Journal of the Inst. of Math. Jussieu (2010) **9**(4), 673–704
doi:10.1017/S1474748010000125 © Cambridge University Press 2010

ON THE ADJOINT QUOTIENT OF CHEVALLEY GROUPS OVER ARBITRARY BASE SCHEMES

PIERRE-EMMANUEL CHAPUT[1] AND MATTHIEU ROMAGNY[2]

[1]*Laboratoire de Mathématiques Jean Leray, UMR 6629 du CNRS, UFR Sciences et Techniques, 2 rue de la Houssinière, BP 92208, 44322 Nantes Cedex 03, France* (pierre-emmanuel.chaput@math.univ-nantes.fr)
[2]*Institut de Mathématiques, Théorie des Nombres, Université Pierre et Marie Curie, Case 82, 4, place Jussieu, F-75252 Paris Cedex 05, France* (romagny@math.jussieu.fr)

(Received 9 January 2009; revised 9 August 2009, 2 October 2009; accepted 16 October 2009)

Abstract For a split semisimple Chevalley group scheme G with Lie algebra $\mathfrak{g}$ over an arbitrary base scheme S, we consider the quotient of $\mathfrak{g}$ by the adjoint action of G. We study in detail the structure of $\mathfrak{g}$ over S. Given a maximal torus T with Lie algebra $\mathfrak{t}$ and associated Weyl group W, we show that the Chevalley morphism $\pi : \mathfrak{t}/W \to \mathfrak{g}/G$ is an isomorphism except for the group Sp_{2n} over a base with 2-torsion. In this case this morphism is only dominant and we compute it explicitly. We compute the adjoint quotient in some other classical cases, yielding examples where the formation of the quotient $\mathfrak{g} \to \mathfrak{g}/G$ commutes, or does not commute, with base change on S.

Keywords: Chevalley groups; adjoint action; invariant theory; base change

AMS 2010 *Mathematics subject classification:* Primary 13A50; 20G15

Contents

1. Introduction

Let G be a split semisimple Chevalley group scheme over a base scheme S and let $\mathfrak{g}$ be its Lie algebra. The quotient of $\mathfrak{g}$ by the adjoint action of G in the category of schemes affine over S, that is to say, the spectrum of the sheaf of G-invariant functions of $\mathfrak{g}$, is traditionally called the *adjoint quotient* of $\mathfrak{g}$ and denoted $\mathfrak{g}/G$. Let $T \subset G$ be a maximal torus and $\mathfrak{t}$ its Lie algebra. There is an induced action of the Weyl group $W = W_T$ on $\mathfrak{t}$ and the inclusion $\mathfrak{t} \subset \mathfrak{g}$ induces a natural morphism $\pi : \mathfrak{t}/W \to \mathfrak{g}/G$. In this paper, we call it the *Chevalley morphism*.

The situation where the base is the spectrum of an algebraically closed field whose characteristic does not divide the order of the Weyl group is well documented. In this case π is an isomorphism, as proven by Springer and Steinberg [**16**]. It is known also that the adjoint quotient is an affine space (see [**6**, **7**, **20**]). There are counterexamples to these statements when the characteristic divides the order of the Weyl group. Another difficulty comes from the fact that we are considering the quotient $\mathfrak{g}/\operatorname{Ad}(G)$ of the Lie algebra, and not $G/\operatorname{Int}(G)$, and at some point this derivation causes some trouble (Steinberg [**17**, p. 51] was also led to the same conclusion).

In this paper, we turn our attention to the integral structure of the adjoint quotient and the Chevalley morphism, including the characteristics that divide the order of W. In other words we are interested in an arbitrary base scheme S, and in the behaviour of the previous objects under base change $S' \to S$. It is not hard to extend the results from simple to semisimple groups, so for simplicity we restrict to simple Chevalley groups.

Our main result (Theorems 3.6 and 3.11) is that in most cases the Chevalley morphism is an isomorphism, therefore reducing the calculation of $\mathfrak{g}/G$ to the calculation of a quotient by a finite group.

Theorem 1.1. *Let G be a split simple Chevalley group scheme over a base scheme S. Then the Chevalley morphism $\pi : \mathfrak{t}/W \to \mathfrak{g}/G$ is schematically dominant, and is an isomorphism if G is not isomorphic to Sp_{2n}, $n \geqslant 1$.*

Note that even when the base is a field, this improves the known results. Our proof follows a classical strategy. The main new inputs are over a base field, a close analysis of the root systems and determination of the conditions of non-vanishing of the differentials of the roots (Lemma 1.4), and over a general base, a careful control of the poles along the singular locus for the relative meromorphic functions involved in the proof. We treat separately the exceptional case (Theorem 6.6).

Theorem 1.2. *If $G = \mathrm{Sp}_{2n}$ then the Chevalley morphism is an isomorphism if and only if the base has no 2-torsion. Moreover, over an open affine subscheme $\mathrm{Spec}(A) \subset S$, the ring of functions of $\mathfrak{g}/G$ is*

$$A[c_2, c_4, \dots, c_{2n}],$$

where the functions c_{2i} are the coefficients of the characteristic polynomial. The formation of the adjoint quotient commutes with arbitrary base change.

We see that for $G = \mathrm{Sp}_{2n}$, the formation of the adjoint quotient commutes with base change. If this was true for all split simple Chevalley groups, then we could deduce the main Theorem 1.1 above from the case $S = \mathrm{Spec}(\mathbb{Z})$ which is significantly easier (see Corollary 3.7). Unfortunately it is not always so, and in order to see this, we study in detail the orthogonal groups in types B and D. Our main result is the following theorem (the missing notation appearing in it is briefly defined after the statement and further explained in § 4.2).

Theorem 1.3. *If $G = \mathrm{SO}_{2n}$ or $G = \mathrm{SO}_{2n+1}$ then over an open affine subscheme $\mathrm{Spec}(A) \subset S$, the ring of functions of $\mathfrak{g}/G$ is the following.*

(i) *If $G = \mathrm{SO}_{2n}$: $A[c_2, c_4, \dots, c_{2n-2}, \mathrm{pf}; x(\pi_1)^{\epsilon_1} \cdots (\pi_{n-1})^{\epsilon_{n-1}}]$, where x runs through a set of generators of the 2-torsion ideal $A[2] \subset A$, and $\epsilon_i = 0$ or 1, not all 0.*

(ii) *If $G = \mathrm{SO}_{2n+1}$: $A[c_2, c_4, \dots, c_{2n}; x(\pi_1)^{\epsilon_1} \cdots (\pi_n)^{\epsilon_n}]$, where x runs through a set of generators of $A[2]$ and $\epsilon_i = 0$ or 1, not all 0.*

The functions that appear in the preceding theorem are the coefficients of the characteristic polynomial c_{2i}, the Pfaffian pf and some functions π_i which we call the coefficients of the Pfaffian polynomial. The functions c_{2i} and pf are invariant, but the functions π_i are invariant only after multiplication by a 2-torsion element. The definition of these objets needs some care, since it is not always the straightforward definition one would think of.

Using the theorem above, we prove that the formation of the adjoint quotient for the orthogonal groups commutes with a base change $f : S' \to S$ if and only if $f^*S[2] = S'[2]$, where $S[2]$ is the closed subscheme defined by the ideal of 2-torsion. This holds in particular if 2 is invertible in $\mathcal{O}_S$, or if $2 = 0$ in $\mathcal{O}_S$, or if $S' \to S$ is flat. We prove also that if S is noetherian and connected then the quotient is of finite type over S, and is flat over S if and only if $S[2] = S$ or $S[2] = \emptyset$.

We feel it useful to say that when we first decided to study the adjoint quotient over a base other than a field, we started with some examples among the classical Chevalley groups and considered their Lie algebras. To our surprise, already in the classical case we could not find concrete descriptions of them in the existing literature (for example the Lie algebra of PSL_n over $\mathbb{Z}$). This lead to our study of the classical Lie algebras over arbitrary bases (§ 2.4). We also faced the problem of relating the Lie algebra of a group scheme and of any finite quotient of it (§ 2.1); note that the results of § 2.1 hold for any smooth group scheme, not necessarily affine over the base. Let us finally mention that spin groups over $\mathbb{Z}$ have also been studied very recently in such a concrete way by Ikai [**12, 13**].

Here is the outline of the article. At the end of this section we give our notation and prove a combinatorial lemma about root systems which is crucial throughout the paper. In § 2 we give two dual exact sequences

$$0 \to \mathscr{L}\mathrm{ie}(K)^\vee \to \mathscr{L}\mathrm{ie}(G)^\vee \to \omega^1_{H/S} \to 0$$

and

$$0 \to \mathscr{L}\mathrm{ie}(G) \to \mathscr{L}\mathrm{ie}(K) \to (\omega^1_{H/S})^\dagger \to 0$$

describing the relation between the Lie algebra of a smooth group scheme G and the Lie algebra of a quotient $K := G/H$ (see more precise assumptions in Propositions 2.2 and 2.7). Then we specialize to Chevalley groups and their Lie algebras over $\mathbb{Z}$. We describe their weight decomposition (§ 2.2), the intermediate quotients of $G \to G^{\mathrm{ad}}$ and $\mathrm{Lie}(G) \to \mathrm{Lie}(G^{\mathrm{ad}})$ (§ 2.3) and we illustrate our results by describing the classical Chevalley Lie algebras (§ 2.4). In § 3 we prove Theorem 1.1 above. In the remaining sections (§§ 4–6) we treat the examples of Theorems 1.2 and 1.3 above by computing explicitly the map $\mathfrak{t}/W \to \mathfrak{g}/G$ (see Theorem 4.8, Corollary 4.9, Theorem 5.3 and Theorem 6.6).

1.1. General notation

All rings are commutative with unit. If A is a ring, we denote by $A[2]$ its 2-torsion ideal, defined by $A[2] = \{a \in A,\ 2a = 0\}$. If S is a scheme, we denote by $S[2]$ its closed subscheme defined by the 2-torsion ideal sheaf.

If X is an affine scheme over $\mathrm{Spec}(A)$ we always denote by $A[X]$ its function ring.

If S is a scheme, X is a scheme over S, and $T \to S$ is a base change morphism, we denote by $X \times_S T$ or simply X_T the T-scheme obtained by base change. In all the article, we call relative Cartier divisor of X over S an effective Cartier divisor in X which is flat over S.

Finally, the linear dual of an $\mathcal{O}_S$-module $\mathcal{F}$ is denoted $\mathcal{F}^\vee := \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{F}, \mathcal{O}_S)$.

1.2. Notation on group schemes

Let S be a scheme and let G be a group scheme over S. We will use the following standard notation: $e_G : S \to G$ is the unit section of G/S; $\Omega^1_{G/S}$ is the sheaf of relative differential 1-forms of G/S; and $\omega^1_{G/S} = e_G^*\Omega^1_{G/S}$. Recall that $\Omega^1_{G/S} = f^*\omega^1_{G/S}$, where

$f : G \to S$ is the structure map, so that $\Omega^1_{G/S}$ is locally free over G if and only if $\omega^1_{G/S}$ is locally free over S.

We will write $\mathrm{Lie}(G/S)$ (or simply $\mathrm{Lie}(G)$) for the Lie algebra of G/S, and $\mathscr{L}\mathrm{ie}(G/S)$ (or simply $\mathscr{L}\mathrm{ie}(G)$) for the sheaf of sections of $\mathrm{Lie}(G/S)$. Note that $\mathrm{Lie}(G/S)$ is the vector bundle $\mathbb{V}(\omega^1_{G/S})$, with the Grothendieck notation. Sometimes we shall also use Gothic style letters for Lie algebras, like $\mathfrak{g}$, $\mathfrak{t}$, $\mathfrak{psl}$, $\mathfrak{so}$, etc.

By Chevalley group scheme over a scheme S, we mean a deployable reductive group scheme over S, with the terminology of [**8**, Exposé XXII, Définition 1.13]. By [**8**, Exposé XXIII, Corollaire 5.3], such a group is characterized up to isomorphism by its type (as defined in [**8**, Exposé XXII, Définition 2.7]: this is essentially the root datum together with a module included in the weight lattice and containing the root lattice) and is equal to G_S, where G is a Chevalley group scheme over the ring of integers.

1.3. Roots that are integer multiples of weights

The next lemma comes up at various places in the article. It has as a consequence the fact that the differential of a root can vanish along the Lie algebra of a maximal torus in a simple Chevalley group only in case this group is Sp_{2n} (including $\mathrm{Sp}_2 \simeq \mathrm{SL}_2$)—see Lemma 2.13. This will be crucial throughout the article: Lemma 3.2, on which relies the proof of Theorem 3.11, is again a consequence of this lemma, as well as the fact that a simply connected Lie algebra is equal to its own derived algebra in all cases but $\mathfrak{sp}_{2n}$, see Proposition 2.11.

Lemma 1.4. *Let R be a simple reduced root system, $Q(R)$ the root lattice and $P(R)$ the weight lattice. Assume there exists $\alpha \in R$, $\lambda \in P(R)$, $l \in \mathbb{N}$ such that $\alpha = l\lambda$ and $l \geqslant 2$. Then $l = 2$, and either R is of type A_1, or R is of type C_n and α is a long root.*

Proof. Let us assume that R is the root system defined in [**5**, Planches I–IX]. If R is of type A_1, then the roots are $\alpha = \epsilon_1 - \epsilon_2$ and $-\alpha$. Since $\epsilon_1 - (\epsilon_1 + \epsilon_2)/2 = (\epsilon_1 - \epsilon_2)/2$ is a weight, α is indeed twice a weight. Now let us assume that R is of rank greater than 1.

The hypothesis of the lemma implies that

$$\forall \beta \in R, \quad \langle \beta^\vee, \alpha \rangle = l \langle \beta^\vee, \lambda \rangle \in l\mathbb{Z}. \tag{1.1}$$

Let β be a root. If α and β have the same length, by [**5**, VI, No. 1.3, Proposition 8], $\langle \beta^\vee, \alpha \rangle \in \{-1, 0, 1\}$. If moreover we know that $\langle \beta^\vee, \alpha \rangle \neq 0$, we see that (1.1) cannot hold. By [**5**, VI, No. 1, Proposition 15, p. 154], we can assume that α is a simple root. This implies that in the Dynkin diagram of R, all edges containing the vertex corresponding to α must be multiple edges.

This excludes all simply laced root systems, as well as the root system of type F_4. Moreover, if R is of type B_n with $n \geqslant 3$, then α has to equal α_n, but since $\langle \alpha_{n-1}^\vee, \alpha_n \rangle = -1$, we have a contradiction. If R is of type C_n, then α has to equal α_n again. Since $\alpha_n = 2\epsilon_n$, we have indeed $\alpha \in lP(R)$ with $l = 2$. Since $B_2 = C_2$, the last case to be settled is that of G_2. But in this case $Q(R) = P(R)$; since R is reduced, it is not possible that a root be a multiple of a weight. □

2. On the Lie algebra of Chevalley groups

2.1. Lie algebras of quotients and coverings

In this section, our aim is to relate the Lie algebra of a group G and the Lie algebra of a quotient G/H. More precisely, we consider a scheme S, a flat S-group scheme of finite presentation G, and a closed subgroup scheme $H \subset G$ which is flat and of finite presentation over S. These group schemes define sheaves for the fppf topology (recall that fppf stands for faithfully flat of finite presentation). We assume that the quotient fppf sheaf $K := G/H$ is representable by a scheme; this is always the case for Chevalley groups, because they are defined over $\mathbb{Z}$ and then one may apply [**1**, Theorem 4.C].

