Transformation Groups, Vol. 14, No. 2, 2009, pp. 417–461

VINBERG'S θ-GROUPS IN POSITIVE CHARACTERISTIC AND KOSTANT–WEIERSTRASS SLICES

PAUL LEVY

EPFL SB IGAT
Bâtiment BCH
CH-1015, Lausanne, Switzerland
paul.levy@epfl.ch

Abstract. We generalize the basic results of Vinberg's θ-groups, or periodically graded reductive Lie algebras, to fields of good positive characteristic. To this end we clarify the relationship between the little Weyl group and the (standard) Weyl group. We deduce that the ring of invariants associated to the grading is a polynomial ring. This approach allows us to prove the existence of a KW-section for a classical graded Lie algebra (in zero or odd positive characteristic), confirming a conjecture of Popov in this case.

Introduction

Classical results of invariant theory relate the geometry of the adjoint representation of a reductive group to familiar properties of elements of the Lie algebra. In particular, Cartan subalgebras, Weyl groups and semisimple and nilpotent elements appear naturally in the description of invariants, closed orbits and fibres of the quotient map. On the other hand, there are many circumstances in which the concepts of Cartan subalgebra, Weyl group and nilpotent cone have analogues with similar properties. In [Vi], Vinberg studied such generalizations for representations arising from periodic gradings of complex reductive Lie algebras. Specifically, let G be a complex reductive group, let $\mathfrak{g} = \mathrm{Lie}(G)$, let θ be an automorphism of G of order m and let $\zeta = e^{2\pi i/m}$. There is a grading of $\mathfrak{g}$ induced by $d\theta$:

$$\mathfrak{g} = \bigoplus_{i\in\mathbb{Z}/m\mathbb{Z}} \mathfrak{g}(i), \qquad \text{where} \qquad \mathfrak{g}(i) = \{x \in \mathfrak{g} \mid d\theta(x) = \zeta^i x\}.$$

Clearly $[\mathfrak{g}(i), \mathfrak{g}(j)] \subset \mathfrak{g}(i + j)$ for any $i, j \in \mathbb{Z}/m\mathbb{Z}$. Let $G(0) = (G^\theta)^\circ$. Then $\mathrm{Lie}(G(0)) = \mathfrak{g}(0)$ and $G(0)$ normalizes $\mathfrak{g}(1)$. A *Cartan subspace* of $\mathfrak{g}(1)$ is a maximal commutative subspace consisting of semisimple elements. The principal results of [Vi] are:

— any two Cartan subspaces of $\mathfrak{g}(1)$ are $G(0)$-conjugate and any semisimple element is contained in a Cartan subspace;

— the $G(0)$-orbit through $x \in \mathfrak{g}(1)$ is closed if and only if x is semisimple;

DOI: 10.1007/s00031-009-9056-y
Received April 15, 2008. Accepted March 4, 2009. Published online April 29, 2009

— the embedding $\mathfrak{c} \hookrightarrow \mathfrak{g}(1)$ induces an isomorphism $k[\mathfrak{g}(1)]^{G(0)} \to k[\mathfrak{c}]^{W_\mathfrak{c}}$, where $\mathfrak{c}$ is any Cartan subspace of $\mathfrak{g}(1)$ and $W_\mathfrak{c} = N_{G(0)}(\mathfrak{c})/Z_{G(0)}(\mathfrak{c})$; and
— the little Weyl group $W_\mathfrak{c}$ is generated by pseudoreflections and hence $k[\mathfrak{c}]^{W_\mathfrak{c}}$ is a polynomial ring.

In the case of an involution, the grading $\mathfrak{g} = \mathfrak{g}(0) \oplus \mathfrak{g}(1)$ is known as the symmetric space decomposition and has been studied extensively, especially since the seminal work of Kostant and Rallis [KR]. In this case the little Weyl group is itself a Weyl group (for a root system which can be related in a natural way to the root system of G). Hence, while the geometric properties of symmetric spaces are quite close to those of the adjoint representation, the $m > 2$ case is more interesting from the point of view of reflection groups. Most of the results of Kostant–Rallis are now known to hold in good positive characteristic by work of the author [L2]. However, with the exception of [Ka] (and perhaps [Pa1]), there has been little work on (general) θ-groups in positive characteristic. The first main task of this paper will be to extend Vinberg's above mentioned results to the case where G is a reductive group over a field of good positive characteristic p, $p \nmid m$. The major obstacles concern separability of the quotient morphism $\mathfrak{g}(1) \to \mathfrak{g}(1)/\!\!/G(0) := \mathrm{Spec}(k[\mathfrak{g}(1)]^{G(0)})$ and the failure of the Shephard–Todd theorem in positive characteristic. The former problem can be resolved by a careful analysis of the centralizer of a Cartan subspace. To show that the little Weyl group is generated by pseudoreflections and that its ring of invariants is polynomial, we prove directly that Vinberg's description [Vi, Section 7] of $W_\mathfrak{c}$ for G of classical type holds in good positive characteristic, and apply a result of Panyushev and an inspection of orders of centralizers in Weyl groups for the exceptional types. While our approach requires somewhat more work than that of [Vi], it makes the relationship between the little Weyl group and the Weyl group of G clear (for G classical). This allows us to prove for classical graded Lie algebras a long-standing conjecture in this field, the existence of a slice in $\mathfrak{g}(1)$ analogous to Kostant's slice to the regular orbits in $\mathfrak{g}$.

We provide the following criterion for a Cartan subspace to be contained in the centre of $\mathfrak{g}$. An automorphism θ is of zero rank if any element of $\mathfrak{g}(1)$ is nilpotent.

Lemma 0.1. *Suppose $p > 2$. Then the following are equivalent:*

(i) $\mathfrak{g}(1)$ *contains no noncentral semsimple elements;*
(ii) $\theta|_{G'}$ *is either of order less than m or is of zero rank;*
(iii) $\mathfrak{g}(1) = \mathfrak{s} \oplus \mathfrak{n}$, *where $\mathfrak{s}$ (resp. $\mathfrak{n}$) is the set of semisimple (resp. nilpotent) elements of $\mathfrak{g}(1)$ and $\mathfrak{s} \subseteq \mathfrak{z}(\mathfrak{g})$.*

We remark that the above result fails if $p = 2$. We prove the following Lemma by some simple geometric arguments.

Lemma 0.2. *Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}(1)$.*

(i) *The morphism $G(0) \times \mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}) \to \mathfrak{g}(1)$ is dominant and separable.*
(ii) *Any two Cartan subspaces of $\mathfrak{g}(1)$ are conjugate by an element of $G(0)$.*

If θ is an involution and $T \subset G$ is a θ-stable torus, then it is not difficult to see that $T = T_+ \cdot T_-$, where $T_+ = (T^\theta)^\circ$ and $T_- = \{t \in T \mid \theta(t) = t^{-1}\}^\circ$. Moreover, the Lie algebras of T_+ and T_- are, respectively, the $(+1)$ and (-1) eigenspaces for the differential of θ on $\mathrm{Lie}(T)$ [Ri, p. 290]. An important tool in our analysis will be a generalization of this decomposition to arbitrary m. Roughly speaking, one decomposes T as a product of subtori T_d, $d \mid m$, such that 'the minimal polynomial of $e^{2\pi di/m}$ applied to θ' acts trivially on T_d.

Lemma 0.3. *Let T be a θ-stable torus and let $\mathfrak{t} = \mathrm{Lie}(T)$. We have $T = \prod_{d|m} T_d$ (see Lemma 1.10 for definitions) and $\mathfrak{t} = \bigoplus_{d|m} \mathrm{Lie}(T_d)$. Moreover, $\mathrm{Lie}(T_d) = \bigoplus_{(i,m)=d} \mathfrak{t} \cap \mathfrak{g}(i)$. In particular, $T_m = (T^\theta)^\circ$.*

We turn next to consideration of the quotient morphism $\pi : \mathfrak{g}(1) \to \mathfrak{g}(1)/\!\!/G(0)$. Recall that each fibre of π contains a unique closed orbit (which is also the unique orbit of minimal dimension) and for $x \in \mathfrak{g}(1)$, $\pi(x) = \pi(0)$ if and only if 0 is contained in the closure of $G(0)\cdot x$. Arguing in a similar manner to [Vi] we obtain:

Lemma 0.4. *If $x \in \mathfrak{g}(1)$ then $G(0)\cdot x$ is closed if and only if x is semisimple. On the other hand, 0 is contained in the closure of $G(0)\cdot x$ if and only if x is nilpotent.*

In general, the quotient morphism for the action of a reductive group on an affine variety need not be separable. Here we face a certain difficulty because a separability criterion established by Richardson [Ri, 9.3] (that the action is stable) does not in general hold. However, Lemmas 0.1 and 0.2 allow us (after a little work) to adapt Richardson's arguments to the present circumstances.

Lemma 0.5. *Assume $p > 2$. Then $k(\mathfrak{g}(1))^{G(0)}$ is the fraction field of $k[\mathfrak{g}(1)]^{G(0)}$ and hence $\pi : \mathfrak{g}(1) \to \mathfrak{g}(1)/\!\!/G(0)$ is a separable morphism.*

We can then employ some fairly standard invariant theoretic arguments to generalize Vinberg's version [Vi, Theorem 7] of the Chevalley Restriction Theorem. Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}(1)$. We denote by $W_\mathfrak{c}$ the little Weyl group $N_{G(0)}(\mathfrak{c})/Z_{G(0)}(\mathfrak{c})$.

Theorem 0.6. *Suppose $p > 2$. Then the embedding $\mathfrak{c} \hookrightarrow \mathfrak{g}(1)$ induces an isomorphism $\mathfrak{c}/W_\mathfrak{c} \to \mathfrak{g}(1)/\!\!/G(0)$.*

Next we turn to the consideration of the group $W_\mathfrak{c}$. For G of classical type Vinberg gave a precise description of the little Weyl group. The basic approach of [Vi, Section 7] is to classify inner automorphisms $\mathrm{Int}\, g$ of G by considering the eigenvalues of g, and similarly for outer automorphisms. In essence, this perspective fixes a maximal torus of (G containing a maximal torus of) $G(0)$. Here we follow a different approach more in common with the classification of involutions (see [Sp] or [He]): we fix a (suitable) θ-stable maximal torus T whose Lie algebra $\mathfrak{t}$ contains a Cartan subspace $\mathfrak{c}$ of $\mathfrak{g}(1)$. This choice is in some sense 'opposite' to Vinberg's choice of maximal torus: we seek to maximize $\dim(\mathfrak{t} \cap \mathfrak{g}(1))$, while in Vinberg's setting, $\dim(\mathfrak{t} \cap \mathfrak{g}(0))$ is maximal. (If G is simple and θ is inner, then these two choices of maximal torus can only be equal if θ is of zero rank, that is, $\mathfrak{c}$ is trivial. The maximal tori can also be equal for a small number of classes of (positive rank) outer automorphisms, mostly involutions.) Hence we describe an inner automorphism as $\mathrm{Int}\, n_w$, where $n_w \in N_G(T)$ and $w = n_w T \in W$ is an element of order m (and similarly for outer automorphisms). This allows us to relate $W_{\mathfrak{c}}$ to the centralizer of w in W:

— If G is of classical type then $W_{\mathfrak{c}}$ is of the form $G(m',1,r)$ or $G(m',2,r)$ where $m' \in \{m/2, m, 2m\}$ (cf. [Vi]).
— If G is of exceptional type and $m > 2$ or if G is of type D_4 and $\operatorname{char} k = p > 3$ then the order of $W_{\mathfrak{c}}$ is coprime to p.

This, along with a reduction theorem to the almost simple case (Section 3) and application of a result of Panyushev [Pa1] gives us the following result for any G satisfying the 'standard hypotheses' (see Section 3).

Theorem 0.7. *The group $W_{\mathfrak{c}}$ is generated by pseudoreflections and $\mathfrak{c}/W_{\mathfrak{c}}$ is isomorphic to a vector space of dimension $r = \dim \mathfrak{c}$.*

Recall that a Kostant–Weierstrass slice or KW-section for (G, θ) is an affine-linear subvariety $\mathfrak{v}$ of $\mathfrak{g}(1)$ for which restricting functions from $\mathfrak{g}(1)$ to $\mathfrak{v}$ induces an isomorphism $k[\mathfrak{g}(1)]^{G(0)} \to k[\mathfrak{v}]$. The existence of KW-sections for θ-groups is a long-standing conjecture of Popov in characteristic zero [Po1]. In [Pa2, Cor. 5] Panyushev proved that a KW-section exists if $\mathfrak{g}(0)$ is semisimple. More recently, Panyushev proved in [Pa3, Theorem 3.5] that KW-sections exist for 'N-regular' gradings, that is, those such that $\mathfrak{g}(1)$ contains a regular nilpotent element of $\mathfrak{g}$. Here we prove the existence of a KW-section for a classical graded Lie algebra in zero or good positive characteristic. Our approach to describing the little Weyl group makes it clear that if G is of classical type then there is an N-regular minimal θ-stable semisimple subgroup L of G whose Lie algebra contains $\mathfrak{c}$ and such that all elements of $W_{\mathfrak{c}}$ have representatives in $L(0)$. The proof of Popov's conjecture for classical graded Lie algebras can therefore be reduced to the subgroups L constructed in this way. The solution in characteristic zero is then immediate due to Panyushev [Pa3]; in positive characteristic we generalize Panyushev's result using similar reasoning.

Theorem 0.8. *Let $\operatorname{char} k = 0$ or $p > 2$ and let G be of classical type, that is, one of $\mathrm{GL}(n,k)$, $\mathrm{SL}(n,k)$, $\mathrm{SO}(n,k)$, $\mathrm{Sp}(2n,k)$. Then the grading of $\mathfrak{g}$ induced by θ admits a KW-section.*

Notation. For G an affine algebraic group, we denote by $\operatorname{Int} g$ the corresponding inner automorphism of G, by $\operatorname{Ad} g$ the differential of $\operatorname{Int} g$, an automorphism of the Lie algebra $\mathfrak{g}$ of G, and by G' the derived subgroup of G. G will usually denote a connected (reductive) group; if H is any affine algebraic group then we write H° for the connected component of H. If θ is a rational automorphism of G then denote by G^θ the isotropy subgroup of G. Write $x = x_s x_u$ (resp. $x = x_s + x_n$) for the Jordan–Chevalley decomposition of $x \in G$ (resp. $x \in \mathfrak{g}$). We denote by $[n/m]$ the integer part of the fraction n/m.

Acknowledgements. I would like to thank Alexander Premet for many helpful remarks and conversations, and Ross Lawther for advice concerning conjugacy classes in exceptional type Weyl groups. I would also like to express appreciation for the helpful comments of Dmitri Panyushev and the referees, particularly for the shortened proof of Lemma 2.17.

1. Preliminaries

Let Φ be an irreducible root system with basis $\Delta = \{\alpha_1, \ldots, \alpha_n\}$. Recall that p is *good* for Φ if for any $\alpha = \sum_{i=1}^n m_i\alpha_i \in \Phi$, $p > |m_i|$ for all i. Specifically, 2 is a bad prime for all irreducible root systems other than type A, 3 is bad for all exceptional type root systems and 5 is bad for type E_8; otherwise p is good. More generally, p is good for a root system Φ if it is good for each irreducible component of Φ, and it is good for a reductive algebraic group if it is good for its root system.

Let G be a reductive algebraic group over the algebraically closed field k of characteristic $p > 0$ and let $\mathfrak{g} = \mathrm{Lie}(G)$. It follows from the equivalent definition of good primes given in [SpSt, I.4.1] and the discussion in [MS, Prop. 16] that, if p is good for G then p is good for any pseudo-Levi subgroup of G. (A pseudo-Levi subgroup of G is a subgroup of the form $Z_G(s)^\circ$, where $s \in G$ is semisimple. For p good, the possible root systems for such subgroups are given by proper subsets of the extended Dynkin diagram of G, see [So, Prop. 2] in characteristic zero, [MS, Prop. 20] in good positive characteristic.)

Recall that the Lie algebra of any affine algebraic group over k is *restricted*. Hence there is a map $[p] : \mathfrak{g} \to \mathfrak{g}$, $x \mapsto x^{[p]}$, such that:

— $\mathrm{ad}\, x^{[p]} = (\mathrm{ad}\, x)^p$ for all $x \in \mathfrak{g}$;

— the map $\xi : \mathfrak{g} \to U(\mathfrak{g})$, $x \mapsto x^p - x^{[p]}$ is semilinear, that is $\xi(\lambda x + y) = \lambda^p \xi(x) + \xi(y)$ for all $x, y \in \mathfrak{g}$, $\lambda \in k$.

We denote by $x \mapsto x^{[p^i]}$ the ith iteration of $[p]$. Recall also that $x \in \mathfrak{g}$ is semisimple if and only if $x \in \sum_{i \geqslant 1} kx^{[p^i]}$, and is nilpotent if and only if $x^{[p^N]} = 0$ for large enough N.

Let $\theta : G \to G$ be an automorphism of order m, $p \nmid m$ and let $d\theta : \mathfrak{g} \to \mathfrak{g}$ be the corresponding restricted Lie algebra automorphism of $\mathfrak{g}$. Fix once and for all a primitive mth root of unity ζ in k. Then there is a direct sum decomposition $\mathfrak{g} = \mathfrak{g}(0) \oplus \mathfrak{g}(1) \oplus \cdots \oplus \mathfrak{g}(m-1)$, where $\mathfrak{g}(i) = \{x \in \mathfrak{g} \mid d\theta(x) = \zeta^i x\}$. In fact, this is a $\mathbb{Z}/m\mathbb{Z}$-grading of $\mathfrak{g}$: if $x \in \mathfrak{g}(i)$, $y \in \mathfrak{g}(j)$ then $[x, y] \in \mathfrak{g}(i + j)$ $(i, j \in \mathbb{Z}/m\mathbb{Z})$. Let $G(0) = (G^\theta)^\circ$. Then $G(0)$ is reductive [St, 8.1] and $\mathrm{Lie}(G(0)) = \mathfrak{g}(0)$ [Bo, 9.1]. Clearly the adjoint action of $G(0)$ stabilizes each of the subspaces $\mathfrak{g}(i)$.

We are interested in the properties of the $G(0)$-representation $\mathfrak{g}(1)$. Note that the action of $G(0)$ on any $\mathfrak{g}(i)$ $(i \neq 0)$ can be reduced to this case. Indeed, if $0 < i < m$ then let $\psi = \theta^{(m,i)}$, let $\overline{G} = (G^\psi)^\circ$ and let $\overline{\mathfrak{g}} = \mathrm{Lie}(\overline{G})$ (cf. [Vi, Section 2.1]). Then $\overline{G}$ is θ-stable, reductive and contains $G(0)$, and $\overline{\mathfrak{g}} = \sum_{0 \leqslant j < m/(m,i)} \overline{\mathfrak{g}}(j)$, where $\overline{\mathfrak{g}}(j) = \mathfrak{g}(ij)$. In particular, $\overline{\mathfrak{g}}(1) = \mathfrak{g}(i)$.

Lemma 1.1. *If p is good for G then it is also good for $G(0)$ and $\overline{G}$.*

Proof. It suffices to show this for $G(0)$ since ψ is also of order coprime to p. Since $G(0)' \subset G'$ we may clearly assume that G is semisimple. The (scheme-theoretic) centre Z of G is preserved by θ, hence θ induces an automorphism of the corresponding adjoint group G/Z. Thus, after replacing G by G/Z, we may assume that G is of adjoint type, and therefore that G is a direct product of (adjoint type) simple groups. We can reduce further to the case that G is of the form $G_1 \times G_2 \times \cdots \times G_l$, with $\theta(G_i) = G_{i+1}$ $(i = 1, \ldots, l-1)$ and $\theta(G_l) = G_1$. But now G^θ is isomorphic to $(G_1)^{\theta^l}$, hence we may assume that G is simple. Now there are the following possibilities: (i) θ is inner; (ii) θ is outer but θ^2 is inner (and G is of type A_n, D_n or E_6); (iii) θ is outer but θ^3 is inner (and G is of type D_4). If θ is inner then $G(0)$ is a pseudo-Levi subgroup of G and p is good for $G(0)$ as remarked above. In case (ii) we can replace G by G^{θ^2}, and by the same argument as above we can assume once again that G is simple (and that θ is outer). Then θ is an involution of G and p can only be bad for $G(0)$ if $p = 3$ and $G(0)$ is of exceptional type, or $p = 5$ and $G(0)$ is of type E_8. But if G is of classical type then so is $G(0)$ by the classification of involutions, which is independent of (odd) characteristic [Sp]: if G is of type A_{2n} then (since θ is outer) $G(0)$ is of type B_n; if G is of type A_{2n-1} then $G(0)$ is of type C_n or D_n; if G is of type D_n, then $G(0)$ is of type $\mathsf{B}_i \times \mathsf{C}_{n-1-i}$ for some $i \in \{0, \ldots, n-1\}$. Thus if $G(0)$ is of exceptional type then so is G, and hence $p > 3$; if G is simple then $G(0)$ cannot be of type E_8. Finally, in case (iii) $p > 3$ and hence p must be good for G (since $G(0)$ is not of type E_8). □

Lemma 1.2.

(a) *Let $x \in \mathfrak{g}$, and let $x = x_s + x_n$ be the Jordan–Chevalley decomposition of x. Then $x \in \mathfrak{g}(i)$ if and only if $x_s, x_n \in \mathfrak{g}(i)$.*
(b) *If $x \in \mathfrak{g}(i)$ then $x^{[p]} \in \mathfrak{g}(ip)$.*

Proof. For any (rational) automorphism θ of G, $d\theta(x^{[p]}) = d\theta(x)^{[p]}$, hence (b) is immediate. Since any restricted Lie algebra automorphism of $\mathfrak{g}$ preserves semisimplicity and nilpotency, $d\theta(x_s)$ (resp. $d\theta(x_n)$) is semisimple (resp. nilpotent) and $[d\theta(x_s), d\theta(x_n)] = 0$. Hence $d\theta(x) = d\theta(x_s) + d\theta(x_n)$ is the Jordan–Chevalley decomposition of $d\theta(x)$. This proves (a). □

The following result of Steinberg [St, 7.5] is essential to any discussion of automorphisms of G. (This was earlier proved for connected H by Winter [W].)

— *For any rational automorphism σ of a linear algebraic group H there exists a σ-stable Borel subgroup of H. If σ is semisimple then there is a σ-stable maximal torus of H contained in a σ-stable Borel subgroup.*

Following Springer for the case $m = 2$, we call a pair (B, T), B a θ-stable Borel subgroup of G and T a θ-stable maximal torus of B a *fundamental pair*. Let $\Phi = \Phi(G, T)$ be the roots of G relative to T, let Φ^+ be the positive system in Φ associated to B and let Δ be the corresponding basis for Φ. For each $\alpha \in \Phi$, denote by $\alpha^\vee$ the corresponding coroot. Let $X(T) := \mathrm{Hom}(T, k^\times)$ and let $Y(T) := \mathrm{Hom}(k^\times, T)$. Consider the coroots as elements of $Y(T)$ via the perfect pairing $\langle \cdot\, , \cdot \rangle : X(T) \times Y(T) \to \mathbb{Z}$. Let γ be the graph automorphism of Φ induced by θ (i.e., such that $d\theta(\mathfrak{g}_\alpha) = \mathfrak{g}_{\gamma(\alpha)}$). Then γ permutes the elements of Δ. Let $\{h_\alpha, e_\beta : \alpha \in \Delta, \beta \in \Phi\}$ be a Chevalley basis for $[\mathfrak{g}, \mathfrak{g}]$.

Remark 1.3. In fact the $h_\alpha = [e_\alpha, e_{-\alpha}] = d\alpha^\vee(1)$ need not be linearly independent (or even nonzero!), but this problem can be solved by removing some of the h_α. We remark that the error of assuming that the h_α are linearly independent and span $\mathrm{Lie}(T \cap G')$ appears in the work of the author on involutions [L2, p. 512]. This error can easily be remedied by applying Lemma 1.6(b) below to pass from $[\mathfrak{g}, \mathfrak{g}]$ to all of $\mathfrak{g}$. The h_α are linearly independent if G' is semisimple and simply-connected or if G' is separably isogenous to a simply-connected group. (In particular, this is the case if we assume the standard hypotheses on G, see the beginning of Section 3.)

For the remainder of this section we fix a fundamental pair (B,T) for θ. There exist constants $c(\alpha)\in k^\times$, $\alpha\in\Phi$, such that:

— $d\theta(e_\alpha)=c(\alpha)e_{\gamma(\alpha)}$, $\alpha\in\Phi$;
— $d\theta(h_\alpha)=h_{\gamma(\alpha)}$, $\alpha\in\Delta$;
— $c(\alpha)c(-\alpha)=1$, $\alpha\in\Phi$;
— $c(\alpha)c(\gamma(\alpha))\cdots c(\gamma^{m-1}(\alpha))=1$.

The second statement follows immediately from the fact that $h_\alpha=d\alpha^\vee(1)$. But $h_\alpha=[e_\alpha,e_{-\alpha}]$, hence the third statement also follows.

Following Kawanaka [Ka] let $l(\alpha)$ denote the cardinality of the set $(\alpha)=\{\alpha,\gamma(\alpha),\ldots,\gamma^{m-1}(\alpha)\}$ and let $C(\alpha)=c(\alpha)c(\gamma(\alpha))\ldots c(\gamma^{l(\alpha)-1}(\alpha))$. Then clearly $C(\alpha)^{m/l(\alpha)}=1$. Let $n(\alpha)$ denote the order of $C(\alpha)$ (as a root of unity) and let $\mathfrak{g}_{(\alpha)}=\sum_{\beta\in(\alpha)}\mathfrak{g}_\alpha$. It is easy to verify that:

— $\dim\mathfrak{g}_{(\alpha)}\cap\mathfrak{g}(1)=\begin{cases}1 & \text{if } n(\alpha)=m/l(\alpha),\\ 0 & \text{otherwise.}\end{cases}$

The following lemma first appeared in [Ka, 2.2.5], with the slight error that case (ii) for $l(\alpha)>2$ was omitted. The results of [Ka] remain valid simply by modifying the definition [Ka, p. 582] of $w_{(\alpha)}$: in case (ii) we set

$$w_{(\alpha)}=\prod_{i=1}^{l(\alpha)/2-1} w_{\gamma^i(\alpha)}w_{\gamma^{i+l(\alpha)/2}(\alpha)}w_{\gamma^i(\alpha)}.$$

This is consistent with [Ka] in the case $l(\alpha)=2$.

