq 3$ and let $(\mathfrak{g}, [p])$ be a restricted Lie algebra of Cartan type W, S or H with generic torus $\mathfrak{t} \subseteq \mathfrak{g}$. Then the restriction map induces an isomorphism $k[\bar{S}_{\mathfrak{g}}]^G \xrightarrow{\sim} k[\mathfrak{t}]^{\mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)}$. In particular, $k[\bar{S}_{\mathfrak{g}}]^G$ is a polynomial ring in $\mu(\mathfrak{g})$ variables.*

1. Generic Tori and Weyl Groups

Throughout, we shall be working over an algebraically closed field k of characteristic $\mathrm{char}(k) = p > 0$. Unless mentioned otherwise, all algebras and modules are assumed to be finite-dimensional. Given a restricted Lie algebra $(\mathfrak{g}, [p])$, we let $G := \mathrm{Aut}_p(\mathfrak{g})^\circ$ be the identity component of its automorphism group. We denote by $\mu(\mathfrak{g})$ and $\mathrm{rk}(\mathfrak{g})$ the maximal dimension of all tori $\mathfrak{t} \subseteq \mathfrak{g}$ and the minimal dimension of all Cartan subalgebras $\mathfrak{h} \subseteq \mathfrak{g}$, respectively. According to [7, (7.4)], the set

$$\mathfrak{Tor}(\mathfrak{g}) := \{\mathfrak{t} \subseteq \mathfrak{g} \; ; \; \mathfrak{t} \text{ torus}, \; \dim_k \mathfrak{t} = \mu(\mathfrak{g})\}$$

of tori of maximal dimension is locally closed within the Grassmanian $\mathrm{Gr}_{\mu(\mathfrak{g})}(\mathfrak{g})$ of $\mathfrak{g}$. Thanks to [8, (1.6)] and [7, (3.5)], the variety $\mathfrak{Tor}(\mathfrak{g})$ is irreducible of dimension $\dim \mathfrak{Tor}(\mathfrak{g}) = \dim_k \mathfrak{g} - \mathrm{rk}(\mathfrak{g})$.

Let M_k and Ens be the categories of commutative k-algebras (of arbitrary dimension) and sets, respectively. For a torus $\mathfrak{t} \in \mathfrak{Tor}(\mathfrak{g})$, we consider the scheme $\mathfrak{T}_{\mathfrak{g}} : M_k \longrightarrow$ Ens, given by

$$\mathfrak{T}_{\mathfrak{g}}(R) := \{\varphi \in \mathrm{Hom}_p(\mathfrak{t} \otimes_k R, \mathfrak{g} \otimes_k R) \; ; \; \varphi \text{ is a split injective } R\text{-linear map}\}$$

for every $R \in M_k$. Here $\mathrm{Hom}_p(\mathfrak{t} \otimes_k R, \mathfrak{g} \otimes_k R)$ denotes the set of homomorphisms of restricted R-Lie algebras and $\mathfrak{g} \otimes_k R$ carries the natural structure of a restricted R-Lie algebra, with bracket and p-mapping defined via

$$[x \otimes r, y \otimes s] := [x,y] \otimes rs \ \text{ and } \ (x \otimes r)^{[p]} := x^{[p]} \otimes r^p \quad \forall\, x, y \in \mathfrak{g},\, r, s \in R,$$

respectively. According to [8, (1.4),(1.6)], $\mathcal{T}_\mathfrak{g}$ is a smooth affine scheme of dimension $\dim_k \mathfrak{g} - \mathrm{rk}(\mathfrak{g})$.

In what follows, we shall be mainly concerned with the variety $\mathcal{T}_\mathfrak{g}(k)$ of k-rational points of $\mathcal{T}_\mathfrak{g}$, that is, the variety of embeddings $\varphi : \mathfrak{t} \longrightarrow \mathfrak{g}$ of restricted Lie algebras. The automorphism groups $\mathrm{Aut}_p(\mathfrak{g})$ and $\mathrm{Aut}_p(\mathfrak{t})$ naturally act on $\mathcal{T}_\mathfrak{g}(k)$ via

$$g.\varphi := g \circ \varphi \ \text{ and } \ h.\varphi := \varphi \circ h^{-1} \quad \forall\, \varphi \in \mathcal{T}_\mathfrak{g}(k),\, g \in \mathrm{Aut}_p(\mathfrak{g}),\, h \in \mathrm{Aut}_p(\mathfrak{t}),$$

respectively. Both actions commute, and $\mathrm{Aut}_p(\mathfrak{t}) \cong \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$ is a finite group. We shall also consider the canonical action of G on $\mathfrak{g}$ and write

$$g.x := g(x) \quad \forall\, g \in G,\, x \in \mathfrak{g}.$$

Let $\iota : \mathfrak{t} \hookrightarrow \mathfrak{g}$ be the standard embedding, defined by the inclusion $\mathfrak{t} \subseteq \mathfrak{g}$. Since $\mathcal{T}_\mathfrak{g}(k)$ is smooth, its irreducible components coincide with its connected components. Hence there exists exactly one irreducible component $\mathcal{X}_\mathfrak{t}(k) \subseteq \mathcal{T}_\mathfrak{g}(k)$ containing the inclusion ι. We let

$$S(\mathfrak{g}, \mathfrak{t}) := \mathrm{Stab}_{\mathrm{Aut}_p(\mathfrak{t})}(\mathcal{X}_\mathfrak{t}(k))$$

be the stabilizer of the component $\mathcal{X}_\mathfrak{t}(k)$ in $\mathrm{Aut}_p(\mathfrak{t})$. For future reference, we recall the following result, cf. [7, (4.1)]:

Theorem 1.1. *Let* $(\mathfrak{g}, [p])$ *be a restricted Lie algebra,* $\mathfrak{t} \subseteq \mathfrak{g}$ *be a torus of dimension* $\mu(\mathfrak{g})$*. Then the following statements hold:*
  (1) $\mathcal{T}_\mathfrak{g}(k) = \bigcup_{h \in \mathrm{Aut}_p(\mathfrak{t})} h.\mathcal{X}_\mathfrak{t}(k)$ *and* $\mathcal{T}_\mathfrak{g}(k)$ *has* $[\mathrm{Aut}_p(\mathfrak{t}) : S(\mathfrak{g}, \mathfrak{t})]$ *irreducible components.*
  (2) *If* $\mathfrak{t}' \subseteq \mathfrak{g}$ *is another torus of dimension* $\mu(\mathfrak{g})$*, then there exists an isomorphism* $h : \mathfrak{t} \longrightarrow \mathfrak{t}'$ *such that* $S(\mathfrak{g}, \mathfrak{t}') = hS(\mathfrak{g}, \mathfrak{t})h^{-1}$. $\qquad\square$

We let $\mathrm{Nor}_G(\mathfrak{t})$ and $\mathrm{Cent}_G(\mathfrak{t})$ be the *normalizer* and the *centralizer* of $\mathfrak{t}$ in G, respectively. In view of the above result, we make the following:

Definition. Let $(\mathfrak{g}, [p])$ be a restricted Lie algebra with automorphism group $G = \mathrm{Aut}_p(\mathfrak{g})^\circ$, $\mathfrak{t} \subseteq \mathfrak{g}$ be a torus of dimension $\mu(\mathfrak{g})$. Then

$$S(\mathfrak{g}) := S(\mathfrak{g}, \mathfrak{t})$$

is called the *toral stabilizer of* $\mathfrak{g}$. The group

$$W(\mathfrak{g}, \mathfrak{t}) := \mathrm{Nor}_G(\mathfrak{t}) / \mathrm{Cent}_G(\mathfrak{t})$$

is referred to as the *Weyl group of* $\mathfrak{g}$ *relative to* $\mathfrak{t}$.

The group G naturally acts on the variety $\mathfrak{Tor}(\mathfrak{g})$ of tori of maximal dimension. Since $W(\mathfrak{g}, g.\mathfrak{t}) \cong W(\mathfrak{g}, \mathfrak{t})$ for every $g \in G$, the Weyl group $W(\mathfrak{g}, \mathfrak{t})$ only depends on the orbit $G.\mathfrak{t} \subseteq \mathfrak{Tor}(\mathfrak{g})$.

Lemma 1.2. *Let* $(\mathfrak{g}, [p])$ *be a restricted Lie algebra with connected automorphism group* $G := \mathrm{Aut}_p(\mathfrak{g})^\circ$*,* $\mathfrak{t} \subseteq \mathfrak{g}$ *be a torus of dimension* $\mu(\mathfrak{g})$*. Given* $\varphi \in \mathcal{X}_\mathfrak{t}(k)$*, the map*

$$\Theta_\varphi : \mathrm{Nor}_G(\varphi(\mathfrak{t})) \longrightarrow \mathrm{Aut}_p(\mathfrak{t}) \ \ ; \ \ g \mapsto \varphi^{-1} \circ g \circ \varphi$$

is a homomorphism of groups that induces an injective homomorphism

$$\bar{\Theta}_\varphi : W(\mathfrak{g}, \varphi(\mathfrak{t})) \hookrightarrow S(\mathfrak{g}, \mathfrak{t}) \ \ ; \ \ \bar{g} \mapsto \varphi^{-1} \circ g \circ \varphi.$$

Proof. Since the connected group G acts morphically on $\mathcal{T}_{\mathfrak{g}}(k)$, [11, (8.2)] ensures that G stabilizes the connected component $\mathcal{X}_{\mathfrak{t}}(k)$. Let $g \in \mathrm{Nor}_G(\varphi(\mathfrak{t}))$. Setting $h := \Theta_\varphi(g)$, we consider the automorphism

$$\rho_h : \mathcal{T}_{\mathfrak{g}}(k) \longrightarrow \mathcal{T}_{\mathfrak{g}}(k) \; ; \;\; \psi \mapsto \psi \circ h$$

of the variety $\mathcal{T}_{\mathfrak{g}}(k)$. Then $\rho_h(\mathcal{X}_{\mathfrak{t}}(k))$ is a connected component of $\mathcal{T}_{\mathfrak{g}}(k)$. Since

$$\rho_h(\varphi) = \varphi \circ \Theta_\varphi(g) = g \circ \varphi \in \mathcal{X}_{\mathfrak{t}}(k),$$

we obtain $\rho_h(\mathcal{X}_{\mathfrak{t}}(k)) = \mathcal{X}_{\mathfrak{t}}(k)$. As a result, $\Theta_\varphi(g) \in S(\mathfrak{g}, \mathfrak{t})$. Directly from the definition we obtain the identity $\ker \Theta_\varphi = \mathrm{Cent}_G(\varphi(\mathfrak{t}))$, so that the induced map $\bar{\Theta}_\varphi : W(\mathfrak{g}, \varphi(\mathfrak{t})) \longrightarrow S(\mathfrak{g}, \mathfrak{t})$ is actually injective. $\square$

By virtue of Theorem 1.1, every torus $\mathfrak{t}' \subseteq \mathfrak{g}$ of dimension $\mu(\mathfrak{g})$ is of the form $\mathfrak{t}' = \varphi(\mathfrak{t})$ for some $\varphi \in \mathcal{X}_{\mathfrak{t}}(k)$. The foregoing Lemma then provides an embedding

$$\bar{\Theta}_\varphi : W(\mathfrak{g}, \mathfrak{t}') \hookrightarrow S(\mathfrak{g}, \mathfrak{t}),$$

sending the Weyl group $W(\mathfrak{g}, \mathfrak{t}')$ of $\mathfrak{t}'$ into the toral stabilizer $S(\mathfrak{g}, \mathfrak{t})$. If $\mathfrak{g}$ is of classical type, then this map is an isomorphism, see [7, (4.6)] or Theorem 1.5 below.

Our main goal of this section is to provide a criterion ensuring that $W(\mathfrak{g}, \mathfrak{t}) \cong S(\mathfrak{g})$ for some torus $\mathfrak{t} \in \mathfrak{Tor}(\mathfrak{g})$.

Definition. A torus $\mathfrak{t} \in \mathfrak{Tor}(\mathfrak{g})$ is called *generic* if the orbit $G.\mathfrak{t}$ is a dense subset of $\mathfrak{Tor}(\mathfrak{g})$.

Let $\mathfrak{g} := \mathrm{Lie}(G)$ be the Lie algebra of a connected algebraic group. In view of [10, (13.3),(13.5)] (see also [7, (4.4)]), any two tori of $\mathfrak{g}$ of maximal dimension are conjugate via the adjoint action. Accordingly, each of these tori is generic.

Lemma 1.3. *Let* $(\mathfrak{g}, [p])$ *be a restricted Lie algebra with connected automorphism group* $G := \mathrm{Aut}_p(G)^\circ$, $\mathfrak{t} \subseteq \mathfrak{g}$ *be a torus of dimension* $\mu(\mathfrak{g})$. *Then*

$$\dim G.\varphi(\mathfrak{t}) = \dim G.\varphi + \mu(\mathfrak{g})$$

for every $\varphi \in \mathcal{X}_{\mathfrak{t}}(k)$.

Proof. We consider the morphism

$$\omega : \left\{ \begin{array}{ccc} \mathcal{X}_{\mathfrak{t}}(k) \times \mathfrak{t} & \longrightarrow & \mathfrak{g} \\ (\varphi, t) & \mapsto & \varphi(t) \end{array} \right.$$

of irreducible varieties. Given $t \in \mathfrak{t}$, we let $(kt)_p$ denote the p-subalgebra of $\mathfrak{g}$ generated by kt. Lemma 3.2 of [7] provides a non-empty open subset $U \subseteq \mathfrak{t}$ with $\mathfrak{t} = (kt)_p$ for every $t \in U$. Let (φ, t) be an element of $\mathcal{X}_{\mathfrak{t}}(k) \times U$. If $(\psi, s) \in \omega^{-1}(\omega(\varphi, t))$, then $\psi(s) = \varphi(t)$, so that

$$\varphi(t) \in \mathrm{im}\,\psi.$$

By choice of t, this implies that $\mathrm{im}\,\varphi \subseteq \mathrm{im}\,\psi$, whence $\mathrm{im}\,\varphi = \mathrm{im}\,\psi$. Hence there exists an element $h \in \mathrm{Aut}_p(\mathfrak{t})$ with

$$\psi = \varphi \circ h^{-1}.$$

In particular, $\varphi(h^{-1}(s)) = \psi(s) = \varphi(t)$, so that $s = h(t)$. As a result, the fiber $\omega^{-1}(\omega(\varphi, t)) \subseteq \{(\varphi \circ h^{-1}, h(t)) \; ; \; h \in \mathrm{Aut}_p(\mathfrak{t})\}$ is finite.

Now let $\varphi \in \mathcal{X}_{\mathfrak{t}}(k)$ be arbitrary. Then ω induces a surjective homomorphism

$$\omega : (G.\varphi) \times \mathfrak{t} \longrightarrow G.\varphi(\mathfrak{t})$$

of irreducible varieties. By the above argument, the fibers of this morphism are finite on the dense open subset $(G.\varphi) \times U$ of $(G.\varphi) \times \mathfrak{t}$. By virtue of [16, I.§8, Corollary 1], we obtain

$$\dim G.\varphi(\mathfrak{t}) = \dim((G.\varphi) \times \mathfrak{t}) = \dim G.\varphi + \dim_k \mathfrak{t}$$
$$= \dim G.\varphi + \mu(\mathfrak{g}),$$

as desired. □

Let $S_{\mathfrak{g}}$ denote the set of semi-simple elements of $\mathfrak{g}$. The following result relates dense orbits in $\mathfrak{Tor}(\mathfrak{g})$ and $\mathfrak{X}_{\mathfrak{t}}(k)$ to dense G-saturations of tori in $\overline{S}_{\mathfrak{g}}$ relative to the canonical action of G on $\mathfrak{g}$.

Proposition 1.4. *Let $(\mathfrak{g}, [p])$ be a restricted Lie algebra, $G = \mathrm{Aut}_p(\mathfrak{g})^{\circ}$ be its connected automorphism group, and $\mathfrak{t} \subseteq \mathfrak{g}$ be a torus of maximal dimension. For a torus $\mathfrak{t}_0 \in \mathfrak{Tor}(\mathfrak{g})$, the following statements are equivalent:*
  (1) *The torus $\mathfrak{t}_0$ is generic.*
  (2) *There exists $\varphi_0 \in \mathfrak{X}_{\mathfrak{t}}(k)$ such that $\varphi_0(\mathfrak{t}) = \mathfrak{t}_0$ and $\overline{G.\varphi_0} = \mathfrak{X}_{\mathfrak{t}}(k)$.*
  (3) *$G.\mathfrak{t}_0$ is a dense subset of $\overline{S}_{\mathfrak{g}}$.*

Proof. (1) $\Rightarrow$ (2). According to [7, p. 4226], the map

$$\zeta_{\mathfrak{t}} : \mathfrak{X}_{\mathfrak{t}}(k) \longrightarrow \mathfrak{Tor}(\mathfrak{g}) \; ; \quad \varphi \mapsto \varphi(\mathfrak{t})$$

is a surjective morphism with finite fibers between two irreducible varieties of dimension $\dim_k \mathfrak{g} - \mathrm{rk}(\mathfrak{g})$. Let $\varphi \in \zeta_t^{-1}(\mathfrak{t}_0)$, so that $\varphi_0(\mathfrak{t}) = \mathfrak{t}_0$. Since ζ_t is G-equivariant, our present assumption implies that the morphism $\zeta_{\mathfrak{t}}|_{\overline{G.\varphi_0}} : \overline{G.\varphi_0} \longrightarrow \mathfrak{Tor}(\mathfrak{g})$ is dominant. Consequently,

$$\dim \overline{G.\varphi_0} = \dim \mathfrak{Tor}(\mathfrak{g}) = \dim \mathfrak{X}_{\mathfrak{t}}(k),$$

so that $\mathfrak{X}_{\mathfrak{t}}(k) = \overline{G.\varphi_0}$.
  (2) $\Rightarrow$ (3). According to [7, (4.1)] and [7, (3.7)] (see also [17, Theorem 2(iii)]), the variety $\bar{S}_{\mathfrak{g}}$ is irreducible, and of dimension

$$\dim \bar{S}_{\mathfrak{g}} = \dim \mathfrak{X}_{\mathfrak{t}}(k) + \mu(\mathfrak{g}).$$

Lemma 1.3 now implies

$$\dim G.\mathfrak{t}_0 = \dim G.\varphi_0 + \mu(\mathfrak{g}) = \dim \overline{S}_{\mathfrak{g}},$$

so that $G.\mathfrak{t}_0$ is a dense subset of the irreducible variety $\overline{S}_{\mathfrak{g}}$.
  (3) $\Rightarrow$ (1). Thanks to Theorem 1.1, there exists an element $\varphi_0 \in \mathfrak{X}_{\mathfrak{t}}(k)$ with $\mathfrak{t}_0 = \varphi_0(\mathfrak{t})$. According to Lemma 1.3, we have

$$\dim G.\varphi_0 = \dim G.\mathfrak{t}_0 - \mu(\mathfrak{g}) = \dim \bar{S}_{\mathfrak{g}} - \mu(\mathfrak{g}) = \dim \mathfrak{X}_{\mathfrak{t}}(k),$$

so that the orbit $G.\varphi_0$ lies dense in $\mathfrak{X}_{\mathfrak{t}}(k)$. Hence

$$\mathfrak{Tor}(\mathfrak{g}) = \zeta_{\mathfrak{t}}(\mathfrak{X}_{\mathfrak{t}}(k)) = \zeta_{\mathfrak{t}}(\overline{G.\varphi_0}) \subseteq \overline{\zeta_{\mathfrak{t}}(G.\varphi_0)} = \overline{G.\mathfrak{t}_0},$$

and $\mathfrak{t}_0$ is a generic torus. □

Theorem 1.5. *Let $(\mathfrak{g}, [p])$ be a restricted Lie algebra with connected automorphism group $G :=$ $\mathrm{Aut}_p(\mathfrak{g})^{\circ}$. If $\mathfrak{t} \in \mathfrak{Tor}(\mathfrak{g})$ is a generic torus, then the map*

$$\mathrm{Nor}_G(\mathfrak{t}) \longrightarrow \mathrm{Aut}_p(\mathfrak{t}) \; ; \quad g \mapsto g|_{\mathfrak{t}}$$

induces an isomorphism $W(\mathfrak{g}, \mathfrak{t}) \cong S(\mathfrak{g}, \mathfrak{t})$ of groups.

Proof. Thanks to Proposition 1.4, there exists $\varphi_0 \in \mathfrak{X}_{\mathfrak{t}}(k)$ with $\varphi_0(\mathfrak{t}) = \mathfrak{t}$ such that the orbit $G.\varphi_0$ lies dense in $\mathfrak{X}_{\mathfrak{t}}(k)$. It follows that $G.\varphi_0$ is an open subset of the irreducible variety $\mathfrak{X}_{\mathfrak{t}}(k)$. Consequently, $G.\varphi_0$ is the unique dense orbit of $\mathfrak{X}_{\mathfrak{t}}(k)$.