Remark 2.1. In general, it follows from a theorem of Artin that the quotient fppf sheaf is representable by an algebraic space over S. Indeed, this claim is Zariski local on S so one may check it for affine schemes S. If S is the spectrum of a ring of finite type over $\mathbb{Z}$, the result follows from Corollary 6.3 of [**2**]. In general, since G and H are of finite presentation they are pullbacks of group schemes G_0 and H_0 over an affine scheme $S_0 = \mathrm{Spec}(A_0)$, where A_0 is a ring of finite type over $\mathbb{Z}$, and we can apply the previous case. Thus, the reader familiar with algebraic spaces may use the subsequent results in this setting.

We let $\pi\colon G \to K$ denote the quotient morphism, and $e_K := \pi \circ e_G$. We write $\mathrm{Tan}(K)$ for the restriction of the tangent space along e_K and $\mathscr{T}\mathrm{an}(K)$ for its sheaf of sections.

Proposition 2.2. *Let G be a flat S-group scheme of finite presentation, $H \subset G$ a closed subgroup scheme which is flat and of finite presentation, and assume that the quotient fppf sheaf $K = G/H$ is representable by a scheme.*

(1) *There is a canonical exact sequence of quasi-coherent $\mathcal{O}_S$-modules:*

$$\omega^1_{K/S} \to \omega^1_{G/S} \to \omega^1_{H/S} \to 0,$$

where $\omega^1_{G/S} \to \omega^1_{H/S}$ is the natural map deduced from the inclusion $H \subset G$.

(2) *Assume furthermore that G is smooth over S and that there is schematically dominant morphism $i : U \to S$ such that $H \times_S U$ is smooth over U. Then, there is a canonical exact sequence of coherent $\mathcal{O}_S$-modules:*

$$0 \to \mathscr{T}\mathrm{an}(K)^\vee \to \mathscr{L}\mathrm{ie}(G)^\vee \to \omega^1_{H/S} \to 0$$

and $\mathscr{L}\mathrm{ie}(G)^\vee \to \omega^1_{H/S}$ is the natural map deduced from the inclusion $H \subset G$.

Typically, in the applications, U will be an open subscheme of S or the spectrum of the local ring of a generic point.

Proof. (1) We have the fundamental exact sequence for differential 1-forms:

$$\pi^*\Omega^1_{K/S} \to \Omega^1_{G/S} \to \Omega^1_{G/K} \to 0.$$

By right exactness of the tensor product, the sequence remains exact after we pullback via e_G. The only thing left to prove is that there is a canonical isomorphism $e_G^*\Omega^1_{G/K} \simeq \omega^1_{H/S}$. In order to do so, we use the fact that $G \to K$ is an H-torsor, so that we have an isomorphism $t\colon H \times_S G \to G \times_K G$ given by $t(h,g) = (hg, g)$. We consider the fibre square:

$$\begin{tikzcd} H \times_S G \arrow[r, "t"] & G \times_K G \arrow[r, "\mathrm{pr}_2"] \arrow[d, "\mathrm{pr}_1"'] & G \arrow[d, "\pi"] \\ & G \arrow[r, "\pi"] & K \end{tikzcd}$$

Then, if we call $f\colon H \times_S G \to H$ the projection, we have the sequence of isomorphisms on $H \times_S G$:

$$t^* \operatorname{pr}_1^* \Omega^1_{G/K} \simeq t^* \Omega^1_{G \times_K G/G} \simeq \Omega^1_{H \times_S G/G} \simeq f^* \Omega^1_{H/S}$$

(the first and the third isomorphisms come from the invariance of the module of relative differentials by base change [**9**, IV.16.4.5]). Pulling back along $e_H \times e_G$, we get the desired result. Moreover, following the identifications, we see that the map $\omega^1_{G/S} \to \omega^1_{H/S}$ is the same as the map induced by the inclusion $H \subset G$.

(2) Since G is smooth over S and $G \to K$ is faithfully flat, then K is also smooth over S. Hence $\mathcal{M} = \omega^1_{K/S}$ and $\mathcal{N} = \omega^1_{G/S}$ are locally free $\mathcal{O}_S$-modules of finite rank, so that

$$\mathcal{M} \simeq \mathscr{T}\mathrm{an}(K)^\vee \quad \text{and} \quad \mathcal{N} \simeq \mathscr{L}\mathrm{ie}(G)^\vee.$$

It remains to check that $\mathcal{M} \to \mathcal{N}$ is injective. This will follow from the diagram

$$\begin{tikzcd} i_*i^*\mathcal{M} \arrow[r, hook] & i_*i^*\mathcal{N} \\ \mathcal{M} \arrow[u, hook] \arrow[r] & \mathcal{N} \arrow[u] \end{tikzcd}$$

if we describe the injective morphisms therein. Since $i : U \to S$ is schematically dominant and $\mathcal{M}$ is flat, we have an injective morphism $\mathcal{M} \to \mathcal{M} \otimes i_*\mathcal{O}_U$ and the target module is isomorphic to $i_*i^*\mathcal{M}$ by the projection formula. Besides, the morphism $G \times_S U \to G/H \times_S U$ is smooth since $H \times_S U$ is smooth over U, so by the short exact sequence of Ω^1s for a smooth morphism, the morphism $i^*\mathcal{M} \to i^*\mathcal{N}$ is injective. By left exactness the morphism $i_*i^*\mathcal{M} \to i_*i^*\mathcal{N}$ is injective also. $\square$

If H is finite over S, like in the cases we have in mind, we can dualize the exact sequence of Proposition 2.2 thanks to a Pontryagin duality for certain torsion modules, which we now present. Let A be a commutative ring and let Q be the total quotient ring of A, i.e. the localization with respect to the multiplicative set of non-zero divisors (in fact we should better consider the module of global sections of the sheaf of total quotient rings on $\mathrm{Spec}(A)$, but in this informal discussion it does not matter). We wish to associate to any finitely presented torsion A-module M a dual $M^\dagger = \mathrm{Hom}_A(M, Q/A)$. For general M this does not lead to nice properties such as biduality; for example, if $A = k[x,y]$ is a polynomial ring in two variables and $M = A/(x, y)$, it is easy to see that $M^\dagger = 0$. In this example there is a presentation $A^2 \to A \to M \to 0$ but one can see that there is no presentation $A^n \to A^m \to M \to 0$ with $n = m$. In fact, this is a consequence of our results below. Note that the fact that M is torsion implies $n \geqslant m$, thus if we can find a presentation with $n = m$ it is natural to say that M has *few relations*. By the structure theorem for modules over a principal ideal domain, all finite abelian groups have few relations, and from our point of view, this is the crucial property of finite abelian groups that makes Pontryagin duality work. These considerations explain the following definition.

Definition 2.3. Let $\mathcal{F}$ be a coherent $\mathcal{O}_S$-module; denote by $\mathcal{K}$ the sheaf of total quotient rings of $\mathcal{O}_S$. We say that $\mathcal{F}$ is a *torsion module with few relations* if $\mathcal{F} \otimes \mathcal{K} = 0$ and $\mathcal{F}$ is locally isomorphic to the cokernel of a morphism $(\mathcal{O}_S)^n \to (\mathcal{O}_S)^n$ for some $n \geqslant 1$.

We have the following easy characterization.

Proposition 2.4. *Let $\varphi : \mathcal{E}_1 \to \mathcal{E}_2$ be a morphism between locally free $\mathcal{O}_S$-modules of the same finite rank and let $\mathcal{F} = \mathrm{coker}(\varphi)$. Then $\mathcal{F}$ is a torsion module with few relations if and only if the sequence $0 \to \mathcal{E}_1 \to \mathcal{E}_2 \to \mathcal{F} \to 0$ is exact, i.e. φ is injective.*

Proof. If φ is injective, then locally over an open set where $\mathcal{E}_1$ and $\mathcal{E}_2$ are free, its determinant $\det(\varphi) \in \mathcal{O}_S$ is a non-zero divisor. Therefore, $\varphi \otimes \mathrm{Id} : \mathcal{E}_1 \otimes \mathcal{K} \to \mathcal{E}_2 \otimes \mathcal{K}$ is surjective, hence an isomorphism. It follows that $\mathcal{F} \otimes \mathcal{K} = \mathrm{coker}(\varphi \otimes \mathrm{Id}) = 0$. Conversely, if $\mathcal{F}$ is a torsion module with few relations, then $\mathrm{coker}(\varphi \otimes \mathrm{Id}) = \mathcal{F} \otimes \mathcal{K} = 0$ so that $\varphi \otimes \mathrm{Id}$ is an isomorphism. Since $\mathcal{E}_1$ and $\mathcal{E}_2$ are flat we have injections

$$\begin{tikzcd}
\mathcal{E}_1 \otimes \mathcal{K} \arrow[r, hook] & \mathcal{E}_2 \otimes \mathcal{K} \\
\mathcal{E}_1 \arrow[r] \arrow[u, hook] & \mathcal{E}_2 \arrow[u, hook]
\end{tikzcd}$$

and it follows that φ is injective. $\square$

Definition 2.5. Given a coherent $\mathcal{O}_S$-module $\mathcal{F}$ we define its *Pontryagin dual* by

$$\mathcal{F}^\dagger = \mathcal{H}om_{\mathcal{O}_S}(\mathcal{F}, \mathcal{K}/\mathcal{O}_S).$$

As the following proposition proves, there is a satisfactory duality if we restrict to torsion modules with few relations.

Proposition 2.6. *Let $\mathcal{F}$ be a torsion $\mathcal{O}_S$-module with few relations. Then*

(1) *$\mathcal{F}^\dagger$ is also a torsion $\mathcal{O}_S$-module with few relations, and the canonical morphism $\mathcal{F} \to \mathcal{F}^{\dagger\dagger}$ is an isomorphism;*

(2) *for each exact sequence $0 \to \mathcal{E}_1 \to \mathcal{E}_2 \to \mathcal{F} \to 0$ where $\mathcal{E}_1$, $\mathcal{E}_2$ are locally free $\mathcal{O}_S$-modules of the same finite rank, we have a canonical exact sequence $0 \to \mathcal{E}_2^\vee \to \mathcal{E}_1^\vee \to \mathcal{F}^\dagger \to 0$.*

Proof. The assertions in point (1) are local over S and therefore are easy consequences of point (2). In order to prove point (2) we set $\mathcal{G} = \operatorname{coker}(\mathcal{E}_2^\vee \to \mathcal{E}_1^\vee)$ and we construct a canonical non-degenerate pairing $\mathcal{F} \times \mathcal{G} \to \mathcal{K}/\mathcal{O}_S$, as follows. Since $\mathcal{F}$ is torsion and finitely generated, locally (over an open subset $U \subset S$) there is a non-zero divisor $a \in \mathcal{O}_S$ such that $a\mathcal{E}_2 \subset \mathcal{E}_1$. Given two sections $f \in \mathcal{E}_2$ and $g \in \mathcal{E}_1^\vee$ over U, we let $\langle f, g\rangle$ denote the class of $(1/a)g(af) \in \mathcal{K}$ modulo $\mathcal{O}_S$. It is easy to check that this is independent of the choice of a. If $f \in \mathcal{E}_1$ or if $g \in \mathcal{E}_2^\vee$, then $\langle f, g\rangle = 0$ so there results a pairing $\mathcal{F} \times \mathcal{G} \to \mathcal{K}/\mathcal{O}_S$ and we will now check that it induces isomorphisms $\mathcal{F} \to \mathcal{G}^\dagger$ and $\mathcal{G} \to \mathcal{F}^\dagger$. By symmetry we will consider only $\sigma : \mathcal{G} \to \mathcal{F}^\dagger$. If $\langle\cdot\,, g\rangle$ is zero then we claim that $g \in \mathcal{E}_1^\vee$ extends to a form on $\mathcal{E}_2$. Indeed, for each $f \in \mathcal{E}_2$ we have $(1/a)g(af) \in \mathcal{O}_S$ so that the definition $g(f) := (1/a)g(af)$ is unambiguous, since a is a non-zero divisor. It follows that σ is injective. In order to check surjectivity we may assume that S is the spectrum of a local ring, and in this case $\mathcal{E}_1$, $\mathcal{E}_2$ are trivial. Any $u : \mathcal{F} \to \mathcal{K}/\mathcal{O}_S$ factors through $(1/a)\mathcal{O}_S/\mathcal{O}_S \subset \mathcal{K}/\mathcal{O}_S$ and then induces a morphism $\mathcal{E}_2 \to \mathcal{O}_S/a\mathcal{O}_S$. Since $\mathcal{E}_2$ is trivial this map lifts to $u' : \mathcal{E}_2 \to \mathcal{O}_S$. Moreover, if $x \in \mathcal{E}_1$ then $u'(x) \in a\mathcal{O}_S$, so we can set $v(x) = (1/a)u'(x)$; then it is easy to check that v is a form g on $\mathcal{E}_1$ that gives rise to u. Hence σ is surjective. $\square$

If S is a Dedekind scheme, that is to say a noetherian normal scheme of dimension 1, then all coherent torsion $\mathcal{O}_S$-modules are torsion modules with few relations (by the structure theorem for modules of finite type). However in general it is not so, as soon as $\dim(S) \geqslant 2$, and we saw a counterexample before Definition 2.3.

We are now able to dualize the sequence of Lie algebras in Proposition 2.2 (2) either if H is smooth or if it is finite.

Proposition 2.7. *Let G be a smooth S-group scheme and $H \subset G$ a closed normal subgroup scheme which is flat and of finite presentation over S. Let $K = G/H$ be the quotient.*

(1) *If H is smooth over S, then we have an exact sequence of locally free Lie algebra $\mathcal{O}_S$-modules*
$$0 \to \mathscr{L}\mathrm{ie}(H) \to \mathscr{L}\mathrm{ie}(G) \to \mathscr{L}\mathrm{ie}(K) \to 0$$
and if furthermore K is commutative, we have
$$[\mathscr{L}\mathrm{ie}(G), \mathscr{L}\mathrm{ie}(G)] \subset \mathscr{L}\mathrm{ie}(H).$$

(2) *If H is finite over S and there is a schematically dominant morphism $i : U \to S$ such that $H \times_S U$ is étale over U, then there is a canonical exact sequence of coherent $\mathcal{O}_S$-modules:*
$$0 \to \mathscr{L}\mathrm{ie}(G) \to \mathscr{L}\mathrm{ie}(K) \to (\omega^1_{H/S})^\dagger \to 0,$$
and if furthermore H is commutative, then
$$[\mathscr{L}\mathrm{ie}(K), \mathscr{L}\mathrm{ie}(K)] \subset \mathscr{L}\mathrm{ie}(G).$$

Proof. (1) All the sheaves in the exact sequence 2.2 (2) are locally free, so dualization yields the asserted result. It is clear that the resulting sequence is an exact sequence of sheaves of Lie algebras, so $[\mathscr{L}\mathrm{ie}(G), \mathscr{L}\mathrm{ie}(G)] \subset \mathscr{L}\mathrm{ie}(H)$ in case K is commutative.