Lemma 1.4. *For $\alpha\in\Phi$, one of the following two cases occurs:*

(i) *$l(\alpha)=1$, or $l(\alpha)\geqslant 2$ and any two roots in (α) are orthogonal.*
(ii) *$l(\alpha)$ is even, the elements of (α) generate a subsystem of Φ of type $\mathsf{A}_2^{l(\alpha)/2}$, and $\langle\alpha,\gamma^{l(\alpha)/2}(\alpha)\rangle=-1$.*

Proof. This follows from the classification of root systems and the fact that γ induces an automorphism of the subsystem of Φ spanned by the roots in (α). □

We deduce that:

Lemma 1.5. *Let S be a maximal torus of $G(0)$. Then S is regular in G.*

Proof. With the above description of θ, $\alpha^\vee(t)\gamma(\alpha)^\vee(t)\cdots\gamma^{l(\alpha)-1}(\alpha)^\vee(t)\in G(0)$ for all $\alpha\in\Phi^+$, $t\in k^\times$. But then we may assume that S contains the torus generated by all $(\alpha^\vee+\gamma(\alpha)^\vee+\cdots+\gamma^{l(\alpha)-1}(\alpha)^\vee)(k^\times)$, $\alpha\in\Phi$. Since $\langle\alpha^\vee+\gamma(\alpha)^\vee+\cdots+\gamma^{l(\alpha)-1}(\alpha)^\vee,\alpha\rangle\neq 0$ by Lemma 1.4, $\mathfrak{g}^S=\mathrm{Lie}(T)$ and hence S is regular in G. □

We make the following slight modification to [L2, Lemma 1.1]. The only difference is the final statement of (a) (which is immediate since μ_m is a group of order coprime to p) and the inclusion of (b), which is proved in exactly the same way as (a). Recall that a *toral element* of $\mathfrak{g}$ is an element x such that $x^{[p]}=x$; a toral *algebra* is a commutative subalgebra $\mathfrak{s}$ which has a basis consisting of toral elements. If $\mathfrak{s}$ is a toral algebra then denote by $\mathfrak{s}^{\mathrm{tor}}$ the set of toral elements of $\mathfrak{s}$. In this case $\mathfrak{s}\cong\mathfrak{s}^{\mathrm{tor}}\otimes_{\mathbb{F}_p}k$.

Lemma 1.6.

(a) *Let θ be an automorphism of G of order m, $p \nmid m$, let T be a θ-stable maximal torus of G and let $\mathfrak{t} = \mathrm{Lie}(T)$, $\mathfrak{t}' = \mathrm{Lie}(T \cap G')$. There exists a θ-stable toral algebra $\mathfrak{s}$ such that $\mathfrak{t} = \mathfrak{t}' \oplus \mathfrak{s}$, and hence $\mathfrak{g} = \mathfrak{g}' \oplus \mathfrak{s}$ (vector space direct sum).*
If $m \,|\, (p-1)$, then we can choose a toral basis for $\mathfrak{s}$ consisting of eigenvectors for $d\theta$. More generally, $\mathfrak{s}^{\mathrm{tor}}$ decomposes as a sum of irreducible $\mathbb{F}_p[\mu_m]$-modules (where μ_m here denotes the cyclic group of order m).

(b) *The above statements all hold if one replaces $\mathfrak{t}'$ by $\mathfrak{t}'' = \mathfrak{t} \cap [\mathfrak{g}, \mathfrak{g}]$.*

Remark 1.7. It is perhaps instructive to give an explicit description of the irreducible $\mathbb{F}_p[\mu_m]$-modules: let σ be a generator for μ_m. Then V is irreducible if and only if it has a basis $v_1, v_2, \ldots, v_r$ $(r \,|\, m)$ such that $\sigma(v_i) = v_{i+1}$ $(1 \leqslant i < r)$ and $\sigma(v_r) = l v_1$ for some $l \in \mathbb{F}_p^\times$ of order m/r.

We will also need the following result of Steinberg.

Lemma 1.8. *Suppose G is semisimple and $\pi : \widehat{G} \to G$ is the universal covering of G. There exists a unique automorphism $\widehat{\theta}$ of $\widehat{G}$ such that the following diagram commutes:*

$$\begin{array}{ccc} \widehat{G} & \xrightarrow{\widehat{\theta}} & \widehat{G} \\ {\scriptstyle \pi}\big\downarrow & & \big\downarrow{\scriptstyle \pi} \\ G & \xrightarrow{\theta} & G \end{array} \quad .$$

Moreover, $\widehat{\theta}$ is of order m.

Proof. Existence and uniqueness are proved in [St, 9.16]. It follows immediately that $\widehat{\theta}$ has the same order as θ. $\square$

Lemma 1.9. *Suppose the order of $\theta|_{G'}$ is strictly less than m. Then $\mathfrak{g}(1) \subset \mathfrak{z}(\mathfrak{g})$.*

Proof. Recall that any nilpotent element of $\mathfrak{g}$ is contained in $\mathfrak{g}' = \mathrm{Lie}(G')$. (This follows from, e.g., [Bo, 14.26 and 11.3(2)].) But therefore if $\theta|_{G'}$ is of order $m' < m$ then there are no nilpotent elements in $\mathfrak{g}(1)$. In fact, let $\mathfrak{n}$ (resp. $\mathfrak{n}^-$) be the Lie algebra of the unipotent radical of B (resp. its opposite Borel subgroup); then $\mathfrak{g} = \mathfrak{n}^- \oplus \mathfrak{t} \oplus \mathfrak{n}$. Moreover $\mathfrak{n}, \mathfrak{n}^- \subset \mathfrak{g}' \subset \sum_{i \in \mathbb{Z}} \mathfrak{g}(im/m')$, hence $\mathfrak{g}(1) \subset \mathfrak{t}$. Suppose $h \in \mathfrak{g}(1)$. Let $\alpha \in \Phi$: then $e_\alpha \in \sum_{i \in \mathbb{Z}} \mathfrak{g}(im/m')$. But hence $[h, e_\alpha] = d\alpha(h) e_\alpha \in \sum_{i \in \mathbb{Z}} \mathfrak{g}(im/m') \cap \sum_{i \in \mathbb{Z}} \mathfrak{g}(im/m' + 1)$. Thus $d\alpha(h) = 0$. Since this is true for all $\alpha \in \Phi$, $h \in \mathfrak{z}(\mathfrak{g})$. $\square$

If $m = 2$ and T is a θ-stable torus in G, then it is not difficult to see that there is a decomposition $T = T_+ \cdot T_-$, where $T_+ = \{t \in T \mid \theta(t) = t\}^\circ$, $T_- = \{t \in T \mid \theta(t) = t^{-1}\}^\circ$, and that the intersection is finite. In fact, one also has a direct sum decomposition $\mathrm{Lie}(T) = \mathrm{Lie}(T_+) \oplus \mathrm{Lie}(T_-)$, hence the product map $T_+ \times T_- \to T$ is a separable isogeny (see [Ri, p. 290]). Here we formulate a generalization of this result to arbitrary m. For $d \geqslant 1$, denote by $p_d(x)$ the minimal polynomial over $\mathbb{Q}$ of a primitive dth root of unity. Since $p_d(x)$ has integer coefficients for each d, we can (and will) also consider $p_d(x)$ as a polynomial in $\mathbb{F}_p[x]$ or $k[x]$. If $p \nmid d$, then $p_d(x)$ has no repeated roots in k. If T is a θ-stable torus and $q(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ then we write $\overline{q}(\theta)$ for the rational endomorphism of T defined by $t \mapsto \prod_{i=0}^n \theta^i(t)^{a_i}$. The correspondence $q \mapsto \overline{q}(\theta)$ defines a homomorphism of rings $\mathbb{Z}[x] \to \mathrm{End}(T)$, $x \mapsto \theta$. (Here the addition in $\mathrm{End}(T)$ is the pointwise product, and the multiplication is a composition of endomorphisms.)

Lemma 1.10. *Let T be a θ-stable torus in G and let $\mathfrak{t} = \mathrm{Lie}(T)$. For each positive $d\,|\,m$ let $T_d = \{t \in T \mid \overline{p_{m/d}}(\theta)(t) = e\}$. (We count 1 as a divisor of m). Then T_d is a subtorus of T, the intersection $T_{d_1} \cap T_{d_2}$ is finite for any distinct $d_1, d_2 | m$, and $T = \prod_{d|m} T_d$ (almost direct product).*

Moreover, $\mathfrak{t} = \sum_{i=1}^m \mathfrak{t}(i)$ (where $\mathfrak{t}(i) = \mathfrak{t} \cap \mathfrak{g}(i)$) and $\sum_{(i,m)=d} \mathfrak{t}(i) = \mathrm{Lie}(T_d)$. In particular, T_1 is the minimal subtorus of T whose Lie algebra contains $\mathfrak{t}(1)$, and $\mathrm{Lie}(T_m) = \mathfrak{t}(0)$.

Proof. Clearly $\mathrm{Lie}(T_d) \subseteq \{t \in \mathfrak{t} \mid p_{m/d}(d\theta)(t) = 0\}$ and hence $\mathrm{Lie}(T_{d_1} \cap T_{d_2}) \subseteq \mathrm{Lie}(T_{d_1}) \cap \mathrm{Lie}(T_{d_2}) = \{0\}$ for $d_1 \neq d_2$ since there exist $f, g \in k[t]$ such that $fp_{m/d_1} + gp_{m/d_2} = 1$. Thus $\mathrm{Lie}(T) \supset \bigoplus_{d|m} \mathrm{Lie}(T_d)$, $T_{d_1} \cap T_{d_2}$ is finite for $d_1 \neq d_2$ and T contains the almost direct product of the T_d. For $d\,|\,m$, let $p'_{m/d}(x) = (x^m - 1)/p_{m/d}(x)$. Then $\overline{p_{m/d}}(\theta) \circ \overline{p'_{m/d}}(\theta)$ is trivial on T, hence $\overline{p'_{m/d}}(\theta)(T) \subseteq T_d$. Moreover, $p'_{m/d}(d\theta)$ is bijective on $\mathrm{Lie}(T_d)$. By dimensional considerations, $T_d = \overline{p'_d}(\theta)(T)$, $T = \prod_{d|m} T_d$ and $\mathfrak{t} = \bigoplus_{d|m} \mathrm{Lie}(T_d)$. $\square$

We remark that Lemma 1.10 holds for an arbitrary torus acted on by an automorphism of order m. Recall that if θ is an involution then a (θ-stable) torus is called θ-split or θ-anisotropic if $\theta(t) = t^{-1}$ for all $t \in T$. For $m > 2$ we wish to distinguish two different cases.

Definition 1.11. We say that a θ-stable torus S is *θ-split* if $S = S_1$, and is *θ-anisotropic* if $S_m = (S^\theta)^\circ$ is trivial. (Hence any θ-split torus is θ-anisotropic.)

We say that θ is *of zero rank* if $\mathfrak{g}(1)$ contains no nonzero semisimple elements.

Lemma 1.12. *If $p > 2$ or if the root system of G has no irreducible components of type A_1 or D_4, then the following are equivalent:*

(i) $\mathfrak{g}(1)$ *contains no noncentral semisimple elements;*
(ii) $\theta|_{G'}$ *is either of order less than m, or is of zero rank;*
(iii) $\mathfrak{g}(1) = \mathfrak{s} \oplus \mathfrak{n}$, *where $\mathfrak{s}$ (resp. $\mathfrak{n}$) is the set of semisimple (resp. nilpotent) elements of $\mathfrak{g}(1)$ and $\mathfrak{s} \subseteq \mathfrak{z}(\mathfrak{g})$.*

Proof. We show first of all that (i) implies (ii). If $\theta|_{G'}$ is of order less than m then all three conditions hold by Lemma 1.9. Hence suppose $\theta|_{G'}$ is of order m. Assume G is semisimple; we will show that if $\mathfrak{g}(1)$ contains no noncentral semisimple elements of $\mathfrak{g}$ then it contains no nonzero semisimple elements. Let $\pi : \widehat{G} \to G$ be the universal covering of G. By Lemma 1.8, there exists a unique lift $\widehat{\theta}$ of θ to $\widehat{G}$. We claim that θ is of zero rank if and only if $\widehat{\theta}$ is of zero rank. Indeed, suppose $\mathfrak{c} \subseteq \mathfrak{g}(1)$ is a commutative subspace consisting of semisimple elements. Let T be a θ-stable maximal torus of $L = Z_G(\mathfrak{c})$. Then $\mathfrak{c} \subseteq \mathfrak{z}(\mathfrak{l}) \subseteq \mathfrak{t} = \mathrm{Lie}(T)$. (See [L1, Lemma 2.2] for the second inclusion.) Let $T = \prod_{i|m} T_i$ be the decomposition of T into subtori given by Lemma 1.10. Then $\mathfrak{c} \subseteq \mathfrak{t}(1)$ and hence T_1 is nontrivial. Let $\widehat{T}$ be the unique maximal torus of $\widehat{G}$ such that $\pi(\widehat{T}) = T$. Then $\widehat{T}$ is $\widehat{\theta}$-stable by uniqueness and there is a decomposition $\widehat{T} = \prod_{i|d} \widehat{T}_i$ into subtori $\widehat{T}_i$ analogous to the T_i. Moreover, it is easy to see from Lemma 1.10 that $\pi(\widehat{T}_i) = T_i$. Hence θ is of zero rank if and only if $\widehat{\theta}$ is of zero rank. Furthermore, it is well known that $\ker d\pi \subseteq \mathfrak{z}(\widehat{\mathfrak{g}})$. Since $d\alpha(d\pi(h)) = d\alpha(h)$ for any $h \in \mathrm{Lie}(\widehat{T})$, it follows that if $\mathfrak{g}(1)$ contains no noncentral semisimple elements of $\mathfrak{g}$ then $\widehat{\mathfrak{g}}(1)$ contains no noncentral semisimple elements of $\widehat{\mathfrak{g}}$. To prove that (i) implies (ii), we may therefore assume that G is (semisimple and) simply-connected.

Since G is the direct product of its minimal θ-stable connected normal subgroups, we may assume G is θ-simple, that is, it has no nontrivial proper connected θ-stable normal subgroups. In this case, $G = G_1 \times G_2 \times \cdots \times G_r$, where the G_i are isomorphic almost simple (semisimple) groups, $\theta(G_i) = G_{i+1}$ $(1 \leqslant i < r)$ and $\theta(G_r) = G_1$. (Thus $r \mid m$.) It clearly changes nothing to replace G, θ and m by G_1, θ^r and m/r: hence we may assume G is simple. (We may of course have $r = m$. This reduces to 'the $m = 1$ case', which is just the adjoint action of G on $\mathfrak{g}$.) But now $\mathfrak{z}(\mathfrak{g})$ is trivial unless G is of type A_{ip-1} for some i; or G is of type E_6 and $p = 3$; or G is of type B_n, C_n, D_n or E_7 and $p = 2$. If $m = 1$, then $\mathfrak{g}$ has some noncentral semisimple elements by a straightforward check. If $m = 2$ then ($p \neq 2$ and) there exists some nontrivial θ-split torus $A \subset G$ by [Vu, Prop. 1]. Moreover, if G is of type A_{ip-1} then (p is good and hence) $Z_G(A) = Z_G(\mathrm{Lie}(A))$ by [L2, Lemma 2.4]. If G is of type E_6 then $\dim A \geqslant 2$ by inspection of the tables in [Sp], hence $\mathrm{Lie}(A)$ contains some noncentral element of $\mathfrak{g}$. Thus the assumption that there are no noncentral semisimple elements in $\mathfrak{g}(1)$ implies that $m \geqslant 3$. But by our assumptions on G, $\dim \mathfrak{z}(\mathfrak{g}) = 0$ or 1 and the differential of any automorphism of G acts as either $(+1)$ or (-1) on $\mathfrak{z}(\mathfrak{g})$ by a standard description of the automorphism group via inner automorphisms and graph automorphisms (see, e.g., [Hu, Section 27.4]. Here we use the fact that G is not of type D_4 if $p = 2$.) Therefore $\mathfrak{g}(1)$ contains no nonzero semisimple elements. Thus (i) implies that $\theta|_{G'}$ is of zero rank.

To prove that (ii) implies (iii), we may assume once more that $\theta|_{G'}$ has order m by Lemma 1.9. By Lemma 1.6 there is a $d\theta$-stable toral algebra $\mathfrak{h} \subset \mathfrak{g}$ such that $\mathfrak{g} = \mathfrak{g}' \oplus \mathfrak{h}$ (where $\mathfrak{g}' = \mathrm{Lie}(G')$). Thus clearly $\mathfrak{g}(1) = \mathfrak{g}'(1) \oplus \mathfrak{h}(1)$. But $\mathfrak{g}'(1)$ consists of nilpotent elements, hence it remains only to show that $\mathfrak{h}(1) \subseteq \mathfrak{z}(\mathfrak{g})$. For this, let T be a θ-stable maximal torus of G such that $\mathfrak{h} \subset \mathfrak{t} = \mathrm{Lie}(T)$, let $T' = T \cap G'$ and let $Z = Z(G)^\circ$. Since $T = T' \cdot Z$ and $\theta|_{G'}$ is of zero rank, the kernel of the map $\overline{p'_1}(\theta) : T \to T$ (see Lemma 1.10) contains T'. Hence T_1 is contained in Z. It follows that $\mathfrak{t}(1) = \mathfrak{s} \subseteq \mathrm{Lie}(Z) \subseteq \mathfrak{z}(\mathfrak{g})$. Since (iii) trivially implies (i), the proof of the lemma is complete. □

Remark 1.13. The cases $m = 1$, $G = \mathrm{SL}(2)$; and $m = 3$, $G = \mathrm{Spin}(8)$, θ outer give counter-examples to Lemma 1.12 in characteristic 2. However, from Section 3 onwards we will assume the standard hypotheses hold for G (that p is good for G, that G' is simply-connected and that there exists a nondegenerate G-equivariant symmetric bilinear form $\kappa : \mathfrak{g} \times \mathfrak{g} \to k$). In these circumstances Lemma 1.12 then holds in characteristic 2. This can be seen from the Reduction Theorem 3.1 which allows us to restrict attention to the case $G = \tilde{G}$, hence to the cases

$G = \mathrm{SL}(2m+1, k)$ or $G = \mathrm{GL}(2m, k)$. The proof of Lemma 1.12 only falls down in characteristic 2 due to the possibility that all semisimple elements of $\mathfrak{g}(1)$ are contained in the centre of $\mathfrak{g}$. Hence this problem no longer occurs under the standard hypotheses. On the other hand, we gain very little with this observation, since G' is then isomorphic to a product of groups of the form $\mathrm{SL}(V_i)$ and θ is inner.

Definition 1.14. We say that θ is of *zero semisimple rank* if the conditions of Lemma 1.12 hold.

Finally, we state the following slightly modified version of [L2, Lemma 1.4(v)] for use in Section 3.

Lemma 1.15. *Let* $G = \mathrm{GL}(n, k)$, $\mathfrak{g} = \mathrm{Lie}(G)$, $\mathfrak{g}' = \mathrm{Lie}(G')$, *where* $p \,|\, n$. *Denote by* $\mathrm{Aut}\, G$ (*resp.* $\mathrm{Aut}\, \mathfrak{g}$) *the* (*abstract*) *group of algebraic* (*resp. restricted Lie algebra*) *automorphisms of* G (*resp.* $\mathfrak{g}$). *If* η *is an automorphism of* $\mathfrak{g}'$ *of order* m, $p \nmid m$ *then there is a unique* $\theta \in \mathrm{Aut}\, G$ (*resp.* $\psi \in \mathrm{Aut}\, \mathfrak{g}$) *of order* m *such that* $d\theta|_{\mathfrak{g}'} = \eta$ (*resp.* $\psi|_{\mathfrak{g}'} = \eta$).

Proof. Although one assumes $p \neq 2$ in [L2] this is not used in the proof of [L2, Lemma 1.4]. In particular, $\mathrm{Aut}\, \mathfrak{g} \cong \mathrm{Aut}\, \mathfrak{g}' \times \mu_p$ and hence there exists a unique automorphism of $\mathfrak{g}$ of order m whose restriction to $\mathfrak{g}'$ is η [L2, Lemma 1.4(iv)]. On the other hand, $\mathrm{Aut}\, G \cong \mathrm{Aut}\, G'$ (by restriction) unless $n = 2$, in which case the kernel of the natural map $\mathrm{Aut}\, G \to \mathrm{Aut}\, G'$ is of order 2 [L2, Lemma 1.4(ii)]. Since differentiation $d : \mathrm{Aut}\, G' \to \mathrm{Aut}\, \mathfrak{g}'$ is bijective [L2, Lemma 1.4(iii)] this completes the proof. □

2. Cartan subspaces

Definition 2.1. A subspace $\mathfrak{c}$ of $\mathfrak{g}(1)$ is a *Cartan subspace* if it is maximal among the commutative subspaces of $\mathfrak{g}(1)$ consisting of semisimple elements.

If $m = 2$ then a Cartan subspace $\mathfrak{c}$ of $\mathfrak{g}(1)$ satisfies $\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}) = \mathfrak{c}$. For $m > 2$ this may no longer hold. (This can already be seen in the zero rank case.) Recall that if $\mathfrak{h} \subset \mathfrak{g}$ is a nilpotent subalgebra then there is a **Fitting decomposition** $\mathfrak{g} = \mathfrak{g}^0(\mathfrak{h}) \oplus \mathfrak{g}^1(\mathfrak{h})$, where $\mathrm{ad}\, \mathfrak{h}$ acts nilpotently on $\mathfrak{g}^0(\mathfrak{h})$ and all weights of $\mathfrak{h}$ on $\mathfrak{g}^1(\mathfrak{h})$ are nonzero. There is an open subset U of $\mathfrak{h}$ such that for $x \in U$, $\mathrm{ad}\, x$ is nilpotent on $\mathfrak{g}^0(\mathfrak{h})$ and invertible on $\mathfrak{g}^1(\mathfrak{h})$, that is, $\mathfrak{g}^i(\mathfrak{h}) = \mathfrak{g}^i(kx)$ for $i = 0, 1$. The following lemma is a slight modification of [KR, Lemma 1].

Lemma 2.2. *Let* $\mathfrak{h} \subseteq \mathfrak{g}(1)$ *be a commutative subspace. Then* $\mathfrak{g}(1) = \mathfrak{g}^0(\mathfrak{h}) \cap \mathfrak{g}(1) \oplus \mathfrak{g}^1(\mathfrak{h}) \cap \mathfrak{g}(1)$.

Proof. Let $x \in U$, where U is the set defined in the paragraph above. Since $(\mathrm{ad}\, x)$ acts invertibly (resp. nilpotently) on $\mathfrak{g}^1(\mathfrak{h})$ (resp. $\mathfrak{g}^0(\mathfrak{h})$), so does $(\mathrm{ad}\, x)^m$. But $(\mathrm{ad}\, x)^m(\mathfrak{g}(i)) \subset \mathfrak{g}(i)$ for each $i \in \mathbb{Z}/m\mathbb{Z}$. □

If $\mathfrak{h} \subseteq \mathfrak{g}(1)$ is a commutative subspace then write $\mathfrak{g}^i(\mathfrak{h})(1)$ for $\mathfrak{g}^i(\mathfrak{h}) \cap \mathfrak{g}(1)$. Lemma 2.2 allows us to prove the following lemma by a standard argument.

Lemma 2.3. *Let* $\mathfrak{h} \subset \mathfrak{g}(1)$ *be commutative. Then the morphism* $\phi : G(0) \times \mathfrak{g}^0(\mathfrak{h})(1) \to \mathfrak{g}(1)$, $(g, x) \mapsto \mathrm{Ad}\, g(x)$, *is dominant and separable.*

Proof. Let $h \in \mathfrak{h}$ be such that $\mathfrak{g}^0(kh) = \mathfrak{g}^0(\mathfrak{h})$ and $\mathfrak{g}^1(kh) = \mathfrak{g}^1(\mathfrak{h})$. We claim that $d\phi_{(e,h)}$ is surjective. Indeed, identifying $T_{(e,h)}(G(0) \times \mathfrak{g}^0(\mathfrak{h})(1))$ with $\mathfrak{g}(0) \oplus \mathfrak{g}^0(\mathfrak{h})(1)$ in the natural way, it can easily be seen that $d\phi_{(e,h)}(x,y) = [x,h] + y$. Hence $\operatorname{im} d\phi_{(e,h)} = [\mathfrak{g}(0),h] + \mathfrak{g}^0(\mathfrak{h})(1)$. But $[\mathfrak{g}(0),h] = [\mathfrak{g},h] \cap \mathfrak{g}(1) \supset \mathfrak{g}^1(\mathfrak{h})(1)$, thus $d\phi_{(e,h)}$ is surjective. By [Bo, AG. 17.3], ϕ is dominant and separable. □

Corollary 2.4. *Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}(1)$. Then the morphism $G(0) \times \mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}) \to \mathfrak{g}(1)$, $(g,x) \to \operatorname{Ad} g(x)$ is dominant and separable.*

Proof. Since $\mathfrak{g}$ is a completely reducible $\operatorname{ad}\mathfrak{c}$-module, $\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}) = \mathfrak{g}^0(\mathfrak{c})(1)$. Hence we can apply Lemma 2.3. □

Recall from [Vi, § 3] that $c \in \mathfrak{c}$ is *an element in general position* if $\mathfrak{z}_{\mathfrak{g}}(c) = \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c})$. In common with [Vi], denote by $R(\mathfrak{c})$ the set of $x \in \mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c})$ such that the semisimple part of x (necessarily in $\mathfrak{c}$) is an element in general position. Since $\mathfrak{g}$ is a sum of weight-spaces for $\mathfrak{c}$, $R(\mathfrak{c})$ is the complement of a union of hyperplanes and hence is nonempty.

Theorem 2.5. *Any two Cartan subspaces of $\mathfrak{g}(1)$ are conjugate by an element of $G(0)$.*

Proof. Let $\mathfrak{c}_1$ and $\mathfrak{c}_2$ be two Cartan subspaces. By Corollary 2.4, $G(0)\cdot\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}_1)$ and $G(0)\cdot\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}_2)$ are dense constructible (i.e., unions of locally closed) subsets of $\mathfrak{g}(1)$. But hence $(G(0)\cdot\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}_1)) \cap \mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}_2)$ contains a nonempty open subset of $\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}_2)$. Since $R(\mathfrak{c}_2)$ is dense in $\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}_2)$, it intersects nontrivially with $G(0)\cdot\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}_1)$. But for any $x \in R(\mathfrak{c}_2)$, $\mathfrak{c}_2$ is the set of semisimple elements of $\mathfrak{z}_{\mathfrak{g}(1)}(x)$. Hence if $\operatorname{Ad} g^{-1}(x) \in \mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}_1)$ then clearly $\operatorname{Ad} g^{-1}(\mathfrak{c}_2) = \mathfrak{c}_1$. □

Corollary 2.6. *Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}(1)$. Then any semisimple element of $\mathfrak{g}(1)$ is conjugate to an element of $\mathfrak{c}$.*

Note that if $p > 2$ or G satisfies the standard hypotheses then $\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c}) = \mathfrak{c} \oplus \mathfrak{u}$ for a subspace $\mathfrak{u}$ consisting of nilpotent elements by Lemma 1.12. The assumption $p > 2$ is not required for Theorem 2.5 to hold.