Given $h \in S(\mathfrak{g}, \mathfrak{t})$, we consider the automorphism

$$w_h : \mathfrak{X}_{\mathfrak{t}}(k) \longrightarrow \mathfrak{X}_{\mathfrak{t}}(k) \ ; \ \ \varphi \mapsto \varphi \circ h$$

of the variety $\mathfrak{X}_{\mathfrak{t}}(k)$. Then w_h is G-equivariant, so that

$$w_h(G.\varphi_0) = G.w_h(\varphi_0)$$

is a dense orbit of $\mathfrak{X}_{\mathfrak{t}}(k)$. By our observation above, we have $G.w_h(\varphi_0) = G.\varphi_0$, and there exists an element $g \in G$ with

(1.1) $$w_h(\varphi_0) = g \circ \varphi_0.$$

In particular, we obtain

$$g(\varphi_0(t)) = \varphi_0(h(t)) \in \varphi_0(\mathfrak{t}) = \mathfrak{t}$$

for every $t \in \mathfrak{t}$, whence $g \in \mathrm{Nor}_G(\varphi_0(\mathfrak{t})) = \mathrm{Nor}_G(\mathfrak{t})$. Consequently, (1.1) implies $h = \Theta_{\varphi_0}(g)$, so that Θ_{φ_0} is surjective. Thanks to Lemma 1.2, the homomorphism $\bar{\Theta}_{\varphi_0} : W(\mathfrak{g}, \mathfrak{t}) \longrightarrow S(\mathfrak{g}, \mathfrak{t})$ is bijective, so that the groups $W(\mathfrak{g}, \mathfrak{t})$ and $S(\mathfrak{g}, \mathfrak{t})$ have the same order. We may now apply Lemma 1.2 to the canonical embedding $\iota : \mathfrak{t} \hookrightarrow \mathfrak{g}$ to see that $\bar{\Theta}_{\iota}$ is the desired isomorphism. $\square$

We provide another density result which compensates for the lack of a generic torus to some extent. Given a torus $\mathfrak{t} \subseteq \mathfrak{g}$, we let $C_{\mathfrak{g}}(\mathfrak{t})$ be the *centralizer* of $\mathfrak{t}$ in $\mathfrak{g}$.

Lemma 1.6. *Let* $(\mathfrak{g}, [p])$ *be a restricted Lie algebra. Then* $\mathfrak{T} := \bigcup_{\mathfrak{t} \in \mathfrak{Tor}(\mathfrak{g})} \mathfrak{t}$ *is a dense subset of* $\bar{S}_{\mathfrak{g}}$.

Proof. We put $A = k[\mathfrak{X}_{\mathfrak{t}}]$ and $\tilde{\mathfrak{g}} = \mathfrak{g} \otimes_k A$. Let $j : \mathfrak{t} \hookrightarrow \tilde{\mathfrak{g}}$ be the universal embedding. The torus $\mathfrak{t}$ acts on $\tilde{\mathfrak{g}}$ via j; we denote by $\tilde{\mathfrak{g}}_0 \subseteq \tilde{\mathfrak{g}}$ the corresponding zero weight space. For any homomorphism $x \in \mathrm{Spec}_k(A)(k)$, let $\varphi_x := (\mathrm{id}_{\mathfrak{g}} \otimes x) \circ j \in \mathfrak{T}_{\mathfrak{g}}(k)$ denote the corresponding embedding. Then $\mathfrak{g}_0(x) = (\mathrm{id}_{\mathfrak{g}} \otimes x)(\tilde{\mathfrak{g}}_0)$ is the zero weight space relative to the torus $\varphi_x(\mathfrak{t})$. Consider the variety

$$\mathcal{V} = \{(x, y) \in \mathfrak{X}_{\mathfrak{t}}(k) \times \mathfrak{g} \ ; \ \exists v \in \tilde{\mathfrak{g}}_0 \text{ with } (\mathrm{id}_{\mathfrak{g}} \otimes x)(v) = y\}.$$

Owing to [7, (3.4)], the projection $\pi_{\mathfrak{g}} : \mathcal{V} \longrightarrow \mathfrak{g}$ is a dominant morphism with image

$$\mathrm{im}\, \pi_{\mathfrak{g}} = \bigcup_{x \in \mathfrak{X}_{\mathfrak{t}}(k)} \tilde{\mathfrak{g}}_0(x) = \bigcup_{x \in \mathfrak{X}_{\mathfrak{t}}(k)} C_{\mathfrak{g}}(\varphi_x(\mathfrak{t})).$$

Also, for $n = \dim_k \mathfrak{g}$, the morphism $\zeta : \mathfrak{g} \longrightarrow \bar{S}_{\mathfrak{g}} \ ; \ y \mapsto y^{[p]^n}$ is dominant. Thus, $\zeta \circ \pi_{\mathfrak{g}}$ is dominant, and we have

(1.2) $$\mathrm{im}\, \zeta \circ \pi_{\mathfrak{g}} = \bigcup_{x \in \mathfrak{X}_{\mathfrak{t}}(k)} C_{\mathfrak{g}}(\varphi_x(\mathfrak{t}))^{[p]^n} = \bigcup_{x \in \mathfrak{X}_{\mathfrak{t}}(k)} \varphi_x(\mathfrak{t}).$$

Since the right hand set is dense in $\bar{S}_{\mathfrak{g}}$ and contained in $\mathfrak{T}$, our assertion follows. $\square$

Remark. In the proof, we used the fact that the morphism $\mathfrak{g} \longrightarrow \mathfrak{g} \ ; \ y \mapsto y^{[p]^n}$ is dominant for $n = \dim_k \mathfrak{g}$. In fact, there are lower values of n for which this property holds, see the Remark p. 7 and Corollary 6.3.4.

We next record analogous properties of Cartan subalgebras. Thanks to [7, (7.2),(7.4)]

$$\mathfrak{Car}(\mathfrak{g}) := \{\mathfrak{h} \subseteq \mathfrak{g} \; ; \; \mathfrak{h} \text{ Cartan subalgebra}, \; \dim_k \mathfrak{h} = \mathrm{rk}(\mathfrak{g})\}$$

is a locally closed subset of the Grassmann variety $\mathrm{Gr}_{\mathrm{rk}(\mathfrak{g})}(\mathfrak{g})$. In view of [7, (8.2)], the variety $\mathfrak{Car}(\mathfrak{g})$ is irreducible of dimension $\dim_k \mathfrak{g} - \mathrm{rk}(\mathfrak{g})$. Note that G naturally acts on $\mathfrak{Car}(\mathfrak{g})$.

By general theory, the Cartan subalgebras of $\mathfrak{g}$ are precisely the centralizers of the maximal tori, see for instance [23, (II.4.1)]. Moreover, $C_{\mathfrak{g}}(\mathfrak{t}) \in \mathfrak{Car}(\mathfrak{g})$ for every $\mathfrak{t} \in \mathfrak{Tor}(\mathfrak{g})$, cf. [7, (3.5(1))].

Remark. Let $\ell := \mathrm{rk}(\mathfrak{g}) - \mu(\mathfrak{g})$, and $\zeta_\ell : \mathfrak{g} \longrightarrow \mathfrak{g} \; ; \; y \mapsto y^{[p]^\ell}$. Then ζ_ℓ induces a dominant morphism $\mathfrak{g} \to \bar{S}_{\mathfrak{g}}$. Indeed, since $\pi_{\mathfrak{g}} : \mathcal{V} \longrightarrow \mathfrak{g}$ is dominant, it is enough to show that $\zeta_\ell \circ \pi_{\mathfrak{g}}$ is dominant. We first check it under for $\mathfrak{g}$ nilpotent. Then the set $N(\mathfrak{g})$ of p-unipotent elements form a p-subalgebra of $\mathfrak{g}$ of dimension ℓ. Hence, for all $x_n \in N(\mathfrak{g})$, we have $x_n^{[p]^\ell} = 0$. Furthermore, $\mathfrak{g}$ affords a unique torus $\mathfrak{t}$ of dimension $\mu(\mathfrak{g})$. Then it is then easy to see that $x^{[p]^\ell} \in \mathfrak{t}$, whence $\mathfrak{g}^{[p]^\ell} = \mathfrak{t} = S_{\mathfrak{g}}$ as we needed. Now when $\mathfrak{g}$ is arbitrary, we have

$$\mathrm{im}\, \zeta_\ell \circ \pi_{\mathfrak{g}} = \bigcup_{x \in \mathcal{X}_{\mathfrak{t}}(k)} C_{\mathfrak{g}}(\varphi_x(\mathfrak{t}))^{[p]^\ell}.$$

Since each $\mathfrak{h} := C_{\mathfrak{g}}(\varphi_x(\mathfrak{t}))$ is a nilpotent subalgebra of dimension $\mathrm{rk}(\mathfrak{g})$ with $\mu(\mathfrak{h}) = \mu(\mathfrak{g})$, we have $\mathfrak{h}^{[p]^\ell} = \varphi_x(\mathfrak{t})$. Comparing with Equation (1.2) yields $\mathrm{im}\, \zeta_\ell \circ \pi_{\mathfrak{g}} = \mathrm{im}\, \zeta \circ \pi_{\mathfrak{g}}$, a dense subset of $\bar{S}_{\mathfrak{g}}$.

Definition. A Cartan subalgebra $\mathfrak{h} \in \mathfrak{Car}(\mathfrak{g})$ is called *generic* if the orbit $G.\mathfrak{h}$ is dense in $\mathfrak{Car}(\mathfrak{g})$.

As before, the Cartan subalgebras of the Lie algebras that are associated with algebraic groups are generic.

Proposition 1.7. *Let $(\mathfrak{g}, [p])$ be a restricted Lie algebra with connected automorphism group $G := \mathrm{Aut}_p(\mathfrak{g})^\circ$. Suppose that $\mathfrak{t}_0 \in \mathfrak{Tor}(\mathfrak{g})$ is a torus, and let $\mathfrak{h}_0 := C_{\mathfrak{g}}(\mathfrak{t}_0) \in \mathfrak{Car}(\mathfrak{g})$ be the corresponding Cartan subalgebra. Then the following statements are equivalent:*
  (1) *The Cartan subalgebra $\mathfrak{h}_0$ is generic.*
  (2) *The torus $\mathfrak{t}_0$ is generic.*
  (3) *The G-saturation $G.\mathfrak{h}_0 \subseteq \mathfrak{g}$ is a dense subset of $\mathfrak{g}$.*

Proof. (1) $\Rightarrow$ (2). A consecutive application of [7, (9.3)] and [7, (8.2)] shows that

$$C_{\mathfrak{g}} : \mathfrak{Tor}(\mathfrak{g}) \longrightarrow \mathfrak{Car}(\mathfrak{g}) \; ; \; \mathfrak{t} \mapsto C_{\mathfrak{g}}(\mathfrak{t})$$

is an injective morphism, whose image $\mathrm{im}\, C_{\mathfrak{g}} = \{\mathfrak{h} \in \mathfrak{Car}(\mathfrak{g}) \; ; \; \mu(\mathfrak{h}) = \mu(\mathfrak{g})\}$ is a dense open subset of $\mathfrak{Car}(\mathfrak{g})$. Since $C_{\mathfrak{g}}$ is G-equivariant, we obtain

$$C_{\mathfrak{g}}(G.\mathfrak{t}_0) = G.\mathfrak{h}_0,$$

so that the morphism $C_{\mathfrak{g}} : \overline{G.\mathfrak{t}_0} \longrightarrow \mathfrak{Car}(\mathfrak{g})$ is dominant. Consequently,

$$\dim \overline{G.\mathfrak{t}_0} = \dim \mathfrak{Car}(\mathfrak{g}) = \dim \mathfrak{Tor}(\mathfrak{g}).$$

As $\mathfrak{Tor}(\mathfrak{g})$ is irreducible, we conclude $\overline{G.\mathfrak{t}_0} = \mathfrak{Tor}(\mathfrak{g})$, showing that $\mathfrak{t}_0$ is a generic torus.

(2) $\Rightarrow$ (3). It follows from [7, (1.6)] that the variety

$$\mathcal{V} := \{(x, \varphi) \in \mathfrak{g} \times \mathcal{X}_{\mathfrak{t}_0}(k) \; ; \; x \in C_{\mathfrak{g}}(\varphi(\mathfrak{t}_0))\}$$

is irreducible. Moreover, [7, (3.1)] implies that the morphism

$$\pi_{\mathfrak{g}} : \mathcal{V} \longrightarrow \mathfrak{g} \; ; \; (x, \varphi) \mapsto x$$

is dominant. Since $\mathfrak{t}_0$ is generic, Proposition 1.4 provides an element $\varphi_0 \in \mathfrak{X}_{\mathfrak{t}_0}(k)$ with image $\varphi_0(\mathfrak{t}_0) = \mathfrak{t}_0$ and such that $\overline{G.\varphi_0} = \mathfrak{X}_{\mathfrak{t}_0}(k)$. Hence $G.\varphi_0$ is open in $\mathfrak{X}_{\mathfrak{t}_0}(k)$, and

$$\mathcal{O} := (\mathfrak{g} \times G.\varphi_0) \cap \mathcal{V}$$

is open in $\mathcal{V}$. Thus, $\mathcal{O}$ is a dense subset of $\mathcal{V}$, and we obtain

$$\mathfrak{g} = \overline{\pi_{\mathfrak{g}}(\mathcal{V})} = \overline{\pi_{\mathfrak{g}}(\overline{\mathcal{O}})} \subseteq \overline{\pi_{\mathfrak{g}}(\mathcal{O})} = \overline{G.C_{\mathfrak{g}}(\varphi_0(\mathfrak{t}_0))} = \overline{G.\mathfrak{h}_0},$$

as desired.

(3) $\Rightarrow$ (1). Suppose that $\mathfrak{g} = \overline{G.\mathfrak{h}_0}$. Setting $\ell := \dim_k \mathfrak{g}$, we recall that

$$f : \mathfrak{g} \longrightarrow \mathfrak{g} \ ; \ \ x \mapsto x^{[p]^\ell}$$

is a G-equivariant morphism, whose image coincides with $S_{\mathfrak{g}}$. Moreover,

$$f(\mathfrak{h}_0) = \mathfrak{h}_0 \cap S_{\mathfrak{g}} = \mathfrak{t}_0,$$

so that $f(G.\mathfrak{h}_0) = G.\mathfrak{t}_0$. Consequently,

$$\overline{S_{\mathfrak{g}}} = \overline{f(\mathfrak{g})} = \overline{f(\overline{G.\mathfrak{h}_0})} \subseteq \overline{f(G.\mathfrak{h}_0)} = \overline{G.\mathfrak{t}_0},$$

and Proposition 1.4 implies that $\mathfrak{t}_0$ is generic. Thus,

$$\mathfrak{Car}(\mathfrak{g}) = \overline{C_{\mathfrak{g}}(\mathfrak{Tor}(\mathfrak{g}))} \subseteq \overline{C_{\mathfrak{g}}(G.\mathfrak{t}_0)} = \overline{G.\mathfrak{h}_0},$$

proving that $\mathfrak{h}_0$ is a generic Cartan subalgebra of $\mathfrak{g}$. $\square$

Lemma 1.8. *Let* $(\mathfrak{g}, [p])$ *be a restricted Lie algebra,* $V \subseteq \mathfrak{g}$ *be a subspace of* $\mathfrak{g}$.
  (1) $\mathfrak{Tor}(\mathfrak{g})^V := \{\mathfrak{t} \in \mathfrak{Tor}(\mathfrak{g}) \ ; \ \mathfrak{t} \cap V = (0)\}$ *is open in* $\mathfrak{Tor}(\mathfrak{g})$.
  (2) $\mathfrak{Tor}(\mathfrak{g})_V := \{\mathfrak{t} \in \mathfrak{Tor}(\mathfrak{g}) \ ; \ \mathfrak{t} \subseteq V\}$ *is closed in* $\mathfrak{Tor}(\mathfrak{g})$.
  (3) $\mathfrak{Car}(\mathfrak{g})^V := \{\mathfrak{h} \in \mathfrak{Car}(\mathfrak{g}) \ ; \ \mathfrak{h} \cap V = (0)\}$ *is open in* $\mathfrak{Car}(\mathfrak{g})$.
  (4) $\mathfrak{Car}(\mathfrak{g})_V := \{\mathfrak{h} \in \mathfrak{Car}(\mathfrak{g}) \ ; \ \mathfrak{h} \subseteq V\}$ *is closed in* $\mathfrak{Car}(\mathfrak{g})$.

Proof. Let $d \in \mathbb{N}$. According to [7, (7.3)], the map

$$f_{d,V} : \mathrm{Gr}_d(\mathfrak{g}) \longrightarrow \mathbb{N}_0 \ ; \ \ X \mapsto \dim_k X \cap V$$

is upper semicontinuous. Consequently, $\mathfrak{Tor}(\mathfrak{g})^V = \mathfrak{Tor}(\mathfrak{g}) \setminus f_{\mu(\mathfrak{g}),V}^{-1}(\{n \in \mathbb{N}_0 \ ; \ n \geq 1\})$ is open in $\mathfrak{Tor}(\mathfrak{g})$. By the same token, $\mathfrak{Tor}(\mathfrak{g})_V = \mathfrak{Tor}(\mathfrak{g}) \cap f_{\mu(\mathfrak{g}),V}^{-1}(\{n \in \mathbb{N}_0 \ ; \ n \geq \mu(\mathfrak{g})\})$ is closed. The proofs of (3) and (4) follow analogously. $\square$

2. Basic Properties of Toral Stabilizers

Our computations of toral stabilizers necessitate information concerning their behavior with respect to inclusions and passage to factor algebras. Let $(\mathfrak{g}, [p])$ be a restricted Lie algebra with torus $\mathfrak{t} \subseteq \mathfrak{g}$ of maximal dimension. Recall that $S(\mathfrak{g}, \mathfrak{t})$ is a subgroup of $\mathrm{Aut}_p(\mathfrak{t})$.

Lemma 2.1. *Let* $\mathfrak{h} \subseteq \mathfrak{g}$ *be a* p-*subalgebra of the restricted Lie algebra* $(\mathfrak{g}, [p])$.
  (1) *If* $\mu(\mathfrak{h}) = \mu(\mathfrak{g})$, *then* $S(\mathfrak{h}, \mathfrak{t}) \subseteq S(\mathfrak{g}, \mathfrak{t})$ *for every torus* $\mathfrak{t} \subseteq \mathfrak{h}$ *of dimension* $\mu(\mathfrak{h})$.
  (2) *If* $\mathfrak{h} \trianglelefteq \mathfrak{g}$ *is an ideal such that* $\mathfrak{g}/\mathfrak{h}$ *is* p-*unipotent, then* $\mu(\mathfrak{h}) = \mu(\mathfrak{g})$ *and* $S(\mathfrak{h}, \mathfrak{t}) = S(\mathfrak{g}, \mathfrak{t})$ *for every torus* $\mathfrak{t} \subseteq \mathfrak{h}$ *of dimension* $\mu(\mathfrak{h})$.

Proof. (1) Let $\mathfrak{t} \subseteq \mathfrak{h}$ be a torus of dimension $\mu(\mathfrak{h})$. The canonical inclusion $\iota : \mathfrak{h} \hookrightarrow \mathfrak{g}$ induces an injective morphism

$$\iota_* : \mathfrak{T}_{\mathfrak{h}}(k) \longrightarrow \mathfrak{T}_{\mathfrak{g}}(k) \ ; \ \ \varphi \mapsto \iota \circ \varphi.$$

Consequently, $\iota_*(\mathfrak{X}_{\mathfrak{t}}(k)) \subseteq \mathfrak{T}_{\mathfrak{g}}(k)$ is a connected subspace containing the canonical inclusion $\iota|_{\mathfrak{t}} : \mathfrak{t} \hookrightarrow \mathfrak{g}$, so that

$$\iota_*(\mathfrak{X}_{\mathfrak{t}}(k)) \subseteq \mathfrak{X}'_{\mathfrak{t}}(k),$$

where the latter space denotes the connected component of $\mathfrak{T}_{\mathfrak{g}}(k)$ containing $\iota|_{\mathfrak{t}}$. Let h be an element of $S(\mathfrak{h}, \mathfrak{t})$. Denoting the inclusion $\mathfrak{t} \hookrightarrow \mathfrak{h}$ by $\tilde{\iota}$, we obtain

$$h.\iota|_{\mathfrak{t}} = \iota_*(h.\tilde{\iota}) \in \mathfrak{X}'_{\mathfrak{t}}(k).$$

Since $\varphi \mapsto h.\varphi$ is a morphism, we see that $h.\mathfrak{X}'_{\mathfrak{t}}(k) \subseteq \mathfrak{X}'_{\mathfrak{t}}(k)$. This implies $h \in S(\mathfrak{g}, \mathfrak{t})$, as desired.