(2) The exact sequence in Proposition 2.2 (2) and Proposition 2.4 imply that $\omega^1_{H/S}$ is a torsion module with few relations. We get the dual sequence from Proposition 2.6. Here $(\omega^1_{H/S})^\dagger$ is not a Lie algebra, so it is a little more subtle to deduce that $[\mathscr{L}\mathrm{ie}(K), \mathscr{L}\mathrm{ie}(K)] \subset \mathscr{L}\mathrm{ie}(G)$. The assertion is local on S so we may assume that H is embedded into an abelian scheme A/S (that is to say a smooth proper group scheme over S with geometrically connected fibres), by a theorem of Raynaud [**3**, Theorem 3.1.1]. Let $\pi : A \to B = A/H$ be the quotient abelian scheme, and let $G' = (G \times_S A)/H$ where H acts by $h(g, a) = (hg, h^{-1}a)$. We have two exact sequences of smooth S-schemes:

$$1 \to G \to G' \xrightarrow{p} B \to 1$$

and

$$1 \to A \to G' \to K \to 1.$$

By smoothness we derive exact sequences of sheaves of Lie algebras

$$0 \to \mathscr{L}\mathrm{ie}(G) \to \mathscr{L}\mathrm{ie}(G') \xrightarrow{p} \mathscr{L}\mathrm{ie}(B) \to 0$$

and

$$0 \to \mathscr{L}\mathrm{ie}(A) \xrightarrow{i} \mathscr{L}\mathrm{ie}(G') \to \mathscr{L}\mathrm{ie}(K) \to 0.$$

Combining these exact sequences we have an exact sequence

$$0 \to \mathscr{L}\mathrm{ie}(G) \to \mathscr{L}\mathrm{ie}(K) \to \mathscr{L}\mathrm{ie}(B)/\pi(\mathscr{L}\mathrm{ie}(A)) \to 0,$$

where $\pi = p \circ i$. Here, the arrow $\mathscr{L}\mathrm{ie}(K) \to \mathscr{L}\mathrm{ie}(B)/\pi(\mathscr{L}\mathrm{ie}(A))$ is induced by p which is a morphism of Lie algebras. It follows immediately that $[\mathscr{L}\mathrm{ie}(K), \mathscr{L}\mathrm{ie}(K)] \subset \mathscr{L}\mathrm{ie}(G)$. $\square$

2.2. Lie algebras of Chevalley group schemes

Let G be a split simple Chevalley group scheme over $\mathbb{Z}$, $T \subset G$ a split maximal torus over $\mathbb{Z}$, and write as in [**8**] $T = D_{\mathbb{Z}}(M)$, where M is a free $\mathbb{Z}$-module. Since G is smooth, $\mathrm{Lie}(G)$ is a vector bundle and hence is determined by $\mathscr{L}\mathrm{ie}(G)$. Since the base is affine, this is in turn determined by the free $\mathbb{Z}$-module $\mathscr{L}\mathrm{ie}(G)(\mathbb{Z}) = \mathrm{Lie}(G)(\mathbb{Z})$ together with its Lie bracket.

Proposition 2.8. *There is a weight decomposition*

$$\mathrm{Lie}(G)(\mathbb{Z}) = \mathrm{Lie}(T)(\mathbb{Z}) \oplus \bigoplus_{\alpha} \mathrm{Lie}(G)(\mathbb{Z})_\alpha$$

over the integers. Moreover, letting $Q(R)$ (respectively $P(R)$) denote the root (respectively weight) lattice, we have $Q(R) \subset M \subset P(R)$.

Proof. Since G is a smooth split reductive group scheme over $\mathbb{Z}$, this essentially follows from [**8**, Exposé I, 4.7.3], as explained in [**8**, Exposé XIX, No. 3]. $\square$

Now let H be a closed subgroup scheme of the centre of G and let i_H denote the inclusion of the character group of T/H in that of T.

Proposition 2.9. *Under the natural inclusions*

$$\mathrm{Lie}(G)(\mathbb{Z}) \subset \mathrm{Lie}(G)(\mathbb{Q}) = \mathrm{Lie}(G/H)(\mathbb{Q}) \supset \mathrm{Lie}(G/H)(\mathbb{Z}),$$

we have $\mathrm{Lie}(G)(\mathbb{Z})_{i_H(\alpha)} = \mathrm{Lie}(G/H)(\mathbb{Z})_\alpha$.

Proof. Since $H \subset T$, by Proposition 2.7, there are injections $\mathrm{Lie}(G)(\mathbb{Z}) \subset \mathrm{Lie}(G/H)(\mathbb{Z})$ and $\mathrm{Lie}(T)(\mathbb{Z}) \subset \mathrm{Lie}(T/H)(\mathbb{Z})$, both of index $|H|$. All these maps are compatible with the injection in $\mathrm{Lie}(G)(\mathbb{Q})$. Thus for each α, the inclusion $\mathrm{Lie}(G)(\mathbb{Z})_{i_H(\alpha)} \subset \mathrm{Lie}(G/H)(\mathbb{Z})_\alpha$ must be of index 1, proving the proposition.

This proposition also follows from Chevalley's construction of the simple group schemes [**8**, Exposé XXV]. $\square$

Remark 2.10. The Lie algebra over $\mathbb{Z}$ defined by generators and relations by Serre [**15**] is the simply connected one, that is to say the Lie algebra of the simply connected corresponding group scheme, because, with his notation, the generators H_i are by definition the coroots.

Recall that $\pi : G \to G/H$ denotes the quotient morphism.

Proposition 2.11. *Assume G is simply connected.*

(1) *When G is not Sp_{2n}, $n \geqslant 1$, we have*

$$[\mathrm{Lie}(G)(\mathbb{Z}), \mathrm{Lie}(G)(\mathbb{Z})] = \mathrm{Lie}(G)(\mathbb{Z})$$

and $[\mathrm{Lie}(G/H)(\mathbb{Z}), \mathrm{Lie}(G/H)(\mathbb{Z})] = \mathrm{d}\pi(\mathrm{Lie}(G)(\mathbb{Z}))$.

(2) *If $G = \mathrm{Sp}_{2n}$, then* $[\mathrm{Lie}(G)(\mathbb{Z}), \mathrm{Lie}(G)(\mathbb{Z})]$ *has index* 2^{2n} *in* $\mathrm{Lie}(G)(\mathbb{Z})$.

Proof. (1) Let $\mathfrak{g} = \mathrm{Lie}(G)(\mathbb{Z})$ and choose a Cartan $\mathbb{Z}$-subalgebra $\mathfrak{h} \subset \mathfrak{g}$. Choose a basis of the roots, and denote by $\mathfrak{u}_+, \mathfrak{u}_- \subset \mathfrak{g}$ the direct sum of the positive (respectively negative) root spaces. By Corollary 2.8, we have $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{u}_+ \oplus \mathfrak{u}_-$. Since G is neither SL_2 ($= \mathrm{Sp}_2$) nor Sp_{2n}, by Lemma 1.4, no root is an integer multiple of a weight, and so $[\mathfrak{h}, \mathfrak{u}_\pm] = \mathfrak{u}_\pm$. Moreover, it follows from Serre's presentation of the simple Lie algebras in terms of the Cartan matrix (see Remark 2.10) that in this case $[\mathfrak{g}, \mathfrak{g}] \supset \mathfrak{h}$. In particular,

$$\begin{aligned} \mathrm{d}\pi(\mathrm{Lie}(G)(\mathbb{Z})) &= \mathrm{d}\pi([\mathrm{Lie}(G)(\mathbb{Z}), \mathrm{Lie}(G)(\mathbb{Z})]) \\ &= [\mathrm{d}\pi(\mathrm{Lie}(G)(\mathbb{Z})), \mathrm{d}\pi(\mathrm{Lie}(G)(\mathbb{Z}))] \\ &\subset [\mathrm{Lie}(G/H)(\mathbb{Z}), \mathrm{Lie}(G/H)(\mathbb{Z})]. \end{aligned}$$

The reverse inclusion follows from Proposition 2.7.

(2) Assume that G stabilizes the form $\left(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right)$, where I_n stands for the identity matrix. Then

$$\mathfrak{g} = \left\{ \begin{pmatrix} A & B \\ C & -{}^{\mathrm{t}}A \end{pmatrix} : {}^{\mathrm{t}}B = B,\ {}^{\mathrm{t}}C = C \right\},$$

where ${}^{\mathrm{t}}A$ denotes the transpose of the matrix A. If A is an arbitrary matrix and B is symmetric, then we have the equality

$$\left[\begin{pmatrix} A & 0 \\ 0 & -{}^{\mathrm{t}}A \end{pmatrix}, \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \right] = \begin{pmatrix} 0 & AB + B\,{}^{\mathrm{t}}A \\ 0 & 0 \end{pmatrix}.$$

From this it follows that $[\mathfrak{g}, \mathfrak{g}] \subset \mathfrak{g}$ is the $\mathbb{Z}$-submodule of elements $\left(\begin{smallmatrix} A & B \\ C & -{}^{\mathrm{t}}A \end{smallmatrix}\right)$ with B and C having even diagonal elements. Therefore, it is a submodule of index 2^{2n}. $\square$

2.3. The differential of the quotient maps

We will now describe the differentials of the quotient maps between Chevalley groups in the neighbourhood of a prime $p \in \operatorname{Spec}(\mathbb{Z})$. So we consider the base ring $R = \mathbb{Z}_{(p)}$. Let G be simply connected and let n be the order of the centre of G. Assume moreover that the centre of G is the group of nth roots of unity μ_n (this is the case if G is not of type D_{2l}; for this particular case see § 2.4). Write $n = p^k m$ with m prime to p, and $G_i := G/\mu_{p^i}$. We have the successive quotients

$$G = G_0 \to G_1 \to G_2 \to \cdots \to G_k \to G^{\mathrm{ad}}$$

and the corresponding sequence of Lie algebras

$$\operatorname{Lie}(G) = \operatorname{Lie}(G_0) \to \operatorname{Lie}(G_1) \to \operatorname{Lie}(G_2) \to \cdots \to \operatorname{Lie}(G_k) \xrightarrow{\simeq} \operatorname{Lie}(G^{\mathrm{ad}}).$$

On the generic fibre all these maps are isomorphisms. In order to study what happens on the closed fibre, we set $\mathfrak{g} = \operatorname{Lie}(G)(\mathbb{F}_p)$ and $\mathfrak{g}_i = \operatorname{Lie}(G_i)(\mathbb{F}_p)$, and we let $\mathfrak{z}_i$ respectively $\mathfrak{z}$ denote the centre of $\mathfrak{g}_i$ respectively $\mathfrak{g}$. We start with a lemma.

Lemma 2.12. *The centre $\mathfrak{z}_i$ is isomorphic to the one-dimensional Lie algebra $\mathbb{F}_p$ if $i < k$, and the algebra $\mathfrak{g}_k$ has trivial centre.*

Proof. Let $x \in \mathfrak{g}_i$ be a central element. According to the decomposition of Proposition 2.8, we can write $x = \sum x_\alpha + h$. The lemma is easily checked directly when $\mathfrak{g}_i = \mathfrak{sl}_2$ or $\mathfrak{g}_i = \mathfrak{sp}_{2n}$, so assume we are not in these cases.

According to the following Lemma 2.13, for any root β there exists a finite extension $K/\mathbb{F}_p$ and a point $t \in \mathfrak{t} \otimes K$ such that $\mathrm{d}\beta(t) \neq 0$. We then have $0 = [t, x] = \sum \mathrm{d}\alpha(t) x_\alpha$, from which it follows that $x_\beta = 0$. Thus $x = h \in \mathfrak{t}$. Now, let again β be an arbitrary root and let $0 \neq y \in (\mathfrak{g}_k)_\beta$. We have $0 = [x, y] = \mathrm{d}\beta(x) \cdot y$, therefore $\mathrm{d}\beta(x) = 0$.

Since we can reverse the above argument, the centre of $\mathfrak{g}_i$ consists of all the elements in $\mathfrak{t}$ along which all the roots vanish. With the notation of Proposition 2.8, $\mathfrak{t} \simeq M^\vee \otimes \mathbb{F}_p$, and therefore $\mathfrak{z}_i \simeq \operatorname{Hom}(M/Q(R), \mathbb{F}_p)$. Since $M/Q(R) \subset P(R)/Q(R)$ and in our case $P(R)/Q(R)$ is principal, $M/Q(R)$ is also principal and $\mathfrak{z}_i$ can be at most one dimensional. Moreover, it is trivial if and only if $Q(R) = M$, which means that $\mathfrak{g}_i$ is adjoint, or $i = k$. $\square$

Lemma 2.13. *Assume that $\mathfrak{g}$ is neither isomorphic to $\mathfrak{sl}_2$ nor $\mathfrak{sp}_{2n}$, or that the characteristic of $\mathbb{F}_p$ is not 2. Then there exists a finite extension K of $\mathbb{F}_p$ and $t \in \mathfrak{t} \otimes K$ such that $\forall \alpha \in R$, $\mathrm{d}\alpha(t) \neq 0$.*

Proof. Let R denote the root system of G. By Proposition 2.8 we have $Q(R) \subset M \subset P(R)$. The linear functions on $\mathfrak{t}$ defined over $\mathbb{F}_p$ are in bijection with $M \otimes \mathbb{F}_p$; therefore a root $\alpha \in Q(R)$ will yield a vanishing function on $\mathfrak{t}$ if and only if it is a p-multiple of some element in M. By Lemma 1.4, this can occur only if $p = 2$, $M = P(R)$ (thus G is simply connected) and G is of type A_1 or C_r. By assumption we are not in these cases. Let N be the number of positive roots. Taking a finite extension $K/\mathbb{F}_p$ if needed, $\mathfrak{t}$ is not a union of N hyperplanes, so the lemma is proved. □

Let $\mathfrak{g}' := \mathfrak{g}/\mathfrak{z}$. We can now describe the maps $\mathrm{Lie}(G_i) \to \mathrm{Lie}(G_{i+1})$ on the closed fibre.

Proposition 2.14. *The Lie algebras $\mathfrak{g}_i$ are described as follows.*

(1) *For all i with $0 < i < k$, we have an isomorphism of Lie algebras $\mathfrak{g}_i \simeq \mathfrak{g}' \oplus \mathbb{F}_p$. In particular, all these Lie algebras are isomorphic.*

(2) *For $i = 0$ we have a non-split exact sequence of Lie algebras $0 \to \mathbb{F}_p \to \mathfrak{g}_0 \to \mathfrak{g}' \to 0$.*

(3) *For $i = k$ we have a non-split exact sequence of Lie algebras $0 \to \mathfrak{g}' \to \mathfrak{g}_k \to \mathbb{F}_p \to 0$.*

In these terms, the maps $\mathfrak{g}_i \to \mathfrak{g}_{i+1}$ are described as follows. The map $\mathfrak{g}_0 \to \mathfrak{g}_1$ takes $\mathbb{F}_p$ to zero and maps onto $\mathfrak{g}' \subset \mathfrak{g}_1$, and for all i with $0 < i < k$, the map $\mathfrak{g}_i \to \mathfrak{g}_{i+1}$ takes $\mathbb{F}_p$ to zero and maps $\mathfrak{g}' \subset \mathfrak{g}_i$ isomorphically onto $\mathfrak{g}' \subset \mathfrak{g}_{i+1}$.

Proof. Let $Z_i := \ker(G_i \to G_{i+1})$. For all $i \leqslant k-1$, we have $Z_i \simeq \mu_p$, and its Lie algebra is included in $\mathfrak{z}_i$. Because $Z_i \to G_{i+1}$ is trivial, the map $\mathfrak{g}_i \to \mathfrak{g}_{i+1}$ takes $\mathfrak{z}_i$ to 0.

By tensoring the result of Proposition 2.7 by $\mathbb{F}_p$, there is an exact sequence

$$\mathfrak{g}_i \to \mathfrak{g}_{i+1} \to \mathbb{Z}/p\mathbb{Z} \to 0,$$

from which it follows that $\mathfrak{g}_i/\mathfrak{z}_i$ is mapped isomorphically onto a codimension 1 subalgebra of $\mathfrak{g}_{i+1,\mathbb{F}_p}$ denoted $\mathfrak{g}'_{i+1,\mathbb{F}_p}$. By Lemma 2.12, no $x \in \mathfrak{g}'_{i+1,\mathbb{F}_p}$ can be central in $\mathfrak{g}_{i+1}$ so that we have, for $0 < i < k$,

$$\mathfrak{g}_{i,\mathbb{F}_p} = \mathfrak{g}'_{i,\mathbb{F}_p} \oplus \mathfrak{z}_{i,\mathbb{F}_p}$$

as vector spaces. Since $\mathfrak{g}'_{i,\mathbb{F}_p}$ is a Lie subalgebra, it is also an equality of Lie algebras. In particular all the Lie algebras $\mathfrak{g}_i$ for $0 < i < k$ are isomorphic.