There is a natural relationship between Cartan subspaces of $\mathfrak{g}(1)$ and maximal θ-split tori in G. (By a maximal θ-split torus, we mean a torus which is maximal among the collection of θ-split tori in G.) Denote by $\varphi(m)$ the Euler number of m. Recall that if T is a maximal torus of G and Y is a set of elements of $\operatorname{Lie}(T)$ then $Z_G(Y)^\circ$ is reductive. In fact, let Σ be the set of $\alpha \in \Phi = \Phi(G,T)$ such that $d\alpha(t) = 0$ for all $t \in Y$; then Σ is a closed subsystem of Φ and $Z_G(Y)^\circ$ is the subgroup of G generated by T and all root subgroups U_α (see, e.g., [Hu, 26.3]) with $\alpha \in \Sigma$, which is reductive by [Ch, 17.2]. (This argument appears in [SpSt, II.4.1]. If $\operatorname{char} k$ is zero or is a nontorsion prime and G is simply-connected, then $Z_G(x)$ is connected for any semisimple $x \in \mathfrak{g}$ [SpSt, II.3.19].)

Lemma 2.7. *Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}(1)$. Then there exists a maximal θ-split torus T_1 such that $\operatorname{Lie}(T_1) \supset \mathfrak{c}$. Moreover, $\dim T_1 = \dim \mathfrak{c} \cdot \varphi(m)$ and T_1 is a minimal torus in G such that $\mathfrak{c} \subset \operatorname{Lie}(T_1)$. If $p > 2$ or if G satisfies the standard hypotheses, then T_1 is unique.*

Proof. Let $L = Z_G(\mathfrak{c})^\circ$, a θ-stable connected (reductive, by the above discussion) subgroup of G and let T be any θ-stable maximal torus of L (which exists by the result of Steinberg mentioned after Lemma 1.2). Then $\mathfrak{z}(\mathfrak{l}) = \mathfrak{z}_s \oplus \mathfrak{z}_n$, where $\mathfrak{z}_s$ (resp. $\mathfrak{z}_n$) is the set of semisimple (resp. nilpotent) elements of $\mathfrak{z}$. Moreover, $\mathfrak{z}_s \subset \mathrm{Lie}(T)$ by [L1, 2.1]. Since $\mathrm{Lie}(L) = \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c})$ by [Bo, 9.1], this shows that $\mathfrak{c} \subset \mathrm{Lie}(T)$. Let T_d, $d \,|\, m$ be the subtori of T given by Lemma 1.10. Then $\mathfrak{c} \subset \mathrm{Lie}(T_1)$ and hence by maximality $\mathfrak{c} = \mathrm{Lie}(T_1)(1)$. But if T_1 is properly contained in a θ-split torus of G then $\mathfrak{c}$ cannot be a Cartan subspace, hence T_1 is maximal. This proves the first statement of the lemma. The second follows from Lemma 1.10. For the final assertion, $\theta|_{L'}$ is of zero rank, hence $T_1 \subseteq Z(L)^\circ$ by Lemma 1.12 and Remark 1.13. But therefore T_1 is the unique maximal θ-split torus of L. □

Remark 2.8. (a) We stress that T_1 need not be (in fact is very rarely) a maximal torus of G. If $G = \mathrm{SL}(n,k)$, for example, then there are no inner automorphisms for which this happens unless n is prime, in which case there is one conjugacy class of such automorphisms, the unique class of inner automorphisms of order n and rank 1 (see Lemma 4.5).

(b) We do not use reductivity of L (or G) in the proof of the first part of Lemma 2.7. Indeed, all of the discussion in this section, up to and including all but the last statement of Lemma 2.7, goes through for an arbitrary affine algebraic group G.

(c) Lemma 1.10 describes the decomposition of *any* θ-stable torus into the subtori T_i. Lemma 2.7 concerns only those θ-stable tori T which are maximal subject to $T = T_1$. Note that $\mathfrak{c} \subset \mathrm{Lie}(T_1)$ and hence $\mathfrak{c} \subset \mathfrak{z}(\mathfrak{g}^{T_1})$. Thus $Z_G(T_1) \subset Z_G(\mathfrak{c})^\circ$. But if T_1 is unique, then $gT_1g^{-1} = T_1$ for all $g \in Z_G(\mathfrak{c})$, whence $Z_G(\mathfrak{c})^\circ \subset N_G(T_1)^\circ = Z_G(T_1)$. Thus $Z_G(\mathfrak{c})^\circ = Z_G(T_1)$.

The following lemma is a slightly modified version of [Ri, 11.1]. The proof is essentially identical; we include it for the reader's convenience.

Lemma 2.9. *Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}(1)$ and let $Y \subset \mathfrak{c}$ be a subset of $\mathfrak{c}$. If $g \in G(0)$ is such that $\mathrm{Ad}\, g(Y) \subset \mathfrak{c}$ then there exists $n \in N_{G(0)}(\mathfrak{c})$ such that $\mathrm{Ad}\, n(y) = \mathrm{Ad}\, g(y)$ for all $y \in Y$.*

Proof. Let $L = Z_G(\mathrm{Ad}\, g(Y))^\circ$ and $\mathfrak{l} = \mathrm{Lie}(L) = \mathfrak{z}_{\mathfrak{g}}(\mathrm{Ad}\, g(Y))$ by [Bo, III.9.1]. Then L is a θ-stable reductive subgroup of G by the remark made before Lemma 2.7 and $\mathfrak{c}, \mathrm{Ad}\, g(\mathfrak{c})$ are Cartan subspaces of $\mathfrak{l}(1)$. Therefore we can apply Theorem 2.5. Thus there is $h \in L(0) \subseteq L \cap G(0)$ such that $\mathrm{Ad}\, hg(\mathfrak{c}) = \mathfrak{c}$. But $\mathrm{Ad}\, hg(y) = \mathrm{Ad}\, g(y)$ for all $y \in Y$. □

Remark 2.10. It is clear from the above proof that the Lemma is valid on replacing $G(0)$ and $N_{G(0)}(\mathfrak{c})$ by G^θ and $N_{G^\theta}(\mathfrak{c})$ (resp. $G^\theta_Z = \{g \in G \mid g^{-1}\theta(g) \in Z(G)\}$ and $N_{G^\theta_Z}(\mathfrak{c})$).

We now consider properties of $G(0)$-orbits in $\mathfrak{g}(1)$. Let V be a finite-dimensional k-vector space on which G acts linearly (and rationally). Denote by $g \cdot v$ the action of $g \in G$ on $v \in V$ and, similarly $G \cdot v$ the G-orbit through v. For a subset Y of an affine variety X, let $\overline{Y}$ denote the Zariski closure of Y in X. (The variety X will always be clear from the context. In particular, $X = \mathfrak{g}(1)$ unless otherwise specified.) Recall that $v \in V$ is *unstable* if $0 \in \overline{G \cdot v}$. By the Hilbert–Mumford criterion (see [Ke, Theorem 1.4], for example), v is unstable if and only if there exists a cocharacter $\lambda : k^\times \to G$ such that v is $\lambda(k^\times)$-unstable. To prove the next result in all characteristics we will use the Kempf–Rousseau theory, or the theory of optimal cocharacters for unstable elements, which we now briefly introduce.

Let T be a θ-stable maximal torus of G, let $Y(T)$ be the lattice of cocharacters in G and let $Y(T)_\mathbb{R} = Y(T) \otimes_\mathbb{Z} \mathbb{R}$. Let $(\cdot\,,\cdot) : Y(T) \otimes Y(T) \to \mathbb{Z}$ be a positive-definite W-equivariant and θ-equivariant symmetric bilinear form, extended linearly to an inner product $(\cdot\,,\cdot) : Y(T)_\mathbb{R} \times Y(T)_\mathbb{R} \to \mathbb{R}$. We define a norm function $\|\cdot\| : Y(G) \to \mathbb{R}_{\geqslant 0}$, where $Y(G)$ is the set of cocharacters in G by setting $\|\operatorname{Int} g \circ \lambda\| = \sqrt{(\lambda, \lambda)}$ for any $\lambda \in Y(T)$, $g \in G$. It follows from the W-equivariance and θ-equivariance of $(\cdot\,,\cdot)$ that $\|\theta \circ \lambda\| = \|\operatorname{Int} g \circ \lambda\| = \|\lambda\|$ for any $g \in G$. For $\lambda \in Y(G)$ there is a decomposition $V = \bigoplus_{i\in\mathbb{Z}} V(i;\lambda)$, where $V(i;\lambda) = \{v \in V \mid \lambda(t)\cdot v = t^i v \text{ for all } t \in k^\times\}$. If $\lambda \in Y(G)$ and $v = \sum_{i\in\mathbb{Z}} v_i$ with $v_i \in V(i;\lambda)$ then we define $m_v(\lambda) = \min_{v_i \neq 0} i$. If v is G-unstable, then λ is an *optimal cocharacter* for v if

$$\frac{m_v(\lambda)}{\|\lambda\|} \geqslant \frac{m_v(\mu)}{\|\mu\|}$$

for all cocharacters $\mu \in Y(G)$. (Note that by the Hilbert–Mumford criterion, $m_v(\lambda) > 0$ for some $\lambda \in Y(G)$.)

The main results of the Kempf–Rousseau theory [Ke], [Ro] are:

(i) optimal cocharacters exist for all unstable elements;

(ii) if v is unstable then the parabolic subgroup

$$P_\lambda = \{g \in G \mid \lim_{t\to 0} \lambda(t) g \lambda(t^{-1}) \text{ exists}\}$$

(see, e.g., [Sl] for details) of G is independent of the choice of optimal parabolic λ for v. It is called the instability parabolic for v, often denoted P_v;

(iii) The centralizer $Z_G(v) \subset P_v$;

(iv) for any maximal torus T of P_v there is a (unique) cocharacter $\lambda \in Y(T)$ such that λ is optimal for v; (iv) any two optimal cocharacters for v are conjugate by an element of P_v, and if λ is an optimal cocharacter for v then so is $\operatorname{Int} g \circ \lambda$ for any $g \in P_v$.

Lemma 2.11. *Let $x \in \mathfrak{g}(1)$ be nilpotent. Then x is $G(0)$-unstable.*

Proof. We can clearly assume that x is nonzero. Since x is nilpotent, it is G-unstable and has an associated instability parabolic $P_x = P_\lambda$ for some optimal cocharacter λ for x. But $d\theta(x) = \zeta x$ and hence by θ-invariance of the norm, $\theta \circ \lambda$ is also optimal for x. Thus P_x is θ-stable. But, therefore, by the result of Steinberg mentioned immediately after Lemma 1.2, P_x has a θ-stable maximal torus T. Since T is a maximal torus of P_x, there is an optimal cocharacter $\lambda \in Y(T)$ for x. But then $\theta \circ \lambda \in Y(T)$ is also optimal for x, and thus $\theta \circ \lambda = \lambda$. Therefore there is an optimal cocharacter for x such that $\lambda(k^\times) \subset G(0)$. □

Remark 2.12. Let $x \in \mathfrak{g}$ be any nilpotent element. Then a cocharacter $\lambda : k^\times \to G$ is an *associated cocharacter* for x if:

— $\mathrm{Ad}\,\lambda(t)(x) = t^2 x$ for all $t \in k^\times$, that is, $x \in \mathfrak{g}(2;\lambda)$.
— $\mathfrak{z}_\mathfrak{g}(x) \subseteq \sum_{i \geqslant 0} \mathfrak{g}(i;\lambda)$.
— There exists a Levi subgroup L of G such that $\lambda(k^\times) \subset L'$ and e is a distinguished nilpotent element of $\mathrm{Lie}(L)$.

According to the Bala–Carter–Pommerening theorem (see [Pr2] for a recent proof) any nilpotent orbit in $\mathfrak{g}$ has an associated cocharacter when the characteristic of the ground field is good. If $e \in \mathfrak{g}(1)$ then the argument in [L2, Cor. 5.4] (using Kawanaka's theorem [Ka]) shows that, for p good, e has an associated cocharacter λ such that $\lambda(k^\times) \subset G(0)$. (Moreover, any two such are conjugate by an element of $Z_{G(0)}(e)^\circ$.) Since (in good characteristic) any associated cocharacter is also an optimal cocharacter for e [Pr2, Theorem 2.3], this result is somewhat stronger than Lemma 2.11; on the other hand, Lemma 2.11 is true in arbitrary characteristic.

For the following lemma we essentially follow Vinberg's proof in characteristic zero [Vi, 1.3-4].

Lemma 2.13. *Let $x \in \mathfrak{g}(1)$ be semisimple. Then each irreducible component of $G \cdot x \cap \mathfrak{g}(1)$ is a single $G(0)$-orbit and, conversely, each $G(0)$-orbit in $G \cdot x \cap \mathfrak{g}(1)$ is an irreducible component. Hence all semisimple $G(0)$-orbits in $\mathfrak{g}(1)$ are closed.*

Proof. It is well known that $G\cdot x$ is closed for any semisimple x, hence $G\cdot x \cap \mathfrak{g}(1)$ is closed for $x \in \mathfrak{g}(1)$ semisimple. Since x is semisimple, $T_x(G\cdot x) = [\mathfrak{g}, x]$ (making the obvious identifications) and hence $T_x(G\cdot x \cap \mathfrak{g}(1)) \subseteq [\mathfrak{g}, x] \cap \mathfrak{g}(1) = [\mathfrak{g}(0), x]$. On the other hand, $\mathfrak{z}_{\mathfrak{g}(0)}(x) = \mathfrak{z}_\mathfrak{g}(x) \cap \mathfrak{g}(0) = \mathrm{Lie}((Z_G(x)^\theta)$ and hence $T_x(G(0)\cdot x) = [\mathfrak{g}(0), x]$ by equality of dimensions. But clearly $T_x(G\cdot x \cap \mathfrak{g}(1)) \supseteq T_x(G(0)\cdot x)$, hence equality holds. It follows that the dimension of any irreducible component of $G \cdot x \cap \mathfrak{g}(1)$ containing x is at most $\dim G(0) \cdot x$. Thus x is a smooth point of $G \cdot x \cap \mathfrak{g}(1)$ and (therefore) $G(0) \cdot x$ is the unique irreducible component of $G\cdot x \cap \mathfrak{g}(1)$ containing x. □

Corollary 2.14. *Let $x \in \mathfrak{g}(1)$. Then $G(0)\cdot x_s$ is the unique closed orbit in $\overline{G(0) \cdot x}$.*

Proof. Let $L = Z_G(x_s)^\circ$, a θ-stable reductive subgroup of G by the remark before Lemma 2.7. Then $x_n \in \mathrm{Lie}(L) \cap \mathfrak{g}(1)$ and hence by Lemma 2.11, the closure $\overline{(L \cap G(0)) \cdot x_n}$ contains 0. It follows that $x_s \in \overline{(L \cap G(0)) \cdot x} \subseteq \overline{G(0) \cdot x}$. Moreover, $G(0)\cdot x_s$ is closed by Lemma 2.13. But it is well known that $\overline{G(0) \cdot x}$ contains a unique closed $G(0)$-orbit (see, e.g., [Hu, 8.3]). □

We briefly recall the basic definition and properties of the categorical quotient. Let H be an affine algebraic group such that H° is reductive (possibly trivial) and let X be an affine variety. We say that H acts *morphically* on X if H acts on X, and the corresponding map $H \times X \to X$ is a morphism of varieties. The ring of invariants $k[X]^H$ is finitely generated. (In positive characteristic this is due to Haboush [Ha].) The corresponding affine variety $\mathrm{Spec}(k[X]^H)$ is the *categorical quotient* of X by H and the morphism $\pi = \pi_{X,H} : X \to X/\!\!/H$ induced by the algebra embedding $k[X]^H \hookrightarrow k[X]$ is the *quotient morphism.* We have the following well known properties.

Properties of the Quotient Morphism, 2.15.

(a) π *is surjective.*

(b) *If* U_1, U_2 *are disjoint* H*-stable closed subsets of* X *then there exists* $f \in k[X]^H$ *such that* $f(x) = 0$ *for all* $x \in U_1$ *and* $f(x) = 1$ *for all* $x \in U_2$.

(c) *Each fibre* $\pi^{-1}(\xi)$ *is a finite union of* H*-orbits and contains a unique closed* H*-orbit, which we denote* $T(\xi)$*, and which is also the unique orbit of minimal dimension.*

(d) *For* $x \in X$ *and* $\xi \in X/\!\!/H$, $\pi(x) = \xi$ *if and only if* $\overline{H \cdot x} \supseteq T(\xi)$.

(e) *If* X *is normal, then so is* $X/\!\!/G$.

In the present circumstances we are interested in the quotient $\mathfrak{g}(1)/\!\!/G(0)$. The closed orbits in $\mathfrak{g}(1)$ are precisely the semisimple orbits (Lemma 2.13) and each semisimple orbit meets $\mathfrak{c}$ (Corollary 2.6). Furthermore, two elements of $\mathfrak{c}$ are conjugate by an element of $G(0)$ if and only if they are conjugate by an element of $N_{G(0)}(\mathfrak{c})$ by Lemma 2.9. Let $W_\mathfrak{c} = N_{G(0)}(\mathfrak{c})/Z_{G(0)}(\mathfrak{c})$. Hence the embedding $j : \mathfrak{c} \hookrightarrow \mathfrak{g}(1)$ induces a bijective morphism $j' : \mathfrak{c}/W_\mathfrak{c} \to \mathfrak{g}(1)/\!\!/G(0)$ such that the following diagram is commutative:

$$\begin{array}{ccc} \mathfrak{c} & \xrightarrow{\ j\ } & \mathfrak{g}(1) \\ \downarrow & & \downarrow \\ \mathfrak{c}/W_\mathfrak{c} & \xrightarrow{\ j'\ } & \mathfrak{g}(1)/\!\!/G(0) \end{array} .$$

Since j' is bijective and $\mathfrak{c}/W_\mathfrak{c}$ and $\mathfrak{g}(1)/\!\!/G(0)$ are normal varieties, it follows that $\mathrm{Frac}(k[\mathfrak{c}]^{W_\mathfrak{c}})$ is a purely inseparable extension of $(j')^*(\mathrm{Frac}(k[\mathfrak{g}(1)]^{G(0)})$, and in particular is finite. But $\pi_\mathfrak{c} : \mathfrak{c} \to \mathfrak{c}/W_\mathfrak{c}$ is also finite and hence the composition $j' \circ \pi_\mathfrak{c}$ maps open sets to open sets [Hu, 4.2]. Since the set of elements of $\mathfrak{c}$ in general position is clearly open, its image $\pi_{\mathfrak{g}(1)}(R(\mathfrak{c}))$ is also open in $\mathfrak{g}(1)/\!\!/G(0)$. Thus we have proved:

Lemma 2.16. $G(0) \cdot R(\mathfrak{c})$ *is open in* $\mathfrak{g}(1)$.

We recall that the quotient morphism is not in general separable, even if X is a vector space [MN]. The present case poses some difficulties, since a commonly used criterion for separability [Ri, 9.3] does not apply. The following result, which appeared in [Vi] in the case of characteristic zero, provides the solution.

Lemma 2.17. *Assume* $p > 2$ *or that* G *satisfies the standard hypotheses* (*see Section* 3). *Then* $k(\mathfrak{g}(1))^{G(0)} = \mathrm{Frac}(k[\mathfrak{g}(1)]^{G(0)})$.

Proof. As above, let $R(\mathfrak{c})$ denote the set of $x \in \mathfrak{z}_{\mathfrak{g}(1)}\mathfrak{c})$ such that the semisimple part of x is an element in general position in $\mathfrak{c}$. Let $L = Z_G(\mathfrak{c})^\circ$, a θ-stable reductive subgroup of G, and let $\mathfrak{l} = \mathrm{Lie}(L) = \mathfrak{z}_\mathfrak{g}(\mathfrak{c})$, $L(0) = (L^\theta)^\circ$. By Lemma 1.12, $\mathfrak{l}(1) = \mathfrak{c} \oplus \mathfrak{u}$, where $\mathfrak{u}$ is the set of nilpotent elements of $\mathfrak{l}(1)$. Let $h \in k(\mathfrak{g}(1))^{G(0)}$. Then the domain $\mathrm{dom}\, h$ of h is open in $\mathfrak{g}(1)$ and hence intersects nontrivially with $G(0) \cdot R(\mathfrak{c})$. By $G(0)$-invariance, it intersects nontrivially with $R(\mathfrak{c})$, hence h restricts to a rational function $h|_{\mathfrak{l}(1)} \in k(\mathfrak{l}(1))^{L(0)}$. Let $c + u \in R(\mathfrak{c})$, where

$c \in \mathfrak{c}, u \in \mathfrak{u}$. We claim that $c+u \in \operatorname{dom} h$ if and only if $c \in \operatorname{dom} h$. Indeed, suppose $c+u \in \operatorname{dom} h$. Then u is a nilpotent element of $\operatorname{Lie}(L)(1)$ and hence there exists an optimal cocharacter $\lambda : k^\times \to L(0)$ for u by Lemma 2.11. But then $\lim_{t\to 0} \operatorname{Ad}\lambda(t)(c+u) = c$, and since h is $G(0)$-invariant, $h(\operatorname{Ad}\lambda(t)(c+u)) = h(c+u)$ is independent of $t \neq 0$. Thus $c \in \operatorname{dom} h$.

On the other hand, suppose $c \in \operatorname{dom} h$ and let $u \in \mathfrak{u}$. Since $k[\mathfrak{c}\oplus\mathfrak{u}] \cong k[\mathfrak{c}] \otimes k[\mathfrak{u}]$ is a unique factorization domain, we can write h as f/g, where f and g are coprime polynomials. Since $g(c) \neq 0$, g is not identically zero on $c+\mathfrak{u}$. Let $\mathcal{O}$ be the dense $L(0)$-orbit in $\mathfrak{u}$; then g is not identically zero on $c+\mathcal{O}$ and hence $\operatorname{dom} h$ intersects nontrivially with $c+\mathcal{O}$. Thus by $L(0)$-invariance, $\operatorname{dom} h \supset c+\mathcal{O}$ and, furthermore, h is constant on $c+\mathcal{O}$. Therefore $\operatorname{dom} h \supset c+\mathfrak{u}$ and h is constant on $c+\mathfrak{u}$.

Returning to the general case (where θ is no longer of zero semisimple rank), we can now apply the argument of [Ri, 9.3]. Hence let $X_1 = \mathfrak{g}(1)\backslash(G(0)\cdot R(\mathfrak{c}))$. Thus $Y = X_1 \cup \mathfrak{g}(1)\backslash \operatorname{dom} h$ is closed in $\mathfrak{g}(1)$. Let $x \in \mathfrak{g}(1)\backslash Y = (G(0)\cdot R(\mathfrak{c})) \cap \operatorname{dom} h$. Then the semisimple part of x is $G(0)$-conjugate to an element c of $\mathfrak{c}$ in general position. Let $U = G(0)\cdot(c+\mathfrak{u})$. Since $U = \pi^{-1}(\pi(c))$ by Corollary 2.14, U is closed (and $G(0)$-stable) in $\mathfrak{g}(1)$. Moreover, h is defined at each point of U and hence $U \cap Y = \emptyset$. Thus there exists $g \in k[\mathfrak{g}(1)]^{G(0)}$ such that $g(u) = 1$ for all $u \in U$ and $g(y) = 0$ for all $y \in Y$. In particular, $\operatorname{dom} h$ contains $\mathfrak{g}(1)_g = \{x \in \mathfrak{g}(1) \mid g(x) \neq 0\}$. It follows that $h = f/g^r$ for some $r \geqslant 0$ and some $f \in k[\mathfrak{g}(1)]$. Hence $h \in \operatorname{Frac} k[\mathfrak{g}(1)]^{G(0)}$. □

Remark 2.18. In the proof above we showed that restricting rational functions from $\mathfrak{g}(1)$ to $\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c})$ induces a (well-defined) injective homomorphism from $k(\mathfrak{g}(1))^{G(0)}$ to $k(\mathfrak{c})$, hence that $k(\mathfrak{g}(1))^{G(0)}$ is a subfield of $k(\mathfrak{c})^W = \operatorname{Frac} k[\mathfrak{c}]^W$. One can check that this also holds if $m = 1$, $G = \mathrm{SL}(2)$ and $\operatorname{char} k = 2$. However, the Chevalley restriction theorem (Theorem 2.20 below) does not hold in this case. In fact, in this case the quotient morphism is separable, but the induced morphism $\mathfrak{c} = \mathfrak{c}/W \to \mathfrak{g}(1)/\!\!/G(0)$ is purely inseparable. This comes down to the fact that the natural morphism $\mathfrak{c} \times \mathcal{N}(\mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c})) \to \mathfrak{z}_{\mathfrak{g}(1)}(\mathfrak{c})$ is inseparable.

Corollary 2.19. *If $p > 2$ or if G satisfies the standard hypotheses* (*see Section* 3) *then the quotient morphism $\mathfrak{g}(1) \to \mathfrak{g}(1)/\!\!/G(0)$ is separable.*

Proof. By [Bo, Section AG. 2.4] the field extension $k(\mathfrak{g}(1)) \supset k(\mathfrak{g}(1))^{G(0)}$ is separable. Hence we apply Lemma 2.17. □

This preparation allows us to prove the following form of the Chevalley Restriction Theorem. Our proof follows [Ri, 11.3].