(2) Since $\mathfrak{g}/\mathfrak{h}$ is p-unipotent, we have $\mu(\mathfrak{g}/\mathfrak{h}) = 0$ and [9, (3.3)] implies $\mu(\mathfrak{h}) = \mu(\mathfrak{g})$. Let $\pi : \mathfrak{g} \longrightarrow \mathfrak{g}/\mathfrak{h}$ be the canonical projection. Given $\varphi \in \mathfrak{T}_{\mathfrak{g}}(k)$, the p-subalgebra $(\pi \circ \varphi)(\mathfrak{t}) \subseteq \mathfrak{g}/\mathfrak{h}$ is a torus, so that $(\pi \circ \varphi)(\mathfrak{t}) = (0)$ and $\varphi(\mathfrak{t}) \subseteq \ker \pi = \mathfrak{h}$. Consequently, φ factors through $\mathfrak{h}$, and the morphism

$$\iota_* : \mathfrak{T}_{\mathfrak{h}}(k) \longrightarrow \mathfrak{T}_{\mathfrak{g}}(k)$$

is bijective. As a result, $\iota_*(\mathfrak{X}_{\mathfrak{t}}(k)) = \mathfrak{X}'_{\mathfrak{t}}(k)$ and $S(\mathfrak{g}, \mathfrak{t}) = S(\mathfrak{h}, \mathfrak{t})$. $\qquad \square$

Corollary 2.2. *Let $\mathfrak{t} \subseteq \mathfrak{g}$ be a torus of dimension $\mu(\mathfrak{g})$, $\mathfrak{s} \subseteq \mathfrak{t}$ be a subtorus. Then we have a natural inclusion*

$$S(C_{\mathfrak{g}}(\mathfrak{s}), \mathfrak{t}) \subseteq \{g \in S(\mathfrak{g}, \mathfrak{t}) \ ; \ g|_{\mathfrak{s}} = \mathrm{id}_{\mathfrak{s}}\}.$$

Proof. We consider the p-subalgebra $\mathfrak{h} := C_{\mathfrak{g}}(\mathfrak{s})$. By definition, $\mu(\mathfrak{h}) = \mu(\mathfrak{g})$, and Lemma 2.1 provides an inclusion $S(\mathfrak{h}, \mathfrak{t}) \subseteq S(\mathfrak{g}, \mathfrak{t})$. In view of [7, (5.11)], each element of $S(\mathfrak{h}, \mathfrak{t})$ belongs to the centralizer of $\mathfrak{s}$ in $\mathrm{Aut}_p(\mathfrak{t})$. $\qquad \square$

For a direct sum $\mathfrak{t}_1 \oplus \mathfrak{t}_2$ of vector spaces, we denote by $\iota_{\mathfrak{t}_i}$ and $\pi_{\mathfrak{t}_i}$ the canonical injection from $\mathfrak{t}_i$ and the projection onto $\mathfrak{t}_i$, respectively. Recall the identification

$$(2.1) \qquad \mathrm{End}_k(\mathfrak{t}_1 \oplus \mathfrak{t}_2) \equiv \left(\begin{array}{c|c} \mathrm{End}_k(\mathfrak{t}_1) & \mathrm{Hom}_k(\mathfrak{t}_2, \mathfrak{t}_1) \\ \hline \mathrm{Hom}_k(\mathfrak{t}_1, \mathfrak{t}_2) & \mathrm{End}_k(\mathfrak{t}_2) \end{array} \right),$$

where the maps from $\mathrm{End}_k(\mathfrak{t}_1 \oplus \mathfrak{t}_2)$ to any of the blocks arise via composition with ι's and π's: For example, the projection $\mathrm{End}_k(\mathfrak{t}_1 \oplus \mathfrak{t}_2) \twoheadrightarrow \mathrm{Hom}_k(\mathfrak{t}_2, \mathfrak{t}_1)$ is given by $g \mapsto \pi_{\mathfrak{t}_1} \circ g \circ \iota_{\mathfrak{t}_2}$.

The groups $\mathrm{GL}(\mathfrak{t}_1)$ and $\mathrm{GL}(\mathfrak{t}_2)$ canonically act on $\mathrm{Hom}_k(\mathfrak{t}_2, \mathfrak{t}_1)$ from the left and right, respectively. The semi-direct product $\mathrm{GL}(\mathfrak{t}_2) \ltimes \mathrm{Hom}_k(\mathfrak{t}_2, \mathfrak{t}_1)$ can be identified with a subgroup of $\mathrm{GL}(\mathfrak{t}_1 \oplus \mathfrak{t}_2)$, namely:

$$\mathrm{GL}(\mathfrak{t}_2) \ltimes \mathrm{Hom}_k(\mathfrak{t}_2, \mathfrak{t}_1) \equiv \left(\begin{array}{c|c} I_{\mathfrak{t}_1} & \mathrm{Hom}_k(\mathfrak{t}_2, \mathfrak{t}_1) \\ \hline 0 & \mathrm{GL}(\mathfrak{t}_2) \end{array} \right).$$

(Note that the sizes of boxes are given by the dimensions of the relevant subspaces of $\mathfrak{t}$, so that there is no entry in the first row and column for $\mathfrak{t}_1 = (0)$, say.)

For tori $\mathfrak{t}, \mathfrak{t}'$, let $\mathrm{Lie}_p(\mathfrak{t}, \mathfrak{t}')$ denote the additive group of restricted homomorphisms $\mathfrak{t} \to \mathfrak{t}'$. It affords a natural right action by $\mathrm{Aut}_p(\mathfrak{t})$ and a natural left action by $\mathrm{Aut}_p(\mathfrak{t}')$. We first generalize a basic result from [7].

Proposition 2.3. *Let $(\mathfrak{g}, [p])$ be a restricted Lie algebra, $\mathfrak{n} \trianglelefteq \mathfrak{g}$ be a p-ideal. Then the following statements hold:*

(1) *If $\mathfrak{t} \subseteq \mathfrak{g}$ is a torus of maximal dimension, then $\mathfrak{t} \cap \mathfrak{n}$ and $(\mathfrak{t} + \mathfrak{n})/\mathfrak{n}$ are tori of maximal dimension of $\mathfrak{n}$ and $\mathfrak{g}/\mathfrak{n}$, respectively.*

(2) *The restriction map $\mathrm{Hom}_k(\mathfrak{t}, \mathfrak{g}) \longrightarrow \mathrm{Hom}_k(\mathfrak{t} \cap \mathfrak{n}, \mathfrak{g})$ induces a morphism $\mathrm{res} : \mathfrak{X}_{\mathfrak{t}}(k) \longrightarrow \mathfrak{X}_{\mathfrak{t} \cap \mathfrak{n}}(k)$.*

(3) *Let $\mathfrak{t}' \subseteq \mathfrak{t}$ be a torus such that $\mathfrak{t} = (\mathfrak{t} \cap \mathfrak{n}) \oplus \mathfrak{t}'$. Then the canonical identification (2.1) induces an injective homomorphism*

$$S(\mathfrak{g}, \mathfrak{t}) \hookrightarrow \left(\begin{array}{c|c} S(\mathfrak{n}, \mathfrak{t} \cap \mathfrak{n}) & \mathrm{Lie}_p(\mathfrak{t}', \mathfrak{t} \cap \mathfrak{n}) \\ \hline 0 & S(\mathfrak{g}/\mathfrak{n}, \mathfrak{t}') \end{array} \right)$$

of finite groups.

Proof. (1) According to [9, (3.3)], the p-subalgebra $(\mathfrak{t} + \mathfrak{n})/\mathfrak{n} \subseteq \mathfrak{g}/\mathfrak{n}$ is a torus of $\mathfrak{g}/\mathfrak{n}$ of maximal dimension. By the same token, we have

$$\mu(\mathfrak{g}) = \mu(\mathfrak{n}) + \mu(\mathfrak{g}/\mathfrak{n}).$$

Since $\dim_k \mathfrak{t} = \dim_k(\mathfrak{t} \cap \mathfrak{n}) + \dim_k(\mathfrak{t} + \mathfrak{n})/\mathfrak{n}$, it follows that $\mathfrak{t} \cap \mathfrak{n}$ is a torus of $\mathfrak{n}$ of maximal dimension.

(2) Let $\iota : \mathfrak{t} \hookrightarrow \mathfrak{g}$ be the canonical embedding. We first verify

($\ast$) *We have $\varphi(\mathfrak{t} \cap \mathfrak{n}) \subseteq \mathfrak{n}$ for every $\varphi \in \mathfrak{X}_{\mathfrak{t}}(k)$ and $g(\mathfrak{t} \cap \mathfrak{n}) = \mathfrak{t} \cap \mathfrak{n}$ for every $g \in S(\mathfrak{g}, \mathfrak{t})$.*

According to [7, (5.2)], there exists a subtorus $\mathfrak{t}_{\mathfrak{n}} \subseteq \mathfrak{t}$ such that $\varphi^{-1}(\mathfrak{n}) = \mathfrak{t}_{\mathfrak{n}}$ for every $\varphi \in \mathfrak{X}_{\mathfrak{t}}(k)$. Specializing $\varphi = \iota$, we obtain $\mathfrak{t}_{\mathfrak{n}} = \mathfrak{t} \cap \mathfrak{n}$, whence $\varphi(\mathfrak{t} \cap \mathfrak{n}) \subseteq \mathfrak{n}$ for every $\varphi \in \mathfrak{X}_{\mathfrak{t}}(k)$.

Now let $g \in S(\mathfrak{g}, \mathfrak{t})$. Then we have $g = g^{-1}.\iota \in \mathfrak{X}_{\mathfrak{t}}(k)$, so that $g(\mathfrak{t} \cap \mathfrak{n}) \subseteq \mathfrak{t} \cap \mathfrak{n}$. $\diamond$

Owing to ($\ast$), the canonical restriction map induces a morphism

$$\mathrm{res} : \mathfrak{X}_{\mathfrak{t}}(k) \longrightarrow \mathfrak{T}_{\mathfrak{n}}(k) \ ; \quad \varphi \mapsto \varphi|_{\mathfrak{t} \cap \mathfrak{n}}$$

of affine varieties. As res is continuous, we have $\mathrm{im} \, \mathrm{res} \subseteq \mathfrak{X}_{\mathfrak{t} \cap \mathfrak{n}}(k)$.

(3) Let g be an element of $S(\mathfrak{g}, \mathfrak{t})$. Owing to ($\ast$), we have $g(\mathfrak{t} \cap \mathfrak{n}) = \mathfrak{t} \cap \mathfrak{n}$. Thus,

$$\iota|_{\mathfrak{t} \cap \mathfrak{n}} \circ g|_{\mathfrak{t} \cap \mathfrak{n}} = (\iota \circ g)|_{\mathfrak{t} \cap \mathfrak{n}} = \mathrm{res}(\iota \circ g) \in \mathfrak{X}_{\mathfrak{t} \cap \mathfrak{n}}(k),$$

proving $g|_{\mathfrak{t} \cap \mathfrak{n}} \in S(\mathfrak{n}, \mathfrak{t} \cap \mathfrak{n})$.

According to [7, (5.3)], the natural projection $\pi : \mathfrak{g} \longrightarrow \mathfrak{g}/\mathfrak{n}$ induces a morphism

$$\Pi : \mathfrak{X}_{\mathfrak{t}}(k) \longrightarrow \mathfrak{X}_{\mathfrak{t}'}(k) \ ; \quad \varphi \mapsto \pi \circ \varphi|_{\mathfrak{t}'}$$

of affine varieties. Property ($\ast$) implies that each $g \in S(\mathfrak{g}, \mathfrak{t})$ induces a unique element $\bar{g} \in \mathrm{Aut}_p((\mathfrak{t} + \mathfrak{n})/\mathfrak{n})$ such that $\bar{g} \circ \pi|_{\mathfrak{t}} = \pi \circ g$. Since π restricts to an isomorphism $\mathfrak{t}' \longrightarrow (\mathfrak{t} + \mathfrak{n})/\mathfrak{n}$, there is a unique automorphism $\tilde{g} \in \mathrm{Aut}_p(\mathfrak{t}')$ such that $\bar{g} \circ \pi|_{\mathfrak{t}'} = \pi|_{\mathfrak{t}'} \circ \tilde{g}$. Note that $\pi|_{\mathfrak{t}'} : \mathfrak{t}' \hookrightarrow \mathfrak{g}/\mathfrak{n}$ is the canonical inclusion, defining the connected component $\mathfrak{X}_{\mathfrak{t}'}(k) \subseteq \mathfrak{T}_{\mathfrak{g}/\mathfrak{n}}(k)$. Hence we obtain for $g \in S(\mathfrak{g}, \mathfrak{t})$

$$\tilde{g}.\pi|_{\mathfrak{t}'} = \pi|_{\mathfrak{t}'} \circ \tilde{g}^{-1} = \pi \circ g^{-1}|_{\mathfrak{t}'} = \Pi(g^{-1}) \in \mathfrak{X}_{\mathfrak{t}'}(k),$$

so that $\tilde{g} \in S(\mathfrak{g}/\mathfrak{n}, \mathfrak{t}')$. Since $g \mapsto \tilde{g}$ defines a homomorphism of groups, we obtain the desired embedding of finite groups. $\square$

Remarks. (1) Let $\mathfrak{t}' \subseteq \mathfrak{t}$ be tori. Let $\{t_1, \ldots, t_n\}$ be a toral basis of $\mathfrak{t}$ and denote by V the $\mathbb{F}_p$-subspace of $\mathfrak{t}$ generated by $\{t_1, \ldots, t_n\}$. Since V is the set of toral elements of $\mathfrak{t}$, there exists a subspace $V' \subseteq V$, whose k-span coincides with $\mathfrak{t}'$. Choose a complement W' of V' in V. Then its k-span $\mathfrak{s}$ is a subtorus of $\mathfrak{t}$ such that $\mathfrak{t} = \mathfrak{t}' \oplus \mathfrak{s}$.

(2) One can show that the restriction morphism $\mathrm{res} : \mathfrak{X}_\mathfrak{t}(k) \longrightarrow \mathfrak{X}_{\mathfrak{t} \cap \mathfrak{n}}(k)$ is smooth. In particular, res is open and dominant.

Corollary 2.4. *Let* $\mathfrak{g}_1, \mathfrak{g}_2$ *be restricted Lie algebras and* $\mathfrak{t}_i \subseteq \mathfrak{g}_i$ *be tori of maximal dimension for* $i \in \{1, 2\}$*. Then* $\mathfrak{t}_1 \oplus \mathfrak{t}_2 \subseteq \mathfrak{g}_1 \oplus \mathfrak{g}_2$ *is a torus of maximal dimension, and*

$$S(\mathfrak{g}_1 \oplus \mathfrak{g}_2, \mathfrak{t}_1 \oplus \mathfrak{t}_2) \simeq S(\mathfrak{g}_1, \mathfrak{t}_1) \times S(\mathfrak{g}_2, \mathfrak{t}_2).$$

Proof. We put $\mathfrak{g} := \mathfrak{g}_1 \oplus \mathfrak{g}_2$ and $\mathfrak{t} := \mathfrak{t}_1 \oplus \mathfrak{t}_2$, and denote by $\iota : \mathfrak{t} \hookrightarrow \mathfrak{g}$ the canonical embedding. Let $\mathfrak{T}_\mathfrak{g}$ be the scheme of embeddings of $\mathfrak{g}$ and $\mathfrak{X} \subseteq \mathfrak{T}_\mathfrak{g}$ be the connected component containing ι. For $i \in \{1, 2\}$, we denote similarly $\iota_i : \mathfrak{t}_i \hookrightarrow \mathfrak{g}_i$ and the schemes $\mathfrak{X}_i \subseteq \mathfrak{T}_{\mathfrak{g}_i}$. According to Proposition 2.3, we have

$$(*) \qquad \varphi(\mathfrak{t}_i) \subseteq \mathfrak{g}_i \quad \forall\, \varphi \in \mathfrak{X}(k) \;\; \text{and} \;\; g(\mathfrak{t}_i) = \mathfrak{t}_i \quad \forall\, g \in S(\mathfrak{g}, \mathfrak{t})$$

for each $i \in \{1, 2\}$. Consequently, Proposition 2.3 shows that

$$S(\mathfrak{g}, \mathfrak{t}) \longrightarrow S(\mathfrak{g}_1, \mathfrak{t}_1) \times S(\mathfrak{g}_2, \mathfrak{t}_2) \;\; ; \;\; g \mapsto (\pi_1 \circ g \circ \iota_1, \pi_2 \circ g \circ \iota_2)$$

is an injective homomorphism of groups.

Given $i \in \{1, 2\}$, the map

$$\zeta_i : \begin{cases} \mathfrak{X}_i(k) \longrightarrow \mathfrak{X}(k) \\ \varphi_i \mapsto \varphi_i \oplus \iota_{3-i} \end{cases}$$

is a morphism of affine varieties. As a result, given $g_i \in S(\mathfrak{g}_i, \mathfrak{t}_i)$, the elements $g_1 \oplus \mathrm{id}_{\mathfrak{t}_2}$ and $\mathrm{id}_{\mathfrak{t}_1} \oplus g_2$ belong to $S(\mathfrak{g}, \mathfrak{t})$, and the above map is also surjective. $\square$

3. Automorphisms and generic tori for Lie algebras of Cartan type

Henceforth, we will assume that k *is an algebraically closed field of characteristic* $p \geq 3$. We shall apply the results of Section 1 in the situation where $\mathfrak{g}$ is a restricted Lie algebra of Cartan type. By definition, these simple restricted Lie algebras possess a *restricted $\mathbb{Z}$-grading*

$$\mathfrak{g} = \bigoplus_{i=-r}^{s} \mathfrak{g}_i \;\; ; \;\; [\mathfrak{g}_i, \mathfrak{g}_j] \subseteq \mathfrak{g}_{i+j} \;\; ; \;\; \mathfrak{g}_i^{[p]} \subseteq \mathfrak{g}_{pi} \qquad (r, s \geq 1),$$

where we set $\mathfrak{g}_i := (0)$ for $i \notin \{-r, \ldots, s\}$. Given such an algebra $\mathfrak{g}$, we consider the associated descending filtration $(\mathfrak{g}_{(i)})_{i \geq -r}$, defined via

$$\mathfrak{g}_{(i)} := \sum_{j \geq i} \mathfrak{g}_j.$$

By definition, the restricted Lie algebras of Cartan type are p-subalgebras of the algebra of derivations of the truncated polynomial rings

$$\mathfrak{A}_n := k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p) \qquad (n \geq 1),$$

whose canonical generators will be denoted $x_1, \ldots, x_n$.

The Lie algebra $W(n) := \mathrm{Der}_k(\mathfrak{A}_n)$ is called the *n-th Jacobson-Witt algebra*. Its p-map is the standard p-th power of linear operators. We let $\partial_i \in W(n)$ denote the partial derivative with respect to the variable x_i. Then $\{\partial_1, \ldots, \partial_n\}$ is a basis of the $\mathfrak{A}_n$-module $W(n)$, so that $\dim_k W(n) = np^n$.

Here and further, we use the standard multi-index notation and write $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $|\alpha| := \sum_{i=1}^n \alpha_i$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$. Setting $\tau := (p-1, \ldots, p-1)$, the Lie algebra $W(n)$ obtains a restricted grading $W(n) = \bigoplus_{j=-1}^{|\tau|-1} W(n)_j$ via

$$W(n)_j := \sum_{i=1}^n \sum_{|\alpha|=j+1} k x^\alpha \partial_i.$$

We briefly describe the other Cartan type Lie algebras in terms of differential forms; the reader is also referred to [23, Chap. IV] and [13] for further details.

We set $\Omega^0(\mathfrak{A}_n) = \mathfrak{A}_n$ as well as $\Omega^1(\mathfrak{A}_n) := \mathrm{Hom}_{\mathfrak{A}_n}(W(n), \mathfrak{A}_n)$. The latter space carries canonical structures of an $\mathfrak{A}_n$-module and a $W(n)$-module (cf. [13] or [23]) via

$$(u.f)(D) := u.f(D) \quad \text{and} \quad (E.f)(D) = E(f(D)) - f([E, D]),$$

for all $u \in \mathfrak{A}_n$, $D, E \in W(n)$, $f \in \Omega^1(\mathfrak{A}_n)$. Let $\Omega^r(\mathfrak{A}_n) := \bigwedge^r \Omega^1(\mathfrak{A}_n)$ be the r-fold exterior power over $\mathfrak{A}_n$ and define

$$\Omega(\mathfrak{A}_n) := \bigoplus_{r=0}^n \Omega^r(\mathfrak{A}_n).$$

Let $r \geq 2$. Direct computation shows that

$$D.(f_1 \wedge f_2 \wedge \cdots \wedge f_r) := \sum_{i=1}^r f_1 \wedge f_2 \wedge \cdots \wedge f_{i-1} \wedge D.f_i \wedge f_{i+1} \wedge \cdots \wedge f_r,$$

$D \in W(n)$, $f_i \in \Omega^1(\mathfrak{A}_n)$ endows $\Omega^r(\mathfrak{A}_n)$ with the structure of a $W(n)$-module.

Consider the k-linear map $\mathsf{d} : \Omega^0(\mathfrak{A}_n) \longrightarrow \Omega^1(\mathfrak{A}_n)$, given by

$$\mathsf{d}u(D) = D(u) \qquad \forall\, u \in \mathfrak{A}_n,\ D \in W(n).$$

Associated with the *Cartan differential forms* $\omega_S = \mathsf{d}x_1 \wedge \cdots \wedge \mathsf{d}x_n$; $\omega_H = \sum_{i=1}^r \mathsf{d}x_i \wedge \mathsf{d}x_{i+r}$ for $n = 2r$, and $\omega_K = \mathsf{d}x_{2r+1} + \sum_{i=1}^r (x_{i+r}\mathsf{d}x_i - x_i\mathsf{d}x_{i+r})$ for $n = 2r+1$, there are the simple Cartan type Lie algebras $X(n) = X''(n)^{(2)}$, where $X''(n) = \{D \in W(n)\ ;\ D.\omega_X = 0\}$ if $X = S, H$ and $K''(n) := \{D \in W(n)\ ;\ D.\omega_K \in \mathfrak{A}_n \omega_K\}$.

Recall that, given a $2r$-dimensional k-vector space with a non-degenerate symplectic form $\langle\, ,\, \rangle : V \times V \longrightarrow k$, the group

$$G\,\mathrm{Sp}(V) := \{g \in \mathrm{GL}(V)\ ;\ \exists\, c(g) \in k^\times\ ,\ \langle g(x), g(y)\rangle = c(g)\langle x, y\rangle\ \forall\, x, y \in V\}$$

is referred to as the *group of similitudes* of the symplectic space $(V, \langle\, ,\, \rangle)$.