For $i = 0$, we have an exact sequence of Lie algebras $0 \to \mathbb{F}_p \to \mathfrak{g}_{0,\mathbb{F}_p} \to \mathfrak{g}' \to 0$, but this sequence does not split (in fact if it did split, then we would have $[\mathfrak{g}_{0,\mathbb{F}_p}, \mathfrak{g}_{0,\mathbb{F}_p}] \subset \mathfrak{g}'$, contradicting Proposition 2.11).

For $i = k > 0$, we have a sequence $0 \to \mathfrak{g}' \to \mathfrak{g}_{k,\mathbb{F}_p} \to \mathbb{F}_p \to 0$, which again cannot split because $\mathfrak{g}_{k,\mathbb{F}_p}$ has trivial centre, by Lemma 2.12. □

Remark 2.15. For $0 < i < k$, consider the Lie algebras $\mathrm{Lie}(G_i)$, as schemes over $\mathrm{Spec}(\mathbb{Z}_{(p)})$. They have isomorphic underlying vector bundles (namely the trivial vector bundle), and their generic fibres as well as their special fibres are isomorphic as Lie algebras. However, they need not be isomorphic. For example, if $G = \mathrm{SL}_{p^k}$ then it is immediate from Proposition 2.11 that $G_i = G/\mu_{p^i}$ uniquely determines i, because $[\mathrm{Lie}(G_i)(\mathbb{Z}), \mathrm{Lie}(G_i)(\mathbb{Z})] = \mathrm{Lie}(G)(\mathbb{Z})$ and the quotient $\mathrm{Lie}(G_i)(\mathbb{Z})/\mathrm{Lie}(G)(\mathbb{Z})$ is a cyclic abelian group of order p^i. In fact the only difference between them comes from the definition of the Lie bracket on the total space.

2.4. Classical Lie algebras

We now give an explicit description of some of the classical Chevalley Lie algebras, in which the exact sequence of Proposition 2.2 will become very transparent.

Let M be a free $\mathbb{Z}$-module of rank n, and let m be an integer dividing n. We define a $\mathbb{Z}$-Lie algebra $L(M|m)$ as follows: let $\mathrm{Hom}(M, (1/m)M)$ denote the $\mathbb{Z}$-module of linear maps $f : M \otimes \mathbb{Q} \to M \otimes \mathbb{Q}$ such that $f(M) \subset (1/m)M$. The trace of such a map is an element in $(1/m)\mathbb{Z}$. Any such map induces a map $\bar{f} : M/mM \to (1/m)M/M$. Note that multiplication by m induces a canonical isomorphism $(1/m)M/M \simeq M/mM$ so that $\bar{f}$ may be seen as an endomorphism of the free $\mathbb{Z}/m\mathbb{Z}$-module M/mM. Finally, let $L(M|m)$ (respectively $S(M|m)$) denote the submodule of $\mathrm{Hom}(M, (1/m)M)$ of elements f such that $\bar{f}$ is a homothety (respectively $\bar{f}$ is a homothety and f has vanishing trace). These are obviously Lie subalgebras of $\mathrm{End}(M \otimes \mathbb{Q})$.

Proposition 2.16. *Let n, m be as above; then* $\mathrm{Lie}(\mathrm{SL}_n/\mu_m)(\mathbb{Z}) \simeq S(\mathbb{Z}^n|m)$.

Proof. Let n, m be integers such that m divides n. Let $\mathfrak{sl}_n$ denote the Lie algebra of SL_n, and let $\mathfrak{sl}_{n,m}$ denote the Lie algebra of the quotient SL_n/μ_m.

The exact sequence of Proposition 2.2 translates in our case to

$$0 \to \mathfrak{sl}_{n,m}(\mathbb{Z})^\vee \to \mathfrak{sl}_n(\mathbb{Z})^\vee \to \mathbb{Z}/m\mathbb{Z} \to 0.$$

To compute the morphism $\mathfrak{sl}_n(\mathbb{Z})^\vee \to \mathbb{Z}/m\mathbb{Z}$, let us first compute the analogous morphism $\mathfrak{gl}_n(\mathbb{Z})^\vee \to \mathbb{Z}/m\mathbb{Z}$ given by the inclusion $\mu_m \subset \mathrm{GL}_n$. We decompose this inclusion as $\mu_m \subset \mathrm{GL}_1 \subset \mathrm{GL}_n$. The corresponding morphisms are

$$\mathfrak{gl}_n(\mathbb{Z})^\vee \to \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},$$

where the first map is evaluation at the identity (in fact, it is the dual map to the inclusion $\mathrm{Lie}(\mathrm{GL}_1) \to \mathrm{Lie}(\mathrm{GL}_n)$) and the second is the quotient morphism. By restriction to SL_n, the morphism $\mathfrak{sl}_n(\mathbb{Z})^\vee \to \mathbb{Z}/m\mathbb{Z}$ is given by evaluation at I_n modulo m (note that this is well defined since $\mathfrak{sl}_n(\mathbb{Z})^\vee = \mathfrak{gl}_n(\mathbb{Z})^\vee/(\mathrm{trace})$). Let $f_{i,j} : \mathfrak{sl}_n(\mathbb{Q}) \to \mathbb{Q}$ be the linear form $M \mapsto M_{i,j}$. Thus $\mathfrak{sl}_{n,m}(\mathbb{Z})^\vee \subset \mathfrak{sl}_n(\mathbb{Z})^\vee$ is the set of linear forms $\sum \lambda_{i,j} f_{i,j}$ with $m | \sum \lambda_{i,i}$. Since $\mathfrak{sl}_{n,m}(\mathbb{Z})$ is the dual in $\mathfrak{sl}_n(\mathbb{Q})$ of $\mathfrak{sl}_{n,m}(\mathbb{Z})^\vee$, it follows applying $f_{i,j}$ $(i \neq j)$ (respectively $mf_{i,i}$, $f_{i,i} - f_{j,j}$) that if $M \in \mathfrak{sl}_n(\mathbb{Q})$ belongs to $\mathfrak{sl}_{n,m}(\mathbb{Z})$, then $M_{i,j} \in \mathbb{Z}$ (respectively $mM_{i,i} \in \mathbb{Z}$, $M_{i,i} - M_{j,j} \in \mathbb{Z}$). Conversely, matrices satisfying these conditions are certainly in $\mathfrak{sl}_{n,m}(\mathbb{Z})$. The proposition is therefore proved. $\square$

Now, assuming that n is even, we describe the four Lie algebras of type D_n: $\mathfrak{spin}_{2n}$, $\mathfrak{so}_{2n}$, $\mathfrak{pso}_{2n}$, and a fourth one that we denote by $\mathfrak{pspin}_{2n}$. We need to introduce some notation.

Notation 2.17. Let n be an integer and let us consider the following sublattices of $\mathbb{Q}^n$:

- $N_{\mathrm{so}} = \mathbb{Z}^n$;
- N_{ad} is generated by $\mathbb{Z}^n$ and $\frac{1}{2}(1, \ldots, 1)$;
- if l is even, N_{ps} is the sublattice of N_{ad} of elements (x_i) with $\sum x_i$ divisible by 2;
- N_{sc} is the sublattice of $\mathbb{Z}^n$ of elements (x_i) with $\sum x_i$ divisible by 2;
- we denote by L_* ($* \in \{z, \mathrm{ad}, \mathrm{ps}, \mathrm{sc}\}$) the lattice of matrices with off-diagonal coefficients in $\mathbb{Z}$ and with the diagonal in N_*.

Proposition 2.18.

(1) *There is a natural identification of* $\mathfrak{sp}_{2n}(\mathbb{Z})$ *(respectively* $\mathfrak{psp}_{2n}(\mathbb{Z})$*) with the Lie algebra of matrices of the form* $\left(\begin{smallmatrix} A & B \\ C & -{}^{\mathrm{t}}A \end{smallmatrix}\right)$ *with* ${}^{\mathrm{t}}B = B$, ${}^{\mathrm{t}}C = C$ $(n \times n)$*-matrices with coefficients in* $\mathbb{Z}$ *and* $A \in \mathfrak{gl}_n(\mathbb{Z})$ *(respectively* $A \in L(\mathbb{Z}^n|2)$*).*

(2) *Assume n is odd. Then there is a natural identification of* $\mathfrak{so}_{2n}(\mathbb{Z})$ *(respectively* $\mathfrak{pso}_{2n}(\mathbb{Z})$, $\mathfrak{spin}_{2n}(\mathbb{Z})$*) with the Lie algebra of matrices of the form* $\left(\begin{smallmatrix} A & B \\ C & -{}^{\mathrm{t}}A \end{smallmatrix}\right)$ *with* ${}^{\mathrm{t}}B = -B$, ${}^{\mathrm{t}}C = -C$ *and A in* L_{so} *(respectively* L_{ad}, L_{sc}*).*

(3) *Assume n is even. There is a natural identification of* $\mathfrak{so}_{2n}(\mathbb{Z})$ *(respectively* $\mathfrak{pso}_{2n}(\mathbb{Z})$, $\mathfrak{spin}_{2n}(\mathbb{Z})$, $\mathfrak{pspin}_{2n}(\mathbb{Z})$*) with the Lie algebra of matrices of the form* $\left(\begin{smallmatrix} A & B \\ C & -{}^{\mathrm{t}}A \end{smallmatrix}\right)$ *with* ${}^{\mathrm{t}}B = -B$, ${}^{\mathrm{t}}C = -C$ *and A in* L_{so} *(respectively* L_{ad}, L_{sc}, L_{ps}*).*

Proof. This is a direct consequence of Proposition 2.8. For example, let $\mathfrak{g}(\mathbb{Z})$ be a Lie algebra of type D_n over $\mathbb{Z}$. Proposition 2.8 implies that all Lie algebras of type D_n will differ only by their Cartan subalgebras. Therefore, $\mathfrak{g}(\mathbb{Z})$ is in fact a set of matrices of the form $\left(\begin{smallmatrix} A & B \\ C & -{}^{\mathrm{t}}A \end{smallmatrix}\right)$ with ${}^{\mathrm{t}}B = -B$, ${}^{\mathrm{t}}C = -C$, and the off-diagonal coefficients of A in $\mathbb{Z}$. Moreover, with the notation of Proposition 2.8, $\mathfrak{g}(\mathbb{Z})$ corresponds to a module M between the root lattice and the weight lattice, and the Cartan subalgebra (the subalgebra when A is diagonal and $B = C = 0$) identifies with the dual lattice of M. Therefore, the description of the proposition follows from the description of the root and weight lattices in [**5**]. $\square$

Using this description or Lemma 2.12 we can deduce the dimension of the centre of $\mathfrak{g}(\mathbb{F}_2)$:

	$\mathfrak{spin}_{2n}(\mathbb{F}_2)$	$\mathfrak{so}_{2n}(\mathbb{F}_2)$	$\mathfrak{pspin}_{2n}(\mathbb{F}_2)$	$\mathfrak{pso}_{2n}(\mathbb{F}_2)$
n even	2	1	1	0
n odd	1	1	—	0

For example, we give a description of the centre of $\mathfrak{spin}_{2n}(\mathbb{F}_2)$. Let C_1 (respectively C_2) be the matrix of the form $\left(\begin{smallmatrix} A & B \\ C & -{}^{t}A \end{smallmatrix}\right)$ with $B = C = 0$ and $A = I_n$ (the identity matrix, respectively $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, the matrix with only one non-vanishing coefficient in the top-left corner, equal to 2). Note that $C_1, C_2 \in \mathfrak{spin}_{2n}(\mathbb{Z})$ (but C_1, C_2 are not divisible by 2 in $\mathfrak{spin}_{2n}(\mathbb{Z})$). For any matrix B in $\mathfrak{spin}(\mathbb{Z}) \subset \mathfrak{so}(\mathbb{Z})$, we obviously have $[C_1, B] = 0$ and $2|[C_2, B]$. From these remarks it follows that the classes of C_1 and C_2 modulo $2\mathfrak{spin}(\mathbb{Z})$ generate over $\mathbb{F}_2$ the two-dimensional centre of $\mathfrak{spin}_{2n}(\mathbb{F}_2)$.

3. The Chevalley morphism

We start this section by some elementary results on regular elements in Lie algebras of algebraic groups (§ 3.1), to be used in § 3.3, then we prove that the Chevalley morphism is unconditionally schematically dominant (§ 3.2) and finally we prove the the Chevalley morphism is an isomorphism unless $G = \mathrm{Sp}_{2n}$ for some $n \geqslant 1$ (§ 3.3). The case $G = \mathrm{Sp}_{2n}$ will be treated later.

We emphasize that from now on, in contrast for example with § 2.3, the Lie algebras are viewed really as schemes and not merely as vector spaces or modules.

3.1. Regular elements

Let $\mathfrak{g}$ be a restricted Lie algebra of dimension d over a field. For each $x \in \mathfrak{g}$, we denote by $\chi(x) = t^d + c_1(x)t^{d-1} + \cdots + c_{d-1}(x)t + c_d(x)$ the characteristic polynomial of $\operatorname{ad} x$ acting on $\mathfrak{g}$. The *rank* of $\mathfrak{g}$ is the least integer l such that $c_{d-l} \neq 0$, and we set $\delta := c_{d-l}$. An element $x \in \mathfrak{g}$ is called *regular* if the nilspace $\mathfrak{g}_0(\operatorname{ad} x) := \ker(\operatorname{ad} x)^d$ of $\mathfrak{g}$ relative to $\operatorname{ad} x$ has minimal dimension l. (These elements are commonly called *regular semi-simple* and we adopt a simpler terminology within the present article.) For Chevalley groups other than the symplectic group, an element x is regular if and only if $\delta(x) \neq 0$; then, the Cartan subalgebras of minimal dimension are exactly the centralizers of regular elements. For these facts see [**18**, pp. 52–53]. Note also that our definition of regular elements differs from that in [**20**], according to which the singular locus has codimension 3 in $\mathfrak{g}$.

If, furthermore, $\mathfrak{g}$ is the Lie algebra of a smooth connected group G, then in fact the Cartan subalgebras are conjugate, and in particular they all have the same dimension. This is proven in [**10**, Corollary 4.4]. Also, in this case the coefficients of the characteristic polynomial χ are invariant functions for the adjoint action of G on $\mathfrak{g}$.

We will use the notation $\mathrm{Sing}(\mathfrak{g})$ for the closed subscheme of singular elements, defined by the equation $\delta = 0$, and $\mathrm{Reg}(\mathfrak{g})$ for its complement, the open subscheme of regular elements. We have the corresponding subschemes $\mathrm{Sing}(\mathfrak{t})$ and $\mathrm{Reg}(\mathfrak{t})$ in $\mathfrak{t}$.

In the relative situation, if $\mathfrak{g}$ is a Lie algebra of dimension d over a scheme S, then the objects χ, δ, $\mathrm{Reg}(\mathfrak{g})$, $\mathrm{Sing}(\mathfrak{g})$ are defined by the same procedure as above. We recall our general convention that a *relative Cartier divisor* of some S-scheme X is an effective Cartier divisor in X which is flat over S.