Theorem 2.20. *Suppose $p > 2$ or G satisfies the standard hypotheses* (*see Section* 3). *Then the embedding $j : \mathfrak{c} \hookrightarrow \mathfrak{g}(1)$ induces an isomorphism of varieties $j' : \mathfrak{c}/W_{\mathfrak{c}} \to \mathfrak{g}(1)/\!\!/G(0)$.*

Proof. As remarked above, j' is bijective. Since $\mathfrak{c}/W_{\mathfrak{c}}$ and $\mathfrak{g}(1)/\!\!/G(0)$ are normal by 2.15(e) it will suffice to show that j' is separable (since a bijective and separable morphism of normal varieties is an isomorphism by Zariski's main theorem). Let $L = Z_G(\mathfrak{c})^\circ$, a θ-stable reductive subgroup of G, and let $\mathfrak{l} = \operatorname{Lie}(L) = \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c})$. Then $\mathfrak{l}(1) = \mathfrak{c} \oplus \mathfrak{u}$, where $\mathfrak{u}$ is the set of nilpotent elements of $\mathfrak{g}(1)$ commuting with

$\mathfrak{c}$. By Corollary 2.19 the quotient morphism $\pi : \mathfrak{g}(1) \to \mathfrak{g}(1)/\!\!/G(0)$ is separable. Moreover $\phi : G(0) \times \mathfrak{l}(1) \to \mathfrak{g}(1)$, $(g,x) \mapsto \operatorname{Ad} g(x)$, is a separable morphism by Corollary 2.4. Applying the argument in [Ri, 11.3], the induced morphism $\mathfrak{l}(1) \to \mathfrak{g}(1)/\!\!/G(0)$ is separable. Since $L(0)$ acts trivially on $\mathfrak{c}$ and acts on $\mathfrak{u}$ with a dense open orbit, $k[\mathfrak{l}(1)]^{L(0)} = k[\mathfrak{c} \oplus \mathfrak{u}]^{L(0)} = k[\mathfrak{c}]$. Hence the composition σ of the embedding $\mathfrak{c} \to \mathfrak{l}(1)$ with the quotient morphism $\mathfrak{l}(1) \to \mathfrak{l}(1)/\!\!/L(0)$ is a $N_{G(0)}(\mathfrak{c})$-equivariant isomorphism of varieties. It follows that there is an isomorphism $\overline{\sigma}$ making the following diagram commutative:

$$\begin{array}{ccc} \mathfrak{c} & \xrightarrow{\sigma} & \mathfrak{l}(1)/\!\!/L(0) \\ \downarrow & & \downarrow \\ \mathfrak{c}/W_{\mathfrak{c}} & \xrightarrow{\overline{\sigma}} & \mathfrak{l}(1)/\!\!/N_{G(0)}(\mathfrak{c}) \end{array} .$$

On the other hand, the separable morphism $\mathfrak{l}(1) \to \mathfrak{g}(1)/\!\!/G(0)$ clearly factors through $\mathfrak{l}(1) \to \mathfrak{l}(1)/\!\!/N_{G(0)}(\mathfrak{c})$, and hence $\mathfrak{l}(1)/\!\!/N_{G(0)}(\mathfrak{c}) \to \mathfrak{g}(1)/\!\!/G(0)$ is separable. Thus j' is separable. By [Bo, Section AG. 18.2], j' is an isomorphism. □

Remark 2.21. In the case $m = 2$, Theorem 2.20 appeared in [L2], but with the requirement that G satisfy the standard hypotheses.

Following [Vi, Cor. 2 to Theorem 4], we have:

Corollary 2.22. *The fibres of* $\pi : \mathfrak{g}(1) \to \mathfrak{g}(1)/\!\!/G(0)$ *are equidimensional, of dimension* $\dim \mathfrak{g}(1) - r$ (*where* $r = \dim \mathfrak{c}$).

Proof. By standard facts about morphisms of varieties (see, e.g., [Hu, 4.1,4.3]), each irreducible component of each fibre of π has dimension at least $\dim \mathfrak{g}(1) - \dim \mathfrak{g}(1)/\!\!/G(0) = \dim \mathfrak{g}(1) - r$, and there exists an open subset U of $\mathfrak{g}(1)/\!\!/G(0)$ such that the fibre $\pi^{-1}(u)$ is of pure dimension $\mathfrak{g}(1) - r$ for each $u \in U$. Let $q = \min_{x \in \mathfrak{g}(1)} \dim Z_{G(0)}(x)$. Then the set $\{x \in \mathfrak{g}(1) \mid \dim Z_{G(0)}(x) = q\}$ is open in $\mathfrak{g}(1)$ and hence intersects nontrivially with $\pi^{-1}(U)$. Since each irreducible component of each fibre of π has an open orbit, we have $\dim G(0) - q = \dim \mathfrak{g}(1) - r$. But therefore the fibres of π are all of pure codimension r in $\mathfrak{g}(1)$. □

We recall that $\dim \mathfrak{g}(1)/\!\!/G(0) = r$ by Theorem 2.20.

3. A θ-stable reduction

From now on we make the following assumptions on G, often referred to as the *standard hypotheses*:

(A) p is good.
(B) G' is simply-connected.
(C) There is a nondegenerate symmetric bilinear G-equivariant form $\kappa : \mathfrak{g} \times \mathfrak{g} \to k$.

Let $G_1, \ldots, G_r$ be the minimal normal subgroups of G' and let $\mathfrak{g}_i = \operatorname{Lie}(G_i)$. Hence $G' = G_1 \times \cdots \times G_r$ and $\mathfrak{g}' = \operatorname{Lie}(G') = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_r$. Define groups $\tilde{G}_i$, $1 \leqslant i \leqslant r$, as follows:

$$\tilde{G}_i = \begin{cases} \mathrm{GL}(V_i) & \text{if } G_i = \mathrm{SL}(V_i) \text{ and } p \mid \dim V_i, \\ G_i & \text{otherwise.} \end{cases}$$

Set $\tilde{\mathfrak{g}}_i = \mathrm{Lie}(\tilde{G}_i)$ $(1 \leqslant i \leqslant r)$, $\tilde{G} = \tilde{G}_1 \times \cdots \times \tilde{G}_r$ and $\tilde{\mathfrak{g}} = \mathrm{Lie}(\tilde{G})$. Consider $\mathfrak{g}'$ as a Lie subalgebra of both $\mathfrak{g}$ and $\tilde{\mathfrak{g}}$.

Here we prove a generalization of a reduction theorem of Gordon and Premet [GP, 6.2], extended to the case $m = 2$ by the author in [L2]. This can be proved in a similar way to the $m = 2$ case and, therefore, we refer the reader to [L2, Theorem 3.1] for some details. An important corollary is that the nondegenerate form κ in (C) may be chosen to be θ-equivariant.

Proposition 3.1. *There exists a torus T_0, an automorphism $\widehat{\theta}$ of $\widehat{G} = \tilde{G} \times T_0$ and a restricted Lie algebra embedding $\phi : \mathfrak{g} \to \widehat{\mathfrak{g}} = \mathrm{Lie}(\widehat{G})$ such that:*

- (i) *$\widehat{\theta}$ has order m.*
- (ii) *$\phi(d\theta(x)) = d\widehat{\theta}(\phi(x))$ for all $x \in \mathfrak{g}$.*
- (iii) *There is a $d\widehat{\theta}$-stable toral algebra $\mathfrak{t}_1$ such that $\widehat{\mathfrak{g}} = \phi(\mathfrak{g}) \oplus \mathfrak{t}_1$ (Lie algebra direct sum).*
- (iv) *$\widehat{\theta}$ stabilizes $\tilde{G}$ and T_0, and $\widehat{\theta}(\tilde{G}_i) = \tilde{G}_j$ whenever $\theta(G_i) = G_j$.*

Proof. The existence of a toral algebra $\mathfrak{s}_0$ and an injective restricted Lie algebra homomorphism $\eta : \mathfrak{g} \to \tilde{\mathfrak{g}} \oplus \mathfrak{s}_0$ such that $\eta(\mathfrak{g}_i) = \mathfrak{g}_i \subseteq \tilde{\mathfrak{g}}_i$ was proved by Premet [Pr1, Lemma 4.1]. (This holds without the assumption (C).) Moreover, by Gordon and Premet [GP, 6.2] there exists a toral algebra $\mathfrak{t}_1 \subset \widehat{\mathfrak{g}}$ such that $\widehat{\mathfrak{g}} = \eta(\mathfrak{g}) \oplus \mathfrak{t}_1$. Identify $\mathfrak{g}$ with its image $\eta(\mathfrak{g})$, and define a restricted Lie algebra automorphism ϕ of $\widehat{\mathfrak{g}}$ by $\phi(x) = d\theta(x)$ $(x \in \mathfrak{g})$, $\phi(t) = t$ $(t \in \mathfrak{t}_1)$ and linear extension to all of $\widehat{\mathfrak{g}}$. The essential idea is to find ϕ-stable subalgebras $\overline{\mathfrak{g}}$ and $\mathfrak{t}_0$ of $\mathfrak{g}$ such that $\overline{\mathfrak{g}}$ contains $\mathfrak{g}$ and is isomorphic to $\tilde{\mathfrak{g}}$, $\mathfrak{t}_0$ is a toral algebra and $\widehat{\mathfrak{g}} = \overline{\mathfrak{g}} \oplus \mathfrak{t}_0$.

Let (B, T) be a fundamental pair in G for θ, let $\mathfrak{h} = \mathrm{Lie}(T)$, $T' = T \cap G'$, $\mathfrak{h}' = \mathrm{Lie}(T') = \mathfrak{h} \cap \mathfrak{g}'$, $T_i = T \cap G_i$, let $\tilde{T}_i$ (resp. $\tilde{T}, \widehat{T}$) be the unique maximal torus of $\tilde{G}_i$ (resp. $\tilde{G}$, $\widehat{G}$) containing T_i (resp. T') and let $\mathfrak{h}_i = \mathfrak{h} \cap \mathfrak{g}_i = \mathrm{Lie}(T_i)$, $\tilde{\mathfrak{h}}_i = \mathrm{Lie}(\tilde{T}_i)$, $\tilde{\mathfrak{h}} = \mathrm{Lie}(\tilde{T})$, $\widehat{\mathfrak{h}} = \mathrm{Lie}(\widehat{T})$. Let $\Phi = \Phi(G, T)$ be the roots of G relative to T, let $\Phi_i = \Phi(G_i, T \cap G_i) \subset \Phi$ and let Δ (resp. Δ_i) be the basis of Φ (resp. Φ_i) corresponding to B (resp. $B \cap G_i$). Clearly $\Delta = \bigcup_{i=1}^r \Delta_i$, and any element of Φ_i can be considered as an element of $X(\widehat{T})$ (hence also $X(T)$, $X(\tilde{T})$, $X(T')$).

We first construct the ϕ-stable toral algebra $\mathfrak{t}_0$. Let $\mathfrak{z} = \mathfrak{z}(\mathfrak{g})$, $\tilde{\mathfrak{z}} = \mathfrak{z}(\tilde{\mathfrak{g}})$, $\mathfrak{z}_i = \mathfrak{z}(\mathfrak{g}_i)$, $\widehat{\mathfrak{z}} = \mathfrak{z}(\widehat{\mathfrak{g}})$. Clearly $\widehat{\mathfrak{z}} = \mathfrak{z} \oplus \mathfrak{s}_0 = \tilde{\mathfrak{z}} \oplus \mathfrak{t}_1$ and $\tilde{\mathfrak{z}} = \sum \mathfrak{z}_i$, thus $\tilde{\mathfrak{z}} \subseteq \widehat{\mathfrak{z}}$ are ϕ-stable toral algebras. It follows by Maschke's theorem that there is a ϕ-stable toral algebra $\mathfrak{t}_0^{\mathrm{tor}}$ such that $\widehat{\mathfrak{z}}^{\mathrm{tor}} = \mathfrak{t}_0^{\mathrm{tor}} \oplus \tilde{\mathfrak{z}}^{\mathrm{tor}}$. Let $\mathfrak{t}_0$ be the (toral) subalgebra of $\widehat{\mathfrak{h}}$ generated by $\mathfrak{t}_0^{\mathrm{tor}}$. The problem at this point (which does not arise for $m = 2$) is that a toral algebra endowed with an arbitrary (restricted Lie algebra) automorphism cannot, in general, be described as the Lie algebra of a torus with algebraic automorphism. Let $Z = Z(G)^\circ$ and let $Y(Z)$ be the group of cocharacters of Z. The action of θ on Z induces a $\mathbb{Z}$-module automorphism $\theta_Z : Y(Z) \to Y(Z)$. Let $c(t) \in \mathbb{F}_p[t]$ be the reduction modulo p of the characteristic polynomial of θ_Z and let $\tilde{c}(t) \in \mathbb{F}_p[t]$ be the characteristic polynomial of $\phi|_{\tilde{\mathfrak{z}}^{\mathrm{tor}}}$. Then (since $\mathfrak{z} = \mathrm{Lie}(Z)$

[L1, 4.1]) the characteristic polynomial of $\phi|_{\mathfrak{t}_0^{\rm tor}}$ is $(t-1)^{\dim \mathfrak{t}_1} c(t)/\tilde{c}(t)$. Define a restricted Lie algebra automorphism of (the Lie algebra direct sum) $\widehat{\mathfrak{g}} \oplus \tilde{\mathfrak{z}}$ by $(x,y) \mapsto (\phi(x), d\theta(y))$. Clearly $\widehat{\mathfrak{g}} \oplus \tilde{\mathfrak{z}} = \mathfrak{g} \oplus \mathfrak{t}_1 \oplus \tilde{\mathfrak{z}} = \tilde{\mathfrak{g}} \oplus \mathfrak{t}_0 \oplus \tilde{\mathfrak{z}}$. Hence, replacing $\widehat{\mathfrak{g}}$ by $\widehat{\mathfrak{g}} \oplus \tilde{\mathfrak{z}}$ and $\mathfrak{t}_0$ by $\mathfrak{t}_0 \oplus \tilde{\mathfrak{z}}$, we may assume that $\phi|_{\mathfrak{t}_0{}^{\rm tor}}$ has characteristic polynomial $(t-1)^{\dim \mathfrak{t}_1} c(t)$. It is now clear that there exists a torus T_0 and a rational automorphism ψ of T_0 such that $\mathrm{Lie}(T_0) = \mathfrak{t}_0$ and $d\psi = \phi|_{\mathfrak{t}_0}$.

Denote by σ the permutation of the set $\{1, \ldots, r\}$ such that $\sigma(\mathfrak{g}_i) = \mathfrak{g}_{\sigma(i)}$. Next, we construct subalgebras $\overline{\mathfrak{g}}_i$ containing $\mathfrak{g}_i$ such that $\overline{\mathfrak{g}}_i \cong \tilde{\mathfrak{g}}_i$, $\phi(\overline{\mathfrak{g}}_i) = \overline{\mathfrak{g}}_{\sigma(i)}$ and $\sum_{i=1}^r \overline{\mathfrak{g}}_i \oplus \mathfrak{s}_0 = \widehat{\mathfrak{g}}$. There is nothing to do unless $G_i = \mathrm{SL}(V_i)$, where $p \,|\, \dim V_i$. Hence assume that $\tilde{G}_i = \mathrm{GL}(V_i)$ and $p \,|\, \dim V_i$. After renumbering we can clearly assume that $i = 1$, and that for some $l \,|\, m$, $\theta(G_i) = G_{i+1}$ $(1 \leqslant i < l)$ and $\theta(G_l) = G_1$. By the argument in [L2, Step 2, Proof of Theorem 3.1] it is straightforward to construct a ϕ^l-stable toral subalgebra $\overline{\mathfrak{h}}_1$ of $\widehat{\mathfrak{h}}$ which contains $\mathfrak{h}_1$ and such that $\bigcap_{\alpha \in \Delta \setminus \Delta_1} \ker d\alpha = \overline{\mathfrak{h}}_1 \oplus \sum_{i>2} \mathfrak{z}_i \oplus \mathfrak{t}_0$. Moreover, by linear independence of the differentials $d\alpha$, $\alpha \in \Delta$ [L1, 4.2], the restricted Lie subalgebra $\overline{\mathfrak{g}}_1 = \overline{\mathfrak{h}}_1 + \mathfrak{g}_1$ of $\widehat{\mathfrak{g}}$ is isomorphic to $\tilde{\mathfrak{g}}_1$ (as a restricted Lie algebra). It suffices now to take $\overline{\mathfrak{g}}_i = \phi^i(\overline{\mathfrak{g}}_1)$, $2 \leqslant i \leqslant l$. This construction (applied to all minimal ϕ-stable summands in the expression $\mathfrak{g}' = \bigoplus \mathfrak{g}_i$) provides the required decomposition $\widehat{\mathfrak{g}} = \bigoplus_{i=1}^r \overline{\mathfrak{g}}_i \oplus \mathfrak{t}_0$ which is preserved by the action of ϕ. Replacing $\tilde{\mathfrak{g}}$ by $\overline{\mathfrak{g}}$ in the obvious way (see the argument at the end of [L2, Proof of Theorem 3.1]) we may assume that $\phi(\tilde{\mathfrak{g}}_i) = \tilde{\mathfrak{g}}_{\sigma(i)}$. We claim that the restriction $\phi|_{\tilde{\mathfrak{g}}}$ is the differential of a rational automorphism $\tilde{\theta}$ of $\tilde{G}$. Indeed, we need clearly only prove this for the restriction of ϕ to the sum of $\tilde{\mathfrak{g}}_i$ satisfying $\tilde{\mathfrak{g}}_i \neq \mathfrak{g}_i$, and hence we may assume as above that $\tilde{G}_1 = \mathrm{GL}(V_1)$, that $\phi(\mathfrak{g}_i) = \mathfrak{g}_{i+1}$ $(1 \leqslant i < l)$ and $\phi(\mathfrak{g}_l) = \mathfrak{g}_1$. Let m' be the order of $\phi^l|_{\tilde{\mathfrak{g}}_1}$. By Lemma 1.15 there exists a unique automorphism ψ_1 of $\mathrm{GL}(V_1)$ of order m' such that $d\psi_1 = \phi^l|_{\tilde{\mathfrak{g}}_1}$. Hence let $\tilde{\theta}$ act on $\tilde{G}_1 \times \cdots \times \tilde{G}_l$ via $(g_1, \ldots, g_l) \mapsto (\psi_1(g_l), g_1, \ldots, g_{l-1})$. Extending $\tilde{\theta}$ to $\tilde{G} \times T_0$ by $(g,t) \mapsto (\tilde{\theta}(g), \psi(t))$ gives the required automorphism of $\widehat{G}$. □

As a consequence, we have:

Corollary 3.2. *There exists a nondegenerate $d\theta$-equivariant and G-equivariant symmetric bilinear form $\kappa : \mathfrak{g} \times \mathfrak{g} \to k$.*

Proof. The argument of [L2, Cor. 3.2] applies verbatim. □

Remark 3.3. The following example shows the type of problem that can occur if we do not assume the standard hypotheses. Suppose char $k = 2$, let $G_1 = \mathrm{SL}(2,k)$ and let $G = G_1^3/Z_0$ where Z_0 is the diagonal embedding into G_1^3 of the scheme-theoretic centre of G_1. Let $\{h_\alpha, e_{\pm\alpha}\}$ (resp. $\{h_\beta, e_{\pm\beta}\}$, $\{h_\gamma, e_{\pm\gamma}\}$) be a basis of the Lie algebra of the first (resp. second, third) copy of G_1. Then $h_\alpha + h_\beta + h_\gamma = 0$. (The Lie algebra of G is spanned by $h_\alpha, \ldots, e_{-\gamma}$ and an element $H \in \mathrm{Lie}(T)$ satisfying $d\alpha(H) = d\beta(H) = d\gamma(H) = 1$.) Let θ be the automorphism of G of order 3 which satisfies $d\theta(e_{\pm\alpha}) = e_{\pm\beta}$, $d\theta(e_{\pm\beta}) = e_{\pm\gamma}$, $d\theta(e_{\pm\gamma}) = e_{\pm\alpha}$. Then it is not possible to construct $\widehat{G}, \widehat{\theta} \ldots$ as in Proposition 3.1 since in this case $h_\alpha + h_\beta = h_\gamma$ and hence (in the notation of the Proposition) $(\mathfrak{g}_1 + \mathfrak{g}_2) \cap \mathfrak{g}_3 \neq \{0\}$.

4. The little Weyl group

It was proved in [Vi] for the case $k = \mathbb{C}$ that the 'little Weyl group' $W_{\mathfrak{c}} = N_{G(0)}(\mathfrak{c})/Z_{G(0)}(\mathfrak{c}) \hookrightarrow \mathrm{GL}(\mathfrak{c})$ is generated by pseudoreflections. (Recall that an element $g \in \mathrm{GL}(V)$ of finite order is a pseudoreflection if the space of fixed points V^g is of codimension 1 in V.) It follows that the ring of invariants $k[\mathfrak{c}]^{W_{\mathfrak{c}}}$ is a polynomial ring. In the modular case $W_{\mathfrak{c}}$ may have order divisible by the characteristic of the ground field. On the other hand, we show in this section that it is sufficiently 'nice' for the invariants to be polynomial, at least under the assumptions of the standard hypotheses. Proposition 3.1 essentially reduces us to the case that G is almost simple, not of type A_{ip-1}, or that G is isomorphic to $\mathrm{GL}(V)$ for a vector space V of dimension divisible by p. For G of classical type Vinberg [Vi] has described the little Weyl group for all automorphisms. One could use the same approach to verify that Vinberg's description holds in good characteristic. (Most calculations are omitted in [Vi].) However, we provide a slightly different perspective here that also makes clear the precise relationship between the Weyl group of G and $W_{\mathfrak{c}}$. For G of exceptional type we apply a result of Panyushev [Pa1] and an inspection of orders of centralizers in the Weyl group (classified in [Ca]) to deduce the required result. We assume $p > 2$ from now on.

Lemma 4.1. *Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}(1)$, let T_1 be the unique minimal θ-stable torus whose Lie algebra contains $\mathfrak{c}$ (Lemma 2.7), and let T_m be a maximal torus of $(Z_G(\mathfrak{c})^\theta)^\circ$. Then T_mT_1 is regular in G. Moreover, if $T = Z_G(T_1T_m)$ then T_1 and T_m are the subtori of T constructed before Lemma 1.10.*

Proof. Let $L = Z_G(T_1) = Z_G(\mathfrak{c})^\circ$, a θ-stable Levi subgroup of G. Then T_m is regular in L by Lemma 1.5. The final statement is clear. □

The idea of Lemma 4.1 is that, once one has fixed a Cartan subspace $\mathfrak{c}$ (or, equivalently, by Lemma 2.7, a maximal θ-split torus T_1) and a maximal torus T_m of $Z_{G(0)}(\mathfrak{c})$, this also fixes a maximal torus T containing T_1 and T_m. (It is possible, on the other hand, that $T \neq T_1T_m$.) From now on $\mathfrak{c}$, T_m, T_1 will be as in Lemma 4.1 and T will be the unique maximal torus of G containing T_m and T_1, unless otherwise stated. Let $W_{\mathfrak{c}} := N_{G(0)}(\mathfrak{c})/Z_{G(0)}(\mathfrak{c})$, let $G_Z^\theta = \{g \in G \mid g^{-1}\theta(g) \in Z(G)\}$ and let $W_{\mathfrak{c}}^Z := N_{G_Z^\theta}(\mathfrak{c})/Z_{G_Z^\theta}(\mathfrak{c})$. Clearly both $W_{\mathfrak{c}}$ and $W_{\mathfrak{c}}^Z$ are invariant under isogeny; $W_{\mathfrak{c}}$ embeds naturally as a subgroup of $W_{\mathfrak{c}}^Z$. In general $W_{\mathfrak{c}} \neq W_{\mathfrak{c}}^Z$: recall that θ is *saturated* if $W_{\mathfrak{c}} = W_{\mathfrak{c}}^Z$ ([Vi, Section 5]). Let $W = N_G(T)/T$. Since T is θ-stable, θ acts on W.

Lemma 4.2. *$W_{\mathfrak{c}}^Z$ (and hence $W_{\mathfrak{c}}$) embeds naturally as a subgroup of $W^\theta/Z_{W^\theta}(\mathfrak{c})$.*

Proof. Suppose $g \in G_Z^\theta$ normalizes $\mathfrak{c}$. Then g normalizes $L = Z_G(\mathfrak{c})^\circ = Z_G(T_1)$ (by Lemma 2.7) and hence $g^{-1}T_mg$ is a maximal torus of $L(0) = (L^\theta)^\circ \subset Z_{G(0)}(\mathfrak{c})$. Therefore, after replacing g by gh for suitable $h \in L(0)$, we may assume that g normalizes T_m, hence that g normalizes T. It follows that each element of $W_{\mathfrak{c}}^Z$ has a representative in W. But such a representative must clearly be in W^θ. □

In general the inclusion in Lemma 4.2 may be proper. From now on let $W_1 = W^\theta/Z_{W^\theta}(\mathfrak{c})$. It is easy to see that W_1 normalizes $\mathfrak{c}$. As before, r will denote the rank and m the order of θ. Let T_i, $i \mid d$ be the subtori of T defined in Lemma 1.10.

Lemma 4.3. *Let $T'_m = \prod_{i\neq 0} T_i = \{t^{-1}\theta(t) \mid t \in T\}$.*

(a) *Suppose $\{t \in T_m \mid t^m = 1\} \subset T'_m$. If $G^\theta = G(0)$ (if, e.g., G is semisimple and simply-connected), then $W_{\mathfrak{c}} = W_1$.*

(b) *Suppose $\{t \in T_m \mid t^m = 1\} \subset T'_m Z(G)$. Then $W^Z_{\mathfrak{c}} = W_1$.*

Proof. Let $\mathcal{T} = \{t \in T_m \mid t^m = 1\}$. We claim that $\{t \in T \mid t\theta(t)\dots\theta^{m-1}(t) = 1\} = \mathcal{T}\cdot T'_m$. Indeed, it is clear from Lemma 1.10 that $t\theta(t)\dots\theta^{m-1}(t) = 1$ for any $t \in T'_m$. Since $T = T_m \cdot T'_m$, the equality follows. Thus let $w = n_w T \in W^\theta$. Then $x = n_w^{-1}\theta(n_w) \in T$. But clearly $x\theta(x)\dots\theta^{m-1}(x) = 1$, and hence $x \in \mathcal{T}\cdot T'_m$. If $\mathcal{T} \subset T'_m$, then x is contained in the image of the map $T \to T$, $t \mapsto t^{-1}\theta(t)$. Thus $x = t\theta(t^{-1})$ for some $t \in T$ and hence $n_w t \in G^\theta$. If $G^\theta = G(0)$, it follows that $W_{\mathfrak{c}} = W_1$. (If G is semisimple and simply-connected then $G^\theta = G(0)$ by [St, 8.1].) Similarly, if $\mathcal{T} \subset T'_m Z(G)$ then $x = t\theta(t^{-1})z$ for some $t \in T$, $z \in Z(G)$ and thus $n_w t \in G^\theta_Z$. This proves (b). □

With the aid of Lemma 4.3, we now determine the little Weyl group in the case where G is one of the classical groups $\mathrm{SL}(n,k)$, $\mathrm{SO}(n,k)$, $\mathrm{Sp}(2n,k)$. Following [Vi], we call $(\mathfrak{g}, d\theta)$ associated to such a group a *classical graded Lie algebra*. One apparent problem here is that $\mathrm{SO}(n,k)$ is not simply-connected. However, the universal covering $\mathrm{Spin}(n,k) \to \mathrm{SO}(n,k)$ is separable (by the assumption that p is good) and hence any classical graded Lie algebra is the Lie algebra of a group (with automorphism) satisfying the standard hypotheses. On the other hand, all automorphisms of $\mathrm{Spin}(n,k)$ give rise to automorphisms of $\mathrm{SO}(n,k)$ unless $n = 8$. This is obvious if n is odd since then $\mathrm{SO}(n,k)$ is just the quotient of $\mathrm{Spin}(n,k)$ by its centre. Let $\widehat{T}$ be a maximal torus of $\mathrm{Spin}(2n,k)$, let $\Phi(\mathrm{Spin}(2n,k),\widehat{T})$ be identified with the root system Φ of $\mathrm{SO}(2n,k)$, let $\Delta = \{\alpha_1,\dots,\alpha_n\}$ be a basis of Φ (numbered in the standard way) and let $\alpha_i^\vee : k^\times \to \widehat{T}$ be the corresponding coroots. Let $z_0, z_1 \in \mathrm{Spin}(2n,k)$:

$$z_0 = \alpha_{n-1}^\vee(-1)\alpha_n^\vee(-1),$$

$$z_1 = \begin{cases} \alpha_1^\vee(-1)\alpha_3^\vee(-1)\dots\alpha_{n-1}^\vee(-1) & \text{if } n \text{ is even,} \\ \alpha_1^\vee(-1)\alpha_3^\vee(-1)\dots\alpha_{n-1}^\vee(i)\alpha_n^\vee(-i) & \text{if } n \text{ is odd.} \end{cases}$$

It is well known (and easy to show) that

$$Z(\mathrm{Spin}(2n,k)) = \begin{cases} \{1, z_0, z_1, z_0z_1\} \cong (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } n \text{ is even,} \\ \{1, z_1, z_1^2 = z_0, z_1^3\} \cong \mathbb{Z}/4\mathbb{Z} & \text{if } n \text{ is odd,} \end{cases}$$

and the kernel of the covering morphism $\mathrm{Spin}(2n,k) \to \mathrm{SO}(2n,k)$ is generated by z_0.