Theorem 3.1 ([24, 25]). *Let $\mathfrak{g}$ be a restricted Lie algebra of Cartan type $X(n)$ over a field k of characteristic $p \geq 3$. If $\mathfrak{g} = W(1)$ or $H(2)$, assume that $p \geq 5$. Then the following statements hold:*

(1) *The group $G := \mathrm{Aut}_p(\mathfrak{g})$ is connected.*

(2) *The group G is a semidirect product $G = U \rtimes G_0$, where G_0 consists of those automorphisms preserving the $\mathbb{Z}$-grading of $\mathfrak{g}$, and $U := \{g \in G\ ;\ (g - \mathrm{id}_\mathfrak{g})(\mathfrak{g}_{(i)}) \subseteq \mathfrak{g}_{(i+1)}\}$. Furthermore, U is unipotent and G_0 is reductive with*

$$G_0 \cong \begin{cases} \mathrm{GL}(n), & \text{for } X = W, S, \\ G\,\mathrm{Sp}(2r), & \text{for } X = H \text{ and } K \text{ with } n = 2r \text{ and } 2r+1, \text{ respectively.} \end{cases}$$

(3) *We have $g(\mathfrak{g}_{(i)}) = \mathfrak{g}_{(i)}$ for every $g \in G$ and $i \in \mathbb{Z}$.*

Proof. According to Wilson's results [24, Thm. 2], the theorem holds for the group of automorphisms which preserve the standard filtration. So we need to show that under the assumptions of the theorem, all automorphisms of $\mathfrak{g}$ preserve it. Since this is the standard filtration defined with respect to the maximal subalgebra $\mathfrak{g}_{(0)} \subsetneq \mathfrak{g}$ [22, Definition 3.5.1], we have to show that any automorphism preserves this subalgebra. By [22, (4.2.6)], $\mathfrak{g}_{(0)}$ is the unique maximal subalgebra of lowest codimension, except when $p = 3$, and $\mathfrak{g} = W(1)$, $H(2)$ or $K(3)$. When $\mathfrak{g} = K(3)$ and $p = 3$, [22, (4.2.6)] states that $\mathfrak{g}_{(0)}$ is the unique maximal subalgebra $\mathfrak{h}$ of codimension 3 such that the $\mathfrak{h}$-module $\mathfrak{g}/\mathfrak{h}$ is not irreducible. It readily follows that $\mathfrak{g}_{(0)}$ is stable under all automorphisms of $\mathfrak{g}$ in all relevant cases, so the proof is complete. $\qquad\square$

Owing to (3) of Theorem 3.1, the subsets $\mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(i)}}$ and $\mathfrak{Tor}(\mathfrak{g})^{\mathfrak{g}_{(i)}}$ of $\mathfrak{Tor}(\mathfrak{g})$ are G-invariant. It also follows that the function

$$f_0 : \mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(-1)}} \longrightarrow \mathbb{N}_0 \;\; ; \;\; \mathfrak{t} \mapsto \dim_k \mathfrak{t} \cap \mathfrak{g}_{(0)}$$

is constant on the G-orbits of $\mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(-1)}}$.

The following result, which states that f_0 forms a complete set of invariants for the G-orbits of $\mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(-1)}}$, is based on Demuškin's work [3, 4], as corrected in [22, §7]. In our statement below, we represent the contact algebra as in [23, (IV.5)].

Theorem 3.2. *Let $\mathfrak{g}$ be a Lie algebra of Cartan type $X(n)$, where $X \in \{W, S, H, K\}$. Then the following statements hold:*
  (1) *Two tori $\mathfrak{t}, \mathfrak{t}' \in \mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(-1)}}$ belong to the same G-orbit if and only if $f_0(\mathfrak{t}) = f_0(\mathfrak{t}')$.*
  (2) *Each of the following tori represents the unique orbit $G.\mathfrak{t}_0$ of $\mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(-1)}}$ with $f_0(G.\mathfrak{t}_0) = \{0\}$:*
    (W) $\mathfrak{t}_0 = \langle (1+x_1)\partial_1, \ldots, (1+x_n)\partial_n \rangle$ *for $\mathfrak{g} = W(n)$*
    (S) $\mathfrak{t}_0 = \langle (1+x_1)\partial_1 - x_n\partial_n, \ldots, (1+x_{n-1})\partial_{n-1} - x_n\partial_n \rangle$ *for $\mathfrak{g} = S(n)$*
    (H) $\mathfrak{t}_0 = \langle (1+x_1)\partial_1 - x_{r+1}\partial_{r+1}, \ldots, (1+x_r)\partial_{r+1} - x_{2r}\partial_{2r} \rangle$ *for $\mathfrak{g} = H(2r)$*
    (K) $\mathfrak{t}_0 = \langle x_1(1+x_{r+1}), \ldots, x_r(1+x_{2r}), \sum_{i=1}^r x_i x_{r+i} - x_{2r+1} \rangle$ *for $\mathfrak{g} = K(2r+1)$.* $\qquad\square$

The foregoing results yield the following description of the toral stabilizers of the Lie algebras of Cartan types W, S and H.

Proposition 3.3. *Let $\mathfrak{g}$ be a Lie algebra of Cartan type W, S or H. Then $\mathfrak{t}_0$ is a generic torus and*

$$W(\mathfrak{g}, \mathfrak{t}_0) \cong S(\mathfrak{g}).$$

Proof. According to Lemma 1.8 and Theorem 3.1, $\mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(-1)}}$ is a closed, G-invariant subset of $\mathfrak{Tor}(\mathfrak{g})$. By the same token,

$$\mathcal{O} := \mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(-1)}} \cap \mathfrak{Tor}(\mathfrak{g})^{\mathfrak{g}_{(0)}}$$

is an open, G-invariant subset of $\mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(-1)}}$. In view of Theorem 3.2(1), we thus have $\mathcal{O} = G.\mathfrak{t}_0$. In particular, the orbit $G.\mathfrak{t}_0$ is open in $\mathfrak{Tor}(\mathfrak{g})_{\mathfrak{g}_{(-1)}}$. Since $\mathfrak{g} = \mathfrak{g}_{(-1)}$ for $\mathfrak{g} = W(n), S(n), H(2r)$, it follows from the irreducibility of $\mathfrak{Tor}(\mathfrak{g})$ that $\mathfrak{t}_0$ actually is a generic torus of $\mathfrak{g}$. Our second assertion is now a direct consequence of Theorem 1.5. $\qquad\square$

Remark. If $\mathfrak{g}$ is of type K, then $G.\mathfrak{t}_0$ is a subset of $\mathfrak{g}_{(-1)}$. Since $S_\mathfrak{g} \setminus \mathfrak{g}_{(-1)}$ is not empty, the G-saturation of $\mathfrak{t}_0$ is contained in the proper, closed subset $\bar{S}_\mathfrak{g} \cap \mathfrak{g}_{(-1)} \subsetneq \bar{S}_\mathfrak{g}$, and Proposition 1.4 shows that the torus $\mathfrak{t}_0$ is not generic. In fact, we will see in (6.2.3) that contact algebras do not afford generic tori.

4. EMBEDDINGS OF $W(n)$

In preparation for our computation of the toral stabilizers and Weyl groups of the generic tori of the Lie algebras of Cartan types W, S and H, we provide in this section embeddings $W(\mu(\mathfrak{g})) \hookrightarrow \mathfrak{g}$ for such Lie algebras.

The map

$$\operatorname{div} : W(n) \longrightarrow \mathfrak{A}_n \;\; ; \;\; \sum_{j=1}^{n} f_j \partial_j \mapsto \sum_{j=1}^{n} \partial_j(f_j)$$

is called the *divergence* of $W(n)$. The special algebra $S(n)$ is the derived algebra of the subalgebra $\ker \operatorname{div}$, cf. [23, (IV.3)].

Let $r \leq n$. In the sequel, we shall identify $\mathfrak{A}_r$ with the subalgebra of $\mathfrak{A}_n$ that is generated by $x_1, \ldots, x_r$. A derivation $D \in \operatorname{Der}_k(\mathfrak{A}_r)$ will be regarded as an element of $\operatorname{Der}_k(\mathfrak{A}_n)$ by setting $D(x_j) = 0$ for $r+1 \leq j \leq n$. As before, we shall employ multi-index notation. In particular, ε_j denotes the vector, whose coordinates are given by the Kronecker symbols δ_{ij}.

Lemma 4.1. *Let $n \geq 2$. Then*

$$\sigma_n : W(n-1) \longrightarrow S(n) \;\; ; \;\; D \mapsto D - \operatorname{div}(D) x_n \partial_n$$

is an injective homomorphism of restricted Lie algebras.

Proof. Let D be an element of $W(n-1)$. Since

$$\operatorname{div}(\sigma_n(D)) = \operatorname{div}(D) - \partial_n(\operatorname{div}(D) x_n) = \operatorname{div}(D) - \operatorname{div}(D) = 0,$$

we have $\sigma_n(W(n-1)) \subseteq \ker \operatorname{div}$. According to [23, (IV.3.1)], the map div is a derivation. Given $D, E \in W(n-1)$, we thus obtain

$$
\begin{aligned}
[\sigma_n(D), \sigma_n(E)] &= [D - \operatorname{div}(D) x_n \partial_n, E - \operatorname{div}(E) x_n \partial_n] \\
&= [D, E] - D(\operatorname{div}(E)) x_n \partial_n + E(\operatorname{div}(D)) x_n \partial_n + [\operatorname{div}(D) x_n \partial_n, \operatorname{div}(E) x_n \partial_n] \\
&= [D, E] - \operatorname{div}([D, E]) x_n \partial_n + [\operatorname{div}(D) x_n \partial_n, \operatorname{div}(E) x_n \partial_n] \\
&= \sigma_n([D, E]),
\end{aligned}
$$

so that $\sigma_n : W(n-1) \longrightarrow \ker \operatorname{div}$ is a homomorphism of Lie algebras. As $W(n-1)$ is simple, we have

$$\operatorname{im} \sigma_n = \sigma_n([W(n-1), W(n-1)]) \subseteq (\ker \operatorname{div})^{(1)} = S(n).$$

Moreover, the map σ_n is obviously injective.

In view of Jacobson's formula, it suffices to verify the identity $\sigma_n(x^{[p]}) = \sigma_n(x)^{[p]}$ on a basis of $W(n-1)$. Let $a \leq \tau$ be an element of $\mathbb{N}_0^{n-1}$. By virtue of [23, (IV.2.7)], we have

$$(x^a \partial_j)^{[p]} = \begin{cases} 0 & a \neq \varepsilon_j \\ x^{\varepsilon_j} \partial_j & a = \varepsilon_j \end{cases}$$

for every $j \in \{1, \ldots, n-1\}$. Since

$$\sigma_n(x^a \partial_j) = x^a \partial_j - a_j x^{a-\varepsilon_j} x_n \partial_n$$

there exist $\lambda_i \in k$ such that

$$\sigma_n(x^a \partial_j)^{[p]}(x_i) = \lambda_i \, x^{pa+\varepsilon_i - p\varepsilon_j} \qquad \forall \, i \in \{1, \ldots, n-1\}.$$

This expression vanishes unless $a = \varepsilon_j$. In the remaining case, we readily obtain $\sigma_n(x_j \partial_j) = x_j \partial_j - x_n \partial_n$, so that $\sigma_n(x_j \partial_j)^{[p]} = \sigma_n(x_j \partial_j)$. $\qquad \square$

We denote by $\mathcal{P}(2r)$ the *Poisson algebra*, i.e., the space $\mathfrak{A}_{2r}$, endowed with the standard Poisson bracket $\{\,,\,\}$. By definition, $\{\,,\,\}$ is an associative bi-derivation, defined on the generators $x_1, \ldots, x_{2r}$ by the rule:

$$\{x_i, x_{i+r}\} = 1 = -\{x_{i+r}, x_i\} \qquad 1 \leq i \leq r,$$

and the remaining $\{x_i, x_j\} = 0$ (see [23, p.168]). The center of $\mathcal{P}(2r)$ consists of the space k of constant polynomials, and there is an exact sequence

$$(0) \to k \to \mathcal{P}(2r) \overset{D_H}{\longrightarrow} H''(2r)$$

of Lie algebras, where $H''(2r)$ is the annihilator of the Hamiltonian form (see [23, p.163]). In particular, $H''(2r)$ is a p-subalgebra of $W(2r)$. The image $H'(2r)$ of D_H has codimension 1 in $H''(2r)$, and the derived algebra $H'^{(1)} = H(2r)$ is the *Hamiltonian algebra*.

The Lie algebra $\mathcal{P}(2r)$ is restrictable, and any p-mapping of $\mathcal{P}(2r)$ renders the above exact sequence an exact sequence of restricted Lie algebras. We define a p-mapping by the following formula (cf. [22, p. 403]):

$$(4.1) \qquad (x^a)^{[p]} = \begin{cases} 0 & \text{for} \quad a \notin \{0, \varepsilon_i + \varepsilon_{i+r} \; ; \; i = 1, \ldots, r\}, \\ x^a & \text{for} \quad a \in \{0, \varepsilon_i + \varepsilon_{i+r} \; ; \; i = 1, \ldots, r\}. \end{cases}$$

In particular, $1^{[p]} = 1$, and the center is a torus.

Lemma 4.2. *Let $r \geq 1$. Then the map*

$$\varphi_r : W(r) \longrightarrow \mathcal{P}(2r) \;\; ; \;\; \sum_{j=1}^{r} f_j \partial_j \mapsto \sum_{j=1}^{r} x_j f_j(x_{r+1}, \ldots, x_{2r})$$

is an injective homomorphism of restricted Lie algebras.

Proof. We check that φ_r is a Lie algebra homomorphism. Given $f, g \in \mathfrak{A}_r$ and $i, j \in \{1, \ldots, r\}$, we have $[f\partial_i, g\partial_j] = f\partial_i(g)\partial_j - g\partial_j(f)\partial_i$ in $W(r)$. Writing $f(x')$ for $f(x_{r+1}, \ldots, x_{2r})$, we therefore obtain

$$\begin{aligned} \{x_i f(x'), x_j g(x')\} &= \{x_i, x_j g(x')\} f(x') + x_i \{f(x'), x_j g(x')\} \\ &= x_j \{x_i, g(x')\} f(x') + x_i \{f(x'), x_j\} g(x') \\ &= x_j \partial_{i+r}(g(x')) f(x') - x_i \partial_{j+r}(f(x')) g(x') \\ &= \varphi_r([f\partial_i, g\partial_j]). \end{aligned}$$

Recall that $(x^a \partial_i)^{[p]} = 0$ if $a \neq \varepsilon_i$, and $(x_i \partial_i)^{[p]} = x_i \partial_i$ for all $i \in \{1, \ldots, r\}$. A comparison with (4.1), shows that $\varphi_r\big((x^a \partial_i)^{[p]}\big) = \varphi_r(x^a \partial_i)^{[p]}$ for all $a \in \mathbb{N}_0^r$. Consequently, φ_r is an injective homomorphism of restricted Lie algebras. □

As a corollary, we readily obtain:

Lemma 4.3. *Let $r \geq 1$. The map $D_H \circ \varphi_r$ induces an embedding $W(r) \hookrightarrow H(2r)$ of restricted Lie algebras.* □

5. Toral stabilizers of Cartan type Lie algebras

In this section, we turn to the computation of the toral stabilizers of restricted Lie algebras of Cartan type. Our approach involves embeddings of suitable p-subalgebras.

5.1. **Poisson algebras.** We begin by determining the toral stabilizers of the Poisson algebra with toral center. For $r \geq 1$, we consider the Lie algebra

$$\mathfrak{l}_r := kz \oplus kx_1 \oplus \bigoplus_{i=1}^{r} kt_i,$$

whose bracket and p-mapping are given by

$$[t_i, x_1] = \delta_{i1} x_1 \quad \text{and} \quad t_i^{[p]} = t_i \quad , \quad x_1^{[p]} = z = z^{[p]},$$

respectively, with all unspecified products being zero.

Lemma 5.1.1. *For the restricted Lie algebra $(\mathfrak{l}_r, [p])$, we have $S(\mathfrak{l}_r) \simeq \mathbb{Z}/p\mathbb{Z}$.*

Proof. Setting $\mathfrak{t} := \bigoplus_{i=2}^{r} kt_i$, we obtain a direct sum decomposition

$$\mathfrak{l}_r = \mathfrak{l}_1 \oplus \mathfrak{t}$$

of $\mathfrak{l}_r$, whose second summand is a torus. Consequently, Corollary 2.4 implies

$$S(\mathfrak{l}_r) \simeq S(\mathfrak{l}_1) \times S(\mathfrak{t}) \simeq S(\mathfrak{l}_1).$$

According to [7, p.4215], we have $S(\mathfrak{l}_1) \cong \mathbb{Z}/p\mathbb{Z}$, as desired.   □

A restricted Lie algebra $\mathfrak{g}$ is referred to as *trigonalizable* if it can be embedded into a restricted Lie algebra of triangular matrices. This is equivalent to every restricted simple $\mathfrak{g}$-module being one-dimensional.

Theorem 5.1.2. *Let $\mathcal{P}(2r)$ be the restricted Poisson algebra in $2r$ variables with toral center. Then $S(\mathcal{P}(2r)) \simeq \mathrm{GL}_r(\mathbb{F}_p) \ltimes (\mathbb{F}_p)^r$. Moreover, for any torus $\mathfrak{t} \subseteq \mathcal{P}(2r)$ of maximal dimension, we have $S(\mathcal{P}(2r), \mathfrak{t}) = \{g \in \mathrm{Aut}_p(\mathfrak{t}) \; ; \; g(1) = 1\}$.*

Proof. We first show that $S(\mathcal{P}(2r)) \simeq \mathrm{GL}_r(\mathbb{F}_p) \ltimes W$, where $W = (0)$ or $W = (\mathbb{F}_p)^r$ with the natural action by $\mathrm{GL}_r(\mathbb{F}_p)$. In view of Lemma 4.2, there exists an embedding $k \oplus W(r) \hookrightarrow \mathcal{P}(2r)$ originating in the direct sum of the one-dimensional torus k with $W(r)$. Let $\mathfrak{t} = k \oplus \mathfrak{t}'$, where $\mathfrak{t}' \subseteq W(r)$ is any torus of maximal dimension. Thanks to Lemma 2.1, Corollary 2.4 and Proposition 2.3(3), we obtain inclusions

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & S(W(r), \mathfrak{t}') \end{array} \right) \subseteq S(\mathcal{P}(2r), \mathfrak{t}) \subseteq \left(\begin{array}{c|c} 1 & (\mathbb{F}_p)^r \\ \hline 0 & \mathrm{GL}_r(\mathbb{F}_p) \end{array} \right).$$

Owing to [19, Thm. 1] and Proposition 3.3, the group $S(W(r), \mathfrak{t}')$ is isomorphic to $\mathrm{GL}_r(\mathbb{F}_p)$. Since the matrix group on the right identifies with the semi-direct product of $\mathrm{GL}_r(\mathbb{F}_p)$ with the standard module $(\mathbb{F}_p)^r$, we obtain embeddings

$$\mathrm{GL}_r(\mathbb{F}_p) \ltimes (0) \subseteq S(\mathcal{P}(2r), \mathfrak{t}) \subseteq \mathrm{GL}_r(\mathbb{F}_p) \ltimes (\mathbb{F}_p)^r.$$

Consequently, $S(\mathcal{P}(2r), \mathfrak{t}) \simeq \mathrm{GL}_r(\mathbb{F}_p) \ltimes W$, where $W := S(\mathcal{P}(2r), \mathfrak{t}) \cap [(1) \ltimes (\mathbb{F}_p)^r]$ is a $\mathrm{GL}_r(\mathbb{F}_p)$-submodule of $(\mathbb{F}_p)^r$. Since $(\mathbb{F}_p)^r$ is irreducible, we have $W = (0)$ or $W = (\mathbb{F}_p)^r$.

   In order to show that $W \neq (0)$, we consider the subspace

$$\mathfrak{l} = k + k(1 + x_{r+1}) + \sum_{i=1}^{r} kx_i(1 + x_{i+r})$$

of $\mathcal{P}(2r)$. We claim that $\mathfrak{l}$ is a p-subalgebra of $\mathcal{P}(2r)$ which is isomorphic to $\mathfrak{l}_r$. Using the fact that the Poisson bracket is a bi-derivation for the associative structure, we obtain

$$\{x_i(1+x_{i+r}), 1+x_{r+1}\} = \{x_i, 1+x_{r+1}\}(1+x_{i+r}) = \{x_i, x_{r+1}\}(1+x_{i+r}) = \delta_{i1}(1+x_{i+r}).$$

Since polynomials in x_i and x_{i+r} commute with polynomials in the remaining variables, we see that all other brackets are 0. Hence, $\mathfrak{l} \simeq \mathfrak{l}_r$ as abstract Lie algebras. We have $1^{[p]} = 1$ by definition. Also, using Jacobson's formula, we obtain

$$(1+x_{r+1})^{[p]} = 1^{[p]} + x_{r+1}^{[p]} = 1.$$

Setting $t_i = x_i(1+x_{i+r})$, we show that $t_i^{[p]} = t_i$. One can easily check $(\mathrm{ad}\, t_i)^p = \mathrm{ad}\, t_i$ by comparing the action of these derivations on the associative generators $x_1, \ldots, x_r$ and $1+x_{r+1}, \ldots, 1+x_{2r}$ of $\mathcal{P}(2r)$. As the center $C(\mathcal{P}(2r))$ coincides with k, there exists $\lambda \in k$ such that $t_i^{[p]} = t_i + \lambda 1$. Consider the decomposition $t_i = x_i + x_i x_{i+r}$. Jacobson's formula in conjunction with (4.1) yields

$$t_i^{[p]} = x_i^{[p]} + (x_i x_{i+r})^{[p]} + \sum_{j=1}^{p-1} s_j(x_i, x_i x_{i+r}) = x_i x_{i+r} + \sum_{j=1}^{p-1} s_j(x_i, x_i x_{i+r}).$$

Observe that both, x_i and $x_i x_{i+r}$, belong to the subspace $E := x_i \cdot k[x_{i+r}]$. It is easy to check that E is stable under $\mathrm{ad}\, x_i$ and $\mathrm{ad}\, x_i x_{i+r}$. Hence all the $s_j(x_i, x_i x_{i+r})$ belong to E. Consequently, we obtain $\lambda 1 + t_i = t_i^{[p]} \equiv x_i x_{i+r} \mod E$, forcing $\lambda = 0$, as required.