Lemma 3.1. *Let G be a split simple Chevalley group over a scheme S, not isomorphic to Sp_{2n}, $n \geqslant 1$. Let $s : \mathrm{Sing}(\mathfrak{g}) \to S$ be the locus of singular elements. Then $s_*\mathcal{O}_{\mathrm{Sing}(\mathfrak{g})}$ is a free $\mathcal{O}_S$-module, in particular $\mathrm{Sing}(\mathfrak{g})$ is a relative Cartier divisor of $\mathfrak{g}$ over S.*

Proof. Since the objects involved have formation compatible with base change, it is enough to prove the lemma over $S = \mathrm{Spec}(\mathbb{Z})$. We have to prove that the ring $\mathbb{Z}[\mathfrak{g}]/(\delta)$ is free as a $\mathbb{Z}$-module. Since δ is homogeneous, this ring is graded. If we can prove that it is flat over $\mathbb{Z}$, then its homogeneous components are flat also, and since they are finitely generated, they are free over $\mathbb{Z}$, and the result follows. So it is enough to prove that $\mathbb{Z}[\mathfrak{g}]/(\delta)$ is flat. By the corollary to Theorem 22.6 in [**14**], it is enough to prove that the coefficients of δ generate the unit ideal, or in other words, that δ is a non-zero function modulo each prime p. So we may now assume that the base is a field k of characteristic $p \geqslant 0$, and we may also assume that k is algebraically closed. Let $\mathfrak{t}$ be the Lie algebra of a maximal torus T. By Lemma 2.13, we can choose $t \in \mathfrak{t}(k)$ such that $\forall \alpha \in R$, $\mathrm{d}\alpha(t) \neq 0$. Then $\delta(t)$ is the product of the scalars $\mathrm{d}\alpha(t)$, up to a sign. Hence it is non-zero. □

We continue with the split simple Chevalley group G over S. In the sequel, products are understood to be fibred products over S. We now turn our attention to the morphism $G/T \times \mathfrak{t} \to \mathfrak{g}$. We use the same construction as in [**16**, 3.17]: note that the normalizer $N_G(T)$ acts on $G \times \mathfrak{t}$ by $n \cdot (g, \tau) = (gn^{-1}, \mathrm{Ad}(n) \cdot \tau)$ and this induces an action of $W = N_G(T)/T$ on $G/T \times \mathfrak{t}$. The morphism $G/T \times \mathfrak{t} \to \mathfrak{g}$ induced by the adjoint action is clearly W-invariant.

Lemma 3.2. *Let G be a split simple Chevalley group over a scheme S, not isomorphic to Sp_{2n}, $n \geqslant 1$. Then the map $G/T \times \mathfrak{t} \to \mathfrak{g}$ is schematically dominant. Its restriction*

$$b : G/T \times \mathrm{Reg}(\mathfrak{t}) \to \mathrm{Reg}(\mathfrak{g})$$

is a W-torsor and hence induces an isomorphism $(G/T \times \mathrm{Reg}(\mathfrak{t}))/W \to \mathrm{Reg}(\mathfrak{g})$.

Proof. Here again, the objects involved have formation compatible with base change, so it is enough to prove the lemma over $S = \mathrm{Spec}(\mathbb{Z})$. We will first prove that b is a W-torsor. It is enough to prove that b is surjective, étale, and that W is transitive in the fibres. Indeed, if b is étale then the action must also be free and b induces an isomorphism $(G/T \times \mathrm{Reg}(\mathfrak{t}))/W \to \mathrm{Reg}(\mathfrak{g})$.

The map $c = \mathrm{ad} : G \times \mathrm{Reg}(\mathfrak{t}) \to \mathrm{Reg}(\mathfrak{g})$ is surjective because if $x \in \mathrm{Reg}(\mathfrak{g})$, then its centralizer $\mathfrak{z}(x)$ is a Cartan subalgebra, and since Cartan subalgebras are conjugate, there exists $g \in G$ such that $(\mathrm{ad}\, g)(\mathfrak{t}) = \mathfrak{z}(x)$. Thus there is $y \in \mathfrak{t}$ such that $(\mathrm{ad}\, g)(y) = x$ and clearly y is regular. We now prove that c is smooth. Since its source and its target are smooth over S, it is enough to prove that for all $s \in S$, the map c_s is smooth. By homogeneity, it is enough to prove that the differential of c_s at any point $(1, t)$ with $t \in \mathrm{Reg}(\mathfrak{t})$ is surjective.

Then $T_1 G_k = \mathfrak{g}_k$ and the tangent map $\psi = \mathrm{d}c : T_1 G_k \times \mathfrak{t}_k \to \mathfrak{g}_k$ is given by $(x, \tau) \mapsto [x, t] + \tau$. Recall that $\mathfrak{g}_k = \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha \oplus \mathfrak{t}_k$, where $[\tau, x] = \mathrm{d}\alpha(\tau) x$ for all $x \in \mathfrak{g}_\alpha$. Again by Lemma 2.13, we can choose $\tau \in \mathfrak{t}_k$ such that $\forall \alpha \in R$, $\mathrm{d}\alpha(\tau) \neq 0$. Thus, we have $\psi(\mathfrak{g}_k \times \{0\}) = \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha$. Since $\psi(\{0\} \times \mathfrak{t}_k) = \mathfrak{t}_k$, ψ is a surjective linear map. It follows that b is also surjective and smooth, hence étale, by dimension reasons.

Finally, let (g, x) and (h, y) have the same image in $\mathfrak{g}$, for $x, y \in \mathfrak{t}$. This means that $(\mathrm{ad}\, w)(x) = y$, where $w = h^{-1}g$. Thus $(\mathrm{ad}\, w)(\mathfrak{z}(x)) = \mathfrak{z}((\mathrm{ad}\, w)(x)) = \mathfrak{z}(y)$, that is to say

$(\operatorname{ad} w)(\mathfrak{t}) = \mathfrak{t}$ since $\mathfrak{z}(x) = \mathfrak{z}(y) = \mathfrak{t}$. By [**11**, 13.2, 13.3], T is the only maximal torus with Lie algebra $\mathfrak{t}$, so it follows that w normalizes T. Hence w defines an element of the Weyl group W.

Now we consider the map $G/T \times \mathfrak{t} \to \mathfrak{g}$. From the preceding discussion it is dominant in the fibres, and since $G/T \times \mathfrak{t}$ is flat over S, the map is itself schematically dominant by [**9**, Théorème 11.10.9]. This concludes the proof of the lemma. □

3.2. The Chevalley morphism is dominant

We now deal with the cases that are not covered by Lemma 3.1.

Notation 3.3. Consider the following subalgebras of $\mathfrak{sl}_2$ and $\mathfrak{sp}_{2n}$.

- Let $\mathfrak{b} \subset \mathfrak{sl}_2$ be the subalgebra of upper-triangular matrices.
- Let L denote the set of long roots of $\mathfrak{sp}_{2n}$; if α is a root, denote by $\mathfrak{sp}_{2n,\alpha}$ the corresponding root space.
- Let $\mathfrak{h} \subset \mathfrak{sp}_{2n}$ be the sum $\mathfrak{t} \oplus \bigoplus_{\alpha \in L} \mathfrak{sp}_{2n,\alpha}$.

Lemma 3.4. *Let k be a field. Then the maps $(\mathrm{SL}_2)_k \times \mathfrak{b}_k \to (\mathfrak{sl}_2)_k$ and $(\mathrm{Sp}_{2n})_k \times \mathfrak{h}_k \to (\mathfrak{sp}_{2n})_k$, given by restricting the adjoint action, are dominant. Moreover, $\mathfrak{h}$ is isomorphic, as a Lie algebra, to $\mathfrak{sl}_2^{\oplus n}$.*

Combining the two statements of this lemma, it follows that in the proof of Theorem 3.6 below, we will be able to replace the Lie subaglebra $\mathfrak{h} \simeq \mathfrak{sl}_2^{\oplus n}$ by a sum of the form $\mathfrak{b}^{\oplus n}$.

Proof. The result about $(\mathfrak{sl}_2)_k$ is an immediate consequence of the fact that, over an algebraically closed field, any matrix is conjugated to an upper-triangular matrix.

To prove that $(\mathrm{Sp}_{2n})_k \times \mathfrak{h}_k \to (\mathfrak{sp}_{2n})_k$ is dominant, we argue as in Lemma 3.2. Since all the short roots are not integer multiples of a weight, we can choose $t \in \mathfrak{t}_k$ such that for all short roots α, we have $\mathrm{d}\alpha(t) \neq 0$. Let S denote the set of short roots of $\mathfrak{sp}_{2n}$. If ψ denotes the differential at $(1,t)$ of the adjoint action, it follows that $\psi(\mathfrak{sp}_{2n} \times \{0\}) \supset \bigoplus_{\alpha \in S} \mathfrak{sp}_{2n,\alpha}$. Since $\mathfrak{h}_k = \mathfrak{t}_k \oplus \bigoplus_{\alpha \in L} \mathfrak{sp}_{2n,\alpha}$, it follows that ψ is surjective and the restriction of the action is dominant.

To prove that $\mathfrak{h} \simeq \mathfrak{sl}_2^{\oplus n}$, one can compute explicitly in the Lie algebra $\mathfrak{sp}_{2n}$. Assume that $\mathfrak{sp}_{2n}$ is defined by the matrix $\left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$, where I denotes the identity matrix of size n. Then a matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ belongs to $\mathfrak{sp}_{2n}$ if and only if $D = -{}^{\mathrm{t}}\!A$ and B and C are symmetric matrices. Choosing the torus $\mathfrak{t} = \{\left(\begin{smallmatrix} d & 0 \\ 0 & -d \end{smallmatrix}\right)\}$ in $\mathfrak{sl}_{2n}$, and ϵ_i the coordinate forms on $\mathfrak{t}$, it is well known and easy to check that the long roots are $\pm 2\epsilon_i$. It follows that $\mathfrak{h} = \{\left(\begin{smallmatrix} d & \delta \\ \epsilon & -d \end{smallmatrix}\right) : d, \delta, \epsilon \text{ diagonal}\}$. Thus $\mathfrak{h}$ is isomorphic to $\mathfrak{sl}_2^{\oplus n}$. □

Lemma 3.5. *Let $S = \operatorname{Spec}(A)$ be an affine base scheme and $\mathfrak{g} = \mathfrak{sl}_2$. Then the restriction morphism $A[\mathfrak{b}]^T \to A[\mathfrak{t}]$ is bijective.*

Proof. Let $f \in A[\mathfrak{b}]$. Writing a typical element in $\mathfrak{b}$ as $\left(\begin{smallmatrix} a & b \\ 0 & -a \end{smallmatrix}\right)$, we identify f with a polynomial in a, b. Since

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} a & t^2 b \\ 0 & -a \end{pmatrix},$$

f is T-invariant if and only if $f(a,b) = f(a,t^2 b) \in A[a,b,t]$. This means that f does not depend on b, and we indeed have an equality $A[\mathfrak{b}]^T = A[\mathfrak{t}]$. □

Using the two preceding lemmas, we can now prove the main result of this section.

Theorem 3.6. *Let S be a scheme and let G be a split simple Chevalley group over S. Then the Chevalley morphism $\pi : \mathfrak{t}/W \to \mathfrak{g}/G$ is schematically dominant.*

Proof. First, let $S = \mathrm{Spec}(\mathbb{Z})$. Let us write $\mathfrak{h} = \mathfrak{b}$ in the case of SL_2, $\mathfrak{h} = \mathfrak{sl}_2^{\oplus n}$ in the case of Sp_{2n}, and $\mathfrak{h} = \mathfrak{t}$ in the other cases. We also write $H = T$ (respectively $H = \mathrm{SL}_2^{\oplus n}$, $H = T$) in the case of SL_2 (respectively Sp_{2n}, the other cases). The adjoint action restricts to a map $\varphi : G \times \mathfrak{h} \to \mathfrak{g}$. If G acts on itself by left translation, trivially on $\mathfrak{h}$, and by the adjoint action on $\mathfrak{g}$, then φ is G-equivariant. Moreover, by Lemmas 3.2 and 3.4, the restriction φ_k of φ to any fibre of $\mathrm{Spec}(\mathbb{Z})$ is dominant. Since the schemes $G \times \mathfrak{h}$ and $\mathfrak{g}$ are flat over $\mathbb{Z}$, it follows from [**9**, Théorème 11.10.9] that φ is universally schematically dominant.

Now we let S be arbitrary, and prove that π is schematically dominant. The question is local over S so we may assume $S = \mathrm{Spec}(A)$ affine. On the function rings, the Chevalley morphism can be decomposed as two successive restriction morphisms $A[\mathfrak{g}]^G \to A[\mathfrak{h}]^H \to A[\mathfrak{t}]$. The theorem amounts to the fact that this composition is injective.

First we concentrate on $A[\mathfrak{g}]^G \to A[\mathfrak{h}]^H$. We have already proved that the map $\varphi^* : A[\mathfrak{g}] \to A[G] \otimes_A A[\mathfrak{h}]$ is injective. This map is G-equivariant, so if $f \in A[\mathfrak{g}]$ is G-invariant, we have

$$\varphi^*(f) \in (A[G] \otimes_A A[\mathfrak{h}])^G = A[G]^G \otimes_A A[\mathfrak{h}] = A \otimes_A A[\mathfrak{h}] = A[\mathfrak{h}].$$

Therefore, $\varphi^*(f) = 1 \otimes i^*(f)$ where $i : \mathfrak{h} \to \mathfrak{g}$ is the inclusion. Since $\varphi^* : A[\mathfrak{g}] \to A[G] \otimes_A A[\mathfrak{h}]$ is injective, it follows that $A[\mathfrak{g}]^G \to A[\mathfrak{h}]$ is injective.

In case $G \neq \mathrm{Sp}_{2l}$, we have $\mathfrak{t} = \mathfrak{h}$ so the proof of the theorem is complete. In case $G = \mathrm{SL}_2$, Lemma 3.5 shows the injectivity of the Chevalley morphism. Finally, let us consider the case of Sp_{2n} with $n > 1$. Since by Lemma 3.4, $\mathfrak{h} \simeq \mathfrak{sl}_2^{\oplus n}$ and $H \simeq \mathrm{SL}_2^n$, and since the theorem is proved for SL_2, we know that $A[\mathfrak{h}]^H \to A[\mathfrak{t}]$ is injective, and we can once again conclude. □

It is interesting to mention an easy consequence of this theorem: if the base scheme is $\mathrm{Spec}(\mathbb{Z})$, then the Chevalley morphism is an isomorphism, see the corollary below. This will of course be a particular case of Theorems 3.11 and 6.6, however, while Theorem 3.11 needs some more work, we get the present result almost for free. This corollary is in fact worthwhile because it shows that if the formation of the adjoint quotient commuted with base change (which is not the case), then we would get the case of a general base scheme

S from the case $S = \mathrm{Spec}(\mathbb{Z})$ and hence everything would be finished right now. So here is this corollary.