Lemma 4.4.

(a) *If $n > 4$ then any rational automorphism θ of* $\mathrm{Spin}(2n,k)$ *satisfies $\theta(z_0) = z_0$. Hence* $\mathrm{Aut}\,\mathrm{Spin}(2n,k) \cong \mathrm{Aut}\,\mathrm{SO}(2n,k) \cong \mathrm{Aut}(\mathrm{SO}(2n,k)/\{\pm I\}) \cong \mathrm{O}(2n,k)/\{\pm I\}$.

(b) $\mathrm{Aut}\,\mathrm{Spin}(8,k)/\mathrm{Int}\,\mathrm{Spin}(8,k)$ *is isomorphic to the symmetric group S_3. If θ is a rational automorphism of* $\mathrm{Spin}(8,k)$ *then either θ^2 is inner, in which case some* $\mathrm{Aut}\,\mathrm{Spin}(8,k)$*-conjugate of θ preserves z_0, or θ^3 is inner.*

(c) $\mathrm{Aut}\,\mathrm{SO}(8,k) \cong \mathrm{O}(8,k)/\{\pm I\}$.

Proof. We need only check (a) for outer automorphisms, hence for a particular choice of outer automorphism. But there exists an outer automorphism θ which satisfies $\theta(\alpha_i^\vee(t)) = \alpha_i^\vee(t)$ $(1 \leqslant i \leqslant n-2)$, $\theta(\alpha_{n-1}^\vee(t)) = \alpha_n^\vee(t)$ and $\theta(\alpha_n^\vee(t)) = \alpha_{n-1}^\vee(t)$. Hence (a) follows. One deduces (b) from the well known properties of automorphisms of reductive groups, see, e.g., [Hu, 27.4]. Finally, any automorphism of $\mathrm{SO}(8,k)$ lifts to a unique automorphism of $\mathrm{Spin}(8,k)$. But this automorphism must fix z_0, and hence by an easy check is equal to $\mathrm{Int}\, g$ for some $g \in \mathrm{O}(8,k)$. $\square$

4.1. Inner automorphisms of $\mathbf{SL}(n,k)$

For $m, r \in \mathbb{N}$ and q dividing m let $G(m,q,r)$ denote the subgroup of $\mathrm{GL}(r,k)$ consisting of all monomial matrices with entries x_i satisfying $x_i^m = 1$, $(\prod_{i=1}^r x_i)^{m/q} = 1$. Our description below of $W_\mathfrak{c}, W_\mathfrak{c}^Z, W_1$ using this notation refers to the action on $\mathfrak{c}$.

Lemma 4.5. *Let $G = \mathrm{SL}(n,k)$, $p \nmid n$ or $G = \mathrm{GL}(n,k)$ and let θ be inner. Then $W_\mathfrak{c} = W_\mathfrak{c}^Z = W_1 = G(m,1,r)$.*

Proof. Since θ is inner and stabilizes T, it equals $\mathrm{Int}\, n_w$ for some $n_w \in N_G(T)$. We can clearly assume that $n_w^m = I$. Now since T_m is maximal in $Z_G(\mathfrak{c})^\theta$, we claim that $w = n_w T$ is a product of r m-cycles. Indeed, let $w = w_m \cdot w_m'$ be the decomposition of w, where w_m is a product of m-cycles and w_m' is a product of cycles of order less than m. After reordering the indices we may assume that

$$w_m = (1 \dots m)(m+1 \dots 2m) \dots \big((r-1)m+1 \dots rm\big).$$

It is clear that we can choose a basis $\{c_1, \dots, c_r\}$ for $\mathfrak{c}$, where c_i is the diagonal matrix with jth diagonal entry: $\begin{cases} \zeta^{-j} & \text{if } (i-1)m < j \leqslant im, \\ 0 & \text{otherwise.} \end{cases}$

Let $L = Z_G(\mathfrak{c})$. It is easy to see that $L' \cong \mathrm{SL}(n-rm,k)$, that $\mathrm{Lie}(L)$ is the span of $\mathfrak{t}$ and all root subspaces $\mathfrak{g}_\alpha$ with $w_m(\alpha) = \alpha$ and that $\theta|_{L'}$ is an inner automorphism. But since $\theta|_{L'}$ is an inner automorphism of L', there exists a maximal torus of L' which is contained in $G(0)$. By our assumption $T(0)$ is a maximal torus of $L(0)$, and therefore w_m' is trivial.

With this description it is immediate that $W_1 = G(m,1,r)$. Let S be a maximal torus of L'. Since any element of W_1 has a representative in $Z_G(S)$ (hence in $Z_G(S)' \cong \mathrm{SL}(rm,k)$), we may assume that $n = rm$. Now it is clear that any element of T_m has the form

$$\begin{pmatrix} t_1 I_m & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & t_r I_m \end{pmatrix}$$

(where I_m is the $m \times m$ identity matrix and $t_1, \dots, t_r \in k^\times$), and that such an element is in $\mathcal{T}$ if and only if each t_i is a power of ζ. (Recall that ζ is a fixed primitive mth root of unity.) We therefore prove that $\mathcal{T} \subset T_m'$ in the case $r = 1$; this will make it clear that the inclusion holds for arbitrary r. If m is odd, then the matrix $s = \mathrm{diag}(\zeta^{m-1}, \zeta^{m-2}, \dots, 1)$ is of determinant 1 and satisfies $s^{-1}\theta(s) = \zeta I_m$. Hence $\mathcal{T} \subset \{t^{-1}\theta(t) \mid t \in T\} = T_m'$. If m is even, then let ξ be a square-root of ζ. Then ξs is of determinant 1 and $\xi s \theta(\xi s)^{-1} = \zeta I_m$. Thus $\mathcal{T} \subset T_m'$ in this case as well. Applying Lemma 4.3, this completes the proof. $\square$

The above result corresponds to the 'First case' in Vinberg's classification [Vi, §7].

Remark 4.6. We recall that the automorphism θ is *S-regular* if $\mathfrak{g}(1)$ contains a regular semisimple element of $\mathfrak{g}$. It can easily be seen from the proof of Lemma 4.5 that here there is a θ-stable Levi subgroup of G such that $\mathfrak{c}$ is contained in the Lie algebra of its derived subgroup L, $N_{L(0)}(\mathfrak{c})/Z_{L(0)}(\mathfrak{c}) \cong W_{\mathfrak{c}}$ and the restriction of θ to L is S-regular. We have $L \cong \mathrm{SL}(rm, k)$. In fact, $L = H'$, where H is a minimal Levi subgroup of G whose Lie algebra contains T_1. We will see in Section 5 that $\theta|_L$ is in fact N-regular, that is, $\mathfrak{l}(1)$ contains a regular nilpotent element of $\mathfrak{l}$.

4.2. Other classical types: Preparation

For the remaining classical cases, we require a little preparation. It is well known that all automorphisms of a group of type B or C are inner. While this is not true for a group of type D_n, one can (for $n > 4$) nevertheless describe all automorphisms of a Lie algebra of type D_n via elements of the orthogonal group $\mathrm{O}(n, k)$. It will therefore be useful for us to understand, for type D, not the ordinary Weyl group but its analogue in the full orthogonal group $\mathrm{O}(n, k)$, which is a Weyl group of type BC. This explains our introduction of the groups $\overline{G}$ and $\overline{W}$ in the following paragraph. Note that we assume $p \neq 2$ from now on.

Let J_n denote the $n \times n$ matrix with 1 on the antidiagonal and 0 elsewhere and let $\gamma : \mathrm{GL}(n, k) \to \mathrm{GL}(n, k)$, $g \mapsto {}^t g^{-1}$. (By abuse of notation we will use γ to denote this automorphism for arbitrary n.) In our setting, $\mathrm{O}(n, k)$ is the group of $n \times n$ matrices which are stable under $\mathrm{Int}\, J_n \circ \gamma$, $\mathrm{SO}(n, k)$ is the intersection $\mathrm{O}(n, k) \cap \mathrm{SL}(n, k)$ and $\mathrm{Sp}(2n, k)$ is the subgroup of fixed points in $\mathrm{SL}(2n, k)$ under the automorphism $\mathrm{Int} \begin{pmatrix} 0 & J_n \\ -J_n & 0 \end{pmatrix} \circ \gamma$. Until further notice G will be one of $\mathrm{SO}(2n, k)$, $\mathrm{SO}(2n + 1, k)$, $\mathrm{Sp}(2n, k)$. We will choose T to be the maximal torus of diagonal matrices in G:

$$T = \left\{ \begin{pmatrix} t_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & t_1^{-1} \end{pmatrix} \middle| \, t_1, \ldots, t_n \in k^\times \right\}.$$

For the purposes of describing the action of the Weyl group, we identify T with $(k^\times)^n$ via the isomorphism $(k^\times)^n \to T$, $t = (t_1, \ldots, t_n) \mapsto \mathrm{diag}(t_1, \ldots, t_n, t_n^{-1}, \ldots, t_1^{-1})$ (or $(t_1, \ldots, t_n) \to \mathrm{diag}(t_1, \ldots, t_n, 1, t_n^{-1}, \ldots, t_1^{-1})$ in the case $G = \mathrm{SO}(2n + 1, k)$). Let $\overline{G} = \mathrm{O}(2n, k)$ if $G = \mathrm{SO}(2n, k)$, and let $\overline{G} = G$ otherwise. Let $\overline{W} = N_{\overline{G}}(T)/T$. Then $\overline{W} \cong S_n \ltimes (\mu_2)^n \cong G(2, 1, n)$, where μ_2 is the multiplicative group $\{\pm 1\}$. (If $G = \mathrm{SO}(2n, k)$ then $W \cong G(2, 2, n)$.) Specifically, elements of S_n act as permutations $(t_1, t_2, \ldots, t_n) \mapsto (t_{\sigma(1)}, \ldots, t_{\sigma(n)})$, and $(\epsilon_1, \ldots, \epsilon_n) \in \mu_2^n$ sends $(t_1, \ldots, t_n)$ to $(t_1^{\epsilon_1}, \ldots, t_n^{\epsilon_n})$. There is a classification of the conjugacy classes in $\overline{W}$ by *signed cycle types*. That is, if $w \in \overline{W}$ is conjugate to $\sigma = \begin{pmatrix} 1 & \ldots & l \end{pmatrix} \in S_n$ (resp. to $((-1, 1, 1, \ldots, 1), \sigma) \in (\mu_2)^n \ltimes S_n$) then we say that w is a positive (resp. negative) l-cycle. A positive (resp. negative) l-cycle is of order l (resp. $2l$). Extending in the obvious way to products of disjoint cycles one can then associate a (unique) signed permutation type to each $w \in \overline{W}$. This correspondence is one-to-one between conjugacy classes in $\overline{W}$ and signed cycle types $1^{a_1}\overline{1}^{b_1}\ldots l^{a_l}\overline{l}^{b_l}$ with $\sum_{i=1}^{l} i(a_i+b_i) = n$ ([Ca, Prop. 24]). (Here i denotes a positive i-cycle and $\overline{i}$ denotes a negative i-cycle.) Let $J' = \begin{pmatrix} I_{n-1} & 0 & 0 \\ 0 & J_2 & 0 \\ 0 & 0 & I_{n-1} \end{pmatrix} \in \mathrm{O}(2n,k)$ (where I_{n-1} denotes the $(n-1)\times(n-1)$ identity matrix).

Lemma 4.7. *Any semisimple element of* $\mathrm{O}(2n,k)$ *is conjugate to an element of* $T \cup J'T$.

Proof. Since any semisimple element of $G = \mathrm{SO}(2n,k)$ is conjugate to an element of T, it will clearly suffice to show that any semisimple element of $J'G$ is conjugate to an element of $J'T$. But if $J'g$ is semisimple then $\mathrm{Int}\,(J'g)$ stabilizes a maximal torus of G and a Borel subgroup containing it. Let B be the intersection of G with the group of upper-triangular $2n \times 2n$ matrices, a Borel subgroup which contains T. Thus, after conjugating by a suitable element of G, we may assume that $J'g \in N_{\mathrm{O}(2n,k)}(T)$ and that $\mathrm{Int}\,J'g$ normalizes B. But the result is now clear, since $N_B(T) = T$ and $\overline{W}/W$ is of order 2. $\square$

Lemma 4.8. *Let G be one of* $\mathrm{SO}(2n+1,k)$, $\mathrm{SO}(2n,k)$ *or* $\mathrm{Sp}(2n,k)$ *and let m be even. Then $\theta = \mathrm{Int}\,n_w$ for $n_w \in N_{\overline{G}}(T)$. Let $w = n_wT \in \overline{W}$. If $G = \mathrm{SO}(2n+1,k)$ then w is a product of r negative $(m/2)$-cycles. Otherwise w is either a product of r positive m-cycles, a product of r negative $(m/2)$-cycles or, possibly, a product of r negative $(m/2)$-cycles and one negative 1-cycle if $m > 2$ and $G = \mathrm{SO}(2n,k)$.*

If w is a product of positive m-cycles then

$$n_w^m = \begin{cases} I & \text{if } G = \mathrm{Sp}(2n,k), \\ -I & \text{if } G = \mathrm{SO}(2n,k). \end{cases}$$

If w is a product of negative cycles then

$$n_w^m = \begin{cases} -I & \text{if } G = \mathrm{Sp}(2n,k), \\ I & \text{otherwise.} \end{cases}$$

Proof. By Lemma 4.4, any automorphism of G is of the form $\mathrm{Int}\,g$ for some $g \in \overline{G}$. Thus $\theta = \mathrm{Int}\,n_w$ for some $n_w \in N_{\overline{G}}(T)$. Suppose that $G = \mathrm{SO}(m,k)$ or $G = \mathrm{Sp}(m,k)$ and that w is a single negative $(m/2)$-cycle. Then $n_w^m = \pm I$ and the characteristic polynomial of n_w is, correspondingly, $T^m \mp I$. If $G = \mathrm{SO}(m,k)$ (resp. $G = \mathrm{Sp}(m,k)$) then $n_w \notin G$ (resp. $n_w \in G$) and hence $\det n_w = -1$ (resp. $\det n_w = 1$), from which it follows that $n_w^m = I$ (resp. $n_w^m = -I$). Suppose now that $G = \mathrm{SO}(2m,k)$ or $G = \mathrm{Sp}(2m,k)$ and that w is a single positive m-cycle. Then $n_w^m = \pm I$. Note that n_w is a monomial matrix in $\mathrm{SL}(2m,k)$ which corresponds to a product of two m-cycles. Let ξ be a square-root of ζ. Suppose that $n_w^m = I$ (resp. $n_w^m = -I$) and $G = \mathrm{SO}(2m,k)$ (resp. $G = \mathrm{Sp}(2m,k)$). Then n_w has eigenvalues ζ^i (resp. ξ^{2i+1}), $0 \leqslant i < m$, and each eigenvalue is of multiplicity two. But then n_w is G-conjugate to an element of $N_G(T)$ which acts as a product of two negative $m/2$-cycles on T, by the above. This contradicts maximality of $\mathfrak{c}$ and, therefore, $n_w^m = -I$ (resp. $n_w^m = I$) if $G = \mathrm{SO}(2m,k)$ (resp. $G = \mathrm{Sp}(2m,k)$). On the other hand, it is easy to check that if $G = \mathrm{SO}(2m,k)$ (resp. $G = \mathrm{Sp}(2m,k)$) and $g \in G$ is conjugate to $\mathrm{diag}(\xi^{2m-1}, \xi^{2m-3}, \ldots, \xi)$ (resp. $\mathrm{diag}(\zeta^{-1}, \ldots, \zeta, 1, 1, \zeta^{-1}, \ldots, \zeta)$ then $\mathrm{Int}\, g$ is a rank 1 automorphism of G.

We have therefore proved that there is a unique conjugacy class of automorphism of order m of $\mathrm{SO}(m,k)$ (resp. $\mathrm{Sp}(m,k)$, $\mathrm{SO}(2m,k)$. $\mathrm{Sp}(2m,k)$) which acts as a negative $m/2$-cycle (resp. negative $m/2$-cycle, positive m-cycle, positive m-cycle). Let us therefore consider the general case of the lemma. Let $w = w_m^+ w_m^- w_m'$, where w_m^+ is a product of r_1 positive m-cycles, w_m^- is a product of $r_2 = r - r_1$ negative $(m/2)$-cycles, and w_m' is a product of signed cycles of order less than m. (Hence $w_m' = 1$ if $m = 2$.) Let $w_m^+ = w_1 \ldots w_{r_1}$ where the w_i are disjoint positive m-cycles and let $w_m^- = w_{r_1+1} \ldots w_r$, where the w_i are disjoint negative $(m/2)$-cycles. Let $\{c_1, \ldots, c_r\}$ be a basis for $\mathfrak{c}$ such that $w_i(c_j) = \zeta^{\delta_{ij}} c_j$. It is easy to see that there exist θ-stable subgroups $L_1, \ldots, L_r$ of $\overline{G}$ such that $c_i \in \mathrm{Lie}(L_i)$ and

$$L_i \cong \begin{cases} \mathrm{O}(m,k) & \text{if } G = \mathrm{SO}(n,k) \text{ and } 1 \leqslant i \leqslant r_1, \\ \mathrm{O}(2m,k) & \text{if } G = \mathrm{SO}(n,k) \text{ and } r_1 + 1 \leqslant i \leqslant r, \\ \mathrm{Sp}(m,k) & \text{if } G = \mathrm{Sp}(2n,k) \text{ and } 1 \leqslant i \leqslant r_1, \\ \mathrm{Sp}(2m,k) & \text{if } G = \mathrm{Sp}(2n,k) \text{ and } r_1 + 1 \leqslant i \leqslant r. \end{cases}$$

Then $\theta|_{L_i} = \mathrm{Int}\, x_i$ for some $x_i \in L_i$ and $x_i^m = \pm I$ according to the criteria given in the paragraph above. Thus $n_w = x_1 z$, where $z \in Z_{\overline{G}}(L_1)$. But then if $r_1 > 0$, $n_w^m = x_1^m z^m$, and therefore $n_w^m = -I$ (resp. I) if G is of orthogonal (resp. symplectic) type. Similarly, if $r_2 > 0$ then $n_w = x_r z$ for $z \in Z_G(L_r)$) and therefore $n_w^m = I$ (resp. $-I$) if G is of orthogonal (resp. symplectic) type. It follows that either $r_1 = 0$ or $r_2 = 0$, and if $G = \mathrm{SO}(2n+1,k)$ then w is a product of negative cycles. Moreover, $n_w \prod_1^r x_i^{-1} \in Z_{\overline{G}}(\mathfrak{c})$ and represents w_m' as an element of $\overline{W}$. Thus w_m' is trivial if $G = \mathrm{Sp}(2n,k)$ or $G = \mathrm{SO}(2n+1,k)$ and, by Lemma 4.7, w_m' is either trivial or a single negative 2-cycle if $G = \mathrm{SO}(2n,k)$. On the other hand, if w_m' is a negative 2-cycle then clearly $n_w^m = I$ and thus w is a product of negative cycles. □

4.3. Type *C*

Lemma 4.9. *Let $G = \mathrm{Sp}(2n,k)$.*

(a) *If m is odd then $W_\mathfrak{c} = W_\mathfrak{c}^Z = W_1 = G(2m,1,r)$.*
(b) *If m is even then $W_\mathfrak{c} = W_\mathfrak{c}^Z = W_1 = G(m,1,r)$.*

Proof. Since any automorphism of G is inner, $\theta = \mathrm{Ad}\, n_w$ for some $n_w \in N_G(T)$. If m is odd, then $w = n_w T$ is a product of r positive m-cycles by the argument in Lemma 4.8. After conjugating by a suitable element of $N_G(T)$, we may assume that

$$w = (1 \ldots m)(m+1 \ldots 2m) \ldots \big((r-1)m+1 \ldots rm\big).$$

We can construct a basis $\{c_1, \dots, c_r\}$ for $\mathfrak{c}$ in the same way as in the proof of Lemma 4.5. Then it is immediate that $W_1 = G(2m, 1, r)$. Let S be a θ-stable maximal torus of $Z_G(\mathfrak{c})'$. Then any element of W_1 has a representative in $Z_G(S)$, and hence in $Z_G(S)' \cong \mathrm{Sp}(2rm, k)$. Thus we may assume that $n = rm$. As in the proof of Lemma 4.5, it will clearly suffice to prove that $\mathcal{T} \subset T'_m$ in the case $r = 1$. Here T_m consists of matrices of the form $\begin{pmatrix} tI_m & 0 \\ 0 & t^{-1}I_m \end{pmatrix}$. But if $t = \mathrm{diag}(\zeta^{m-1}, \zeta^{m-2}, \dots, \zeta, 1, 1, \zeta^{-1}, \dots, \zeta^2, \zeta)$ then $t^{-1}\theta(t) = \begin{pmatrix} \zeta I_m & 0 \\ 0 & \zeta^{-1}I_m \end{pmatrix}$. By Lemma 4.3, $W_\mathfrak{c} = W_1$.

For (b), Lemma 4.8 shows that w is either a product of r positive m-cycles or a product of r negative $m/2$-cycles. It is easy to see by a similar argument to that used above that $W_1 = G(m, 1, r)$ in either case. Let S be a θ-stable maximal torus of $Z_G(\mathfrak{c})'$: then $Z_G(S)'$ is θ-stable, isomorphic to $\mathrm{Sp}(2mr, k)$ (if w is a product of positive m-cycles) or $\mathrm{Sp}(mr, k)$ (if w is a product of negative $(m/2)$-cycles) and contains T_1 and a representative of each element of W_1. Hence it will suffice to prove the equality $W_\mathfrak{c} = W_1$ in the case $n = mr$ (w a product of positive m-cycles), $n = mr/2$ (w a product of negative $(m/2)$-cycles). For this we apply Lemma 4.3. If w is a product of positive m-cycles then after conjugating by a suitable element of $N_G(T)$ we may assume that $w = (1 \dots m) \dots \big((r-1)m + 1 \dots rm\big)$. In these circumstances T_m is the set of matrices of the form

$$\begin{pmatrix} t_1 I_m & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & t_1^{-1} I_m \end{pmatrix}$$

where $t_1, \dots, t_r \in k^\times$. Such an element is in $\mathcal{T}$ if and only if t_i is a power of ζ for each $1 \leqslant i \leqslant r$. The inclusion $\mathcal{T} \subset T'_m$ can now be proved in exactly the same way as in Lemma 4.5. On the other hand, if w is a product of negative $(m/2)$-cycles then it is easy to see that T_m is trivial. □

In Vinberg's classification [Vi, §7], this is the 'Third case': m odd is Type III; m even, w a product of negative $(m/2)$-cycles is Type I, and m even, w a product of positive m-cycles is Type II.

Remark 4.10. As for inner automorphisms in type A, it is easy to see from the proof of Lemma 4.9 that there is a θ-stable Levi subgroup of G such that $\mathfrak{c}$ is contained in the Lie algebra of its derived subgroup L, $N_{L(0)}(\mathfrak{c})/Z_{L(0)}(\mathfrak{c}) \cong W_\mathfrak{c}$ and $\theta|_L$ is S-regular. We have $L \cong \mathrm{Sp}(rm, k)$ if m is even and w is a product of negative $(m/2)$-cycles, $L \cong \mathrm{SL}(rm, k)$ if m is even and w is a product of positive m-cycles and $L \cong \mathrm{Sp}(2rm, k)$ if m is odd. (If m is even and w is a product of positive m-cycles then we can easily reduce to a subgroup isomorphic to $\mathrm{Sp}(2rm, k)$ whose Lie algebra contains $\mathfrak{c}$. But now any element of $\mathfrak{c}$ is fixed by γ (defined after Remark 4.6) and we can see by Lemma 4.5 that the little Weyl group for the restriction of θ to $G^\gamma \cong \mathrm{GL}(rm, k)$ is $G(m, 1, r)$. Here we restrict to $\mathrm{SL}(rm, k)$ in order to ensure N-regularity.) In common with type A, L is the derived subgroup of a Levi subgroup H of G, and H is a minimal Levi subgroup whose derived subgroup contains T_1.