According to [22, (7.5.10)], the space $\mathfrak{t} := k + \sum_{i+1}^r k t_i \subseteq \mathfrak{l}$ is a torus of $\mathcal{P}(2r)$ of maximal dimension. By Lemma 5.1.1, we have $S(\mathfrak{l}, \mathfrak{t}) \simeq \mathbb{Z}/p\mathbb{Z}$. Since the factor algebra $\mathfrak{l}/k$ is trigonalizable with torus $\mathfrak{t}' := \mathfrak{t}/k$ of maximal dimension, [7, (6.1)] implies $S(\mathfrak{l}/k, \mathfrak{t}') = \{1\}$. Proposition 2.3 now provides an embedding ξ in the top line of the following diagram:

$$
\begin{array}{ccc}
S(\mathfrak{l}, \mathfrak{t}) & \xrightarrow{\ \xi\ } & \left(\begin{array}{c|c} 1 & \mathrm{Lie}_p(\mathfrak{t}', k) \\ \hline 0 & I_{\mathfrak{t}'} \end{array} \right) \\
\alpha \downarrow & & \downarrow \\
S(\mathcal{P}(2r), \mathfrak{t}) & = & \left(\begin{array}{c|c} 1 & W \\ \hline 0 & \mathrm{GL}_r(\mathbb{F}_p) \end{array} \right).
\end{array}
$$

The map α is the inclusion given by Lemma 2.1, and the matrices on the right describe the endomorphisms of $\mathfrak{t} = k \oplus \mathfrak{t}'$ according to the block decomposition (2.1). By construction of all these maps, the diagram is commutative. Since $\mathrm{im}\, \xi \simeq S(\mathfrak{l}, \mathfrak{t}) \neq \{1\}$, we have $W \neq (0)$, as desired.

For the last statement of the theorem, observe that a maximal torus $\mathfrak{t}$ always contains $\mathfrak{n} = k.1$ as a subtorus. Corollary 2.2 provides an inclusion $S(\mathcal{P}(2r), \mathfrak{t}) \subseteq \{g \in \mathrm{Aut}_p(\mathfrak{t}) ; g(1) = 1\}$. As these groups have same order, this inclusion is an equality. $\qquad\square$

5.2. Lie algebras of Cartan type.
The main result of this section reads:

Theorem 5.2.1. *Let $\mathfrak{g}$ be a Lie algebra of Cartan type. Then there is an isomorphism*

$$S(\mathfrak{g}) \cong \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p).$$

Proof. Assume first that $\mathfrak{g}$ is of type W. Also, if $p = 3$ assume that $\mathfrak{g} \neq W(1)$. Proposition 3.3 provides a generic torus $\mathfrak{t}_0 \subseteq \mathfrak{g}$ and an isomorphism

$$W(\mathfrak{g}, \mathfrak{t}_0) \cong S(\mathfrak{g}).$$

The isomorphism $W(\mathfrak{g}, \mathfrak{t}_0) \cong \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$ was established in [19, Thm. 1]. Now assume that $p = 3$ and $\mathfrak{g} = W(1) \cong \mathfrak{sl}_2$. Then $\mathrm{Aut}_p(\mathfrak{g})$ is no longer connected, so we cannot use Premet's result. Note

that $S(\mathfrak{g}) \hookrightarrow \mathrm{GL}_1(\mathbb{F}_3) \cong \mathbb{Z}/(2)$, so that we only need to see that $S(\mathfrak{g})$ is not trivial. This follows from [7, Remark (1), p.4201].

When $\mathfrak{g}$ is of type S or H, Lemmas 4.1 and 4.3 furnish embeddings $W(\mu(\mathfrak{g})) \hookrightarrow \mathfrak{g}$. Lemma 2.1 thus yields $\mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p) \hookrightarrow S(\mathfrak{g})$, so that $S(\mathfrak{g}) \cong \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$.

The rest of the proof is devoted to contact algebras. Let $n = 2r+1$ be an odd number. Following [23, (IV.5)], we endow the truncated polynomial ring $\mathfrak{A}_n$ with the structure of a restricted Lie algebra; the corresponding Lie bracket $\langle\,,\,\rangle$ is called *contact bracket*. In the sequel, $K''(n)$ will denote the vector space $\mathfrak{A}_n$, endowed with this bracket. Then $K(n) = K''(n)^{(1)}$ is the contact algebra.

Let $\mathfrak{t} := \bigoplus_{i=1}^{r} kx_i x_{r+i} \oplus k(1+x_n) \subseteq K(n)$. Then $\mathfrak{t}$ is a torus of maximal dimension in $K(n)$, and we claim that

$$S(K(n), \mathfrak{t}) \simeq \mathrm{GL}_{r+1}(\mathbb{F}_p).$$

We identify $\mathrm{Aut}_p(\mathfrak{t})$ with $\mathrm{GL}_{r+1}(\mathbb{F}_p)$, using the ordered basis $\{1+x_n, x_1 x_{r+1}, \ldots, x_r x_{2r}\}$. Henceforth, all matrix representations will describe automorphisms of $\mathfrak{t}$ by means of this basis.

By [22, (7.5.15)], we know that the centralizer $\mathfrak{c} = C_{K''(n)}(1+x_n)$ is isomorphic to the Poisson algebra $\mathcal{P}(2r)$ with toral center. Since $\mathfrak{t} \subseteq \mathfrak{c}$, Theorem 5.1.2 yields the following matrix description:

$$(5.1) \qquad \begin{pmatrix} 1 & (\mathbb{F}_p)^r \\ 0 & \mathrm{GL}_r(\mathbb{F}_p) \end{pmatrix} \equiv S(\mathfrak{c}, \mathfrak{t}) \subseteq S(K''(n), \mathfrak{t}),$$

with the inclusion following from Lemma 2.1.

We will now embed lower triangular matrices into $S(K''(n), \mathfrak{t})$, by means of a method similar to the one used in Theorem 5.1.2. Consider the subspace

$$\mathfrak{l} := kx_r x_{2r} \oplus kx_r x_{2r}(1+x_n) \oplus k(1+x_n) \subseteq K''(n).$$

We first prove that $\mathfrak{l}$ is a restricted Lie algebra isomorphic to the one in [7, p. 4216] (or to $\mathfrak{l}_1$ in Lemma 5.1.1). We check that such an isomorphism is defined by the assignment

$$z \mapsto x_r x_{2r}, \quad x \mapsto x_r x_{2r}(1+x_n), \quad t \mapsto 1+x_n.$$

Indeed, directly from the rules given in [23, p.173], we obtain

$$\langle x_r x_{2r}, 1+x_n \rangle = 0 = \langle x_r x_{2r}, x_r x_{2r}(1+x_n) \rangle$$

as well as

$$\begin{aligned} \langle 1+x_n, x_r x_{2r}(1+x_n) \rangle &= \langle 1, x_r x_{2r}(1+x_n) \rangle + \langle x_n, x_r x_{2r}(1+x_n) \rangle \\ &= 2x_r x_{2r} + 2x_r x_{2r} x_n = 2x_r x_{2r}(1+x_n). \end{aligned}$$

In view of [23, p.177], we also have

$$(1+x_n)^{[p]} = 1 + x_n^{[p]} = 1+x_n.$$

Moreover, since $\langle x_r x_{2r}, x_r x_{2r} x_n \rangle = 0$, we finally obtain

$$(x_r x_{2r}(1+x_n))^{[p]} = x_r x_{2r}.$$

Now let $\mathfrak{t}' := \sum_{i=1}^{r-1} kx_i x_{i+r}$, so that $\mathfrak{t} = k(1+x_n) + \mathfrak{t}' + kx_r x_{2r}$. Write $\mathfrak{t}_\mathfrak{l} = k(1+x_n) + kx_r x_{2r}$ to ease notation. Since $\langle \mathfrak{t}', \mathfrak{l} \rangle = 0$, there is an embedding $\mathfrak{t}' \oplus \mathfrak{l} \hookrightarrow K''(n)$ of restricted Lie algebras, which in turn yields an embedding

$$S(\mathfrak{t}' \oplus \mathfrak{l}, \mathfrak{t}' \oplus \mathfrak{t}_\mathfrak{l}) \simeq (1) \times S(\mathfrak{l}, \mathfrak{t}_\mathfrak{l}) \hookrightarrow S(K''(n), \mathfrak{t})$$

of finite groups. According to [7, p. 4216], the group $S(\mathfrak{l}, \mathfrak{t}_{\mathfrak{l}})$ is generated by the transformation $x_r x_{2r} \mapsto x_r x_{2r}$, $(1+x_n) \mapsto x_r x_{2r} + (1+x_n)$. Using the previous matrix identification, this yields

$$\begin{pmatrix} 1 & 0 \\ v & I_r \end{pmatrix} \in S(K''(n), \mathfrak{t}), \quad \text{where } v = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}.$$

In view of (5.1), the group $S(K''(n), \mathfrak{t})$ also contains $\begin{pmatrix} 1 & 0 \\ 0 & \mathrm{GL}_r(\mathbb{F}_p) \end{pmatrix}$, so the irreducibility of the $\mathrm{GL}_r(\mathbb{F}_p)$-module $(\mathbb{F}_p)^r$ yields

(5.2)
$$\begin{pmatrix} 1 & 0 \\ (\mathbb{F}_p)^r & \mathrm{GL}_r(\mathbb{F}_p) \end{pmatrix} \subseteq S(K''(n), \mathfrak{t}).$$

Using (5.1) and (5.2), we see that $S(K''(n), \mathfrak{t})$ contains the subgroup generated by all shear matrices, which, owing to [12, Lemma 6.7.1], coincides with $\mathrm{SL}_{r+1}(\mathbb{F}_p)$. By (5.2), it also contains matrices of arbitrary determinant, whence $S(K''(n), \mathfrak{t}) \cong \mathrm{GL}_{r+1}(\mathbb{F}_p)$. Since the factor algebra $K''(n)/K(n)$ is p-unipotent, Lemma 2.1 now yields the result. $\square$

Taking into account Theorem 1.1 (1), we obtain the following remarkable corollary:

Corollary 5.2.2. *Let $\mathfrak{g}$ be a Lie algebra of Cartan type. Then the variety $\mathcal{T}_{\mathfrak{g}}(k)$ is irreducible.* $\square$

5.3. **The Melikian algebra.** For the sake of completeness, we mention the case of the restricted Melikian algebra. Recall that this is a simple graded Lie algebra over a field of characteristic $p = 5$, which is neither classical nor of Cartan type. We refer the reader to [20] for the details. As for contact algebras, it can be shown that this algebra affords infinitely many conjugacy classes of tori of maximal dimension.

Theorem 5.3.1. *Assume that k has characteristic $p = 5$. Let $\mathcal{M}$ be the restricted Melikian algebra. Then there is an isomorphism*

$$S(\mathcal{M}) \cong \mathrm{GL}_2(\mathbb{F}_p),$$

and the variety of embeddings $\mathcal{T}_{\mathcal{M}}(k)$ is irreducible.

Proof. By construction, there exists an embedding $W(2) \hookrightarrow \mathcal{M}$ (see [20, Sect. 1]). By [20, Cor. 4.4], all maximal tori in $\mathcal{M}$ have dimension 2, so that $\mu(W(2)) = \mu(\mathcal{M})$. Let $\mathfrak{t} \subseteq W(2) \subseteq \mathcal{M}$ be a torus of dimension 2. Using Lemma 2.1, we obtain embeddings $S(W(2), \mathfrak{t}) \subseteq S(\mathcal{M}, \mathfrak{t}) \subseteq \mathrm{Aut}_p(\mathfrak{t})$. By Theorem 5.2.1, this forces $S(\mathcal{M}, \mathfrak{t}) = \mathrm{Aut}_p(\mathfrak{t}) \cong \mathrm{GL}_2(\mathbb{F}_p)$. The fact that the variety of embeddings is irreducible now follows from Theorem 1.1. $\square$

6. Applications

The applications to be discussed in this final section pertain to weight space decompositions, the non-existence of generic tori and invariants for certain Lie algebras of Cartan type. While the second topic originates in Demuškin's early work [3, 4] along with Strade's corrections [22], our observations on invariants are motivated by Premet's paper [19].

6.1. **Irreducibility and Weights.** Our first result illustrates why it is reasonable to consider toral stabilizers as a replacement for Weyl groups when dealing with arbitrary restricted Lie algebras.

By definition, a *restricted* $\mathfrak{g}$-*module* M is a $\mathfrak{g}$-module such that for every $x \in \mathfrak{g}$, the operator $m \mapsto x^{[p]}.m$ is the p-th power of the transformation of M effected by x. If $\mathfrak{t} \subseteq \mathfrak{g}$ is a torus, then M is a completely reducible $\mathfrak{t}$-module, giving rise to the *weight space decomposition*

$$M = \bigoplus_{\lambda \in \Lambda_M} M_\lambda.$$

Each $\lambda \in \Lambda_M$ is a linear form satisfying $\lambda(t^{[p]}) = \lambda(t)^p$ for every $t \in \mathfrak{t}$. As a result, $\Lambda_M \subseteq \mathrm{Lie}_p(\mathfrak{t}, k)$ is a subset of the character group of $\mathfrak{t}$, i.e., the additive group of all homomorphisms $\mathfrak{t} \longrightarrow k$ of restricted Lie algebras, where the p-map on k is the associative p-th power. The group $\mathrm{Aut}_p(\mathfrak{t})$ acts contragrediently on $\mathrm{Lie}_p(\mathfrak{t}, k)$ via

$$h.\varphi := \varphi \circ h^{-1} \qquad \forall\, h \in \mathrm{Aut}_p(\mathfrak{t}),\ \varphi \in \mathrm{Lie}_p(\mathfrak{t}, k).$$

If $\mathfrak{t} \subseteq \mathfrak{g}$ is a torus of maximal dimension, then $S(\mathfrak{g}, \mathfrak{t}) \subseteq \mathrm{Aut}_p(\mathfrak{t})$ also acts on $\mathrm{Lie}_p(\mathfrak{t}, k)$.

Theorem 6.1.1. *Let $(\mathfrak{g}, [p])$ be a restricted Lie algebra, $\mathfrak{t} \subseteq \mathfrak{g}$ be a torus of maximal dimension. If M is a restricted $\mathfrak{g}$-module with weight space decomposition*

$$M = \bigoplus_{\lambda \in \Lambda_M} M_\lambda,$$

then $\Lambda_M \subseteq \mathrm{Lie}_p(\mathfrak{t}, k)$ is $S(\mathfrak{g}, \mathfrak{t})$-stable and the dimensions of the weight spaces are constant on the $S(\mathfrak{g}, \mathfrak{t})$-orbits.

Proof. As in the proof of Lemma 1.6, put $A := k[\mathfrak{X}_\mathfrak{t}]$ and let $j : \mathfrak{t} \hookrightarrow \mathfrak{g} \otimes_k A$ be the universal embedding of $\mathfrak{t}$. In particular, given a commutative k-algebra R, an element $\varphi_x : \mathfrak{t} \to \mathfrak{g} \otimes_k R$ corresponds to $x \in \mathrm{Spec}_k(A)(R)$ if and only if $\varphi_x = (\mathrm{id}_\mathfrak{g} \otimes x) \circ j$. Consider the restricted A-Lie algebra $\tilde{\mathfrak{g}} := \mathfrak{g} \otimes_k A$. Then $\tilde{M} := M \otimes_k A$ is a restricted $\tilde{\mathfrak{g}}$-module, and the universal embedding gives rise to a weight space decomposition

$$\tilde{M} = \bigoplus_{\gamma \in \Gamma_{\tilde{M}}} \tilde{M}_\gamma$$

of the $\mathfrak{t}$-module $\tilde{M}$, whose constituents are A-submodules of $\tilde{M}$. Let $x \in \mathrm{Spec}_k(A)(k)$ be a k-rational point. As observed in [7, (4.2)], we have

$$M = \bigoplus_{\gamma \in \Gamma_{\tilde{M}}} M_\gamma(x),$$

where $M_\gamma(x) = M_{\gamma \circ \varphi_x^{-1}}$ is the weight space with weight $\gamma \circ \varphi_x^{-1}$ relative to the torus $\varphi_x(\mathfrak{t}) \subseteq \mathfrak{g}$. Since each $\tilde{M}_\gamma$ is a finitely generated projective module over the integral domain A, it has constant rank and [15, p.166] yields

$$\dim_k M_\gamma(x) = \mathrm{rk}(\tilde{M}_\gamma) \qquad \forall\, x \in \mathfrak{X}_\mathfrak{t}(k).$$

In particular, these dimensions are non-zero integers which depend only on γ.

Let $\iota : \mathfrak{t} \hookrightarrow \mathfrak{g}$ be the canonical inclusion. Given $g \in S(\mathfrak{g}, \mathfrak{t})$, we have $g.\iota = \iota \circ g^{-1} \in \mathfrak{X}_\mathfrak{t}(k)$, and

$$M = \bigoplus_{\gamma \in \Gamma_{\tilde{M}}} M_{\gamma \circ g}$$

is the weight space decomposition of M relative to $\mathfrak{t}$. Thus, $\Lambda_M = g.\Gamma_{\tilde{M}}$ for all $g \in S(\mathfrak{g}, \mathfrak{t})$ and $\dim_k M_{g.\lambda} = \mathrm{rk}(\tilde{M}_\lambda) = \dim_k M_\lambda$ for every $\lambda \in \Lambda_M$. $\square$

Corollary 6.1.2. *Let $\mathfrak{t} \subseteq \mathfrak{g}$ be a torus of maximal dimension, $M = \bigoplus_{\lambda \in \Lambda_M} M_\lambda$ be a restricted $\mathfrak{g}$-module. If the variety $\mathcal{T}_\mathfrak{g}(k)$ is irreducible, then the following statements hold:*
   (1) $\Lambda_M = \{0\}$*, or Λ_M contains* $\mathrm{Lie}_p(\mathfrak{t}, k) \setminus \{0\}$.
   (2) *All weight spaces of M belonging to non-zero weights have the same dimension.*

Proof. Let $\mathfrak{t} \subseteq \mathfrak{g}$ be a torus of maximal dimension, $M = \bigoplus_{\lambda \in \Lambda_M} M_\lambda$ be the corresponding weight space decomposition of M. By Theorem 6.1.1, the set $\Lambda_M \subseteq \mathrm{Lie}_p(\mathfrak{t}, k)$ is $S(\mathfrak{g}, \mathfrak{t})$-stable.

According to Theorem 1.1, the variety $\mathcal{T}_\mathfrak{g}(k)$ has $[\mathrm{Aut}_p(\mathfrak{t}) : S(\mathfrak{g}, \mathfrak{t})]$ irreducible components. In view of our assumption, this yields $S(\mathfrak{g}, \mathfrak{t}) = \mathrm{Aut}_p(\mathfrak{t})$. Consequently $S(\mathfrak{g}, \mathfrak{t}) \cong \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$ acts via two orbits on $\mathrm{Lie}_p(\mathfrak{t}, k) \cong \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^{\mu(\mathfrak{g})}, \mathbb{F}_p)$, namely $\{0\}$ and $\mathrm{Lie}_p(\mathfrak{t}, k) \setminus \{0\}$. $\qquad\square$

Remark. Let $\mathfrak{g}$ be such that $\mathcal{T}_\mathfrak{g}(k)$ is irreducible. For any restricted $\mathfrak{g}$-module $M = \bigoplus_{\lambda \in \Lambda_M} M_\lambda$, we have $\Lambda_M = \{0\}, \mathrm{Lie}_p(\mathfrak{t}, k) \setminus \{0\}$ or $\mathrm{Lie}_p(\mathfrak{t}, k)$. We consider the Jacobson-Witt algebra $\mathfrak{g} = W(n)$ acting via derivations in the truncated polynomial ring $\mathfrak{A}_n$. Then, $k \subseteq \mathfrak{A}_n$ is a submodule, and the three possibilities occur for k, $\mathfrak{A}_n/k$, and $\mathfrak{A}_n$, respectively.

We record the particular case given by the adjoint representation:

Corollary 6.1.3. *Let $\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha$ be the root space decomposition of $\mathfrak{g}$ relative to a torus $\mathfrak{t} \subseteq \mathfrak{g}$ of maximal dimension. If the variety $\mathcal{T}_\mathfrak{g}(k)$ is irreducible, then $\Phi \cup \{0\} = \mathrm{Lie}_p(\mathfrak{t}, k)$, and all root spaces of $\mathfrak{g}$ have the same dimension.*

Proof. If $\Phi = \emptyset$, then $\mathfrak{g} = \mathfrak{g}_0$ is nilpotent and, being an irreducible variety of dimension zero, $\mathcal{T}_\mathfrak{g}(k)$ is a singleton. Consequently, $\mathfrak{t} = (0)$, so that $\mathrm{Lie}_p(\mathfrak{t}, k) = \{0\}$. The case where $\Phi \neq \emptyset$ follows directly from Corollary 6.1.2. $\qquad\square$

6.2. **Non-generic tori.** We will prove that the Weyl groups of the Poisson algebra $\mathcal{P}(2r)$ do not coincide with the toral stabilizer, and obtain as a consequence that contact algebras do not afford generic tori. This result strengthens Strade's observation [22], who showed that $K(2r+1)$ possesses infinitely many conjugacy classes of maximal tori.