Corollary 3.7. *Assume that S is the spectrum of a factorial ring with characteristic prime to the order of W. Then the Chevalley morphism $\pi : \mathfrak{t}/W \to \mathfrak{g}/G$ is an isomorphism.*

Proof. Let $S = \mathrm{Spec}(A)$ and let K be the fraction field of A. By Theorem 3.6 it is enough to prove that the restriction morphism res : $A[\mathfrak{g}]^G \to A[\mathfrak{t}]^W$ is surjective. Let P be a W-invariant function on $\mathfrak{t}$. From the assumption on the characteristic of K, it follows that $K[\mathfrak{g}]^G \to K[\mathfrak{t}]^W$ is an isomorphism, so there is $Q \in K[\mathfrak{g}]^G$ such that $\mathrm{res}(Q) = P$. Since A is factorial, we can write $Q = cQ_0$ where Q_0 is a primitive polynomial (i.e. the greatest common divisor of its coefficients is 1) and $c \in K$ is the content of Q. If we write $c = r/s$ with r and s coprime in A, we claim that s is a unit in A. For, otherwise, some prime $p \in A$ divides s. Then $\mathrm{res}(\overline{rQ_0}) = \overline{sP} = 0$ in $(A/p)[\mathfrak{t}]^W$ so $\mathrm{res}(\bar{Q}_0) = 0$ in $(A/p)[\mathfrak{t}]^W$, since r and s are coprime. By Theorem 3.6 again, it follows that $\bar{Q}_0 = 0$ in $(A/p)[\mathfrak{g}]^G$, in contradiction with the fact that Q_0 is primitive. Hence $Q \in A[\mathfrak{g}]^G$ as was to be proved. $\square$

3.3. The Chevalley morphism is an isomorphism for $G \neq \mathrm{Sp}_{2n}$

Before we can give the proof of the main result (Theorem 3.11), we need a technical result which we establish in a sequence of three lemmas. The starting point, in the first lemma below, is a variation on a statement used in Springer and Steinberg [**16**] (see Chapter II, the proof of Theorem 3.17′, point (2) therein). However, we were not able to understand their proof.* Since moreover we need a slightly more general result, we provide a proof.

In the following, if M is a module over a ring A, we say that $a \in A$ *divides* $m \in M$ if and only if $m = am'$ for some $m' \in M$. In this case, we write $a \mid m$.

Lemma 3.8. *Let k be a field, V a k-vector space, endowed with the trivial G-action. Consider the $k[\mathfrak{g}]$-module $V[\mathfrak{g}] := V \otimes k[\mathfrak{g}]$, endowed with the tensor product action of G. Let $d \in k[\mathfrak{g}]$ and $a \in V[\mathfrak{g}]$ be such that d is G-invariant and the class of a modulo $dV[\mathfrak{g}]$ is G-invariant. Then $d_{|\mathfrak{t}} \mid a_{|\mathfrak{t}}$ implies $d \mid a$.*

Proof. Considering the coordinates of a in a k-basis of V, we may assume that $V = k$. We may further assume that k is algebraically closed. We fix a base of the root system and we consider the Borel subalgebra $\mathfrak{b} = \mathfrak{t} \oplus \bigoplus_{\alpha>0} \mathfrak{g}_\alpha$.

We will use the assumptions to argue that for a point $x \in \mathfrak{g}$ such that $d(x) = 0$, the function a is constant on the closure of the G-orbit of x (the *closed orbit*, for short). To see this, just note that for all $g \in G$, since a is invariant modulo d, there exists $r \in k[\mathfrak{g}]$

* We refer to point (2) of the proof of Theorem 3.17′ in [**16**, Chapter II]. The sentence ‘this can be proved like the corresponding result. . . ’ requires the reader to go to point (2) in the proof of Theorem 6.16 of [**17**]. In this proof, Steinberg uses statement 6.4 that a certain map β is an isomorphism. However, in [**16**] the corresponding map β is precisely the one we want to prove is an isomorphism, so it seems that this justification cannot be used as it stands.

such that $g^{-1}a = a + dr$, so that $a(gx) = a(x) + d(x)r(x) = a(x)$. By continuity, a is constant on the closed orbit of x.

We come to the proof itself. First, assume that d has no square factors. Let $x \in \mathfrak{g}$ be such that $d(x) = 0$; it is enough to show that $a(x) = 0$. Since the Borel subalgebras are conjugated and their union is $\mathfrak{g}$, there exists $g \in G$ such that $x' := gx$ lies in $\mathfrak{b}$. Since d is invariant, we have $d(x') = d(x) = 0$, so that a is constant on the orbit of x and $a(x') = a(x)$. Thus we may replace x by x' and hence assume that x belongs to $\mathfrak{b}$. Write $x = \tau + \sum_{\alpha>0} x_\alpha$ with $\tau \in \mathfrak{t}$ and $x_\alpha \in \mathfrak{g}_\alpha$. It is a standard fact that the toral part τ lies in the closed orbit of x under G. To see this, choose an element $\omega^\vee$ in the coroot lattice such that $n_\alpha := \langle \omega^\vee, \alpha \rangle$ is positive for all roots $\alpha > 0$ (for example, one may take $\omega^\vee$ equal to the sum of the coroots $\alpha^\vee$ for $\alpha > 0$). To it, is associated a one-parameter-subgroup $X : \mathbb{G}_m \to T$ such that $\alpha(X(t)) = t^{n_\alpha}$ for all $\alpha > 0$. Thus X acts via

$$X(t)x = \tau + \sum_{\alpha>0} t^{n_\alpha} x_\alpha$$

and we see that τ is in the closed orbit of x. Therefore, $d(\tau) = d(x) = 0$ and $a(x) = a(\tau)$. Since $d_{|\mathfrak{t}}$ divides $a_{|\mathfrak{t}}$ we get $a(\tau) = 0$ and the lemma is proved in case d is square-free.

Now let d be arbitrary and write $d = d_1 d_2$ where d_1 is the product of the prime factors of d, with multiplicity 1. Thus d_1 is square-free, and since G is connected and hence has no non-trivial characters, we see that d_1 is G-invariant. Since $(d_1)_{|\mathfrak{t}} \mid a_{|\mathfrak{t}}$ we have $d_1 \mid a$ and there exists a_2 such that $a = d_1 a_2$. If $(d_1)_{|\mathfrak{t}} = 0$ then $d_1 = 0$ by invariance, hence $a = 0$ and the lemma is proved. Otherwise, since $k[\mathfrak{t}]$ is a domain, we find that $(d_2)_{|\mathfrak{t}} \mid (a_2)_{|\mathfrak{t}}$, and the lemma follows again by induction on the degree of d. $\square$

Lemma 3.9. *Let A be a complete local ring with maximal ideal M, and let $a, d \in A[\mathfrak{g}]^G$. Assume that the degree of d is equal to the degree of its reduction modulo M. Then $d_{|\mathfrak{t}} \mid a_{|\mathfrak{t}}$ implies $d \mid a$.*

Proof. Let $k := A/M$ and $\tilde{a}$ denote the reduction of a modulo M. It follows from the assumptions that $\tilde{d}_{|\mathfrak{t}}$ divides $\tilde{a}_{|\mathfrak{t}}$, hence $\tilde{d}$ divides $\tilde{a}$ by Lemma 3.8, hence

$$\deg(a) - \deg(d) \geqslant \deg(\tilde{a}) - \deg(d) = \deg(\tilde{a}) - \deg(\tilde{d}) \geqslant 0.$$

Let $A[\mathfrak{g}]_0 \subset A[\mathfrak{g}]$ be the submodule of $A[\mathfrak{g}]$ of polynomials of degree bounded by $\deg(a) - \deg(d)$. We will construct a sequence of elements $b_j \in A[\mathfrak{g}]_0$ such that $a \equiv b_j d$ modulo $M^j[\mathfrak{g}]$, converging to some b such that $a = bd$ in $A[\mathfrak{g}]$. The element b_1 is provided by the lemma above. By induction, assume that b_j has been found. Let $\overline{a - b_j d}$ denote the class of $a - b_j d$ in $M^j/M^{j+1}[\mathfrak{g}]$. Then $\overline{a - b_j d}$ is invariant modulo d and $\overline{(a - b_j d)}_{|\mathfrak{t}}$ is divisible by $d_{|\mathfrak{t}}$. Thus by Lemma 3.8 applied with $V = M^j/M^{j+1}$, there exists $\bar{c} \in M^j/M^{j+1}[\mathfrak{g}]$ such that $\overline{a - b_j d} - \overline{cd} = 0$. Using the assumption that d has the same degree as its reduction modulo M, we find that the degree of $\bar{c}$ is bounded by $\deg(a) - \deg(d)$. Let $c \in M^j[\mathfrak{g}]_0$ be a lift of $\bar{c}$, and set $b_{j+1} = b_j + c$. We get $a - (b_{j+1})d \in M^{j+1}[\mathfrak{g}]_0$. Since $b_{j+1} \equiv b_j$ modulo M^j in the module $A[\mathfrak{g}]_0$ which is a free finitely generated A-module, hence complete, the sequence (b_j) has a limit b in $A[\mathfrak{g}]$, and $a = bd$. $\square$

Lemma 3.10. *Let A be any ring. Let δ be the equation of the locus of singular elements in $\mathfrak{g}$ (see § 3.1). Let $a \in A[\mathfrak{g}]^G$ and assume $\delta_{|\mathfrak{t}} \mid a_{|\mathfrak{t}}$. Then $\delta \mid a$.*

Proof. Let $A_0 \subset A$ be the $\mathbb{Z}$-algebra generated by the finitely many coefficients of a and δ. It is enough to prove that δ divides a in $A_0[\mathfrak{g}]$. In other words, we may replace A by A_0 and hence assume that A is noetherian.

Let $D = \mathrm{Sing}(\mathfrak{g}) = \{\delta = 0\}$ be the locus of singular elements and $p : D \to S = \mathrm{Spec}(A)$ the structure morphism. We claim that the condition $\delta \mid a$ defines a closed subscheme of S. Indeed, from Lemma 3.1 we know that the algebra $p_*\mathcal{O}_D$ is locally free over S. Since the claim is local, we may localize and hence assume it is free. Let a_i be the finitely many non-zero components of $a_{|D}$ on some basis of $\Gamma(D, \mathcal{O}_D)$ as a free A-module. Then $\delta \mid a$ if and only if all the a_i vanish. Since D is a relative Cartier divisor, the formation of these objects commutes with base change, so that the above description is functorial, and the condition $\delta \mid a$ is represented by the closed subscheme $S_0 \subset S$ defined by the ideal $I \subset A$ generated by the coefficients a_i.

We want to prove that $S_0 = S$, or in other words $I = 0$. Since this is a local problem, we may replace A by its localization at some prime ideal. Since A is noetherian, its completion is a faithfully flat ring extension so we may replace A by its completion and hence assume that it is complete. Then the claim is just Lemma 3.9. □

We can now prove our main result.

Theorem 3.11. *Let S be a scheme and let G be a split simple Chevalley group over S. Assume that G is not isomorphic to Sp_{2n}, $n \geqslant 1$. Then the Chevalley morphism $\pi : \mathfrak{t}/W \to \mathfrak{g}/G$ is an isomorphism.*

Proof. By Theorem 3.6 it is enough to prove that the map on functions is surjective. Let f be a W-invariant function on $\mathfrak{t}$ and let f_1 be the function on $G/T \times \mathfrak{t}$ defined by $f_1(g, x) = f(x)$. Since it is W-invariant, it induces a function on $(G/T \times \mathfrak{t})/W$ which we denote by the letter f_1 again. By Lemma 3.2 the function $h := f_1 \circ b^{-1}$ is a G-invariant relative meromorphic function whose domain of definition contains $\mathrm{Reg}(\mathfrak{g})$. We may write $h = k/\delta^m$ for some function k not divisible by δ, and some integer m. Since k is G-invariant on a schematically dense open subset, it is G-invariant. Assume that $m \geqslant 1$. Let $s \in S$ be a point. Since a generic element of $\mathfrak{t}_s$ is regular, h is defined as a relative rational function on $\mathfrak{t}$. By definition of b, we moreover have $h_{|\mathfrak{t}} = f$. It follows that we have

$$k_{|\mathfrak{t}} = f \cdot \delta_{|\mathfrak{t}}^m.$$

Lemma 3.10 implies that δ divides k. This is a contradiction with our assumptions, therefore h is a regular function extending f to a G-invariant function on $\mathfrak{g}$. □

In the remaining sections, we compute explicitly the ring of invariants in the case where G is one of the groups SO_{2n}, SO_{2n+1} or Sp_{2n}.

4. The orthogonal group $\mathbf{SO_{2n}}$

In the case of the group $G = \mathrm{SO}_{2n}$, the explicit computation will prove that the formation of the adjoint quotient for the Lie algebra does not commute with all base changes. In fact, we will be able to describe exactly when commutation holds. We will see also that over a base field, the quotient is always an affine space.

4.1. Definition of $\mathbf{SO_{2n}}$

4.1.1. *The orthogonal group*

The free $\mathbb{Z}$-module of rank $2n$ is denoted by E; we think of it as the trivial vector bundle over $\mathrm{Spec}(\mathbb{Z})$. The standard quadratic form of E is defined for $v = (x_1, y_1, \dots, x_n, y_n)$ by

$$q(v) = x_1y_1 + \cdots + x_ny_n.$$

It is non-degenerate in the sense that $\{q = 0\} \subset \mathbb{P}(E)$ is smooth over $\mathbb{Z}$. The polarization of q is

$$\langle v, v'\rangle = q(v + v') - q(v) - q(v') = x_1y_1' + x_1'y_1 + \cdots + x_ny_n' + x_n'y_n.$$

The orthogonal group O_{2n} is the set of transformations $P \in \mathrm{GL}_{2n}$ that preserve q, more precisely, the zero locus of the morphism Ψ from GL_{2n} to the vector space of quadratic forms defined by $\Psi(P) = q \circ P - q$. Thus the Lie algebra $\mathfrak{o}_{2n}$ is the subscheme of $\mathfrak{gl}_{2n}$ composed of matrices M such that by $d\Psi_{\mathrm{Id}}(M) = 0$ with

$$d\Psi_{\mathrm{Id}}(M)(v) = \langle v, Mv\rangle.$$

It is not hard to verify that $\mathfrak{o}_{2n} \subset \mathfrak{gl}_{2n}$ is a direct summand of the expected dimension, so that O_{2n} is a smooth group scheme over $\mathbb{Z}$.

Remark 4.1. Let us denote by B the matrix of the polarization of q. Clearly, an orthogonal matrix P preserves the polarization, and it follows that ${}^{\mathrm{t}}PBP = B$. However, one checks easily that the closed subgroup scheme $X \subset \mathrm{GL}_{2n}$ defined by the equations ${}^{\mathrm{t}}PBP = B$ is not flat over $\mathbb{Z}$ because its function ring has 2-torsion. In fact O_{2n} is the biggest subscheme of X which is flat over $\mathbb{Z}$. Accordingly $\mathrm{Lie}(X) \subset \mathfrak{gl}_{2n}$ is defined by ${}^{\mathrm{t}}MB + BM = 0$, and $\mathfrak{o}_{2n}$ is the biggest $\mathbb{Z}$-flat subscheme of $\mathrm{Lie}(X)$.

4.1.2. *Dickson's invariant*

Over any field k, it is well known that $\mathrm{O}_{2n} \otimes k$ has two connected components. In odd characteristic, the determinant takes the value 1 on one and -1 on the other. In characteristic 2 the determinant does not help to separate the connected components. Instead one usually uses Dickson's invariant $D(P)$ defined, for an orthogonal matrix P, to be 0 if and only if P acts trivially on the even part of the centre of the Clifford algebra. Equivalently, $D(P) = 0$ if and only if P is a product of an even number of reflections (there is just one exception; see [**19**, p. 160]). Here is a more modern, base-ring-free way to consider the determinant and Dickson's invariant altogether.

Lemma 4.2. *Let* det $\in \mathbb{Z}[\mathrm{O}_{2n}]$ *be the determinant. Then, there is a unique element* $\delta \in \mathbb{Z}[\mathrm{O}_{2n}]$ *such that* $\det = 1 + 2\delta$.