4.4. Type B

Lemma 4.11. *Let G be semisimple of type B_n.*

(a) *If m is odd then $W_{\mathfrak{c}} = W_1 = G(2m, 1, r)$.*
(b) *If m is even then $W_{\mathfrak{c}} = W_1 = G(m, 1, r)$.*

Proof. Let $G = \mathrm{SO}(2n+1, k)$. While it is practical to work with $\mathrm{SO}(2n+1, k)$, things are slightly more difficult than for $\mathrm{Sp}(2n, k)$ since centralizers are not in general connected. If m is odd, on the other hand, we claim that G^θ is connected. Indeed, since all rational automorphisms of G are inner, $\theta = \mathrm{Ad}\, n_w$ for some $n_w \in N_G(T)$. Let $\pi : \widehat{G} = \mathrm{Spin}(2n+1, k) \to G$ be the universal covering of G and let $\widehat{n}_w \in \widehat{G}$ be such that $\pi(\widehat{n}_w) = n_w$. Since the kernel of π is just $Z(\widehat{G})$, G^θ is disconnected if and only if there exists $x \in \widehat{G}$ such that $x^{-1}\widehat{n}_w x \widehat{n}_w^{-1}$ is the nonidentity element of $Z(\widehat{G})$. But $x^{-1}\widehat{n}_w x \widehat{n}_w^{-1} \in \{h \in \widehat{G} \mid h\theta(h)\ldots\theta^{m-1}(h) = 1\}$ and hence $(x^{-1}\widehat{n}_w x \widehat{n}_w^{-1})^m = 1$. Thus $G^\theta = G(0)$ if m is odd. Since $w = n_w T$ contains r positive m-cycles, it is straightforward to check that $Z_G(\mathfrak{c}) \cong (k^\times)^{rm} \times \mathrm{SO}(2(n-rm)+1, k)$. Applying the argument in the proof of Lemma 4.9 and Lemma 4.3(a), we deduce that w is a product of r positive m-cycles and that $W_1 = W_{\mathfrak{c}} = G(2m, 1, r)$.

Suppose therefore that m is even. By Lemma 4.8, $\theta = \mathrm{Int}\, n_w$, where $n_w^m = I$ and $w = n_w T$ is a product of r negative $(m/2)$-cycles. Using the same argument as in Lemma 4.5, it follows that $W_1 = G(m, 1, r)$. Let S be a θ-stable maximal torus of $Z_G(\mathfrak{c})' \cong \mathrm{SO}(2n+1-rm, k)$ and let $L = Z_G(S)'$. Then it is easy to see that $L \cong \mathrm{SO}(rm+1, k)$, that $\mathfrak{c} \subset \mathrm{Lie}(L)$ and that any element of W_1 has a representative in L. Hence it will suffice to prove (b) under the assumption that $n = rm/2$. But now T_m is trivial. Lifting θ (uniquely) to an automorphism of the universal covering $\widehat{G}$ of G (Lemma 1.8), we can apply Lemma 4.3. □

This is half of Vinberg's ‘Second case’ (the other half being $\mathrm{SO}(2n, k)$): m even, w a product of negative $m/2$-cycles is Type I; m odd is Type III. (Type II, where m is even and w is a product of positive m-cycles does not occur by Lemma 4.8.)

Remark 4.12. Once again, it is clear from the proof of Lemma 4.11 that if H is a minimal Levi subgroup of G whose derived subgroup L contains T_1 then $N_{L(0)}(\mathfrak{c})/Z_{L(0)}(\mathfrak{c}) \cong W_{\mathfrak{c}}$ and $\theta|_L$ is S-regular. We have $L \cong \mathrm{SO}(rm+1, k)$ if m is even and w is a product of negative $(m/2)$-cycles, and $L \cong \mathrm{SO}(2rm+1, k)$ if m is odd.

4.5. Type D

Lemma 4.13. *Let $G = \mathrm{SO}(2n, k)$. Then $\theta = \mathrm{Int}\, n_w$ for some $n_w \in N_{\mathrm{O}(2n,k)}(T)$.*

(a) *If m is odd then:*

(i) $$W_1 = \begin{cases} G(2m, 1, r) & \text{if } n > mr, \\ G(2m, 2, r) & \text{if } n = mr. \end{cases}$$

(ii) $W_{\mathfrak{c}}^Z = W_{\mathfrak{c}} = \begin{cases} G(2m,1,r) & \textit{if } n > mr \textit{ and } Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta \neq Z_G(\mathfrak{c})^\theta, \\ G(2m,2,r) & \textit{otherwise.} \end{cases}$

(b) *If m is even and $n_w^m = -I$, then $W_{\mathfrak{c}} = W_1 = G(m,1,r)$. If m is even and $n_w^m = I$, then*

(i) $W_1 = \begin{cases} G(m,1,r) & \textit{if } n > mr/2, \\ G(m,2,r) & \textit{if } n = mr/2. \end{cases}$

(ii) $W_{\mathfrak{c}}^Z = W_{\mathfrak{c}} = \begin{cases} G(m,1,r) & \textit{if } n > mr/2 \textit{ and } Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta \neq Z_G(\mathfrak{c})^\theta, \\ G(m,2,r) & \textit{otherwise.} \end{cases}$

Proof. Suppose m is odd. Then the kernel of the universal covering $\mathrm{Spin}(2n,k) \to G$ contains two elements and, hence, we can apply the argument from Lemma 4.11 to deduce that $G^\theta = G(0)$. Since $Z(G)$ also has two elements, we can apply the same argument to the map $G \to G/Z(G)$ to deduce that $G_Z^\theta = G(0)$. Since $\mathrm{O}(2n,k)/G$ has order 2, clearly $n_w \in G$. Moreover, $w = n_w T$ contains r positive m-cycles and hence it is straightforward to check that $Z_G(\mathfrak{c}) \cong (k^\times)^{mr} \times \mathrm{SO}(2(n-mr),k)$. Since any odd-order automorphism of $\mathrm{SO}(2(n-mr),k)$ is inner, it follows by our choice of T_m that w is equal to a product of r positive m-cycles. After conjugating by a suitable element of $N_G(T)$, we may assume that

$$w = (1 \dots m) \dots \big((m-1)r + 1 \dots mr\big).$$

Thus let c_i, $1 \leqslant i \leqslant r$, be the diagonal matrix with jth entry

$$\begin{cases} \zeta^{-j} & \text{if } (i-1)m < j \leqslant im, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\{c_1, \dots, c_r\}$ is a basis for $\mathfrak{c}$, and the description of W_1 follows immediately. We claim first of all that $W_{\mathfrak{c}} \supset G(2m,2,r)$. For this we may clearly assume that $n = mr$. But now we can apply the argument in Lemma 4.5 to show that $\mathcal{T} \subset T'_m$ and, hence, by Lemma 4.3, $W_{\mathfrak{c}} = W_1$. This proves (a) if $n = mr$. Suppose therefore that $n > mr$. Since an element of $N_{\mathrm{O}(2m,k)}(T)$ which corresponds to a product of m negative 1-cycles in $\overline{W}$ has determinant (-1), it is easy to see that an element of W_1 which acts as -1 on c_1 and 1 on all c_i, $i \geqslant 2$ has a representative in $W_{\mathfrak{c}}$ if and only if $Z_{\mathrm{O}(n,k)}(\mathfrak{c})^\theta$ contains an element of determinant -1. This proves (a).

Suppose therefore that m is even. By Lemma 4.8, $\theta = \mathrm{Int}\, n_w$, where $n_w \in N_{\mathrm{O}(2n,k)}(T)$ and $w = n_w T \in \overline{W}$ is either a product of r positive m-cycles, a product of r negative $m/2$-cycles, or a product of r negative $m/2$-cycles and one negative 1-cycle. Constructing a basis for $\mathfrak{c}$ as above, it is easy to see that $W_1 = G(m,1,r)$ unless $n = mr/2$ and w is a product of r negative $(m/2)$-cycles, in which case $W_1 = G(m,2,r)$. If w is a product of positive m-cycles then $n_w^m = -I$ and hence θ is $\mathrm{Aut}\, G$-conjugate to $\mathrm{Int}\, t$ for a diagonal matrix t with entries of the form ξ^l, where ξ is a square-root of ζ and l is odd. It follows that G^θ is isomorphic to a product of subgroups of the form $\mathrm{GL}(r_i)$ $(r_i \geqslant r)$, and hence is connected. Thus we can apply Lemma 4.3 in this case. Reducing to the case $n = mr$, the argument in the proof of Lemma 4.5 shows that $W_{\mathfrak{c}} = W_1$.

For the case $n_w^m = I$, G^θ has two irreducible components and therefore we cannot apply Lemma 4.3 directly. We claim first of all that $W_{\mathfrak{c}} \supset G(m,2,r)$. For this, we can clearly reduce to the case $n = mr/2$. But now T_m is trivial and, hence, we can lift θ to an automorphism of $\mathrm{Spin}(2n,k)$ (by Lemma 1.8) and apply Lemma 4.3. Thus there remains only the case $n > mr/2$ to deal with. As for the case of m odd above, we associate a vector $c_i \in \mathfrak{c}$ to each negative $m/2$-cycle w_i in the expression for w such that $w_i(c_j) = \zeta^{\delta_{ij}} c_j$; then $\{c_i : 1 \leqslant i \leqslant r\}$ forms a basis for $\mathfrak{c}$. Let L_1 and $x_1 \in L_1$ be as in the proof of Lemma 4.8. Then x_1 normalizes T and corresponds to w_1. Conjugating x_1 by a suitable element of T, we may assume that $\theta(x_1) = x_1$. Let $\overline{w}_1$ be the image of w_1 in W_1. Clearly x_1 has determinant (-1), hence $\overline{w}_1$ has a representative in G^θ if and only if there is some element of $Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta$ of determinant (-1). This proves that $W_{\mathfrak{c}} = G(m,2,r)$ if $Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta = Z_G(\mathfrak{c})^\theta$. But suppose there exists some $g \in Z_{\mathrm{O}(2n,k)}(\mathfrak{c})$ such that $gx_1 \in G_Z^\theta$. Then $gx_1\theta(gx_1)^{-1} = g\theta(g^{-1})$. Since it is evidently impossible that $g\theta(g^{-1}) = -I$, $W_{\mathfrak{c}}^Z = W_{\mathfrak{c}}$.

Suppose therefore that there exists some element $h \in Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta \setminus Z_G(\mathfrak{c})^\theta$. We note that $H = Z_G(\mathfrak{c})' \cong \mathrm{SO}(2n - rm, k)$. Replace h by its semisimple part, which is also in $Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta \setminus Z_G(\mathfrak{c})^\theta$. Thus by Lemma 4.7, after multiplying h by some element of H we may assume that h normalizes T and acts on $T \cap H$ as a single negative 1-cycle. Then $L = Z_G(h)^\circ$ is θ-stable, isomorphic to $\mathrm{SO}(2n-1,k)$, and $\mathrm{Lie}(L)$ contains $\mathfrak{c}$. Moreover, it is easy to see that θ acts on $T \cap L$ as a product of r negative $(m/2)$-cycles. Hence $N_{L(0)}(\mathfrak{c})/Z_{L(0)}(\mathfrak{c}) \cong G(m,1,r)$ by Lemma 4.11. We deduce that each element of W_1 has a representative in $L(0) \subset G(0)$. □

This is the rest of Vinberg's 'Second class', m even, w a product of negative cycles is Type I; m even, w a product of positive m-cycles is Type II; m odd is Type II.

Remark 4.14. (a) Our condition on $Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta$ in Lemma 4.13(a)(ii) is equivalent to the condition given in [Vi]. There Vinberg determines the properties of an automorphism of $\mathrm{SO}(2n,k)$ of the form $\mathrm{Int}\, g$ by considering the eigenvalues of g. Note that $g^m = \pm I$; let $\mathcal{S}$ be the set of mth roots of 1 (resp. -1) if $g^m = I$ (resp. $-I$). Suppose $\theta = \mathrm{Int}\, n_w$ is of odd order. After replacing n_w by $-n_w$, if necessary, we may assume that $n_w^m = I$ and hence that $\mathcal{S} = \{\zeta^i : i \in \mathbb{Z}\}$. Here r is the integer part of half the minimum multiplicity of an eigenvalue of g. Vinberg's condition for $W_{\mathfrak{c}}$ to be equal to $G(2m,2,r)$ is that the multiplicity of 1 is exactly equal to $2r$. Let the multiplicity of ζ^i be $(2r+s_i) = (2r+s_{m-i})$. Let $L = Z_G(\mathfrak{c})' \cong \mathrm{SO}(2(n-rm),k)$; then it is easy to see that $Z_L(n_w) \cong \prod_{i=1}^{(m-1)/2} \mathrm{GL}(s_i,k) \times \mathrm{SO}(s_0,k)$ and, hence, that there is some element of $Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta \setminus Z_G(\mathfrak{c})^\theta$ if and only if $s_0 > 0$. Similarly, if m is even and $n_w^m = I$ (Type I) then Vinberg's condition for $W_{\mathfrak{c}}$ to be equal to $G(m,2,r)$ is that the multiplicity of both 1 and -1 in n_w is equal to r; this is equivalent to the condition in Lemma 4.13(b)(ii).

(b) In Remarks 4.6, 4.10 and 4.12 we pointed out that if H is a minimal Levi subgroup of G whose derived subgroup L contains T_1 then any element of $W_{\mathfrak{c}}$ has a representative in $L(0)$ and $\theta|_L$ is S-regular. In fact, in each of those cases the restriction $\theta|_L$ is also N-regular, that is, $\mathfrak{g}(1)$ contains a regular nilpotent element of $\mathfrak{g}$. (This will be proved in Section 5.) While here we can always find some Levi subgroup such that the restriction of θ to the derived subgroup L is S-regular, it is not in general true that $\theta|_L$ is N-regular. In addition, not every element of $W_{\mathfrak{c}}$ has a representative in L. The exceptions are the cases (i) m is odd and $W_{\mathfrak{c}} = G(2m, 1, r)$ and (ii) m is even, w is a product of negative cycles and $W_{\mathfrak{c}} = G(m, 1, r)$. On the other hand, in the second case there is a reductive subgroup which contains $\mathfrak{c}$ in the right way. To see this, let $L = Z_G(h)^\circ \cong \mathrm{SO}(2n-1, k)$ be as constructed in the final paragraph of the proof of Lemma 4.13. We can then reduce further to a subgroup isomorphic to $\mathrm{SO}(rm+1, k)$, see Remark 4.12. In fact there is a similar construction for the first case as well: let $h \in Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta \backslash Z_G(\mathfrak{c})^\theta$, which we can assume to be semisimple, to normalize T and to act on $Z_G(\mathfrak{c})' \cap T$ as a single negative 1-cycle by the same argument as at the end of the proof above. Then we also have $Z_G(h)^\circ \cong \mathrm{SO}(2n-1, k)$, $\mathfrak{c} \subset \mathfrak{g}^h$ and each element of $W_{\mathfrak{c}}$ has a representative in $Z_G(h)^\circ(0)$. Thus we can take L to be the subgroup of $Z_G(h)^\circ$ constructed as in Remark 4.12. Here we have $L \cong \mathrm{SO}(2rm+1, k)$. For the other cases we can take L to be H', where H is the minimal Levi subgroup of G whose derived subgroup contains T_1. If m is odd and $W_{\mathfrak{c}} = G(2m, 2, r)$ then we have $L \cong \mathrm{SO}(2rm, k)$; if m is even and w is a product of positive m-cycles (that is, $n_w^m = -I$) then $L \cong \mathrm{SL}(rm, k)$; if m is even, $n_w^m = I$ and $W_{\mathfrak{c}} = G(m, 2, r)$ then $L \cong \mathrm{SO}(rm, k)$.

4.6. Outer automorphisms of $\mathrm{SL}(n, k)$

Before we complete the final (classical) case, we require a preparatory lemma. Let $\gamma : \mathrm{SL}(n, k) \to \mathrm{SL}(n, k)$, $g \mapsto {}^t g^{-1}$ and let $\psi = \mathrm{Int}\, J_n \circ \gamma$. (Hence $\psi(T) = T$ and $G^\psi = \mathrm{SO}(n, k)$.) Let $T_+ = \{t \in T \mid \psi(t) = t\}^\circ$ and let $T_- = \{t \in T \mid \psi(t) = t^{-1}\}^\circ$.

Lemma 4.15. *Let $G = \mathrm{SL}(n, k)$, $n > 2$, $\mathrm{char}\, k \neq 2$.*

(a) *Any semisimple outer automorphism of G is conjugate to one of the form $\mathrm{Int}\, t \circ \psi$, where $t \in T_+$.*

(b) *Two semisimple outer automorphisms $\theta = \mathrm{Int}\, g \circ \gamma$, $\sigma = \mathrm{Int}\, h \circ \gamma$ of G are $\mathrm{Int}\, G$-conjugate if and only if $g\gamma(g)$ and $h\gamma(h)$ are G-conjugate.*

Proof. By Steinberg's result on semisimple automorphisms [St, 7.5] any semisimple outer automorphism θ of G stabilizes a maximal torus of G and a Borel subgroup containing it. After conjugation we may therefore assume that $\theta(T) = T$ and $\theta(B) = B$, where B is the group of upper triangular matrices of determinant 1. Since θ is outer, it follows at once that $\theta = \mathrm{Int}\, t \circ \psi$ for some $t \in T$. Moreover, if $s \in T_-$ then $\mathrm{Int}\, s \circ \psi \circ \mathrm{Int}\, s^{-1} = \mathrm{Int}\, s^2 \circ \psi$. Thus we may assume that $t \in T_+$. This proves (a). For (b), suppose θ and σ are conjugate. Then $xg\gamma(x^{-1}) = \xi^{-2} h$ for some $x \in G$, $\xi \in k^\times$. Thus $(\xi x) g \gamma((\xi x)^{-1}) = h$, hence we may assume that $\xi = 1$. It follows that $xg\gamma(g)x^{-1} = h\gamma(h)$. Suppose, on the other hand, that $g\gamma(g)$ and $h\gamma(h)$ are conjugate. After conjugating by inner automorphisms of G if necessary we may assume by (a) that $g, h \in T_+$. But now $g\gamma(g) = g^2$ and $h\gamma(h) = h^2$, and with these assumptions g^2 and h^2 are in fact $\mathrm{O}(n, k)$-conjugate. Now it is easy to see that $g = sh$ for some $s \in T_+ \cap T_-$. Thus θ is $\mathrm{Int}\, G$-conjugate to σ. $\square$

Lemma 4.16.

(a) *Let $G = \mathrm{GL}(l, k)$ and let $g \in N_G(T)$ represent an l-cycle in W. Then there is $t \in T$ such that all but one of the nonzero entries of $tg\gamma(t^{-1})$ is equal to* 1.

(b) *Suppose g is as in* (a)*, that all but one of the nonzero entries of g is equal to 1 and that l is even. Then the remaining entry is $-\det g$ and $(g\gamma(g))^{l/2}$ is a diagonal matrix with $l/2$ entries equal to $-\det g$ and $l/2$ entries equal to $-1/\det g$.*

Proof. A straightforward calculation. □

Note that if in Lemma 4.16(a) all of the nonzero entries of g are equal to ± 1 then $\gamma(g) = g$. This observation will be useful in the proof of Lemma 4.19 below.

Lemma 4.17. *Suppose $G = \mathrm{SL}(n, k)$ and θ is outer. Then $\theta = \mathrm{Int}\, n_w \circ \gamma$ for some $n_w \in N_G(T)$.*

(a) *If $m/2$ is even then $w = n_w T$ is a product of r m-cycles and $[(n - rm)/2]$ 2-cycles.*

(b) *If $m/2$ is odd then either:*
  (i) *$(n_w\gamma(n_w))^{m/2} = -I$ and w is a product of r m-cycles and $[(n - rm)/2]$ 2-cycles, or;*
  (ii) *$(n_w\gamma(n_w))^{m/2} = I$ and w is a product of r $(m/2)$-cycles and $[(n - rm/2)/2]$ 2-cycles.*

Proof. Since $\mathrm{Aut}\, G$ is generated over $\mathrm{Int}\, G$ by γ, clearly $\theta = \mathrm{Int}\, n_w \circ \gamma$ for some $n_w \in N_G(T)$. If $m/2$ is even then $w = w_m \cdot w'_m$, where w_m is a product of r m-cycles and w'_m is a product of cycles of length less than m. Since γ acts trivially on W, we may conjugate θ by $\mathrm{Int}\, g$ for a suitable element $g \in N_G(T)$ such that

$$w_m = (1 \ldots m) \ldots \big((r-1)m + 1 \ldots rm\big).$$

Hence $\mathfrak{c}$ has a basis $\{c_i \mid 1 \leqslant i \leqslant r\}$, where c_i is the matrix with jth diagonal entry:

$$\begin{cases} (-\zeta)^{-j} & \text{if } (i-1)m < j \leqslant im, \\ 0 & \text{otherwise.} \end{cases}$$

Since $m/2$ is even, the $(-\zeta)^{-j}$ are distinct for distinct $j \in \mathbb{Z}/m\mathbb{Z}$ and hence $Z_G(\mathfrak{c}) \cong (k^\times)^{rm-1} \times \mathrm{GL}(n - rm, k)$. Now $L = Z_G(\mathfrak{c})' \cong \mathrm{SL}(n - rm, k)$ and, hence, by Lemma 4.15, $\mathrm{Int}\, n_w$ acts on $T \cap L$ as a product of $[(n - rm)/2]$ 2-cycles. This proves (a).

Let $m/2$ be odd. If $g \in \mathrm{GL}(m/2, k)$ represents an $m/2$-cycle then $(g\gamma(g))$ also represents an $m/2$-cycle and is of determinant 1, hence (since $m/2$ is odd) $(g\gamma(g))^{m/2} = (\det g\gamma(g))I_{m/2} = I_{m/2}$. Returning to the general case, $w = w_m \cdot w_{m/2} \cdot w'_m$, where w_m is a product of r_1 m-cycles, $w_{m/2}$ is a product of $r_2 = r - r_1$ $(m/2)$-cycles, and w'_m is a product of cycles of length less than $m/2$. Write $w_m = w_1 \ldots w_{r_1}$ and $w_{m/2} = w_{r_1+1} \ldots w_r$ and let $c_i \in \mathfrak{c}$ be such that $w_i(c_j) = (-\zeta)^{\delta_{ij}} c_j$. Suppose, $r_2 > 0$: we claim that $(n_w\gamma(n_w))^{m/2} = I$. Indeed, we can easily construct a θ-stable subgroup L_r of G which is isomorphic to $\mathrm{SL}(m/2, k)$ and such that $c_r \in \mathrm{Lie}(L_r)$. Then since $\theta|_{L_r} = \mathrm{Int}\, n_r \circ \gamma$, where $n_r \in L_r$ and $(n_r\gamma(n_r))^{m/2} = I_{m/2}$, we must have $\theta = \mathrm{Int}\, xn_r \circ \gamma$, where $x \in Z_G(L_r)$ and therefore $(xn_r\gamma(xn_r))^{m/2} = (x\gamma(x))^{m/2}$ must be equal to the identity matrix. Suppose on the other hand that w_m is nontrivial. We claim that in this case

$(n_w\gamma(n_w))^{m/2} = -I$. It will clearly suffice to prove this claim when $r = r_1 = 1$ and $n = m$. In this case $n_w\gamma(n_w)$ represents a product of two $(m/2)$-cycles in $N_G(T)$. Thus $(n_w\gamma(n_w))^{m/2} = \pm I$ by Lemma 4.16(b). But if $(n_w\gamma(n_w))^{m/2} = I$ then $n_w\gamma(n_w)$ is conjugate to $\mathrm{diag}(\zeta^{m-1}, \zeta^{m-1}, \zeta^{m-2}, \ldots, 1)$ and therefore by Lemma 4.15(b) θ is conjugate to an automorphism $\mathrm{Int}\, g \circ \gamma$ for some $g \in N_G(T)$ which acts on T as a product of two $(m/2)$-cycles. Since in this case the rank of θ is 2, this contradicts the assumption that $\mathfrak{c}$ is maximal. Thus either $w = w_m \cdot w'_m$ or $w = w_{m/2} \cdot w'_m$. In either case one can apply the argument used in the first paragraph to show that w'_m is a product of 2-cycles as indicated in the lemma. □

Remark 4.18. (a) If $m/2$ is odd and w is a product of r m-cycles and $[(n - rm)/2]$ 2-cycles, the argument in the first part of the proof shows that $Z_G(\mathfrak{c})' = (\mathrm{SL}(2,k)^{m/2})^r \times \mathrm{SL}(n-rm,k)$. It is an easy exercise to check in this case that the condition $(n_w\gamma(n_w))^{m/2} = -I$ implies that θ acts as a zero rank automorphism on the part which is isomorphic to $(\mathrm{SL}(2,k)^{m/2})^r$.

(b) In Vinberg's classification, this is the Fourth case: $m/2$ even is Type III; $m/2$ odd, w a product of m-cycles and 2-cycles is Type II, and $m/2$ odd, w a product of $(m/2)$-cycles and 2-cycles is Type I.

We recall that an automorphism of $\mathrm{SL}(n,k)$ has a unique extension to an automorphism of $\mathrm{GL}(n,k)$ unless $n = 2$ ([L2, Lemma 1.4(ii)]). In the following lemma, we abuse notation and use θ to denote the automorphism of $\mathrm{GL}(n,k)$ induced by the action of θ on $\mathrm{SL}(n,k)$. (This only appears here for $n > 2$ unless θ is of zero rank.)