To do so, we first gather some observations concerning automorphisms of $\mathcal{P}(2r)$. Any Lie algebra automorphism of $\mathcal{P}(2r)$ stabilizes the center $k \subseteq \mathcal{P}(2r)$. The simple Lie algebra $H(2r)$ can be realized as the derived subalgebra of the quotient algebra $\mathcal{P}(2r)/k$. There results a homomorphism

$$\pi : \mathrm{Aut}(\mathcal{P}(2r)) \longrightarrow \mathrm{Aut}(H(2r))$$

of groups. Our analysis of $\mathrm{Aut}(\mathcal{P}(2r))$ involves two classes of automorphisms. A Lie algebra automorphism $\sigma \in \mathrm{Aut}(\mathcal{P}(2r))$ is a *semi-Poisson automorphism* if there exists a non-zero scalar $\alpha \in k^\times$ such that $\alpha\sigma$ preserves the associative structure of $\mathcal{P}(2r)$. If $\alpha = 1$, then σ is referred to as a *Poisson automorphism*. The set of semi-Poisson automorphisms is a subgroup of $\mathrm{Aut}(\mathcal{P}(2r))$, which we denote by $\mathrm{Aut}_{\mathrm{SP}}(\mathcal{P}(2r))$.

Let $\lambda \in \mathcal{P}(2r)^*$ be a linear form which vanishes on $\mathcal{P}(2r)^{(1)}$. Then

$$\varphi_\lambda : \left\{ \begin{array}{rcl} \mathcal{P}(2r) & \to & \mathcal{P}(2r) \\ f & \mapsto & f + \lambda(f) \end{array} \right.$$

is an automorphism of the Lie algebra $\mathcal{P}(2r)$ and $\mathcal{H} := \{\varphi_\lambda \; ; \; \lambda \in (\mathcal{P}(2r)/\mathcal{P}(2r)^{(1)})^*\}$ is a subgroup of $\mathrm{Aut}(\mathcal{P}(2r))$ such that $\mathrm{Aut}_{\mathrm{SP}}(\mathcal{P}(2r)) \cap \mathcal{H} = \{\mathrm{id}_{\mathcal{P}(2r)}\}$.

Theorem 6.2.1. *Let* $\pi : \mathrm{Aut}(\mathcal{P}(2r)) \to \mathrm{Aut}(H(2r))$ *be the natural map. Then* $\ker(\pi) = \mathcal{H}$, *and we have*

$$\mathrm{Aut}(\mathcal{P}(2r)) = \mathrm{Aut}_{\mathrm{SP}}(\mathcal{P}(2r)) \ltimes \mathcal{H}.$$

Proof. It follows from [22, (7.3.6)] that the restriction of π to $\mathrm{Aut}_{SP}(\mathcal{P}(2r))$ is surjective. We will proceed to verify $\ker(\pi) = \mathcal{H}$. This will prove that the restriction of π to $\mathrm{Aut}_{\mathrm{SP}}(\mathcal{P}(2r))$ is also injective, so that $\mathrm{Aut}(\mathcal{P}(2r)) = \mathrm{Aut}_{\mathrm{SP}}(\mathcal{P}(2r)) \ltimes \mathcal{H}$. Given $\sigma \in \ker(\pi)$, there exists a linear map $\mu : \mathcal{P}(2r)^{(1)} \to k$ such that $\sigma(f) = f + \mu(f)$ for all $f \in \mathcal{P}(2r)^{(1)}$. Consequently,

$$
\begin{aligned}
\{f,g\} &= \{f + \mu(f), g + \mu(g)\} = \{\sigma(f), \sigma(g)\} \\
&= \sigma(\{f,g\}) = \{f,g\} + \mu(\{f,g\}),
\end{aligned}
$$

so that $\mu(\{f,g\}) = 0$ for all $f, g \in \mathcal{P}(2r)^{(1)}$. Since $\mathcal{P}(2r)^{(1)}$ is a perfect Lie algebra, we have $\mu \equiv 0$, i.e. $\sigma(f) = f$ for every $f \in \mathcal{P}(2r)^{(1)}$.

We have a vector space decomposition $\mathcal{P}(2r) = \mathcal{P}(2r)^{(1)} \oplus kx^\tau$, where $x^\tau = x_1^{p-1} \cdots x_{2r}^{p-1}$ is the unique monomial of maximal degree $d = 2r(p-1)$. Let $\alpha \in k$ and $g \in \mathcal{P}(2r)^{(1)}$ be such that $\sigma(x^\tau) = \alpha\, x^\tau + g$. Note that g is a linear combination of monomials of degree lower than d. To see that $\sigma \in \mathcal{H}$ we need to show that $\alpha = 1$ and $g \in k$.

Recall the notation $i' = i+r$ (resp. $i-r$) for $i \leq r$ (resp. $i > r$), so that $\{x_i, x_j\} = \delta_{i',j}$. Since the element

$$\{x_i, x^\tau\} = -x_1^{p-1} \cdots x_{i'}^{p-2} \cdots x_{2r}^{p-1},$$

lies in $\mathcal{P}(2r)^{(1)}$, it is fixed by σ. Hence,

$$
\begin{aligned}
-x_1^{p-1} \cdots x_{i'}^{p-2} \cdots x_{2r}^{p-1} &= \sigma\big(\{x_i, x^\tau\}\big) = \{\sigma(x_i), \sigma(x^\tau)\} = \{x_i, \alpha\, x^\tau + g\} \\
&= -\alpha\, x_1^{p-1} \cdots x_{i'}^{p-2} \cdots x_{2r}^{p-1} + \{x_i, g\},
\end{aligned}
$$

so that

$$\{x_i, g\} = (\alpha-1)x_1^{p-1} \cdots x_{i'}^{p-2} \cdots x_{2r}^{p-1}$$

for all $i \in \{1, \ldots, 2r\}$. Since bracketing by x_i lowers the degree by 1, $\{x_i, g\}$ is a linear combination of monomials of degree $< d-1$. Consequently, both sides are zero, so that $\alpha = 1$ and $\{x_i, g\} = 0$ for all i. The latter condition implies that g is central, i.e. $g \in k$ as desired. $\square$

We turn to Weyl groups of the Poisson algebra.

Proposition 6.2.2. *Let* $\mathfrak{t} \subseteq \mathcal{P}(2r)$ *be a torus of maximal dimension,* $H \subseteq \mathrm{Aut}_p(\mathcal{P}(2r))$ *be a subgroup. Then the following statements hold:*
  (1)   *There exists an embedding* $\mathrm{Nor}_H(\mathfrak{t})/\mathrm{Cent}_H(\mathfrak{t}) \hookrightarrow \mathbb{F}_p^* \times \mathrm{GL}_r(\mathbb{F}_p)$.
  (2) $W(\mathcal{P}(2r), \mathfrak{t}) \subsetneq S(\mathcal{P}(2r), \mathfrak{t})$.
  (3)   *The Poisson algebra* $\mathcal{P}(2r)$ *affords no generic torus.*

Proof. (1) Let $\mathfrak{m} \subseteq \mathcal{P}(2r)$ denote the subspace of polynomials without constant term. Being the unique maximal ideal of the local algebra $\mathfrak{A}_{2r}$, $\mathfrak{m}$ is stable under semi-Poisson automorphisms. Owing to [22, (7.5.10)], the torus $\mathfrak{t}$ is conjugate under a Poisson automorphism to one of the following tori:

$$T_q = k \oplus \sum_{i=1}^{q} k(1+x_i)x_{i+r} \oplus \sum_{i=q+1}^{r} x_i x_{i+r}, \qquad q \in \{0, \ldots, r\}.$$

(But the conjugating automorphism is **not** restricted in general.) Each of these tori has the form $k \oplus T'$ for some torus $T' \subseteq \mathfrak{m}$. Since Poisson automorphisms stabilize $\mathfrak{m}$, we also obtain a decomposition $\mathfrak{t} = k \oplus \mathfrak{t}_0$, where $\mathfrak{t}_0 \subseteq \mathfrak{m}$ is a torus.

Let $g \in \operatorname{Nor}_H(\mathfrak{t})$. Thanks to Theorem 6.2.1, the automorphism g is a composite $g = g_0 \circ h$, where g_0 is a semi-Poisson automorphism and $h \in \mathcal{H}$. Now, $\mathfrak{t}$ being a torus, we have $\mathfrak{t} \subseteq \mathcal{P}(2r)^{(1)}$, so that h acts trivially on $\mathfrak{t}$. Thus, g and g_0 induce the same automorphism of $\mathfrak{t}$, whence $g(k) \subseteq k$ and $g(\mathfrak{t}_0) \subseteq \mathfrak{t} \cap \mathfrak{m} = \mathfrak{t}_0$. We obtain a well-defined mapping

$$\operatorname{Nor}_H(\mathfrak{t}) \longrightarrow \operatorname{Aut}_p(k) \times \operatorname{Aut}_p(\mathfrak{t}_0) \ ; \ \ g \mapsto (g|_k, g|_{\mathfrak{t}_0}),$$

which induces the desired embedding $\operatorname{Nor}_H(\mathfrak{t})/\operatorname{Cent}_H(\mathfrak{t}) \hookrightarrow \mathbb{F}_p^* \times \operatorname{GL}_r(\mathbb{F}_p)$.

(2) According to Lemma 1.2, the Weyl group $W(\mathcal{P}(2r), \mathfrak{t})$ is contained in $S(\mathcal{P}(2r), \mathfrak{t})$. By part (1), there is an embedding $W(\mathcal{P}(2r), \mathfrak{t}) \hookrightarrow \mathbb{F}_p^* \times \operatorname{GL}_r(\mathbb{F}_p)$, while Theorem 5.1.2 yields $S(\mathcal{P}(2r), \mathfrak{t}) \simeq \operatorname{GL}_r(\mathbb{F}_p) \ltimes (\mathbb{F}_p)^r$.

(3) This is a direct consequence of (2) and Theorem 1.5. $\qquad\qquad\qquad\qquad\qquad\square$

Theorem 6.2.3. *The contact algebra $K(2r+1)$ affords no generic torus.*

Proof. We write $\mathfrak{g} := K''(2r+1)$ to ease notation, so that $\mathfrak{g}^{(1)} = K(2r+1)$. Note that $\mathfrak{g}^{(1)}$ is a p-ideal of $\mathfrak{g}$ such that the factor algebra is p-unipotent. As a consequence, all tori of $\mathfrak{g}$ are contained in $\mathfrak{g}^{(1)}$, and we have $S_{\mathfrak{g}} = S_{\mathfrak{g}^{(1)}}$. Furthermore, if $\mathfrak{t} \subseteq \mathfrak{g}^{(1)}$ is a torus of maximal dimension, then Lemma 2.1 and Theorem 5.2.1 yield $S(\mathfrak{g}, \mathfrak{t}) = S(\mathfrak{g}^{(1)}, \mathfrak{t}) = \operatorname{Aut}_p(\mathfrak{t})$.

Let us prove that restriction to the derived subalgebra induces a surjective homomorphism res : $\operatorname{Aut}_p(\mathfrak{g})^\circ \to \operatorname{Aut}_p(\mathfrak{g}^{(1)})$. By Theorem 3.1, the group on the right is connected. Thanks to [11, Prop. 7.4 B], it therefore suffices to show the surjectivity of the map $\operatorname{Aut}_p(\mathfrak{g}) \to \operatorname{Aut}_p(\mathfrak{g}^{(1)})$. Setting $\Phi_\mu(D) := \mu \circ D \circ \mu^{-1}$ for every $\mu \in \operatorname{Aut}_k(\mathfrak{A}_{2r+1})$ and $D \in W(2r+1)$, we obtain an isomorphism

$$\Phi : \operatorname{Aut}_k(\mathfrak{A}_{2r+1}) \longrightarrow \operatorname{Aut}_p(W(2r+1)) \ ; \ \ \mu \mapsto \Phi_\mu$$

of groups. The automorphisms of $\mathfrak{A}_{2r+1}$ naturally act on differential forms, and we consider the subgroup

$$G_K := \{\mu \in \operatorname{Aut}_k(\mathfrak{A}_{2r+1}) \ ; \ \mu.\omega_K \in \mathfrak{A}_{2r+1}^\times \omega_K\}.$$

According to [22, (7.3.2)], Φ induces an isomorphism $G_K \simeq \operatorname{Aut}_p(\mathfrak{g}^{(1)})$. From the definition $\mathfrak{g} = \{D \in W(2r+1) \ ; \ D.\omega_K \in \mathfrak{A}_{2r+1}\omega_K\}$, we see that for $\mu \in G_K$, the map Φ_μ induces a restricted automorphism of $\mathfrak{g}$. Thus, any restricted automorphism of $\mathfrak{g}^{(1)}$ extends to $\mathfrak{g}$, as we wanted to show.

In the sequel, we write $G := \operatorname{Aut}_p(\mathfrak{g})^\circ$ and $G_K := \operatorname{Aut}_p(\mathfrak{g}^{(1)})$. Assume that there exists a generic torus $\mathfrak{t} \subseteq \mathfrak{g}^{(1)}$. In view of Proposition 1.4, the saturation $G_K.\mathfrak{t}$ is dense in $\bar{S}_{\mathfrak{g}^{(1)}}$. The above observations yield

$$G.\mathfrak{t} = \operatorname{res}(G).\mathfrak{t} = G_K.\mathfrak{t},$$

so that $G.\mathfrak{t}$ is a dense subset of $\bar{S}_{\mathfrak{g}} = \bar{S}_{\mathfrak{g}^{(1)}}$. Applying Proposition 1.4 again, we conclude that $\mathfrak{t}$ is also a generic torus of $\mathfrak{g}$.

Note that the argument of the remark following Proposition 3.3 applies to any generic torus of $\mathfrak{g}^{(1)}$, yielding $\mathfrak{t} \not\subseteq \mathfrak{g}_{(-1)}^{(1)}$. Since $\mathfrak{t} \subseteq \mathfrak{g}^{(1)}$, this means $\mathfrak{t} \not\subseteq \mathfrak{g}_{(-1)}$. Owing to [22, (7.5.14)], we may assume that $1+x_n \in \mathfrak{t}$. Then $\mathfrak{t}$ is also a torus of maximal dimension of the centralizer $\mathfrak{c} := C_{\mathfrak{g}}(1+x_n)$. By [22, (7.5.15)], there is an isomorphism $\varphi : \mathfrak{c} \to \mathcal{P}(2r)$ of restricted Lie algebras such that $\varphi(1+x_n) = 1$, the canonical central element in the Poisson algebra. Applying Theorem 5.1.2, we obtain $S(\mathfrak{c}, \mathfrak{t}) = \operatorname{Cent}_{\operatorname{Aut}_p(\mathfrak{t})}(1+x_n)$. Since $\mathfrak{t} \subseteq \mathfrak{g}$ is generic, Theorem 1.5 in conjunction with the above observation $S(\mathfrak{g}, \mathfrak{t}) = \operatorname{Aut}_p(\mathfrak{t})$ ensures that the map $\operatorname{Nor}_G(\mathfrak{t}) \longrightarrow \operatorname{Aut}_p(\mathfrak{t})$ is surjective. Thus, given $g \in \operatorname{Aut}_p(\mathfrak{t})$, there exists $\varphi \in G$ such that $\varphi|_\mathfrak{t} = g$. Since g fixes $1+x_n$, we have $\varphi|_\mathfrak{c} \in \operatorname{Aut}_p(\mathfrak{c})$. Setting $H := \operatorname{Aut}_p(\mathfrak{c})$, we obtain a surjection $\operatorname{Nor}_H(\mathfrak{t}) \longrightarrow \operatorname{Aut}_p(\mathfrak{t})$, which contradicts Proposition 6.2.2(1). $\qquad\qquad\qquad\qquad\qquad\square$

6.3. **Invariants for Lie algebras of Cartan Type.** Given a restricted Lie algebra $(\mathfrak{g}, [p])$ with connected automorphism group $G = \mathrm{Aut}_p(\mathfrak{g})^\circ$ and maximal torus $\mathfrak{t} \subseteq \mathfrak{g}$, we are interested in comparing the invariants $k[\mathfrak{g}]^G$ and $k[\mathfrak{t}]^{S(\mathfrak{g})}$ of the respective rings of polynomial functions. In case $S(\mathfrak{g}) = \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$, the generators of the latter algebra were explicitly determined by Dickson, cf. [5].

We begin with some general observations concerning invariants of polynomial functions of a finite-dimensional associative k-algebra A. Let $G \subseteq \mathrm{Aut}(A)$ be a connected, closed subgroup of the automorphism group of A. Given a finite-dimensional A-module M, we let $a_M : M \longrightarrow M$ be the left multiplication effected by the element $a \in A$. Let T be an indeterminate. For $a \in A$, we consider the characteristic polynomial

$$P_M(T; a) := \det(T \cdot \mathrm{id}_M - a_M) \in k[T].$$

Then $\deg P_M(T; a) = \dim_k M =: n$ and the functions $\psi_{M,i} : A \longrightarrow k$, given by

$$P_M(T; a) = \sum_{i=0}^{n} \psi_{M,i}(a) T^i$$

belong to the ring $k[A]$ of polynomial functions on A. Note that $\psi_{M,i} = \psi_{N,i}$ whenever $M \cong N$.

The group G acts contragrediently on $k[A]$ via

$$(g.\psi)(a) := \psi(g^{-1}(a)) \qquad \forall\, g \in G,\, \psi \in k[A],\, a \in A.$$

We record the following basic observation:

Lemma 6.3.1. *Let M be a finite-dimensional A-module. Then we have $\psi_{M,i} \in k[A]^G$ for every $i \in \{0, \dots, \dim_k M\}$.*

Proof. Given $g \in G$, we let $M^{(g)}$ be the A-module with underlying k-space M and twisted action defined via

$$a.m := g^{-1}(a).m \quad \forall\, a \in A,\, m \in M.$$

Then we have $a_{M^{(g)}} = g^{-1}(a)_M$, so that

$$\psi_{M^{(g)},i}(a) = \psi_{M,i}(g^{-1}(a))$$

for every $a \in A$ and $i \in \{0, \dots, \dim_k M\}$.

Let S be a simple A-module. Since the connected group G acts trivially on the set of primitive central idempotents of the algebra $A / \mathrm{Rad}(A)$, it follows that

$$S^{(g)} \cong S \quad \forall\, g \in G.$$

Consequently,

$$(g.\psi_{S,i})(a) = \psi_{S,i}(g^{-1}(a)) = \psi_{S^{(g)},i}(a) = \psi_{S,i}(a) \qquad \forall\, a \in A,\, g \in G,$$

whence $\psi_{S,i} \in k[A]^G$ for $i \in \{0, \dots, \dim_k S\}$.

Let $(0) \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow (0)$ be an exact sequence of finite-dimensional A-modules. The identity

$$P_M(T; a) = P_{M'}(T; a) P_{M''}(T; a) \quad \forall\, a \in A$$

implies that the $\psi_{M,i}$ belong to the subalgebra of $k[A]$ generated by the elements $\psi_{M',j}$ and $\psi_{M'',\ell}$. Our result now follows by induction on the length of M. $\qquad\square$

Returning to our standard set-up, we let $(\mathfrak{g}, [p])$ be a restricted Lie algebra with automorphism group $G = \mathrm{Aut}_p(\mathfrak{g})^\circ$. Consider the two-sided ideal $I \trianglelefteq U(\mathfrak{g})$ of the universal enveloping algebra that is generated by the set $\{x^p - x^{[p]} \; ; \; x \in \mathfrak{g}\}$. The finite-dimensional algebra

$$U_0(\mathfrak{g}) := U(\mathfrak{g})/I$$

is the *restricted enveloping algebra* of $\mathfrak{g}$, see [23, (V.5.3)] for more details. By the universal property of $U_0(\mathfrak{g})$, the group G can be considered a connected subgroup of the automorphism group of $U_0(\mathfrak{g})$. Any finite-dimensional $U_0(\mathfrak{g})$-module M thus gives rise to invariant polynomials $\psi_{M,i}$, whose restrictions to $\mathfrak{g}$ are elements of the ring $k[\mathfrak{g}]^G$ of invariants of polynomial functions on $\mathfrak{g}$. We shall henceforth consider the $\psi_{M,i}$ as elements of this ring.

Let $(\mathfrak{t}, [p])$ be a torus of dimension m. Then $\mathrm{Aut}_p(\mathfrak{t}) \cong \mathrm{GL}_m(\mathbb{F}_p)$ acts contragrediently on the ring $k[\mathfrak{t}]$. The following subsidiary result interprets Dickson's work [5] in this context.

Lemma 6.3.2. *Let $(\mathfrak{t}, [p])$ be a torus of dimension m. Then*

$$k[\mathfrak{t}]^{\mathrm{GL}_m(\mathbb{F}_p)} = k[\{\psi_{U_0(\mathfrak{t}), p^i} \; ; \; 0 \le i \le m-1\}]$$

with algebraically independent generators.

Proof. Let $X(\mathfrak{t})$ be the character group of $\mathfrak{t}$. By definition, $X(\mathfrak{t})$ is the group of algebra homomophisms $\lambda : U_0(\mathfrak{t}) \longrightarrow k$. If $\{t_1, \ldots, t_m\}$ is a toral basis of $\mathfrak{t}$, then the map $\lambda \mapsto (\lambda(t_1), \ldots, \lambda(t_m))$ provides an isomorphism $X(\mathfrak{t}) \cong \mathbb{F}_p^m$ of groups. Since $\mathfrak{t}$ is a torus, the free $U_0(\mathfrak{t})$-module of rank 1 decomposes into a direct sum of one-dimensional restricted $\mathfrak{t}$-modules:

$$U_0(\mathfrak{t}) = \bigoplus_{\lambda \in X(\mathfrak{t})} k_\lambda.$$

Consequently, we obtain for $t = \sum_{i=1}^m x_i t_i \in \mathfrak{t}$ the identities

$$P_{U_0(\mathfrak{t})}(T; t) = \prod_{\lambda \in X(\mathfrak{t})} (T - \lambda(t)) = \prod_{(a_1, \ldots, a_m) \in \mathbb{F}_p^m} (T - a_1 x_1 - \cdots - a_m x_m).$$

Our result now follows directly from Dickson's Theorem [5, (8.1.1)]. $\qquad\qquad\square$

Let M be a $U_0(\mathfrak{g})$-module, $\mathfrak{t} \subseteq \mathfrak{g}$ be a torus of maximal dimension. Thanks to Theorem 6.1.1, the restrictions $\psi_{M,i}|_\mathfrak{t}$ belong to the subring $k[\mathfrak{t}]^{S(\mathfrak{g})}$.