Proof. Since for any $P \in \mathrm{O}_{2n}$, we have $\det(P) \in \{-1, 1\}$, the function $\det -1$ vanishes on the fibre $\mathrm{O}_{2n} \otimes \mathbb{F}_2$. Since $\mathrm{O}_{2n} \otimes \mathbb{F}_2$ is reduced, 2 divides $\det -1$, yielding the existence of δ. It is unique because O_{2n} is flat over $\mathbb{Z}$, and in particular has no 2-torsion. □

Let us introduce the $\mathbb{Z}$-group scheme

$$\mathcal{G} = \mathrm{Spec}\left(\mathbb{Z}\left[u, \frac{1}{1+2u}\right]\right)$$

with unit $u = 0$ and multiplication $u * v = u + v + 2uv$. Its fibre at 2 is isomorphic to the additive group while all other fibres are isomorphic to the multiplicative group. When one passes from det to δ, the multiplicativity formula $\det(P_1P_2) = \det(P_1)\det(P_2)$ gives $\delta(P_1P_2) = \delta(P_1) + \delta(P_2) + 2\delta(P_1)\delta(P_2)$. In other words, we have the following lemma.

Lemma 4.3. δ *defines a morphism of groups* $\mathrm{O}_{2n} \to \mathcal{G}$. □

The schematic image of δ is the subgroup of $\mathcal{G}$ given by $u(u + 1) = 0$, isomorphic to the constant $\mathbb{Z}$-group scheme $\mathbb{Z}/2\mathbb{Z}$.

Definition 4.4. We define SO_{2n} as the kernel of δ.

The group SO_{2n} is smooth over $\mathbb{Z}$ with connected fibres. The closed subgroup scheme T of diagonal matrices in SO_{2n} is a maximal torus, we denote by $\mathfrak{t}$ its Lie algebra and by λ_i its coordinate functions. Its normalizer N is the closed subgroup scheme of orthogonal monomial matrices. The Weyl group $W = N/T$ is the semi-direct product $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$ where $\mathfrak{S}_n$ is the symmetric group on n letters. It acts on T as follows. The subgroup $(\mathbb{Z}/2\mathbb{Z})^{n-1}$ is generated by the transformations $\varepsilon_{i,j}$ which take λ_i and λ_j to their opposite and leave all other λ_k unchanged. The subgroup $\mathfrak{S}_n$ permutes the λ_i. The action of W on $\mathfrak{t}$ has analogous expressions that are immediate to write down.

4.1.3. *The Pfaffian*

Recall that there is a unique function on $\mathfrak{so}_{2n}$, called the *Pfaffian* and denoted pf, such that $\det(M) = (-1)^n(\mathrm{pf}(M))^2$. (The sign $(-1)^n$ comes from the fact that in our context, the Pfaffian is $\mathrm{pf}'(BM)$ where pf' is the usual Pfaffian and B is the matrix of Remark 4.1.) Furthermore, the Pfaffian is invariant for the adjoint action of SO_{2n}.

4.2. Invariants of the Weyl group

We denote by $\mathfrak{t}$ the n-dimensional affine space with coordinate functions X_i, and by W the group generated by the permutations of the coordinates and the reflections $\varepsilon_{i,j}$ which map X_i and X_j to their opposite and leave the other coordinates invariant. We denote by σ_k the complete elementary symmetric functions in n variables.

Proposition 4.5. *Let A be a ring, then $A[\mathfrak{t}]^W$ is generated by $X_1 \cdots X_n$, $\sigma_k(X_i^2)$, and $x\sigma_k(X_i)$, where $k < n$ and x runs through the 2-torsion ideal of A.*

Proof. Let F be a function in $X_1, \dots, X_n$ which is invariant under the Weyl group. Let us say that a monomial is *good* if the exponents of its variables X_i all have the same parity (this is either a monomial in the X_i^2, or $X_1 \cdots X_n$ times a monomial in the X_i^2). We say that it is *bad* otherwise. We can write uniquely F as the sum of its good part and its bad part:

$$F(X_1, \dots, X_n) = F_1(X_1^2, \dots, X_n^2, X_1 \cdots X_n) + F_2(X_1, \dots, X_n).$$

The group W respects this decomposition, hence F being W-invariant, its good and bad parts also are. In particular they are $\mathfrak{S}_n$-invariant, so that

$$F(X_1, \dots, X_n) = G_1(\sigma_1(X_i^2), \dots, \sigma_{n-1}(X_i^2), X_1 \cdots X_n) + G_2(\sigma_1(X_i), \dots, \sigma_n(X_i)).$$

Letting the $\varepsilon_{i,j}$ act, we see that all coefficients of G_2 must be 2-torsion. The proposition is therefore proved. □

4.3. Computation of the Chevalley morphism

In this subsection we will describe explicitly the invariants of $\mathfrak{so}_{2n}$ under SO_{2n} that correspond to the Weyl group invariants under Theorem 3.11, see Theorem 4.8 below. The Lie algebra $\mathfrak{so}_{2n}$ has a universal matrix M whose most important attributes are its characteristic polynomial χ and its Pfaffian $\mathrm{pf} = \mathrm{pf}(\mathsf{M})$. In fact M and χ are the restrictions of the universal matrix of $\mathfrak{gl}_{2n}$ and its characteristic polynomial. From the equality ${}^t\mathsf{M}B + B\mathsf{M} = 0$ (see Remark 4.1) it follows that χ is an even polynomial, that is to say

$$\chi(t) = \det(t\,\mathrm{Id} - \mathsf{M}) = t^{2n} + c_2 t^{2n-2} + \cdots + c_{2n}.$$

The functions c_{2i} are invariants of the adjoint action; note that

$$c_{2n} = \det(\mathsf{M}) = (-1)^n (\mathrm{pf}(\mathsf{M}))^2.$$

There are some more invariants coming from characteristic 2. Indeed, in this case it follows from Proposition 2.18 that homotheties belong to $\mathfrak{so}_{2n}$ and thus we can define the *Pfaffian characteristic polynomial* by

$$\pi_{\mathbb{F}_2}(t) = \mathrm{pf}(t\,\mathrm{Id} - \mathsf{M}_{\mathbb{F}_2}).$$

We have $\chi_{\mathbb{F}_2}(t) = (\pi_{\mathbb{F}_2}(t))^2$. Now let us consider one particular lift of $\pi_{\mathbb{F}_2}$ to $\mathbb{Z}$.

Definition 4.6. Let $\sigma\colon \mathbb{F}_2 \to \mathbb{Z}$ be such that $\sigma(0) = 0$ and $\sigma(1) = 1$. The polynomial $\pi \in \mathbb{Z}[\mathfrak{so}_{2n}][t]$ is defined as $\pi(t) = t^n + \pi_1 t^{n-1} + \cdots + \pi_{n-1} t + \pi_n$ where $\pi_n := \mathrm{pf}(\mathsf{M})$ and the other coefficients π_i $(1 \leqslant i \leqslant n-1)$ are the lifts of the corresponding coefficients of $\pi_{\mathbb{F}_2}$ via σ.

We note that for any ring A, the (images of the) elements $\pi_1, \dots, \pi_{n-1}, \pi_n$ are algebraically independent over A, because they restrict on a maximal torus to the functions $\sigma_i(X_j)$, the symmetric functions in the coordinates, which are themselves algebraically independent over A. We defined the functions π_i by arbitrary lifting, but we can make them somehow universal.

Proposition 4.7. *Let $\mathcal{O}$ be the ring $\mathbb{Z}[X]/(2X)$ and denote by τ the image of X in $\mathcal{O}$. Then $(\mathcal{O}, \tau)$ is universal among rings with a 2-torsion element. Moreover, any monomial function $\tau(\pi_1)^{\alpha_1} \cdots (\pi_{n-1})^{\alpha_{n-1}}$ on $\mathfrak{so}_{2n,\mathcal{O}}$ is independent of the choice of the lifts π_i and invariant under the adjoint action of $\mathrm{SO}_{2n,\mathcal{O}}$. Finally, for each $i \in \{1, \ldots, n\}$ we have $\tau(\pi_i)^2 = \tau c_{2i}$.*

Proof. The universality statement about $(\mathcal{O}, \tau)$ means that for any pair (A, x) where A is a ring and x is a 2-torsion element of A, there is a unique morphism $f : \mathcal{O} \to A$ such that $f(\tau) = x$. This is obvious. Since $2\tau = 0$, it is clear also that $\tau(\pi_1)^{\alpha_1} \cdots (\pi_{n-1})^{\alpha_{n-1}}$ is independent of the choice of π_i. The fact that this monomial is invariant comes from the invariance of the Pfaffian characteristic polynomial in characteristic 2. Finally, the equalities $\tau(\pi_i)^2 = \tau c_{2i}$ come from the equalities $(\pi_i)^2 = c_{2i}$ in characteristic 2. □

Proposition 4.7 implies in particular that for any ring A and any $x \in A[2]$, the quantity $x(\pi_1)^{\alpha_1} \cdots (\pi_{n-1})^{\alpha_{n-1}}$ is a well-defined invariant function on $\mathfrak{so}_{2n,A}$.

Theorem 4.8. *Let A be a ring, $G = \mathrm{SO}_{2n,A}$, $\mathfrak{g} = \mathfrak{so}_{2n,A}$. The ring of invariants $A[\mathfrak{g}]^G$ is*

$$A[c_2, c_4, \ldots, c_{2n-2}, \mathrm{pf}; x(\pi_1)^{\epsilon_1} \cdots (\pi_{n-1})^{\epsilon_{n-1}}],$$

where x runs through a set of generators of the 2-torsion ideal $A[2] \subset A$, and $\epsilon_i = 0$ or 1, not all 0.

Proof. By Theorem 3.11 and Proposition 4.5, we have

$$A[\mathfrak{g}]^G = A[\sigma_k(X_i^2); X_1 \cdots X_n; x\sigma_k(X_i)],$$

where as before the X_i are the coordinate functions on the torus. We now use the previous proposition. Since c_{2k} restricts on the torus to $\pm\sigma_k(X_i^2)$, the Pfaffian restricts to $X_1 \cdots X_n$, $x\pi_k$ restricts to $x\sigma_k(X_i)$, and since $x\pi_i^2 = xc_{2i}$, the theorem is proved. □

The behaviour of the ring of invariants is therefore controlled by the 2-torsion. More precisely, for a scheme S let $S[2]$ be the closed subscheme defined by the ideal of 2-torsion. If $f : S' \to S$ is a morphism of schemes, we always have $S'[2] \subset f^*S[2]$. We have the following corollary.

Corollary 4.9.

(1) *The formation of the quotient in the previous theorem commutes with a base change $f : S' \to S$ if and only if $f^*S[2] = S'[2]$. This holds in particular if 2 is invertible in $\mathcal{O}_S$, or if $2 = 0$ in $\mathcal{O}_S$, or if $S' \to S$ is flat.*

(2) *Assume that S is noetherian and connected. Then the quotient is of finite type over S, and is flat over S if and only if $S[2] = S$ or $S[2] = \emptyset$.*

Proof. First we recall some general facts on the formation of the ring of invariants for the action of an affine S-group scheme G acting on an affine S-scheme X. The formation of $X/G = \mathrm{Spec}((\mathcal{O}_X)^G)$ commutes with flat base change, and in particular with open immersions. It follows that if (S_i) is an open covering of S then with obvious notation X_i/G_i is an open set in X/G, and X/G can be obtained by gluing the schemes X_i/G_i. Therefore, if $(S'_{i,j})$ is an open covering of $S_i \times_S S'$ for all i, the formation of the quotient commutes with the base change $S' \to S$ if and only if for all i, j the formation of the quotient X_i/G_i commutes with the base change $S'_{i,j} \to S_i$. This reduces the proof to the case of a base change of affine schemes $S' = \mathrm{Spec}(A') \to S = \mathrm{Spec}(A)$.

Call B (respectively B') the ring of invariants over A (respectively A'). Observe that B inherits a graduation from the graduation of the function algebra of $\mathfrak{so}_{2n,A}$, and its only homogeneous elements of degree 1 are those of the form $x\pi_1$ with $x \in A[2]$. We proceed to prove (1) and (2).

(1) The base change morphism $B \otimes_A A' \to B'$ is $A'[\underline{c}, \mathrm{pf}, x\underline{\pi}^\epsilon] \to A'[\underline{c}, \mathrm{pf}, x'\underline{\pi}^\epsilon]$ where

$$\underline{c} = (c_2, c_4, \dots, c_{2n-2}), \quad x\underline{\pi}^\epsilon = x(\pi_1)^{\epsilon_1} \cdots (\pi_{n-1})^{\epsilon_{n-1}}, \quad \text{with } x \in A[2],$$

and $x'\underline{\pi}^\epsilon$ is the same quantity with $x' \in A'[2]$. This map is clearly injective. If it is surjective, then in particular for any $x' \in A'[2]$ we have $x'\pi_1 \in A'[\underline{c}, \mathrm{pf}, x\underline{\pi}^\epsilon]$. Thus there is $a' \in A'$ and $x \in A[2]$ such that $x'\pi_1 = a'x\pi_1$. Since π_1 is a non-zero divisor we get $x' = a'x$, so $A'[2]$ is the image of $A[2]$. This is exactly the assertion that $f^*S[2] = S'[2]$. The converse is easy, as well as the particular cases stated in assertion (1).

(2) If A is noetherian, $A[2]$ is finitely generated and then B is of finite type over A. Now let $I := A[2]$. If $I = 0$ then B is a polynomial ring, and this is also the case if $I = A$ because then $c_2, c_4, \dots, c_{2n-2}$ are polynomials in $\mathrm{pf}(\mathsf{M}), \pi_1, \dots, \pi_{n-1}$. It remains to prove that if B is flat over A then $I = 0$ or $I = A$. In this case the 2-torsion ideal of B is IB, as we see from tensoring by B the exact sequence

$$0 \to A/I \xrightarrow{\times 2} A \to A/2A \to 0.$$

So for any $y \in I$, we have $y\pi_1 \in B[2] = IB$ hence we may write $y\pi_1 = i_1b_1 + \cdots + i_rb_r$ with $i_k \in I$ and $b_k \in B$. Let $x_k\pi_1$ be the degree 1 component of b_k, then by taking the components of degree 1 and using the fact that π_1 is a non-zero divisor, we find $y = i_1x_1 + \cdots + i_rx_r \in I^2$. Thus $I = I^2$, and if the spectrum of A is connected, this implies $I = 0$ or $I = A$. □

5. The orthogonal group $\mathbf{SO_{2n+1}}$

For $G = \mathrm{SO}_{2n+1}$, the computation of the quotient is a little more involved since using the natural representation of dimension $2n+1$ brings some trouble, as we explain below. We show which point of view on SO_{2n+1} will lead to the definition of the correct invariants. Then, the results are essentially the same as for $G = \mathrm{SO}_{2n}$.

5.1. Definition of $\mathbf{SO_{2n+1}}$

In this section, E is the free $\mathbb{Z}$-module $\mathbb{Z}^{2n+1}$. Its standard quadratic form q is

$$q(v) = x_1y_1 + \cdots + x_ny_n + z^2,$$

where $v = (x_1, y_1, \dots, x_n, y_n, z)$. It is non-degenerate, and its polarization is

$$\langle v, v' \rangle = q(v + v') - q(v) - q(v') = x_1 y_1' + x_1' y_1 + \cdots + x_n y_n' + x_n' y_n + 2zz'.$$

In contrast with the even-dimensional case, in characteristic 2 the polarization has a non-zero radical which is the line generated by the last basis vector of $E \otimes \mathbb{F}_2$.