Lemma 4.19. *Let $G = \mathrm{SL}(n,k)$ and let θ be outer.*

(a) *If $m/2$ is odd then $W_\mathfrak{c} = W_\mathfrak{c}^Z = W_1 = G(m/2,1,r)$.*
(b) *If $m/2$ is even then $\theta = \mathrm{Int}\, n_w \circ \gamma$ where $n_w \in N_G(T)$. We have $W_\mathfrak{c}^Z = W_1 = G(m,1,r)$ and*

$$W_\mathfrak{c} = \begin{cases} G(m,1,r) & \text{if } (n_w\gamma(n_w))^{m/2} = -I \text{ or } n > mr \\ & \text{and } Z_{\mathrm{GL}(n,k)}(\mathfrak{c})^\theta \neq Z_G(\mathfrak{c})^\theta, \\ G(m,2,r) & \text{otherwise.} \end{cases}$$

Proof. Suppose first of all that $m/2$ is odd. By Lemma 4.17, $\theta = \mathrm{Int}\, n_w \circ \gamma$, where $w = n_wT$ is either a product of r m-cycles and $[(n-rm)/2]$ 2-cycles, or a product of r $(m/2)$-cycles and $[(n-rm/2)/2]$ 2-cycles. After conjugation we may assume that $w = w_m \cdot w_2$, where

$$w_m = \begin{cases} (1\ldots m)\ldots\big((r-1)m+1\ldots rm\big) & \text{if } (n_w\gamma(n_w))^{m/2} = I, \\ (1\ldots m/2)\ldots\big((r-1)m/2+1\ldots rm/2\big) & \text{if } (n_w\gamma(n_w))^{m/2} = -I. \end{cases}$$

We can therefore choose a basis $\{c_1, \ldots, c_r\}$ for $\mathfrak{c}$: let c_i be the diagonal matrix with jth entry equal to $\begin{cases} (-\zeta)^{-j} & \text{if } (i-1)m' < j \leqslant im', \\ 0 & \text{otherwise,} \end{cases}$ where $m' = m$ if w_m is a product of m-cycles, and $m' = m/2$ if w_m is a product of $m/2$-cycles. With this description it is clear that $W_1 = G(m/2,1,r)$ in either case. It will therefore suffice to prove that $W_1 = W_{\mathfrak{c}}$ when $n = mr$ for the first case, or $n = mr/2$ for the second. The second case is a trivial application of Lemma 4.3 since here T_m is trivial. Hence suppose $n = mr$ and w is a product of r m-cycles. It follows from Lemma 4.16 that after conjugating we may assume $\gamma(n_w) = n_w$. (This is no longer true if $n > rm$.) But then $n_w^{m/2} \in G^\theta$, $\mathrm{Ad}\, n_w^{m/2}$ is trivial on $\mathfrak{c}$ and $L = Z_{\mathrm{GL}(n,k)}(n_w^{m/2}) = L_1 \times L_2$, where $L_1 \cong L_2 \cong \mathrm{GL}(rm/2, k)$. Since $n_w^m = -I$, $n_w^{m/2}$ defines a nondegenerate skew-symmetric form on k^n and hence $H = G^{\mathrm{Int}\, n_w^{m/2} \circ \gamma} \cong \mathrm{Sp}(rm, k)$. Thus $H^\gamma = L^\gamma \cong \mathrm{GL}(rm/2, k)$. We deduce that $\theta|_L$ maps L_1 isomorphically onto L_2 and vice versa. We shall show that the little Weyl group for $\theta|_L$ is equal to $G(m/2, 1, r)$, hence the same is true for G by the description of W_1 above. But here it is easy to see that the little Weyl group for $\theta|_L$ is isomorphic to the little Weyl group for $\theta^2|_{L_1}$. We have $n_w \in L$ and therefore we can define the projection of n_w^2 onto L_1. Then, since n_w is conjugate to a diagonal matrix with r entries equal to ξ^{2i-1} for each $i \in \mathbb{Z}/m\mathbb{Z}$ (where ξ is a square-root of ζ), the projection of n_w^2 onto L_1 is conjugate to a diagonal matrix with r entries equal to ζ^{2i+1} for each i, $0 \leqslant i \leqslant m/2 - 1$. It follows that $\mathrm{Int}\, n_w^2|_{T \cap L_1}$ acts as a product of r $m/2$-cycles. Let $\mathfrak{c}_1$ be the projection of $\mathfrak{c} \subset \mathrm{Lie}(L_1) \oplus \mathrm{Lie}(L_2)$ onto $\mathrm{Lie}(L_1)$: then by the above remarks $N_{L(0)}(\mathfrak{c})/Z_{L(0)}(\mathfrak{c}) \cong N_{L_1^{\theta^2}}(\mathfrak{c}_1)/Z_{L_1^{\theta^2}}(\mathfrak{c}_1)$. (We remark that $L_1^{\theta^2}$ is connected since $\theta^2|_{L_1} = \mathrm{Int}\, n_w^2|_{L_1}$.) But the latter group is equal to $G(m/2, 1, r)$ by Lemma 4.5. Hence $W_{\mathfrak{c}} = G(m/2, 1, r)$.

Suppose therefore that $m/2$ is even, hence $\theta = \mathrm{Int}\, n_w \circ \gamma$ where $w = n_w T$ is a product of r m-cycles and $[(n - rm)/2]$ 2-cycles. By a similar argument to that above, it is straightforward to see that $W_1 = G(m, 1, r)$. We claim first of all that $W_{\mathfrak{c}}^Z = W_1$. For this we will apply the criterion of Lemma 4.3(b), for the purposes of which we can reduce to the case $r = 1$. We may assume after suitable conjugation that $w = (1 \ldots m)$. Now T_m is the set of matrices of the form $\mathrm{diag}(t, t^{-1}, \ldots, t^{-1})$ and thus $\mathcal{T}$ is generated by $\mathrm{diag}(\zeta, \zeta^{-1}, \ldots, \zeta^{-1})$. Let $s = \mathrm{diag}(\zeta, \zeta^{-1}, \zeta^3, \zeta^{-3}, \ldots, \zeta^{-1}, \zeta)$; then $s\theta(s^{-1}) = \mathrm{diag}(\zeta^2, 1, \ldots, \zeta^2, 1)$ and hence, by Lemma 4.3, $W_{\mathfrak{c}}^Z = W_1$.

We now claim that $W_{\mathfrak{c}} \supset G(m, 2, r)$ if $(n_w\gamma(n_w))^{m/2} = I$ and $W_{\mathfrak{c}} = G(m, 1, r)$ if $(n_w\gamma(n_w))^{m/2} = -I$. It will clearly suffice to prove this when $n = rm$. Hence by Lemma 4.16 we may assume that $n_w \in N_G(T)^\gamma$. Then $\phi = \mathrm{Int}\, n_w^{m/2} \circ \gamma$ commutes with θ and therefore $L = G^\phi$ is θ-stable (and connected, by a result of Steinberg [St, 8.1]). Moreover, it is easy to see that $\mathfrak{c} \subset \mathfrak{l} = \mathrm{Lie}\, L$ and that $L \cong \mathrm{SO}(rm, k)$ (if $n_w^m = I$) or $L \cong \mathrm{Sp}(rm, k)$ (if $n_w^m = -I$). Examining the possibilities in Lemma 4.8, we see that θ must act on $T \cap L$ as a product of r negative $(m/2)$-cycles. Thus

$$N_{L(0)}(\mathfrak{c})/Z_{L(0)}(\mathfrak{c}) = \begin{cases} G(m, 1, r) & \text{if } L = \mathrm{Sp}(rm, k), \\ G(m, 2, r) & \text{if } L = \mathrm{SO}(rm, k), \end{cases}$$

by Lemmas 4.9 and 4.13. This proves our claim.

Suppose therefore that $(n_w\gamma(n_w))^{m/2} = I$ and that $n > mr$. Let w_i $(1 \leqslant i \leqslant r)$ be the distinct m-cycles in the expression for $w = n_w T$ and let $\{c_i \mid 1 \leqslant i \leqslant r\}$ be a basis for $\mathfrak{c}$ such that $w_i(c_j) = (-\zeta)^{\delta_{ij}} c_j$. After conjugation we may assume that $w_i = ((i-1)m + 1 \ldots im)$. But now, since $(n_w\gamma(n_w))^{m/2} = I$, each $m \times m$

submatrix of n_w corresponding to one of the w_i has determinant -1. It is therefore easy to see that $W_{\mathfrak{c}} = G(m,1,r)$ if and only if there is some element of $Z_{\mathrm{GL}(n,k)}(\mathfrak{c})^\theta$ of determinant -1. (Since any element of $\mathrm{GL}(n,k)^\theta$ is of determinant ± 1, this is equivalent to the statement in the lemma.) □

Remark 4.20. (a) Our condition on $Z_{\mathrm{GL}(n,k)}(\mathfrak{c})^\theta$ in (b) is equivalent to that given by Vinberg in [Vi, §7]. This is the Fourth case of Vinberg's classification; $m/2$ even is 'Type III'. Vinberg determines properties of an outer automorphism of $\mathrm{SL}(n,k)$ of the form $\mathrm{Int}\, g \circ \gamma$ by consideration of the eigenvalues of $g\gamma(g)$ (cf. Lemma 4.15). The condition $(n_w\gamma(n_w))^{m/2} = I$ implies that the eigenvalues of $n_w\gamma(n_w)$ are contained in the set $\mathcal{S} = \{\zeta^{2i} \mid i \in \mathbb{Z}\} \supset \{\pm 1\}$. (This explains the condition $\pm 1 \in \mathcal{S}$ in [Vi, p. 485].) Here r is the integer part of half the minimal multiplicity of $\lambda \in \mathcal{S}$ in $n_w\gamma(n_w)$. Then Vinberg's condition for $W_{\mathfrak{c}}$ to be equal to $G(m,2,r)$ is that the multiplicity of 1 is exactly $2r$. For $i \in \mathbb{Z}/(m/2)\mathbb{Z}$ let $2r + s_i$ be the multiplicity of ζ^{2i} in $n_w\gamma(n_w)$. (Then $s_{m/2-i} = s_i$ and $s_{m/4}$ is even.) A direct calculation shows that $Z_G(\mathfrak{c})^\theta = \prod_{i=1}^{m/4-1} \mathrm{GL}(s_i,k) \times \mathrm{Sp}(s_{m/4},k) \times \mathrm{SO}(s_0,k) \times (k^\times)^{rm}$ and $Z_{\mathrm{GL}(n,k)}(\mathfrak{c})^\theta = \prod_{i=1}^{m/4-1} \mathrm{GL}(s_i,k) \times \mathrm{Sp}(s_{m/4},k) \times \mathrm{O}(s_0,k) \times (k^\times)^{rm}$, hence $W_{\mathfrak{c}} = G(m,2,r)$ if and only if $s_0 = 0$.

(b) In common with type D, there is in general no Levi subgroup of G whose derived subgroup L contains T_1, such that each element of $W_{\mathfrak{c}}$ has a representative in $L(0)$ and $\theta|_{L'}$ is N-regular. In fact, there is only such a Levi subgroup if $m/2$ is odd: if w is a product of r $m/2$-cycles then one can take the derived subgroup L of a standard Levi subgroup such that $L \cong \mathrm{SL}(rm/2,k)$; if w is a product of r m-cycles then the derived subgroup of the group L constructed in the first paragraph is the required group. Moreover, the above proof does show that if $m/2$ is even then there is a reductive subgroup of G which has the properties we desire. If $(n_w\gamma(n_w))^{m/2} = -I$ or if $W_{\mathfrak{c}} = G(m,2,r)$ then let L be the subgroup constructed in the third paragraph of the proof; if $(n_w\gamma(n_w))^{m/2} = I$ then $L \cong \mathrm{SO}(rm,k)$, if $(n_w\gamma(n_w))^{m/2} = -I$ then $L \cong \mathrm{Sp}(rm,k)$. Suppose that $(n_w\gamma(n_w))^{m/2} = I$ and $W_{\mathfrak{c}} = G(m,1,r)$. By the discussion in (a) (following Vinberg) this is true if and only if the multiplicity of 1 in $n_w\gamma(n_w)$ is greater than $2r$. But then, since w is a product of r m-cycles and $[(n-rm)/2]$ 2-cycles, we can clearly reduce to one of two cases: that $n = rm+2$ and the multiplicity of 1 is $2r+2$, or that $n = rm+1$ and the multiplicity of 1 is $2r+1$. In the first case we can now choose an element $g \in Z_{\mathrm{GL}(n,k)}(\mathfrak{c})^\theta \setminus Z_G(\mathfrak{c})$ of order 2 such that any element of $W_{\mathfrak{c}}$ has a representative in $Z_G(g)' \cong \mathrm{SL}(rm+1,k)$. (We can assume $g \in N_G(T)$ and that g represents a 2-cycle in W.) Thus we are reduced to the case $n = rm+1$, where the multiplicity of 1 in $n_w\gamma(n_w)$ is $2r+1$. By Lemma 4.16 we may assume that $\gamma(n_w) = n_w$. Hence $L = G^{\mathrm{Int}\, n_w^{m/2} \circ \gamma} \cong \mathrm{SO}(rm+1,k)$. But $\mathfrak{c} \subset \mathrm{Lie}(L)$ and by Lemma 4.8, θ acts on $T \cap L$ as a product of r negative $m/2$-cycles. It follows by Lemma 4.11 that $N_{L(0)}(\mathfrak{c})/Z_{L(0)}(\mathfrak{c}) = G(m,1,r)$. Now $L = \mathrm{SO}(rm+1,k)$ is a subgroup of G whose Lie algebra contains $\mathfrak{c}$, which has the same little Weyl group as G, and such that $\theta|_L$ is S-regular. These subgroups L constructed in this way will be very useful to us in Section 5.

Lemmas 4.5–4.19 provide a new proof of Vinberg's description of the little Weyl group for classical graded Lie algebras [Vi, Props. 15 and 16]. We deduce from

Lemmas 4.5, 4.9, 4.13 and 4.19 that any classical graded Lie algebra is saturated except for an outer automorphism of $\mathrm{SL}(n,k)$ of order divisible by 4 for which $W_{\mathfrak{c}} = G(m,2,r)$ (cf. [Vi, Prop. 16]). Moreover, we remark that $W_{\mathfrak{c}}^Z = W_1$ unless:

(i) θ is an odd order automorphism of $\mathrm{SO}(2n,k)$, $n > mr$ and $Z_{\mathrm{O}(2n,k}(\mathfrak{c})^\theta = Z_G(\mathfrak{c})^\theta$; or

(ii) $\theta = \mathrm{Int}\, g$ is an even order automorphism of $\mathrm{SO}(2n,k)$, $g^m = I$, $n > mr/2$ and $Z_{\mathrm{O}(2n,k)}(\mathfrak{c})^\theta = Z_G(\mathfrak{c})^\theta$.

(In the notation of [Vi], these cases are:

(i) the Second case, Type III where $n > mr$ and $V'(\pm 1) = 0$; and

(ii) the Second case, Type I where $n > mr/2$ and $V'(\pm 1) = 0$.)

Our proof of the description of $W_{\mathfrak{c}}$ is significantly longer than that in [Vi]. However, as indicated by Remarks 4.6, 4.10, 4.12, 4.14 and 4.20, this alternative perspective on the little Weyl group provides a relatively easy way to establish the existence of a KW-section for all classical graded Lie algebras (see Section 5).

4.7. Polynomial invariants

To prove that $k[\mathfrak{c}]^{W_{\mathfrak{c}}}$ is a polynomial ring we apply the following result of Panyushev [Pa1, Theorem and Prop. 2]:

— *Let $U \subset V$ be vector spaces, let $H \subset \mathrm{GL}(V)$ be a connected reductive group, let $W \subset \mathrm{GL}(U)$ be a finite group of order coprime to* $\mathrm{char}\, k$ *such that $V/\!\!/H \cong U/W$. Then W is generated by pseudoreflections.*

Below we will apply this result to $U = \mathfrak{c}$, $V = \mathfrak{g}(1)$, $H = G(0)$, $W = W_{\mathfrak{c}}$ in the case where G is not of classical type. To prove that the order of $W_{\mathfrak{c}}$ is coprime to $\mathrm{char}\, k$ for exceptional type G, we apply Carter's results on conjugacy classes in Weyl groups. Let us briefly recall the set-up. Thus let W be an arbitrary Weyl group with natural complex representation V. Assume that the root system associated to W is irreducible. Any element $w \in W$ can be expressed as a product $w = w_1 w_2$, where $w_1^2 = w_2^2 = 1$ and $\{v \in V \mid w_1 \cdot v = -v\} \cap \{v \in V \mid w_2 \cdot v = -v\} = \{0\}$. Moreover, any involution w' in W can be expressed as a product of reflections corresponding to $l(w')$ orthogonal roots, where $l(w)$ denotes the number of eigenvalues of $w \in W$ which are not equal to 1 [Ca, Lemma 2]. Thus the expression $w = w_1 w_2$ gives subsets I_1, I_2 of the root system Φ such that $w_i = \prod_{\alpha \in I_i} s_\alpha$ for $i = 1, 2$. Moreover, $\#(I_i) = l(w_i)$ for $i = 1, 2$ and $l(w_1) + l(w_2) = l(w)$. One associates a graph to w with one node for each $\alpha \in I_1$ and one node for each $\beta \in I_2$, with $\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle$ edges between nodes corresponding to *distinct* roots $\alpha, \beta \in I_1 \cup I_2$ (since I_1 and I_2 may not be disjoint). The graph Γ so constructed is uniquely defined by w. For example, if Γ is the Dynkin diagram on the root system associated to W then w is a Coxeter element of W; if Γ is the trivial graph then $w = 1$. If $\Gamma = \Gamma' \cup \Gamma''$, where Γ' and Γ'' are orthogonal subgraphs, then there is a corresponding decomposition $w = w'w''$ and orthogonal root subsystems $\Phi', \Phi'' \subset \Phi$ such that $w' \in W(\Phi')$, $w'' \in W(\Phi'')$. Thus the decomposition of Γ into irreducible components gives a corresponding decomposition of w as a product of commuting elements. The irreducible graphs Γ which can appear via this construction are listed in [Ca, Table 2, p. 10]; the characteristic polynomials (in the natural representation), and hence the orders of such elements are given in [Ca,

Table 3, p. 23]. Tables 7–11 at the end of [Ca] give a classification of conjugacy classes in the exceptional type Weyl groups. A few words of explanation of the symbols which we use in the proof below: Γ is the graph associated to w as detailed above, which we refer to as the type of w; Φ_1 is the minimal root subsystem of Φ containing all roots α associated to nodes in Γ and Φ_2 is the subsystem of all roots in Φ which are orthogonal to Φ_1. If $w \in W$ is of order m, then it is easy to see that the reflection corresponding to an element of Φ_2 acts trivially on $\{v \in V \mid w \cdot v = \zeta v\}$.

Remark 4.21. It may be helpful to give some examples which illustrate the above notation.

(a) Let W be the symmetric group S_n (i.e., of type A_{n-1}). Then an m-cycle in W has type A_{m-1}. The graph associated to a disjoint product of cycles of length $m_1, \ldots, m_r$ is a disjoint union of Coxeter diagrams $\mathsf{A}_{m_1-1}, \ldots, \mathsf{A}_{m_r-1}$: here we say that w has type $\mathsf{A}_{m_1-1} \times \ldots \times \mathsf{A}_{m_r-1}$. In this case the subsystem Φ_2 is isomorphic to $\mathsf{A}_{n-m_1-\cdots-m_r-1}$.

(b) Let W be a Weyl group of type C_n. Then, in the language introduced at the beginning of Section 4.2, a positive m-cycle is of type A_{m-1} and a negative m-cycle is of type C_m. A disjoint product of signed cycles gives rise to a disjoint union of the corresponding Coxeter diagrams. If, for example, w is a negative m-cycle then Φ_2 is isomorphic to C_{n-m}.

(c) For an example of an element for which Γ is not a product of Coxeter graphs, let W be of type D_n and let w be a product of two negative 2-cycles. Then the corresponding graph Γ has a diagram labelled $\mathsf{D}_4(a_1)$ by Carter. (The graph has four vertices forming a square, each vertex linked to two others by a single bond.) In this case, Φ_1 is of type D_4 and Φ_2 is of type D_{n-4}.

Proposition 4.22. *Let G be almost simple.*

(a) *$W_{\mathfrak{c}}$ is generated by pseudoreflections.*
(b) *$k[\mathfrak{c}]^{W_{\mathfrak{c}}}$ is a polynomial ring.*

Proof. This is known for $m = 2$ by [L2, 4.11] (part (a) also follows from Lemma 2.7 and [Ri, Section 4]); hence assume $m \geqslant 3$. For the classical graded Lie algebras, (a) is true by Lemmas 4.5, 4.9, 4.11, 4.13 and 4.19. If G is of exceptional type, or if G is of type D_4 and θ is an outer automorphism such that θ^3 is inner, then we claim that W_1 is of order coprime to p. Indeed, if G is of exceptional type then the assumption that p is good implies that p is coprime to the order of W except in the following cases:

(i) G is of type E_6 and $p = 5$;
(ii) G is of type E_7 and $p = 5$;
(iii) G is of type E_7 and $p = 7$; and
(iv) G is of type E_8 and $p = 7$.

In type E_6, θ could of course be outer. In this case let γ be an involutive automorphism of G satisfying $\gamma(t) = t^{-1}$ for all $t \in T$; then any outer automorphism of G is of the form $\operatorname{Int} g \circ \gamma$ for some $g \in G$, hence $\theta = \operatorname{Int} n_w \circ \gamma$ for some $n_w \in N_G(T)$. Moreover, the induced action of γ on W is trivial and thus $W^\theta = Z_W(w)$, where $w = n_w T$. Hence in type E_6 it will suffice to show that centralizers have order prime to p. An inspection of Tables 9–11 in [Ca] shows that $p \nmid Z_W(w)$ except for the following cases:

(i) w is of type A_1, A_4, or $\mathsf{A}_4 \times \mathsf{A}_1$. The first case is an involution. In the other two cases, w is of order divisible by 5 and thus can only appear if $p > 5$.

(ii) w is of type A_1, A_2, A_4, $\mathsf{A}_4 \times \mathsf{A}_1$, A_1^6, $\mathsf{A}_4 \times \mathsf{A}_2$, D_6, A_1^7, $\mathsf{D}_4 \times \mathsf{A}_1^3$, $\mathsf{D}_6 \times \mathsf{A}_1$ or $\mathsf{E}_7(a_3)$. In the three cases A_1, A_1^6, and A_1^7, θ is an involution. If w is of type A_4, $\mathsf{A}_4 \times \mathsf{A}_1$, $\mathsf{A}_4 \times \mathsf{A}_2$, D_6, $\mathsf{D}_6 \times \mathsf{A}_1$ or $\mathsf{E}_7(a_3)$ then its order is divisible by 5. If w is of type A_2 then $Z_W(w)$ is of order $2^5.3^3.5$. However, here Φ_2 is of type A_5, and hence $Z_{W^\theta}(\mathfrak{c})$ contains a subgroup isomorphic to the symmetric group S_6, and in particular is of order divisible by $6! = 2^4.3^2.5$. It follows that W_1 has order dividing 6. Finally, if w is of type $\mathsf{A}_4 \times \mathsf{A}_2$ then θ is of order (divisible by) 15. However, w acts on $\mathfrak{t}$ with minimal polynomial $(t^4+t^3+t^2+t+1)(t^2+t+1)$ and hence $\mathfrak{c}$ is trivial.

(iii) w is of type A_6, A_1^7 or $\mathsf{E}_7(a_1)$. The case A_1^7 is an involution. If w is of type A_6 or $\mathsf{E}_7(a_1)$ then θ is of order divisible by 7, which contradicts the assumption that m is coprime to p.

(iv) w is of type A_1, A_6, A_1^7, $\mathsf{A}_6 \times \mathsf{A}_1$, $\mathsf{E}_7(a_1)$, A_1^8 or D_8. The cases A_1 and A_1^7 are involutions. If w is of type A_6, $\mathsf{A}_6 \times \mathsf{A}_1$, $\mathsf{E}_7(a_1)$ or D_8 then the order of θ is divisible by 7, which contradicts the assumption on m.

Finally, suppose G is of type D_4 and θ is an outer automorphism such that θ^3 is inner. Then $p > 3$. But $W(\mathsf{D}_4)$ has order $192 = 2^6.3$. Hence W^θ has order coprime to p. Thus W is in all cases generated by pseudoreflections by Panyushev's theorem. This proves (a). Moreover, the Shephard–Todd theorem holds for groups of coprime order (see, e.g., [Be, Theorem 7.2.1]) and hence, if G is of exceptional type (and $m > 2$), $k[\mathfrak{c}]^{W_\mathfrak{c}}$ is a polynomial ring. In the classical case $W_\mathfrak{c}$ is one of $G(m',1,r)$, $G(m',2,r)$ where m' is coprime to p, hence it is easily verified that $k[\mathfrak{c}]^{W_\mathfrak{c}}$ is a polynomial ring. □

Theorem 4.23. *Suppose G satisfies the standard hypotheses. Then $k[\mathfrak{g}(1)]^{G(0)}$ is a polynomial ring.*

Proof. This follows from the construction of $\widehat{\mathfrak{g}} = \tilde{\mathfrak{g}} \oplus \mathfrak{t}_0 = \mathfrak{g} \oplus \mathfrak{t}_1$ in Proposition 3.1. Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}$ and let $\mathfrak{c}_1 = \{t \in \mathfrak{t}_1 \mid d\widehat{\theta}(t) = \zeta t\}$. Clearly $\widehat{\mathfrak{c}} = \mathfrak{c} \oplus \mathfrak{c}_1$ is a Cartan subspace of $\widehat{\mathfrak{g}}$. In fact it is the unique Cartan subspace of $\widehat{\mathfrak{g}}$ which contains $\mathfrak{c} \cap \mathrm{Lie}(G')$. Let $\tilde{\mathfrak{c}} = \widehat{\mathfrak{c}} \cap \tilde{\mathfrak{g}}$. Then $\widehat{\mathfrak{c}} = \tilde{\mathfrak{c}} \oplus \mathfrak{c}_0$, where $\mathfrak{c}_0 = \{t \in \mathfrak{t}_0 \mid d\widehat{\theta}(t) = \zeta t\}$. Clearly $k[\widehat{\mathfrak{c}}]^{W_\mathfrak{c}} = k[\tilde{\mathfrak{c}}]^{W_\mathfrak{c}} \otimes k[\mathfrak{c}_0]$. It is easy to see that Proposition 4.22 extends to a product of almost simple groups and groups of the form $\mathrm{GL}(n,k)$, hence to $\tilde{G}$. Thus $k[\tilde{\mathfrak{c}}]^{W_\mathfrak{c}}$ is a polynomial ring. It follows that $k[\widehat{\mathfrak{c}}]^{W_\mathfrak{c}} = k[\mathfrak{c}]^{W_\mathfrak{c}} \otimes k[\mathfrak{c}_1]$ is also a polynomial ring. Now let J_1 be the maximal ideal of all positive degree elements of $k[\mathfrak{c}_1]$: then J_1 is generated by elements of degree 1 and hence its set of zeros is a hyperplane in $\widehat{\mathfrak{c}}/W_\mathfrak{c}$ (identifying $\widehat{\mathfrak{c}}/W_\mathfrak{c}$ with a vector space of dimension $r + \dim \mathfrak{t}_1$). But therefore $k[\mathfrak{c}]^{W_\mathfrak{c}} \cong k[\widehat{\mathfrak{c}}]^{W_\mathfrak{c}}/J_1 k[\widehat{\mathfrak{c}}]^{W_\mathfrak{c}}$ is a polynomial ring. Thus the result follows by Theorem 2.20. □

5. Kostant–Weierstrass slices

A long-standing conjecture in this field (originally stated in characteristic zero [Po1, no. 7]) is the existence of a KW-section in $\mathfrak{g}(1)$ to the invariants. (For details on Weierstrass slices see [PV, Section 8] or [Po2] for more recent work. In the case of a periodically graded reductive Lie algebra, Panyushev [Pa3] introduced the terminology of Kostant–Weierstrass slice or KW-section because of the analogy with Kostant's slice to the regular conjugacy classes in $\mathfrak{g}$.)

Definition 5.1. A Kostant–Weierstrass slice or KW-section for θ is an affine linear subvariety $\mathfrak{v}$ of $\mathfrak{g}(1)$ such that the embedding $\mathfrak{v} \hookrightarrow \mathfrak{g}(1)$ induces an isomorphism of affine varieties $\mathfrak{v} \to \mathfrak{g}(1)/\!\!/G(0)$.