Given a commutative k-algebra A, we set $A^{p^r} := \{a^{p^r} \; ; \; a \in A\}$. The Krull dimension of A will be denoted $\dim A$. Also, for a restricted Lie algebra $(\mathfrak{g}, [p])$, we define $d(\mathfrak{g}) := \max\{\dim_k(kx)_p \; ; \; x \in \mathfrak{g}\}$. By [7, (8.6(3))], we have $\mu(\mathfrak{g}) \le d(\mathfrak{g}) \le \mathrm{rk}(\mathfrak{g})$. In particular, if $\mathfrak{g}$ admits a self-centralizing torus, then $\mu(\mathfrak{g}) = d(\mathfrak{g}) = \mathrm{rk}(\mathfrak{g})$.

Lemma 6.3.3. *Let $(\mathfrak{g}, [p])$ be a restricted Lie algebra and $\mathfrak{t} \subseteq \mathfrak{g}$ be a torus of maximal dimension. Set $\ell := d(\mathfrak{g}) - \mu(\mathfrak{g})$. Then the following statements hold:*

(1) *There exists a p-polynomial $Q(T; x) \in k[\mathfrak{g}][T]$ of the form*

$$Q(T; x) = \sum_{i=0}^{\mu(\mathfrak{g})} \varphi_i(x) T^{p^{i+\ell}},$$

with $\varphi_{\mu(\mathfrak{g})} = 1$ and $\varphi_0 \ne 0$, such that for all $x \in \mathfrak{g}$, $\sum_{i=0}^{\mu(\mathfrak{g})} \varphi_i(x) x^{[p]^{i+\ell}} = 0$. Furthermore, all coefficients φ_i belong to $k[\mathfrak{g}]^G$.

(2) *Let M be a $U_0(\mathfrak{g})$-module such that $M|_{U_0(\mathfrak{t})}$ is free of rank p^r. Then $P_M(T; x) = Q(T; x)^{p^{r-\ell}}$.*

(3) *For all $t \in \mathfrak{t}$, we have $Q(T; t) = P_{U_0(\mathfrak{t})}(T; t)^{p^\ell}$.*

(4) *For all $i \in \{0, \ldots, \mu(\mathfrak{g})\}$, the function $x \mapsto \varphi_i(x)^{1/p^\ell}$ restricts to a rational function on $\bar{S}_{\mathfrak{g}}$.*

Proof. We set $\mu := \mu(\mathfrak{g})$ and $d := d(\mathfrak{g})$ to ease notation. Also, for $x \in \mathfrak{g}$ we denote by $x = x_s + x_n$ its Jordan-Chevalley decomposition, where x_s and x_n are p-semi-simple and p-nilpotent respectively, and $x_s, x_n \in (kx)_p$ (see [23, (II.3.5)]).

(1) Let ν be the smallest integer for which there exists a non-empty open subset $\Omega \subseteq \mathfrak{g}$ such that $\Omega^{[p]^\nu} \subseteq S_{\mathfrak{g}}$. By [18, Theorem 2], there exist polynomial functions $\varphi_0, \ldots, \varphi_\mu \in k[\mathfrak{g}]$, with $\varphi_\mu = 1$, such that $\sum_{i=0}^{\mu} \varphi_i(x) x^{[p]^{\nu+i}} = 0$ for all $x \in \mathfrak{g}$. We need to check that $\nu = \ell$. Since $\varphi_\mu(x) = 1$, we have $x^{[p]^{\nu+\mu}} \in \sum_{j=0}^{\nu+\mu-1} kx^{[p]^j}$, so that $\nu+\mu \leq d$ and $\nu \leq d-\mu = \ell$.

For the reverse inequality, we consider the subset $\Omega_0 := \{x \in \Omega \ ; \ \dim_k (kx)_p = d \text{ and } \dim_k (kx_s)_p = \mu\}$ of $\mathfrak{g}$. We first show that it is not empty. It suffices to check that the following two sets are non-empty open subsets of $\mathfrak{g}$:

$$\Omega' := \{x \in \mathfrak{g} \ ; \ \dim_k (kx)_p = d\} \quad \text{and} \quad \Omega'' := \{x \in \mathfrak{g} \ ; \ \dim_k (kx_s)_p = \mu\}.$$

By construction Ω' is not empty; for Ω'' it follows for example from [7, 3.5(1)]. An element $x \in \mathfrak{g}$ belongs to Ω' if and only if the system of vectors $\{x, x^{[p]}, \ldots, x^{[p]^{d-1}}\}$ has maximal rank over k. This condition can be expressed in terms of non-vanishing of certain minors depending regularly on x, so Ω' is open. Regarding Ω'', consider the morphism $q : \mathfrak{g} \to S_{\mathfrak{g}} \ ; x \mapsto x^{[p]^{\dim_k \mathfrak{g}}}$. The set $S_{\mathfrak{g}}^0 := \{x \in S_{\mathfrak{g}} \ ; \ \dim_k (kx)_p = \mu\}$ is an open subset of $S_{\mathfrak{g}}$, so that $\Omega'' = q^{-1}(S_{\mathfrak{g}}^0)$ is open as well.

Given $x = x_s + x_n \in \Omega_0$, we have $x^{[p]^\nu} = x_s^{[p]^\nu}$. Our condition $\dim_k (kx_s)_p = \mu$ implies $x_s^{[p]^\mu} \in \sum_{i=0}^{\mu-1} x_s^{[p]^i}$, so that taking p^ν-th powers yields

$$x^{[p]^{\nu+\mu}} = x_s^{[p]^{\nu+\mu}} \in \sum_{i=0}^{\mu-1} k\, x_s^{[p]^{\nu+i}} = \sum_{i=0}^{\mu-1} k\, x^{[p]^{\nu+i}}.$$

Consequently, $d = \dim_k (kx)_p \leq \nu+\mu$, whence $d-\mu \leq \nu$, as desired.

The G-invariance of the coefficients φ_i will be proved at the end of (2).

(2) First we show that $P_M(T;x)$ is a p-polynomial in T. Note that for any torus $\mathfrak{t}' \subseteq \mathfrak{g}$ of maximal dimension, the module $M|_{U_0(\mathfrak{t}')}$ is also free of rank p^r. Indeed, consider the weight space decompositions $M = \bigoplus_{\lambda \in \Lambda} M_\lambda = \bigoplus_{\lambda' \in \Lambda'} M_{\lambda'}$ relative to $\mathfrak{t}$ and $\mathfrak{t}'$ respectively. By [7, (4.2)], there exists an isomorphism $\varphi : \mathfrak{t}' \to \mathfrak{t}$ such that $\lambda \mapsto \lambda \circ \varphi$ is a bijection $\Lambda \to \Lambda'$ satisfying $\dim_k M_{\lambda \circ \varphi} = \dim_k M_\lambda$ for every $\lambda \in \Lambda$. Because restricted modules over a torus are determined by weights and multiplicities of weight spaces, it readily follows that $M|_{U_0(\mathfrak{t}')}$ is free if and only if $M|_{U_0(\mathfrak{t})}$ is free, of the same rank.

Let $\mathfrak{t} \subseteq \mathfrak{g}$ be a torus of dimension μ. Since $M|_{U_0(\mathfrak{t})} \cong U_0(\mathfrak{t})^{p^r}$, we obtain

$$P_M(T;t) = P_{U_0(\mathfrak{t})}(T;t)^{p^r}$$

for every $t \in \mathfrak{t}$. Let $\mathcal{O} := \{t \in \mathfrak{t} \ ; \ \lambda(t) \neq \lambda'(t) \ \forall \lambda \neq \lambda' \in X(\mathfrak{t})\}$, which is a dense open subset of $\mathfrak{t}$. For $t \in \mathcal{O}$, the polynomial $P_{U_0(\mathfrak{t})}(T;t) \in k[T]$ is square-free, and its set of roots is an additive subgroup of k. Then [11, §20] implies that $P_{U_0(\mathfrak{t})}(T;t)$ is a p-polynomial, whence $\psi_{U_0(t_0),i} = 0$ for $i \notin \{p^j \ ; \ 0 \leq j \leq \mu\}$. Given $t \in \mathfrak{t}$, we obtain

$$\psi_{M,i}(t) = \begin{cases} \psi_{U_0(t_0),p^j}^{p^r}(t) & \text{for } i = p^{r+j}, j \in \{0, \ldots, \mu\} \\ 0 & \text{otherwise.} \end{cases}$$

Suppose that i is not of the form p^{r+j} with $j \in \{0, \ldots, \mu\}$. Then the polynomial function $\psi_{M,i}(x)$ vanishes on $\mathfrak{T} := \bigcup_{t \in \mathfrak{Tor}(\mathfrak{g})} \mathfrak{t}$. By Lemma 1.6, $\mathfrak{T}$ is dense in $\bar{S}_{\mathfrak{g}}$, so that $\psi_{M,i}$ vanishes on $\bar{S}_{\mathfrak{g}}$. Thus

we obtain

$$(6.1) \qquad P_M(T;x) = \sum_{j=0}^{\mu} \psi_{M,p^{r+j}}(x) T^{p^{r+j}} \qquad \forall\, x \in \bar{S}_{\mathfrak{g}}.$$

For arbitrary $x = x_s + x_n \in \mathfrak{g}$, the elements x_s and x_n act as commuting semi-simple and nilpotent endomorphisms on M, so that $P_M(T;x) = P_M(T;x_s)$. Since $x_s \in \bar{S}_{\mathfrak{g}}$, the above formula implies $\psi_{M,i}(x) = 0$ unless $i = p^{r+j}$ for some $j \in \{0,\ldots,\mu\}$, showing that Formula (6.1) holds for all $x \in \mathfrak{g}$.

Next we check that $P_M(T;x) = Q(T,x)^{p^{r-\ell}}$, considered as elements of $k[T]$. It suffices to verify the identity for all x in some dense open subset of $\mathfrak{g}$. Since $P_M(T;x)$ and $Q(T;x)^{p^{r-\ell}}$ are monic p-polynomials in T of the same degree, it is enough to show that they have the same set of roots. For each $x \in \mathfrak{g}$, denote by $\mathrm{Rac}_Q(x)$ and $\mathrm{Rac}_P(x)$ the set of roots of $Q(T;x)$ and $P_M(T;x)$. Since $Q(T;x)$ annihilates x in $\mathfrak{g}$, it also annihilates $x_M \in \mathrm{End}_k(M)$, the action of x in M. Therefore, it must be divisible by the minimal polynomial of x_M. Since the latter has the same roots as $P_M(T;x)$, we obtain $\mathrm{Rac}_P(x) \subseteq \mathrm{Rac}_Q(x)$ for all $x \in \mathfrak{g}$. Conversely, for $x = x_s + x_n$, we have $\mathrm{Rac}_P(x) = \mathrm{Rac}_P(x_s)$. When $x \in \Omega_0$ as above, the torus $(kx_s)_p$ has dimension μ, and $\mathrm{Rac}_P(x_s)$ is an elementary abelian p-group of rank μ. On the other hand, since $Q(T;x)$ has degree p^d and is the p^ℓ-th power of a p-polynomial of degree p^μ, $\mathrm{Rac}_Q(x)$ is an elementary abelian p-group of rank at most $d-\ell = \mu$. This forces $\mathrm{Rac}_P(x) = \mathrm{Rac}_Q(x)$ when $x \in \Omega_0$, as we needed.

We now show that the coefficients of $Q(T;x)$ are G-invariant. Note that there always exists a module M such that $M|_{U_0(\mathfrak{t})}$ is free of rank p^r for some r: for example, take $M = U_0(\mathfrak{g})$ with the left regular action, and $r = \dim_k \mathfrak{g} - \mu$. By Lemma 6.3.1, the coefficients of $P_M(T;x)$ are G-invariant. Since the coefficients of $Q(T;x)$ are their $p^{r-\ell}$-th powers, they are G-invariant as well: this is clear when $r-\ell \geq 0$, and easy to check if $r-\ell < 0$.

(3) readily follows from the proof of (2).

(4) Let β be an alternating μ-linear form on $\mathfrak{g}$, and let $\Omega_\beta := \{x \in \mathfrak{g}\ ;\ \beta(x^{[p]^\ell},\ldots,x^{[p]^{d-1}}) \neq 0\}$. The collection of all Ω_β forms an open covering of the set of all $x \in \mathfrak{g}$ such that $\{x^{[p]^\ell},\ldots,x^{[p]^{d-1}}\}$ is a linearly independent family. Using the relation $x^{[p]^d} = -\sum_{i=0}^{\mu} \varphi_i(x) x^{[p]^{\ell+i}}$, we obtain for all $i \in \{0,\ldots,\mu-1\}$:

$$(6.2) \qquad \varphi_i(x) = -\frac{\beta(x^{[p]^\ell},\ldots,x^{[p]^d},\ldots,x^{[p]^{d-1}})}{\beta(x^{[p]^\ell},\ldots,x^{[p]^{\ell+i}},\ldots,x^{[p]^{d-1}})} \qquad \forall\, x \in \Omega_\beta.$$

Now let $\mathfrak{t} \in \mathfrak{Tor}(\mathfrak{g})$. If $\mathfrak{t} \cap \Omega_\beta \neq \emptyset$, then β does not vanish on $\mathfrak{t}$, and there exists $\lambda \in k^\times$ such that $\beta(t_1^{[p]^\ell},\ldots,t_\mu^{[p]^\ell}) = \lambda\beta(t_1,\ldots,t_\mu)^{p^\ell}$ for all $t_1,\ldots,t_\mu \in \mathfrak{t}$. Indeed, the p^ℓ-th root of the left hand side defines an alternating μ-linear form on $\mathfrak{t}$, and so must be proportional to β. It follows that

$$(6.3) \qquad \varphi_i(x) = -\frac{\beta(x,\ldots,x^{[p]^\mu},\ldots,x^{[p]^{\mu-1}})^{p^\ell}}{\beta(x,\ldots,x^{[p]^i},\ldots,x^{[p]^{\mu-1}})^{p^\ell}} \qquad \forall\, x \in \mathfrak{t} \cap \Omega_\beta.$$

This shows that $x \mapsto \varphi_i(x)^{1/p^\ell}$ is a rational function on the Zariski closure of $\mathfrak{T} \cap \Omega_\beta$. For a suitable choice of β, this is a non-empty open subset of $\mathfrak{T}$, so by Lemma 1.6 its Zariski closure is $\bar{S}_{\mathfrak{g}}$. $\qquad\square$

We record the following corollary:

Corollary 6.3.4. *Let $(\mathfrak{g},[p])$ be a restricted Lie algebra and $\ell = d(\mathfrak{g}) - \mu(\mathfrak{g})$. Then the morphism $\mathfrak{g} \to \mathfrak{g}\ ;\ x \mapsto x^{[p]^\ell}$ induces a dominant morphism $\mathfrak{g} \to \bar{S}_{\mathfrak{g}}$. In particular, $\ell = 0$ if and only if $\mu(\mathfrak{g}) = \mathrm{rk}(\mathfrak{g})$.*

Proof. Since the p-mapping is invertible on $S_{\mathfrak{g}}$, we always have $S_{\mathfrak{g}} \subseteq \mathfrak{g}^{[p]^\ell}$. In the proof of Lemma 6.3.3 (1), we showed that there exists a dense open subset Ω such that $\Omega^{[p]^\ell} \subseteq S_{\mathfrak{g}}$. Taking Zariski closures yields $\mathfrak{g}^{[p]^\ell} \subseteq \bar{S}_{\mathfrak{g}}$, so $\mathfrak{g}^{[p]^\ell}$ is dense in $\bar{S}_{\mathfrak{g}}$. If $\ell = 0$ then $\mathfrak{g} = \bar{S}_{\mathfrak{g}}$, and [7, (3.7)] yields $\mathrm{rk}(\mathfrak{g}) - \mu(\mathfrak{g}) = 0$. The reverse implication is clear. $\square$

Let $f : A \longrightarrow B$ be an injective homomorphism of finitely generated, commutative k-algebras. If there exists $r \in \mathbb{N}_0$ such that $B^{p^r} \subseteq \mathrm{im}\, f$, then f is called an *inseparable isogeny of exponent $\leq r$*. In that case, the comorphism $f^* : \mathrm{Maxspec}(B) \longrightarrow \mathrm{Maxspec}(A)$ is a homeomorphism.

If G is a group acting on A via automorphisms such that A^G is finitely generated, then the variety $\mathrm{Maxpec}(A)/\!/G := \mathrm{Maxspec}(A^G)$ is called the *algebraic quotient* of $\mathrm{Maxspec}(A)$ by G. If, in addition, all orbits are closed, then $\mathrm{Maxpec}(A)/G := \mathrm{Maxspec}(A^G)$ is referred to as the *geometric quotient* of $\mathrm{Maxspec}(A)$ by G, see [14, (II.3.2)] for more details.

Theorem 6.3.5. *Let $(\mathfrak{g}, [p])$ be a restricted Lie algebra with connected automorphism group $G = \mathrm{Aut}_p(\mathfrak{g})^\circ$ and $\mathfrak{t}$ a torus of maximal dimension. Set $\ell := d(\mathfrak{g}) - \mu(\mathfrak{g})$.*

(1) The canonical restriction map $k[\mathfrak{g}] \longrightarrow k[\mathfrak{t}]$ induces an algebra homomorphism $\mathrm{res} : k[\bar{S}_{\mathfrak{g}}]^G \to k[\mathfrak{t}]^{W(\mathfrak{g},\mathfrak{t})}$, whose image contains $(k[\mathfrak{t}]^{\mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)})^{p^\ell}$.

(2) We have $\dim k[\bar{S}_{\mathfrak{g}}]^G \geq \mu(\mathfrak{g})$. Equality holds if and only if res is injective.

Assume further that $\mathfrak{g}$ affords a generic torus $\mathfrak{t}_0$. Then:

(3) The algebra $k[\bar{S}_{\mathfrak{g}}]^G$ is finitely generated and of Krull dimension $\mu(\mathfrak{g})$.

(4) If $W(\mathfrak{g}, \mathfrak{t}_0) = \mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$, then $\mathrm{res} : k[\bar{S}_{\mathfrak{g}}]^G \hookrightarrow k[\mathfrak{t}_0]^{W(\mathfrak{g},\mathfrak{t}_0)}$ is an inseparable isogeny of exponent $\leq \ell$. In particular, the varieties $\bar{S}_{\mathfrak{g}}/\!/G$ and $\mathfrak{t}_0/W(\mathfrak{g}, \mathfrak{t}_0)$ are homeomorphic.

Proof. We will write GL_μ instead of $\mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)$ to ease notation.

(1) Clearly, the restriction map induces a homomorphism $\mathrm{res} : k[\bar{S}_{\mathfrak{g}}]^G \to k[\mathfrak{t}]^{W(\mathfrak{g},\mathfrak{t})}$. Let $Q(T; x)$ be as in Lemma 6.3.3, so that its coefficients φ_i belong to $k[\mathfrak{g}]^G$. By Lemma 6.3.3(3), we have $\mathrm{res}(\varphi_i) = \psi_{U_0(\mathfrak{t}),p^i}^{p^\ell}$ for all $i \in \{0, \ldots, \mu\}$. In view of Lemma 6.3.2, the $\psi_{U_0(\mathfrak{t}),p^i}$ generate $k[\mathfrak{t}]^{\mathrm{GL}_\mu}$, whence $(k[\mathfrak{t}]^{\mathrm{GL}_\mu})^{p^\ell} \subseteq \mathrm{im}\,\mathrm{res}$.

(2) We have $(k[\mathfrak{t}]^{\mathrm{GL}_\mu})^{p^\ell} \subseteq A := \mathrm{im}\,\mathrm{res} \subseteq k[\mathfrak{t}]$. By the Theorem of Hilbert-Noether [1, (1.3.1)], $k[\mathfrak{t}]$ is a finitely generated module over the noetherian ring $k[\mathfrak{t}]^{\mathrm{GL}_\mu}$. So it is also a finitely generated module over $B := (k[\mathfrak{t}]^{\mathrm{GL}_\mu})^{p^\ell}$. Being a B-submodule of $k[\mathfrak{t}]$, the algebra A is noetherian as well. Consequently, A is a finitely generated integral domain.

Owing to Lemma 6.3.2, the algebras $(k[\mathfrak{t}]^{\mathrm{GL}_\mu})^{p^\ell}$ and $k[\mathfrak{t}]$ have common Krull dimension $\mu(\mathfrak{g})$. Using [6, (8.2.1.A)], we obtain $\dim A = \mu(\mathfrak{g})$. It readily follows that $\dim k[\bar{S}_{\mathfrak{g}}]^G \geq \mu(\mathfrak{g})$. Furthermore, since $\bar{S}_{\mathfrak{g}}$ is irreducible (see [17, §2] or [7, (3.7)]), $k[\bar{S}_{\mathfrak{g}}]^G$ is an integral domain. Therefore, $\dim k[\bar{S}_{\mathfrak{g}}]^G = \dim A$ if and only if $\ker \mathrm{res} = (0)$.

(3) Owing to Proposition 1.4, the G-saturation $G.\mathfrak{t}_0$ lies dense in $\bar{S}_{\mathfrak{g}}$. This readily implies that $\mathrm{res} : k[\bar{S}_{\mathfrak{g}}]^G \to k[\mathfrak{t}]^{W(\mathfrak{g},\mathfrak{t}_0)}$ is injective, hence $k[\bar{S}_{\mathfrak{g}}]^G \simeq A$ is a finitely generated algebra of Krull dimension $\mu(\mathfrak{g})$.