Now, let $\tilde{E} = \mathbb{Z}^{2n+2}$ with canonical basis $(e_1, e_1', \dots, e_{n+1}, e_{n+1}')$ and standard quadratic form defined (as in § 4.1) by $q(v) = x_1 y_1 + \cdots + x_{n+1} y_{n+1}$, where $v = (x_1, y_1, \dots, x_{n+1}, y_{n+1})$. We consider the isometric embedding $i \colon E \hookrightarrow \tilde{E}$ given by

$$i(x_1, y_1, \dots, x_n, y_n, z) = (x_1, y_1, \dots, x_n, y_n, z, z).$$

Since i is an isometry, it is harmless to use the same letter for q and for $q_{|E}$. The orthogonal subspace of E in $\tilde{E}$ is the free rank 1 submodule generated by the vector $\varepsilon = e_{n+1} - e_{n+1}'$. Note that the group of transformations of $(\tilde{E}, q)$ is the group O_{2n+2} as defined in § 4.1. Then we define SO_{2n+1} as a closed subgroup scheme of SO_{2n+2} by

$$\mathrm{SO}_{2n+1} = \{P \in \mathrm{SO}_{2n+2},\ P(\varepsilon) = \varepsilon\}.$$

Accordingly, its Lie algebra is

$$\mathfrak{so}_{2n+1} = \{M \in \mathfrak{so}_{2n+2},\ M(\varepsilon) = 0\}.$$

It is a simple exercise to verify that $\mathfrak{so}_{2n+1} \subset \mathfrak{so}_{2n+2}$ is a direct summand of the expected dimension, so that SO_{2n+1} is a smooth group scheme over $\mathbb{Z}$.

Remark 5.1. Let $O(q_{|E})$ be the group of linear transformations of E that preserve q, and $\mathrm{SO}(q_{|E})$ the kernel of the Dickson invariant. Since a matrix $P \in \mathrm{SO}_{2n+1}$ preserves the line generated by ε, it preserves its orthogonal E. This leads to a morphism $\mathrm{SO}_{2n+1} \to \mathrm{SO}(q_{|E})$. However, because of the existence of a one-dimensional radical in characteristic 2, one can see that the fibre $\mathrm{SO}(q_{|E}) \otimes \mathbb{F}_2$ is non-reduced and its reduced subscheme is the closed subgroup scheme H of transformations that act as the identity on the radical. Thus $\mathrm{SO}_{2n+1} \to \mathrm{SO}(q_{|E})$ is not an isomorphism. In fact, one may see that this map realizes SO_{2n+1} as the dilatation of $\mathrm{SO}(q_{|E})$ with centre H. Recall from [**4**, 3.2] that the dilatation is a map $\pi \colon \mathrm{SO}_{2n+1} \to \mathrm{SO}(q_{|E})$ which is universal for the properties: SO_{2n+1} is $\mathbb{Z}$-flat and its special fibre at 2 is mapped into H. It can be checked that the dilatation is indeed smooth over $\mathbb{Z}$ and is the Chevalley orthogonal group. In this formulation, the special orthogonal group is not naturally a group of matrices. This is why we used another presentation. □

The closed subgroup scheme $T \subset \mathrm{SO}_{2n+2}$ of diagonal matrices fixing ε is a maximal torus of SO_{2n+1}, we denote by $\mathfrak{t}$ its Lie algebra and by λ_i its coordinate functions. Its normalizer N is the closed subgroup scheme of orthogonal monomial matrices fixing ε. The Weyl group $W = N/T$ is the semi-direct product $(\mathbb{Z}/2\mathbb{Z})^n \rtimes \mathfrak{S}_n$. It acts on T as follows. The subgroup $(\mathbb{Z}/2\mathbb{Z})^{n-1}$ is generated by the transformations ε_i which take λ_i to its opposite and leave all other λ_k unchanged. The subgroup $\mathfrak{S}_n$ permutes the λ_i.

5.2. Explicit computation of the Chevalley morphism

Let M be the universal matrix over $\mathfrak{so}_{2n+1}$. Using the embedding of $\mathfrak{so}_{2n+1}$ into $\mathfrak{so}_{2n+2}$, we define invariants by restriction from those of $\mathfrak{so}_{2n+2}$ defined in § 4.3. For example, let us view the universal matrix M as a matrix in $\mathfrak{so}_{2n+2}$. Since $M(\varepsilon) = 0$, the determinant of M vanishes and hence its characteristic polynomial in dimension $2n + 2$ is

$$t^{2n+2} + c_2t^{2n} + \cdots + c_{2n}t^2.$$

We *define* the *characteristic polynomial of* M as

$$\chi(t) = t^{2n+1} + c_2t^{2n-1} + \cdots + c_{2n}t.$$

Note that this is not the characteristic polynomial associated to an actual action on the natural representation of dimension $2n + 1$. Using again the embedding in $\mathfrak{so}_{2n+2}$, we see that in characteristic 2 we have again a polynomial $\pi(t)$ defined uniquely by the identity $\chi_{\mathbb{F}_2}(t) = t(\pi_{\mathbb{F}_2}(t))^2$. By abuse, we call it again *Pfaffian characteristic polynomial.* We may define lifts of its coefficients by the same process as in Definition 4.6 and we obtain a polynomial $\pi(t) = t^n + \pi_1t^{n-1} + \cdots + \pi_{n-1}t + \pi_n$ where $\pi_i \in \mathbb{Z}[\mathfrak{so}_{2n}]$. As in § 4.3, for any ring A the elements $\pi_1, \ldots, \pi_{n-1}, \pi_n$ are algebraically independent over A. In the same way as in § 4.3, we prove the following proposition.

Proposition 5.2. *Let $(\mathcal{O}, \tau)$ be the ring defined in Proposition 4.7. Then any monomial function $\tau(\pi_1)^{\alpha_1} \cdots (\pi_n)^{\alpha_n}$ on $\mathfrak{so}_{2n+1,\mathcal{O}}$ is independent of the choice of the lifts π_i and invariant under the adjoint action of $\mathrm{SO}_{2n+1,\mathcal{O}}$. Also, for each $i \in \{1, \ldots, n\}$ we have $\tau(\pi_i)^2 = \tau c_{2i}$.* □

So for any ring A and any $x \in A[2]$, the quantity $x(\pi_1)^{\alpha_1} \cdots (\pi_n)^{\alpha_n}$ is a well-defined invariant function on $\mathfrak{so}_{2n+1,A}$. Exactly the same proof as the proof of Theorem 4.8 gives the following theorem.

Theorem 5.3. *Let A be a ring and $G = \mathrm{SO}_{2n+1,A}$. Then the ring of functions of $\mathfrak{g}/G$ is*

$$A[c_2, c_4, \ldots, c_{2n}; x(\pi_1)^{\epsilon_1} \cdots (\pi_n)^{\epsilon_n}],$$

where x runs through a set of generators of the 2-torsion ideal $A[2] \subset A$, and $\epsilon_i = 0$ or 1, not all 0. □

Finally, all the statements of Corollary 4.9 also hold word for word for $G = \mathrm{SO}_{2n+1}$.

6. The symplectic group Sp_{2n}

The computation of the adjoint quotient and of the Chevalley morphism $\pi : \mathfrak{t}/W \to \mathfrak{g}/G$ for Sp_{2n} requires the preliminary computation of the corresponding quantity for the group SL_2. We also found it interesting to deal with the case of PSL_2.

6.1. Preliminary cases: SL_2 and PSL_2

We denote by $\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ the universal matrix of $\mathfrak{sl}_2$; therefore $A[a]$ is the ring of functions on $\mathfrak{t}$ over A. The same proof as that of Proposition 4.5 yields the following fact.

Fact 6.1. *Let A be a ring, then $A[\mathfrak{t}]^W$ is equal to $A[a^2] \oplus aA[2][a^2]$.*

We set $\det(a,b,c) = -a^2 - bc$. This fact and the next proposition show that we do not have $\mathfrak{t}/W \simeq \mathfrak{g}/G$.

Proposition 6.2. *Let A be a ring, then $A[\mathfrak{sl}_2]^{\mathrm{SL}_2} = A[\det]$.*

Proof. The action of the diagonal matrix $\left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right)$ on the coordinate functions reads

$$\left.\begin{aligned} a &\mapsto a, \\ b &\mapsto u^2 b, \\ c &\mapsto u^{-2} c. \end{aligned}\right\} \tag{6.1}$$

Any invariant polynomial can therefore be written as a polynomial in a and bc.
On the other hand, the action of the unipotent element $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$ reads

$$\left.\begin{aligned} a &\mapsto a + tc, \\ b &\mapsto b - 2ta - t^2 c, \\ c &\mapsto c. \end{aligned}\right\} \tag{6.2}$$

Assume we have a homogeneous invariant of odd degree $2d+1$. Since it is a polynomial in a and bc, it can be written as $af(a^2, bc)$, with f homogeneous of degree d. We consider the identity

$$af(a^2, bc) = (a+tc)f((a+tc)^2, (b - 2ta - t^2c)c),$$

and specialize to $a = 0$. We get $tcf(t^2c^2, bc - t^2c^2) = 0$ so $f(t^2c^2, bc - t^2c^2) = 0$. Performing the invertible change of coordinates $d = b + t^2c$, we therefore get $f(t^2c^2, cd) = 0 = c^d f(t^2c, d)$, from which it follows that $f = 0$.

Thus there are no invariants of odd degree and the image of the restriction morphism is included in $A[a^2]$. Since det is an invariant, this image is exactly $A[a^2]$, which implies the proposition. $\square$

We pass to PSL_2. By Proposition 2.16 and its proof, the coordinate ring of $\mathfrak{psl}_2$ over A is $A[\alpha, b, c]$, where $\alpha = 2a$.

Fact 6.3. *Let A be a ring, then $A[\mathfrak{t}]^W$ is equal to $A[\alpha^2] \oplus \alpha A[2][\alpha^2]$.*

Proposition 6.4. *Let A be a ring, then $A[\mathfrak{psl}_2]^{\mathrm{PSL}_2} = A[4\det] + \alpha A[2][4\det]$.*

Proof. We know from Theorem 3.6 that $A[\mathfrak{psl}_2]^{\mathrm{PSL}_2}$ injects into $A[\mathfrak{t}]^W = A[\alpha^2] \oplus \alpha A[2][\alpha^2]$. On the other hand, $4\det = -\alpha^2 - 4bc$ is certainly an invariant in the coordinate ring, as well as $x\alpha$, if $x \in A$ is a 2-torsion element, since by (6.2) α is mapped to $\alpha + 2tc$ under the action of the unipotent element $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$. Thus the proposition is proved. $\square$

6.2. Explicit computation of the Chevalley morphism

We denote by $\mathfrak{t}$ the n-dimensional affine space with coordinate functions X_i, and W the group generated by the permutations of the coordinates and the reflections ε_i which map X_i to its opposite and leave the other coordinates invariant. Recall that σ_k denotes the complete elementary symmetric functions in n variables. The same proof as for Proposition 4.5 yields the following proposition.

Proposition 6.5. *Let A be a ring, then $A[\mathfrak{t}]^W$ is generated by $\sigma_k(X_i^2)$ and $x\sigma_k(X_i)$, where $k < n$ and x runs through the 2-torsion ideal of A.* □

We denote by E the natural representation of $G = \mathrm{Sp}_{2n}$, of dimension $2n$. By definition, we therefore have a morphism $G \to \mathrm{GL}(E)$, which also induces a morphism $\mathfrak{g} \to \mathfrak{gl}(E)$. Let M be the universal matrix over $\mathfrak{gl}(E)$, and let χ be its characteristic polynomial:

$$\chi(t) = \det(t\,\mathrm{Id} - \mathsf{M}) = t^{2n} - c_1 t^{2n-1} + c_2 t^{n-2} + \cdots + c_{2n}.$$

Theorem 6.6. *Let A be a ring and let $G = \mathrm{Sp}_{2n,A}$. Then the morphism $\pi : \mathfrak{t}/W \to \mathfrak{g}/G$ is an isomorphism if and only if A has no 2-torsion. Moreover, the ring of functions of $\mathfrak{g}/G$ is*

$$A[c_2, c_4, \ldots, c_{2n}].$$

The formation of the adjoint quotient $\mathfrak{g} \to \mathfrak{g}/G$ over a scheme S commutes with any base change $S' \to S$.

Proof. Let $G = \mathrm{Sp}_{2n,A}$ and $\mathfrak{g} = \mathrm{Lie}(G)$. By Theorem 3.6 and Proposition 6.5, $A[\mathfrak{g}]^G$ is a subring of $A[\mathfrak{t}]^W = A[\sigma_k(X_i^2); x.\sigma_k(X_i)]$. With the notation of Lemma 3.4, it is also a subring of the image of $A[\mathfrak{h}]^H$ in $A[\sigma_k(X_i^2); x.\sigma_k(X_i)]$. The latter is $A[\sigma_k(X_i^2)]$ by Proposition 6.2. Since $c_{2k} \in A[\mathfrak{g}]^G$ maps to $\pm\sigma_k(X_i^2) \in A[\mathfrak{t}]^W$, the theorem is proved. □

Acknowledgements. We thank the referee for his comments and suggestions that helped to clarify a number of points in the article.

References

1. S. Anantharaman, Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension 1, *Bull. Soc. Math. France* **33** (1973), 5–79.
2. M. Artin, Versal deformations and algebraic stacks, *Invent. Math.* **27** (1974), 165–189.
3. P. Berthelot, L. Breen and W. Messing, *Théorie de Dieudonné cristalline*, Volume II, Lecture Notes in Mathematics, Volume 930 (Springer, 1982).
4. S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Volume 21 (Springer, 1990).
5. N. Bourbaki, *Groupes et algèbres de Lie*, Chapters 4–6 (Hermann, Paris, 1968).
6. C. Chevalley, Invariants of finite groups generated by reflections, *Am. J. Math.* **77** (1955), 778–782.
7. M. Demazure, Invariants symétriques entiers des groupes de Weyl et torsion, *Invent. Math.* **21** (1973), 287–301.
8. M. Demazure and A. Grothendieck, *Schémas en groupes, III: structure des schémas en groupes réductifs*, Séminaire de Géométrie Algébrique du Bois Marie 1962/1964 (SGA 3), Lecture Notes in Mathematics, Volume 153 (Springer, 1962/1964).

9. J. Dieudonné and A. Grothendieck, *Éléments de géométrie algébrique*, *Publ. Math. IHÉS* **4**, **8**, **11**, **17**, **20**, **24**, **28**, **32** (1961–1967).
10. R. Farnsteiner, Varieties of tori and Cartan subalgebras of restricted Lie algebras, *Trans. Am. Math. Soc.* **356**(10) (2004), 4181–4236.
11. J. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics, No. 21 (Springer, 1975).
12. H. Ikai, Spin groups over a commutative ring and the associated root data, *Monatsh. Math.* **139**(1) (2003), 33–60.
13. H. Ikai, Spin groups over a commutative ring and the associated root data (odd rank case), *Beit. Alg. Geom.* **46**(2) (2005), 377–395.
14. H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, Volume 8 (Cambridge University Press, 1989).
15. J. P. Serre, *Algèbres de Lie semi-simples complexes* (W. A. Benjamin, New York/ Amsterdam, 1966).
16. T. A. Springer and R. Steinberg, Conjugacy classes, in *Seminar on Algebraic Groups and Related Finite Groups, IAS, Princeton, NJ, 1968/1969* (ed. E. Borel *et al.*), pp. 167–266, Lecture Notes in Mathematics, Volume 131 (Springer, 1970).
17. R. Steinberg, Regular elements of semisimple algebraic groups, *Publ. Math. IHES* **25** (1965), 49–80.
18. H. Strade, *Simple Lie algebras over fields of positive characteristic, I, Structure theory*, de Gruyter Expositions in Mathematics, Volume 38 (de Gruyter, Berlin, 2004).
19. D. Taylor, *The geometry of the classical groups*, Sigma Series in Pure Mathematics, No. 9 (Heldermann, 1992).
20. F. D. Veldkamp, The center of the universal enveloping algebra of a Lie algebra in characteristic p, *Annales Scient. Éc. Norm. Sup.* **5** (1972), 217–240.