The prototype is Kostant's slice $e + \mathfrak{z}_{\mathfrak{g}}(f)$ in $\mathfrak{g}$, where $\{h, e, f\}$ is an $\mathfrak{sl}(2)$-triple such that e is a regular nilpotent element. The case $m = 2$ is also known ([KR] in characteristic zero, [L2] in positive characteristic). Essentially, one can reduce the involution case to the $m = 1$ case by constructing a reductive subalgebra of $\mathfrak{g}$ for which a Cartan subspace of $\mathfrak{g}(1)$ is a Cartan subalgebra. One can then apply the usual construction since an involution is S-regular if and only if it is N-regular. (Recall that θ is S-regular (resp. N-regular) if $\mathfrak{g}(1)$ contains a regular semisimple (resp. nilpotent) element of $\mathfrak{g}$.) Applying such an argument in the general case is problematic since a general finite-order automorphism can be S-regular but not N-regular, and vice versa. On the other hand, it is known due to Panyushev (in characteristic zero) that an N-regular automorphism always admits a KW-section [Pa3]. (Earlier, Panyushev also showed that if $G(0)$ is semisimple then θ admits a KW-section [Pa2].) The slice constructed in [Pa3] is a natural choice: one chooses $e \in \mathfrak{g}(1)$ to be a regular nilpotent element of $\mathfrak{g}$, embeds e in an $\mathfrak{sl}(2)$-triple $\{h, e, f\}$ with $h \in \mathfrak{g}(0)$ and $f \in \mathfrak{g}(-1)$, and sets $\mathfrak{v} = e + \mathfrak{z}_{\mathfrak{g}(1)}(f)$. We will show in this section that Panyushev's theorem can be applied to the case of a classical graded Lie algebra (under the assumption of the standard hypotheses) by fairly straightforward reduction to (certain) N-regular cases. Indeed, almost all of the work required has been carried out in the previous section. Recall from Remarks 4.6, 4.10, 4.12, 4.14 and 4.20 the construction of the semisimple subgroup L such that $\mathfrak{c} \subset \mathrm{Lie}(L)$, each element of $W_{\mathfrak{c}}$ has a representative in $L(0)$, and $\theta|_L$ is S-regular. (The analysis of the Weyl group in Section 4 clearly goes through in exactly the same way if the characteristic of k is zero.)

Remark 5.2. The form of L for each case is summed up in Table 1. A few words on the entries in the table. We use Vinberg's classification, hence, for example, the 'Second case', Type II is denoted 2II. Let $m_0 = m/2$ in the Fourth case, and let $m_0 = m$ otherwise. The column marked 'θ' gives conditions on g, where θ is of the form $\mathrm{Int}\, g$ or $\mathrm{Int}\, g \circ \gamma$. In the column marked L we have placed an asterisk next to the entries of the form $\mathrm{SL}(rm, k)$, $\mathrm{SL}(rm/2, k)$, $\mathrm{SL}(rm/2, k)^2$ since if $p \mid r$ these should be replaced with the corresponding general linear group. This is always possible, if we assume G is not equal to $\mathrm{SL}(V)$ where $p \mid \dim V$. On the other hand, it is clearly also possible if $G = \mathrm{GL}(V)$. In the column $\theta|_L$ we have marked the entry for 4II with a double asterisk since here $L \cong \mathrm{SL}(rm/2, k) \times \mathrm{SL}(rm/2, k)$ and the action of θ is given by $(g_1, g_2) \mapsto (\sigma(g_2), g_1)$, where σ is an inner automorphism of $\mathrm{SL}(rm/2,k)$ of order $m/2$, rank r. Thus, strictly speaking, σ is the First case and not θ.

TABLE 1. Reduction to the N-regular case

Case	G	m_0	θ	$W_{\mathfrak{c}}$	L	$\theta\|_L$
1	$\mathrm{SL}(n,k)$	-	-	$G(m,1,r)$	$\mathrm{SL}(rm,k)^*$	1
2I	$\mathrm{SO}(2n+1,k)$	even	$g^m=I$	$G(m,1,r)$	$\mathrm{SO}(rm+1,k)$	2
2I	$\mathrm{SO}(2n,k)$	even	$g^m=I$ $Z_{\mathrm{O(2n,k)}}(\mathfrak{c})^\theta \neq Z_G(\mathfrak{c})^\theta$	$G(m,1,r)$	$\mathrm{SO}(rm+1,k)$	2
2I	$\mathrm{SO}(2n,k)$	even	$g^m=I$ $Z_{\mathrm{O(2n,k)}}(\mathfrak{c})^\theta = Z_G(\mathfrak{c})^\theta$	$G(m,2,r)$	$\mathrm{SO}(rm,k)$	2
2II	$\mathrm{SO}(2n,k)$	even	$g^m=-I$	$G(m,1,r)$	$\mathrm{SL}(rm,k)^*$	1
2III	$\mathrm{SO}(2n+1,k)$	odd	-	$G(2m,1,r)$	$\mathrm{SO}(2rm+1,k)$	2
2III	$\mathrm{SO}(2n,k)$	odd	$Z_{\mathrm{O(2n,k)}}(\mathfrak{c})^\theta \neq Z_G(\mathfrak{c})^\theta$	$G(2m,1,r)$	$\mathrm{SO}(2rm+1,k)$	2
2III	$\mathrm{SO}(2n,k)$	odd	$Z_{\mathrm{O(2n,k)}}(\mathfrak{c})^\theta = Z_G(\mathfrak{c})^\theta$	$G(2m,2,r)$	$\mathrm{SO}(2rm,k)$	2
3I	$\mathrm{Sp}(2n,k)$	even	$g^m=-I$	$G(m,1,r)$	$\mathrm{Sp}(rm,k)$	3
3II	$\mathrm{Sp}(2n,k)$	even	$g^m=I$	$G(m,1,r)$	$\mathrm{SL}(rm,k)^*$	1
3III	$\mathrm{Sp}(2n,k)$	odd	-	$G(2m,1,r)$	$\mathrm{Sp}(2rm,k)$	3
4I	$\mathrm{SL}(n,k)$	odd	$(g\gamma(g))^{m/2}=I$	$G(m/2,1,r)$	$\mathrm{SL}(rm/2,k)^*$	4
4II	$\mathrm{SL}(n,k)$	odd	$(g\gamma(g))^{m/2}=-I$	$G(m/2,1,r)$	$\mathrm{SL}(rm/2,k)^{2*}$	1**
4III	$\mathrm{SL}(n,k)$	even	$(g\gamma(g))^{m/2}=I$ $Z_{\mathrm{GL}(n,k)}(\mathfrak{c})^\theta \neq Z_G(\mathfrak{c})^\theta$	$G(m,1,r)$	$\mathrm{SO}(rm+1,k)$	2
4III	$\mathrm{SL}(n,k)$	even	$(g\gamma(g))^{m/2}=I$ $Z_{\mathrm{GL}(n,k)}(\mathfrak{c})^\theta = Z_G(\mathfrak{c})^\theta$	$G(m,2,r)$	$\mathrm{SO}(rm,k)$	2
4III	$\mathrm{SL}(n,k)$	even	$(g\gamma(g))^{m/2}=-I$	$G(m,1,r)$	$\mathrm{Sp}(rm,k)$	3

In characteristic zero, it therefore remains only to show that the pairs $(L,\theta|_L)$ listed in Table 1 are N-regular; Panyushev's theorem on N-regular automorphisms [Pa3, Theorem 3.5] then implies that any classical graded Lie algebra admits a KW-section. In positive characteristic, we provide the following generalization of Panyushev's result. Our proof is broadly similar, although Corollary 2.22 allows us to avoid a potentially troublesome argument [Pa3, 3.3] involving $\mathfrak{sl}(2)$-triples.

Proposition 5.3. *Let G be a group satisfying the standard hypotheses and let θ be an automorphism of G of order m, $p \nmid m$. Suppose that θ is N-regular. Then the restriction homomorphism $k[\mathfrak{g}]^G \to k[\mathfrak{g}(1)]^{G(0)}$ is surjective. Let $e \in \mathfrak{g}(1)$ be a regular nilpotent element of $\mathfrak{g}$ and let $\lambda : k^\times \to G(0)$ be an associated cocharacter for e (see Remark 2.12). Let $\mathfrak{u}$ be a $\lambda(k^\times)$-stable subspace of $\mathfrak{g}(1)$ such that $\mathfrak{u} \oplus [\mathfrak{g}(0),e] = \mathfrak{g}(1)$. Then $e+\mathfrak{u}$ is a KW-section for θ.*

Proof. Let $\mathfrak{w}$ be a θ-stable, $\mathrm{Ad}\,\lambda(k^\times)$-stable subspace of $\mathfrak{g}$ such that $\mathfrak{w} \oplus [\mathfrak{g},e] = \mathfrak{g}$. Recall (see [Ve, 6.3–6.5] and [PT, Proof of Lemma 1] in good characteristic) that the embedding $e+\mathfrak{w} \hookrightarrow \mathfrak{g}$ induces an isomorphism $e+\mathfrak{w} \to \mathfrak{g}/\!\!/G$. Let $n = \mathrm{rk}\, G$ and let $F_1,\dots,F_n$ be algebraically independent homogeneous generators of $k[\mathfrak{g}]^G$. Then the differentials $(dF_i)_e|_{\mathfrak{w}}$ are linearly independent elements and span $\mathfrak{w}^*$, hence their restrictions $(dF_i)_e|_{\mathfrak{u}} = (dF_i|_{e+\mathfrak{u}})_e$ span $\mathfrak{u}^*$. Since $\dim \mathfrak{u} = r$ by Corollary 2.22 and separability of orbits (see, e.g., [L2, 4.2]), we may assume after renumbering that $(dF_1|_{e+\mathfrak{u}})_e, \ldots, (dF_r|_{e+\mathfrak{u}})_e$ span $\mathfrak{u}^*$. In particular, $(dF_1|_{\mathfrak{g}(1)})_e, \ldots (dF_r|_{\mathfrak{g}(1)})_e$ are linearly independent. Let $u_1, \ldots, u_r$ be algebraically independent homogeneous generators of $k[\mathfrak{g}(1)]^{G(0)}$, and let h be a monomial in the u_i. Then, since $u_i(e) = 0$ for $1 \leqslant i \leqslant r$, $dh_e = 0$ unless $h = u_i$ for some u_i. Thus we can express $F_i|_{\mathfrak{g}(1)}$, $1 \leqslant i \leqslant r$ (uniquely) as $f_i + g_i$, where f_i is linear in the u_j $(1 \leqslant j \leqslant r)$ and g_i is in the ideal of $k[u_1, \ldots, u_r]$ generated by all $u_i u_j$, $1 \leqslant i \leqslant j \leqslant r$. Note that we have $(dg_i)_x = 0$ for any nilpotent element $x \in \mathfrak{g}(1)$ by Lemma 2.11. Therefore $(dF_i|_{\mathfrak{g}(1)})_e = (df_i)_e$ for each i, $1 \leqslant i \leqslant r$, and the differentials $(df_i)_e$ are linearly independent. It follows that the f_i, $1 \leqslant i \leqslant r$, are algebraically independent and that $k[u_1, \ldots, u_r] = k[f_1, \ldots, f_r]$. Since the F_i are homogeneous, there exist integers m_i, $1 \leqslant i \leqslant r$, such that $F_i(\eta x) = \eta^{m_i} F_i(x)$ for all $\eta \in k$ and all $x \in \mathfrak{g}$. But now, since the expression $F_i|_{\mathfrak{g}(1)} = f_i + g_i$ is unique, it follows that $f_i(\eta x) = \eta^{m_i} x$ for any $\eta \in k$, $x \in \mathfrak{g}(1)$ and similarly for g_i. After reordering we may assume that $m_1 \leqslant \ldots \leqslant m_r$. It now follows that $F_i|_{\mathfrak{g}(1)} \in f_i + k[f_1, \ldots, f_{i-1}]$. Thus the restrictions $F_i|_{\mathfrak{g}(1)}$ (resp. $F_i|_{e+\mathfrak{u}}$), $1 \leqslant i \leqslant r$, are algebraically independent and generate $k[\mathfrak{g}(1)]^{G(0)}$ (resp. $k[e+\mathfrak{u}]$). This completes the proof. $\square$

Proposition 5.4. *Let G be of classical type, let L be the subgroup as listed in Table* 1 *and let $\mathfrak{l} = \mathrm{Lie}(L)$. Then $\theta|_L$ is N-regular.*

Proof. We may assume that $G = L$. We have the following possibilities:

(i) $G = \mathrm{SL}(rm, k)$ or $\mathrm{GL}(rm, k)$ (if $p \mid r$) and θ is inner, w a product of m-cycles;
(ii) $G = \mathrm{SO}(rm+1, k)$ and w is a product of negative $m/2$-cycles (m even);
(iii) $G = \mathrm{SO}(rm, k)$ and w is a product of negative $m/2$-cycles (m even);
(iv) $G = \mathrm{SO}(2rm+1, k)$ and w is a product of positive m-cycles (m odd);
(v) $G = \mathrm{SO}(2rm, k)$ and w is a product of positive m-cycles (m odd);
(vi) $G = \mathrm{Sp}(rm, k)$ and w is a product of negative $m/2$-cycles (m even);
(vii) $G = \mathrm{Sp}(2rm, k)$ and w is a product of positive m-cycles (m odd);
(viii) $G = \mathrm{SL}(rm/2, k)$ or $\mathrm{GL}(rm/2, k)$ (if $p|r$), θ is outer and w is a product of $m/2$-cycles;
(ix) $G = \mathrm{SL}(rm/2, k)^2$ or $\mathrm{GL}(rm/2, k)^2$ (if $p|r$) and θ is an automorphism of the form $(g_1, g_2) \mapsto (\sigma(g_2), g_1)$ where σ is of order $m/2$ and acts on the maximal torus of diagonal matrices in $\mathrm{SL}(rm/2, k)$ as a product of r $m/2$-cycles.

The argument for the last case clearly reduces immediately to verifying the lemma for σ, hence to case (i). Thus we consider the cases (i)–(viii). To prove N-regularity we replace θ by an $\mathrm{Int}\, G$-conjugate such that (B, T) is a fundamental pair for θ. If θ is inner and $G = \mathrm{SL}(n, k)$ then this means that $\theta = \mathrm{Int}\, t$, where $t \in \mathrm{GL}(n, k)$ is diagonal and has r entries equal to ζ^i for each i, $0 \leqslant i \leqslant m-1$. But then we can assume after conjugating by an element of the normalizer of T that $t = \mathrm{diag}(\zeta^{m-1}, \zeta^{m-2}, \ldots, 1)$, in which case the nilpotent element with 1 on the first upper diagonal and zero elsewhere is clearly in $\mathfrak{g}(1)$. One can carry out similar calculations for the automorphisms of $\mathrm{SO}(2n+1, k)$, $\mathrm{SO}(2n, k)$ and $\mathrm{Sp}(2n, k)$. For all cases except (iii) with r odd we may assume after conjugation that $\theta = \operatorname{Int} t$, where $t \in T$ is as given in the following list. Recall that ζ is a primitive mth root of unity and ξ is a square root of ζ.

(a) $t = \operatorname{diag}(1, \zeta^{m-1}, \ldots, 1)$ and $e = \sum_{i=1}^{n} e_{i,i+1} - \sum_{i=n+1}^{2n} e_{i,i+1}$ in cases (ii) $(n = rm/2)$ and (iv) $(n = rm)$.

(b) $t = \operatorname{diag}(\zeta^{m-1}, \zeta^{m-2}, \ldots, 1, 1, \zeta^{-1}, \ldots, \zeta)$ and $e = \sum_{i=1}^{n-1} e_{i,i+1} + e_{n-1,n+1} - e_{n,n+2} - \sum_{n+1}^{2n-1} e_{i,i+1}$ in cases (iii) with r even $(n = rm/2)$ and (v) $(n = rm)$.

(c) $t = \operatorname{diag}(\xi^{2m-1}, \xi^{2m-3}, \ldots, \xi)$ and $e = \sum_{i=1}^{n} e_{i,i+1} - \sum_{i=n+1}^{2n-1} e_{i,i+1}$ in cases (vi) $(n = rm/2)$ and (vii) $(n = rm)$.

To check N-regularity for case (iii) with r odd, let J_2 be the 2×2 matrix with 1 on the antidiagonal and 0 on the diagonal, and let s be the diagonal $(rm/2 - 1) \times (rm/2 - 1)$ matrix with jth entry $-\zeta^{-j}$. Then after conjugation we may assume that $\theta = \operatorname{Int} \begin{pmatrix} s & 0 & 0 \\ 0 & J_2 & 0 \\ 0 & 0 & -s \end{pmatrix}$. Now $e = \sum_{i=1}^{n-1} e_{i,i+1} + e_{n-1,n+1} - e_{n,n+2} - \sum_{i=n+1}^{2n-1} e_{i,i+1}$ is a regular nilpotent element of $\mathfrak{g}(1)$, where $n = rm/2$.

This leaves only the case where $G = L = \mathrm{SL}(rm/2, k)$ and θ is outer. We have $\theta = \operatorname{Int} g \circ \gamma$ and $(g\gamma(g))^{m/2} = I$. Let $\psi = \operatorname{Int}(tJ_n) \circ \gamma$, where $\gamma : x \mapsto {}^t x^{-1}$, J_n is the matrix with 1 on the antidiagonal and 0 elsewhere, and

$$t = \begin{cases} \operatorname{diag}(\zeta^{(m-2)/4}, \zeta^{(m-6)/4}, \ldots, \zeta^{-(m-2)/4}) & \text{if } r \text{ is odd,} \\ \operatorname{diag}(\zeta^{m-1}, \zeta^{m-2}, \ldots, 1, -\zeta^{-1}, -\zeta^{-2}, \ldots, -1) & \text{if } r/2 \text{ is even,} \\ \operatorname{diag}(\zeta^{m-1}, \zeta^{m-2}, \ldots, -1, \zeta^{-1}, \zeta^{-2}, \ldots, -1) & \text{if } r/2 \text{ is odd.} \end{cases}$$

It is an easy calculation to see that $tJ_n\gamma(tJ_n) = tJ_n\gamma(t)J_n^{-1}$ has r entries equal to ζ^{2i} for each i, $0 \leqslant i < m/2$, and hence θ is conjugate to ψ by Lemma 4.16. But ψ is N-regular:

$$e = \begin{cases} \sum_{i=1}^{(n-1)/2} e_{i,i+1} - \sum_{(n+1)/2}^{n-1} e_{i,i+1} & \text{if } r \text{ is odd,} \\ \sum_{i=1}^{n/2} e_{i,i+1} - \sum_{n/2+1}^{n-1} e_{i,i+1} & \text{if } r \text{ is even,} \end{cases}$$

where $n = rm/2$. This proves that θ is N-regular in each of the cases concerned. □

We therefore have:

Theorem 5.5. *Let G be one of* $\mathrm{SL}(n, k)$ $(p \nmid n)$, $\mathrm{GL}(n, k)$, $\mathrm{SO}(n, k)$, $\mathrm{Sp}(2n, k)$. *Then* $(\mathfrak{g}, d\theta)$ *admits a KW-section.*

Proof. By Proposition 5.4, $\theta|_L$ is N-regular. Moreover, by our construction of L (or by inspection of the little Weyl group for θ and $\theta|_L$ in each case), each element of $W_{\mathfrak{c}}$ has a representative in $L(0)$. Thus $\mathfrak{l}(1)/\!\!/L(0) \cong \mathfrak{c}/W_{\mathfrak{c}} \cong \mathfrak{g}(1)/\!\!/G(0)$, and any KW-section for $\theta|_L$ is a KW-section for θ. But, by Proposition 5.3, there exists a KW-section for $\theta|_L$. □

Remark 5.6. (a) In the case where $(\mathfrak{g}, d\theta)$ is N-regular but not S-regular (and locally free), our construction shows that there are many different KW-sections. A trivial example is a zero rank N-regular grading: applying Panyushev's theorem directly, one obtains $\{e\}$ as a KW-section; our construction via the subgroup L gives $\{0\}$.

(b) These methods can be applied to prove the existence of KW-sections for exceptional type Lie algebras, as well as the remaining outer automorphisms in type D_4. While there are a number of cases to deal with, this approach also provides a fairly straightforward way to determine the little Weyl group. We will deal with this in subsequent work.

References

[Be] D. J. Benson, *Polynomial Invariants of Finite Groups*, London Mathematical Society Lecture Notes, Vol. 190, Cambridge University Press, Cambridge, 1993.

[Bo] A. Borel, *Linear Algebraic Groups*, Springer-Verlag, New York, 1991.

[Ca] R. W. Carter, *Conjugacy classes in the Weyl group*, Compositio Math. **25** (1972), 1–59.

[Ch] C. Chevalley, *Classification des Groupes Algébriques Semi-Simples*, Springer, Berlin, 2005. Collected Works, Vol. 3, edited and with a preface by P. Cartier, with the collaboration of Cartier, A. Grothendieck, and M. Lezard.

[GP] I. Gordon, A. Premet, *Block representation type of reduced enveloping algebras*, Trans. Amer. Math. Soc. **354**(4) (2002), 1549–1581.

[Ha] W. J.Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. (2) **102**(1) (1975), 67–83.

[He] A. J. Helminck, *Algebraic groups with a commuting pair of involutions and semisimple symmetric spaces*, Adv. Math. **71**(1) (1988), 21–91.

[Hu] J. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, New York, 1975.

[Ka] N. Kawanaka, *Orbits and stabilizers of nilpotent elements of a graded semisimple Lie algebra*, J. Fac. Sci. Univ. Tokyo Section IA Math. **34**(3) (1987), 573–597.

[Ke] G. R.Kempf, *Instability in invariant theory*, Ann. of Math. (2) **108**(2) (1978), 299–316.

[KR] B. Kostant, S. Rallis, *Orbits and representations associated with symmetric spaces*, Amer. J. Math. **93** (1971), 753–809.

[L1] P. Levy, *Commuting varieties of Lie algebras over fields of prime characteristic*, J. Algebra **250**(2) (2002), 473–484.

[L2] P. Levy, *Involutions of reductive Lie algebras in positive characteristic*, Adv. Math. **210**(2) (2007), 505–559.

[MN] B. Martin, A. Neeman, *The map $V \to V/\!\!/G$ need not be separable*, Math. Res. Lett. **8**(5–6) (2001), 813–817.

[MS] G. J. McNinch, E. Sommers, *Component groups of unipotent centralizers in good characteristic*, J. Algebra **260**(1) (2003), 323–337. Special issue celebrating the 80th birthday of Robert Steinberg.

[Pa1] Д. И. Панюшев, *О пространстве орбит конечных и связных линейных групп*, Изв. Акад. Наук СССР, сер. мат. **46(1)** (1982), 95–99, 191. Engl.

transl.: D. I. Panyushev, *On orbit spaces of finite and connected linear groups*, Math. USSR-Izv. **20** (1983), 97–101.

[Pa2] Д. И. Панюшев, *Регулярные элементы в пространствах линейных представлений*, II., Изв. Акад. Наук СССР, сер. мат. **49**(5) (1985), 979–985, 1120. Engl. transl.: D. I. Panyushev, *Regular elements in spaces of linear representations*, II, Math. USSR.-Izv. **27** 279–284, 1986.

[Pa3] D. I. Panyushev, *On invariant theory of θ-groups*, J. Algebra **283**(2) (2005), 655–670.

[Po1] В. Л. Попов, *Представления со свободным модулем ковариантов*, Функц. анализ и его прил. **10**(3) (1976), 91–92. Engl. transl.: V. L. Popov, *Representations with a free module of covariants*, Functional Anal. Appl. **10** (1976), no. 3, 242–244.

[Po2] V. L. Popov, *Sections in invariant theory*, in: *The Sophus Lie Memorial Conference* (Oslo, 1992), Scandinavian University Press, Oslo, 1994, pp. 315–361.

[PV] Э. Б. Винберг, В. Л. Попов, *Теория инвариантов*, Итоги науки и техн., Совр. пробл. матем., Фунд. направл., ВИНИТИ, Москва, т. 55, 1989, стр. 137–309. Engl. transl.: V. L. Popov, E. B. Vinberg, *Invariant Theory*, in: *Algebraic Geometry* IV, Encycl. Math. Sci., Vol. 55, Springer-Verlag, Heidelberg, 1994, pp. 123–284.

[Pr1] A. Premet, *Complexity of Lie algebra representations and nilpotent elements of the stabilizers of linear forms*, Math. Z. **228**(2) (1998), 255–282.

[Pr2] A. Premet, *Nilpotent orbits in good characteristic and the Kempf–Rousseau theory*, J. Algebra **260**(1) (2003), 338–366. Special issue celebrating the 80th birthday of Robert Steinberg.

[PT] A. Premet, R. Tange, *Zassenhaus varieties of general linear Lie algebras*, J. Algebra **294**(1) (2005), 177–195.

[Ri] R. W. Richardson, *Orbits, invariants, and representations associated to involutions of reductive groups*, Invent. Math. **66**(2) (1982), 287–312.

[Ro] G. Rousseau, *Immeubles sphériques et théorie des invariants*, C. R. Acad. Sci. Paris. Sér. A–B **286**(5) (1978), A247–A250.

[Sl] P. Slodowy, *Die Theorie der optimalen Einparameteruntergruppen für instabile Vektoren*, in: *Algebraische Transformationsgruppen und Invariantentheorie*, *DMV Sem.*, Vol. **13**, Birkhäuser, Basel, 1989, pp. 115–131.

[So] E. Sommers, *A generalization of the Bala–Carter theorem for nilpotent orbits*, Int. Math. Res. Not. **(11)** (1998), 539–562.

[Sp] T. A. Springer, *The classification of involutions of simple algebraic groups*, J. Fac. Sci. Univ. Tokyo Section IA Math. **34**(3) (1987), 655–670. 1987.

[SpSt] T. A. Springer, R. Steinberg, *Conjugacy classes*, in: *Seminar on Algebraic Groups and Related Finite Groups* (The Institute for Advanced Study, Princeton, NJ, 1968/69), Lecture Notes in Mathematics, Vol. 131, Springer-Verlag, Berlin, 1970, pp. 167–266.

[St] R. Steinberg, *Endomorphisms of Linear algebraic groups*, Mem. Amer. Math. Soc. **80**, 1968.

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

[Vi] Э. Б. Винберг, *Группа Вейля градуированной алгебры Ли*, Изв. Акад. Наук СССР, сер. мат. **40**(3) (1976), 488–526, 709. Engl. transl.: È. B. Vinberg, *The Weyl group of a graded Lie algebra*, Math. USSR-Izv. **10** (1977), 463–495.

[Vu] T. Vust, *Opération de groupes réductifs dans un type de cônes presque homogènes*, Bull. Soc. Math. France **102** (1974), 317–333.

[W] D. J. Winter, *Fixed points and stable subgroups of algebraic group automorphisms*, Proc. Amer. Math. Soc. **18** (1967), 1107–1113.