(4) readily follows from properties (1) to (3). $\square$

The following result extends Premet's Theorem [19, Thm. 1] concerning $W(n)$, where $\bar{S}_{W(n)} = W(n)$.

Theorem 6.3.6. *Suppose that $p \geq 3$ and let $(\mathfrak{g}, [p])$ be a restricted Lie algebra of Cartan type W, S or H with generic torus $\mathfrak{t} \subseteq \mathfrak{g}$. Then the restriction map induces an isomorphism $k[\bar{S}_\mathfrak{g}]^G \xrightarrow{\sim} k[\mathfrak{t}]^{\mathrm{GL}_{\mu(\mathfrak{g})}(\mathbb{F}_p)}$. In particular, $k[\bar{S}_\mathfrak{g}]^G$ is a polynomial ring in $\mu(\mathfrak{g})$ variables.*

Proof. First we note that for $\mathfrak{g} = W(n), S(n)$ or $H(n)$, there exists a generic torus $\mathfrak{t} \subseteq \mathfrak{g}$ (Proposition 3.3), and the corresponding Weyl group $W(\mathfrak{g}, \mathfrak{t}) \simeq \mathrm{GL}_{\mu(\mathfrak{g})})(\mathbb{F}_p)$ (Theorems 1.5 and 5.2.1).

(1) Let $\mathfrak{g} = W(n)$. For $p = 3$ and $\mathfrak{g} = W(1)$ our assertion follows from the Chevalley Restriction Theorem. Alternatively, consider the generic torus $\mathfrak{t}_0 \subseteq \mathfrak{g}$, so that $W(\mathfrak{g}, \mathfrak{t}) = \mathrm{GL}_n(\mathbb{F}_p)$. By virtue of [23, (IV.2.5)], the algebra $W(n)$ has a self-centralizing maximal torus; in particular $\ell = d(\mathfrak{g}) - \mu(\mathfrak{g}) = 0$. Now Corollary 6.3.4 yields $\bar{S}_\mathfrak{g} = \mathfrak{g}$, and our assertion follows from Theorem 6.3.5(4).

(2) Let $\mathfrak{g} = H(2r)$ and consider the $W(2r)$-module $\mathfrak{A}_{2r}$. Let $\mathfrak{t}_0$ be a generic torus of $W(2r)$ such that $W(2r) = \mathfrak{t}_0 \oplus W(2r)_{(0)}$. Since $\mathfrak{A}_{2r} \cong U_0(W(2r)) \otimes_{U_0(W(2r)_{(0)})} k$ is a free $U_0(\mathfrak{t}_0)$-module of rank 1, Lemma 6.3.3 implies

$$(6.4) \qquad P_{\mathfrak{A}_{2r}}(T; x) = \sum_{i=0}^{2r} \psi_i(x) T^{p^i} \quad \forall\, x \in W(2r),$$

with each ψ_i being a homogeneous polynomial function of degree $p^{2r} - p^i$ on $W(2r)$. Also note that, for any subtorus $\mathfrak{t} \subseteq \mathfrak{t}_0$ of dimension r, $\mathfrak{A}_{2r}$ is a free $U_0(\mathfrak{t})$-module of rank p^r.

Let $G = \mathrm{Aut}_p(\mathfrak{g})^\circ$. Then $P_{\mathfrak{A}_{2r}}(T; x)$ is the characteristic polynomial of $x \in \mathfrak{g}$ acting on $\mathfrak{A}_{2r}$. By Lemma 6.3.1, the functions $\psi_i|_\mathfrak{g}$ are G-invariant. We show that they are p^r-th powers in $k[\mathfrak{g}]^G$. Consider the Poisson algebra $\mathcal{P}(2r)$ with p-unipotent center. For any $f \in \mathcal{P}(2r)$, the linear map $\mathcal{D}_f = \{f, -\}$ is a derivation of the associative algebra $\mathfrak{A}_{2r}$, so that $\mathcal{D}_f \in W(2r)$. According to [21, Lemma 6.3], there exist polynomial functions $\phi_0, \ldots, \phi_r \in k[\mathcal{P}(2r)]$ such that

$$(6.5) \qquad P_{\mathfrak{A}_{2r}}(T; \mathcal{D}_f) = \sum_{i=0}^{r} \phi_i(f)^{p^r} T^{p^{r+i}} \quad \forall\, f \in \mathcal{P}(2r).$$

The map $\mathcal{D} : \mathcal{P}(2r) \longrightarrow W(2r)$; $f \mapsto \mathcal{D}_f$ induces a surjection $\mathcal{P}(2r)^{(1)} \twoheadrightarrow \mathfrak{g}$. Hence there exists a linear map $\delta : \mathfrak{g} \longrightarrow \mathcal{P}(2r)^{(1)}$ such that $\mathcal{D} \circ \delta = \mathrm{id}_\mathfrak{g}$. In view of (6.4) and (6.5), the polynomial maps $\varphi_i := \phi_i \circ \delta \in k[\mathfrak{g}]$ satisfy the identities

$$\varphi_i(h)^{p^r} = \phi_i(\delta(h))^{p^r} = \psi_i(\mathcal{D}_{\delta(h)}) = \psi_i(h) \quad \forall\, h \in \mathfrak{g},\ i \in \{0, \ldots, r\}.$$

Since $\varphi_i^{p^r} = \psi_i$ is G-invariant, we readily obtain that $\varphi_i \in k[\mathfrak{g}]^G$ as well.

Let $\mathfrak{t} \subseteq \mathfrak{g}$ be a generic torus. Theorem 6.3.5 shows that the restriction map induces an embedding $\mathrm{res} : k[\bar{S}_\mathfrak{g}]^G \hookrightarrow k[\mathfrak{t}]^{\mathrm{GL}_r(\mathbb{F}_p)}$. As noted before, $\mathfrak{A}_{2r}$ is a free $U_0(\mathfrak{t})$-module of rank p^r, so

$$P_{\mathfrak{A}_{2r}}(T; t) = P_{U_0(\mathfrak{t}_0)}(T; t)^{p^r} = \Big(\sum_{i=0}^{r} \kappa_i(t) T^{p^i}\Big)^{p^r} \quad \forall\, t \in \mathfrak{t},$$

where the coefficients $\kappa_i \in k[\mathfrak{t}]$ are the Dickson generators of $k[\mathfrak{t}]^{\mathrm{GL}_r(\mathbb{F}_p)}$. In view of the above, we obtain $\varphi_i(t) = \kappa_i(t)$ for all $i \in \{0, \ldots, r-1\}$ and $t \in \mathfrak{t}$, so that $\kappa_i = \mathrm{res}(\varphi_i)$. Therefore, res is surjective.

(3) Now we consider $\mathfrak{g} = S(n)$ and check that $\ell = d(\mathfrak{g}) - \mu(\mathfrak{g}) = 1$. If $\ell = 0$, then Corollary 6.3.4 implies $\mathrm{rk}(\mathfrak{g}) = \mu(\mathfrak{g})$, a contradiction. Since $S(n) \subseteq W(n)$, we have $d(\mathfrak{g}) \leq d(W(n)) = n$, so that $\mu(S(n)) = n-1$ implies $\ell = d(\mathfrak{g}) - \mu(\mathfrak{g}) \leq 1$. By Theorem 6.3.5 we have an embedding $\mathrm{res} : k[\bar{S}_\mathfrak{g}]^G \hookrightarrow k[\mathfrak{t}]^{\mathrm{GL}_{n-1}(\mathbb{F}_p)}$. Consider the p-polynomial $Q(T; x) = \sum_{i=0}^{n-1} \varphi_i(x) T^{p^{i+1}} \in k[\mathfrak{g}][T]$ given by Lemma 6.3.3; we know that the functions $\mathfrak{g} \to k$; $x \mapsto \varphi_i(x)^{1/p}$ restrict to the Dickson generators of $k[\mathfrak{t}]^{\mathrm{GL}_{n-1}(\mathbb{F}_p)}$. We will show that these functions are polynomial on $\mathfrak{g}$, which will prove that res is surjective.

We use the notation of Section 3 for truncated polynomials and their derivations. Recall the decomposition $\mathfrak{g} = \mathfrak{g}_{(0)} \oplus \mathfrak{g}_{-1}$, where $\mathfrak{g}_{(0)}$ is a G-invariant subalgebra of codimension n. For every $x \in \mathfrak{g}$, there is a unique decomposition $(kx)_p = \mathfrak{t}_x \oplus \mathfrak{n}_x$, where $\mathfrak{t}_x$ is a torus and $\mathfrak{n}_x$ a p-unipotent subalgebra. We consider the set $\Omega := \{x \in \mathfrak{g} \ ; \ \dim_k(kx)_p = n, \ \dim_k \mathfrak{t}_x = n-1, \ \mathfrak{t} \cap \mathfrak{g}_{(0)} = (0)\}$. We check that Ω is a non-empty open set: note that $\Omega = \Omega' \cap \Omega''$, where

$$\Omega' := \{x \in \mathfrak{g} \ ; \ \dim_k(kx)_p = n\} \quad \text{and} \quad \Omega'' := \{x \in \mathfrak{g} \ ; \ \dim_k \mathfrak{t}_x = n-1, \ \mathfrak{t}_x \cap \mathfrak{g}_{(0)} = (0)\}.$$

Since $d(\mathfrak{g}) = \ell + \mu(\mathfrak{g}) = n$, the set Ω' is open and non-empty. For Ω'', we have seen in the proof of Lemma 6.3.3(1) that the condition $\dim_k \mathfrak{t}_x = n-1$ defines a non-empty open subset of $\mathfrak{g}$. Given any such element x, the subspace $\mathfrak{t}_x$ is spanned by the linearly independent family $\{x^{[p]^{\ell+1}}, \ldots, x^{[p]^{\ell+n-1}}\}$. The condition that $\mathfrak{t}_x \cap \mathfrak{g}_{(0)} = (0)$ is equivalent to the fact that the residue classes of $\{x^{[p]^\ell}, \ldots, x^{[p]^{\ell+n-1}}\}$ in $\mathfrak{g}/\mathfrak{g}_{(0)}$ form a system of maximal rank, which is an open condition. Hence Ω'' is open. We check that it is not empty. By Theorem 3.2 there exists a torus $\mathfrak{t}_0$ of maximal dimension such that $\mathfrak{t}_0 \cap \mathfrak{g}_{(0)} = (0)$. By [7, 3.5(1)], there exists $t \in \mathfrak{t}_0$ such that $(kt)_p = \mathfrak{t}_0$: then $t \in \Omega''$.

We will prove below that $\mathfrak{n}_x \subseteq \mathfrak{g}_{(0)}$ for all $x \in \Omega$. First, let us show how this property yields the result we want. Set $\mu = n-1$, and let β be a μ-linear alternating form on $\mathfrak{g}$, whose kernel contains $\mathfrak{g}_{(0)}$. Let $x \in \Omega$. For all $a_1, \ldots, a_\mu \in (kx)_p$ with Jordan-Chevalley decompositions $a_i = s_i + n_i$, we have $n_i \in \mathfrak{n}_x \subseteq \mathfrak{g}_{(0)}$. Hence, we obtain $\beta(a_1, \ldots, a_\mu) = \beta(s_1, \ldots, s_\mu)$. Now consider $\Omega_\beta = \{x \in \Omega \ ; \ \beta(x, x^{[p]}, \ldots, x^{[p]^{\mu-1}}) \neq 0\}$. This is again an open subset of $\mathfrak{g}$, and we can choose β so that it is not empty. Using Equation (6.2), we obtain

$$\varphi_i(x) \quad = \quad \varphi_i(x_s) = -\frac{\beta(x_s, \ldots, x_s^{[p]^\mu}, \ldots, x_s^{[p]^{\mu-1}})^p}{\beta(x_s, \ldots, x_s^{[p]^i}, \ldots, x_s^{[p]^{\mu-1}})^p}$$

$$= \quad -\frac{\beta(x, \ldots, x^{[p]^\mu}, \ldots, x^{[p]^{\mu-1}})^p}{\beta(x, \ldots, x^{[p]^i}, \ldots, x^{[p]^{\mu-1}})^p}.$$

for all $x \in \Omega_\beta$. This shows that $\varphi_i^{1/p}$ is a rational function on Ω_β, whence $\varphi_i^{1/p} \in k(\mathfrak{g})$. Since its p-th power is polynomial and $k[\mathfrak{g}]$ is integrally closed, we obtain $\varphi_i^{1/p} \in k[\mathfrak{g}]$.

Let $x \in \Omega$, so that $\mathfrak{t}_x \cap \mathfrak{g}_{(0)} = (0)$. Consequently, $\mathfrak{t}_x$ is conjugate to the generic torus $\mathfrak{t}_0$ by Theorem 3.2, and we may assume that $\mathfrak{t}_x = \mathfrak{t}_0$. For all $i \in \{1, \ldots, n\}$, let $\xi_i := x_i + 1 \in \mathfrak{A}_n$. Thus $\xi_i^p = 1$ and $\xi_1, \ldots, \xi_n$ are invertible generators of $\mathfrak{A}_n$. We use the multi-index notation $\xi^a = \xi_1^{a_1} \cdots \xi_n^{a_n}$ when $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$. The "partial derivative" ∂_i satisfies $\partial_i(\xi_j) = \delta_{i,j}$ for all i, j. Now for $i \in \{1, \ldots, n-1\}$, let $\theta_i := \xi_i \partial_i - \xi_n \partial_n$, so that $\mathfrak{t}_0 = \sum_{i=1}^{n-1} k\theta_i$. We also set $\theta_n := \xi_n \partial_n \in W(n)$. It is straightforward to check that

$$\theta_i(\xi^a) = (a_i - a_n)\xi^a, \quad \forall \, i \in \{1, \ldots, n-1\}.$$

Hence, the subalgebra $\mathfrak{A}_n^{\mathfrak{t}_0} := \{x \in \mathfrak{A}_n \ ; \ t(x) = 0 \ \forall \, t \in \mathfrak{t}_0\}$ of $\mathfrak{t}_0$-constants in $\mathfrak{A}_n$ is given by

$$\mathfrak{A}_n^{\mathfrak{t}_0} = k[\zeta], \quad \text{with} \quad \zeta = \xi_1 \cdots \xi_{n-1} \xi_n^{-1}.$$

Let us compute the centralizer of $\mathfrak{t}_0$ in $W(n)$. It is easy to check that $\{\theta_1, \ldots, \theta_n\}$ is a basis of the free $\mathfrak{A}_n$-module $W(n)$. Write a derivation $D \in W(n)$ as $D = \sum_{i=1}^n f_n \theta_i$, where $f_i \in \mathfrak{A}_n$ for all i. Note that $[\mathfrak{t}_0, \theta_n] = (0)$, so that $0 = [t, D] = \sum_{i=1}^n t(f_i)\theta_i$ for all $t \in \mathfrak{t}_0$. It readily follows that

$$C_{W(n)}(\mathfrak{t}_0) = \bigoplus_{i=1}^n k[\zeta]\theta_i.$$

If, in addition, $D \in (kx)_p \subseteq C_{W(n)}(\mathfrak{t}_0) \cap S(n)$, then

$$0 = \operatorname{div}(D) = \sum_{i=1}^{n} \operatorname{div}(f_i \theta_i) = \sum_{i=1}^{n} f_i \operatorname{div}(\theta_i) + \theta_i(f_i) = f_n + \theta_n(f_n).$$

Now $f_n = f_n(\zeta)$ is a polynomial expression in ζ. Denote formally $f_n'(\zeta) = df_n/d\zeta$. Then $\theta_n(f_n) = f_n'(\zeta)\theta_n(\zeta) = -\zeta f_n'(\zeta)$. Consequently, we must have $f_n(\zeta) = \zeta f_n'(\zeta)$, whence $f_n \in k\zeta$. Thus, there exists $\lambda \in k$ such that

$$D = \sum_{i=1}^{n-1} f_i \theta_i + \lambda \zeta \theta_n.$$

Thanks to the proof of [2, (2.2.3)], we get that the ring of constants $\mathfrak{A}_n^x \neq k$. Since $\mathfrak{A}_n^x = \mathfrak{A}_n^{(kx)_p} \subseteq \mathfrak{A}_n^{\mathfrak{t}_0} = k[\zeta]$, there exists a non-constant polynomial $g \in k[\zeta]$ such that $D(g) = 0$. Hence,

$$0 = \sum_{i=0}^{n-1} f_i \theta_i(g) + \lambda \zeta \theta_n(g) = \lambda \zeta \theta_n(g) = -\lambda \zeta^2 g'(\zeta).$$

Since ζ is invertible and $g \notin k$, this forces $\lambda = 0$. We have thus shown that

(6.6) $$(kx)_p \subseteq \sum_{i=1}^{n-1} k[\zeta]\theta_i.$$

The projection $\mathfrak{g} \twoheadrightarrow \mathfrak{g}/\mathfrak{g}_{(0)}$ induces a linear map $(kx)_p \to \mathfrak{g}/\mathfrak{g}_{(0)}$. Using the inclusion (6.6) we see that its image is spanned by the images of $\theta_1, \ldots, \theta_{n-1}$, and hence has dimension $n-1$. Therefore the kernel $(kx)_p \cap \mathfrak{g}_{(0)}$ has dimension 1. On the other hand, $(kx)_p \cap \mathfrak{g}_{(0)}$ is a p-subalgebra of $(kx)_p = \mathfrak{t}_0 \oplus \mathfrak{n}_x$ which doesn't intersect $\mathfrak{t}_0$: so it must be $\mathfrak{n}_x$, and $\mathfrak{n}_x \subseteq \mathfrak{g}_{(0)}$, as we wanted to show. $\qquad\square$

REFERENCES

[1] D. Benson, *Polynomial Invariants of Finite Groups.* London Math. Soc. Lecture Notes **190**. Cambridge University Press, 1993.

[2] J.-M. Bois, *Generators of simple Lie algebras II.* To appear in Forum Math.

[3] S. Demuškin, *Cartan subalgebras of the simple Lie-p-algebras W_n and S_n.* Siberian Math. J. **11** (1970), 233–245.

[4] ———, *Cartan subalgebras of simple non-classical Lie algebras.* Math. USSR Izv. **6** (1972), 905–924.

[5] L. 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), 75–98.

[6] D. Eisenbud, *Commutative Algebra.* Graduate Texts in Mathematics **150**. Springer-Verlag, New York, 1996.

[7] R. Farnsteiner, *Varieties of tori and Cartan subalgebras of restricted Lie algebras.* Trans. Amer. Math. Soc. **356** (2004), 4181–4236.

[8] R. Farnsteiner and D. Voigt, *Schemes of tori and the structure of tame restricted Lie algebras.* J. London Math. Soc. **63** (2001), 553–570.

[9] ———, *On infinitesimal groups of tame representation type.* Math. Z. **244** (2003), 479–513.

[10] J. Humphreys, *Algebraic Groups and Modular Lie Algebras.* Mem. Amer. Math. Soc. **71**, (1967).

[11] ———, *Linear Algebraic Groups.* Graduate Texts in Mathematics **21**. Springer-Verlag, New York, 1975.

[12] N. Jacobson, *Basic Algebra I.* W. H. Freeman and Company, New York, 1985.

[13] A. Kostrikin and I. Šafarevič, *Graded Lie algebras of finite characteristic.* Math. USSR Izv. **3** (1969), 237–304.

[14] H. Kraft, *Geometrische Methoden in der Invariantentheorie.* Vieweg-Verlag, 1985.

[15] H. Matsumura, *Commutative Ring Theory.* Cambridge Strudies in Advanced Mathematics **8**. Cambridge University Press, 1997.

[16] D. Mumford, *The Red Book of Varieties and Schemes.* Lecture Notes in Mathematics **1358**. Springer-Verlag, Berlin-Heidelberg, 1999.

[17] A. Premet, *On Cartan subalgebras of Lie-p-algebras.* Math. USSR Izv. **29** (1987), 145–157.

[18] _____, *Regular Cartan subalgebras and nilpotent elements in restricted Lie algebras.* Math. USSR Sbornik **66** (1990), 555–570.

[19] _____, *The theorem on restrictions of invariants and nilpotent elements in W_n.* Math. USSR Sbornik **73** (1992), 135–159.

[20] S. Skryabin, *Tori in the Melikian algebra.* J. Algebra **243** (2001), 69–95.

[21] S. Skryabin, *Invariant polynomial functions on the Poisson algebra in characteristic p.* J. Algebra **256** (2002), 146–179.

[22] H. Strade, *Simple Lie Algebras over Fields of Positive Characteristic, I. Structure Theory.* Walter de Gruyter, Berlin, 2004.

[23] H. Strade and R. Farnsteiner, *Modular Lie Algebras and their Representations.* Pure and Applied Mathematics **116**. Marcel Dekker, Inc. New York, 1988.

[24] R. Wilson, *Automorphisms of graded Lie algebras of Cartan type.* Comm. Algebra **3** (1975), 591–613.

[25] _____, *A structural characterization of the simple Lie algebras of generalized Cartan type over fields of prime characteristic.* J. Algebra **40** (1976), 418–465.

(Jean-Marie Bois) MATHEMATISCHES SEMINAR, CHRISTIAN-ALBRECHTS-UNIVERSITÄT ZU KIEL, LUDEWIG-MEYN-STR. 4, 24098 KIEL, GERMANY
  E-mail address: `bois@math.uni-kiel.de`

(Rolf Farnsteiner) MATHEMATISCHES SEMINAR, CHRISTIAN-ALBRECHTS-UNIVERSITÄT ZU KIEL, LUDEWIG-MEYN-STR. 4, 24098 KIEL, GERMANY
  E-mail address: `rolf@math.uni-kiel.de`

(Bin Shu) DEPARTMENT OF MATHEMATICS, EAST CHINA NORMAL UNIVERSITY, SHANGHAI 200062, CHINA
  E-mail address: `bshu@math.ecnu.edu.cn`