PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

TONNY A. SPRINGER

Some arithmetical results on semi-simple Lie algebras

Publications mathématiques de l'I.H.É.S., tome 30 (1966), p. 115-141

<http://www.numdam.org/item?id=PMIHES_1966__30__115_0>

SOME ARITHMETICAL RESULTS ON SEMI-SIMPLE LIE ALGEBRAS

T. A. SPRINGER

Introduction.

The present paper had its origin in an attempt to prove the existence of regular unipotent elements in a semi-simple linear algebraic group G over an algebraically closed field k (of arbitrary characteristic p). The attempt was not completely successful, it turned out to give results only under some (rather mild) restrictions on p. Our method, which is given in § 4 of this paper, makes an essential use of the explicit formulas for the structure of the unipotent part U of a Borel subgroup B of G, which are due to Chevalley ([9]). The application of these formulas to our problem leads one to investigate an arithmetical problem about semi-simple Lie algebras. This is the following problem. Let $\mathfrak{g}$ be a Lie algebra over the ring of integers **Z**, associated with a complex semi-simple Lie algebra. Let $\{e_r\}$ be the set of " root vectors " of $\mathfrak{g}$, let $n = \sum_s e_s$, where the summation is over a set of simple roots. Determine the elementary divisors of the endomorphism $\mathrm{ad}(a)$ of $\mathfrak{g}$.

This arithmetical problem is dealt with in § 2 of the paper (after some introductory material in § 0 and § 1). The results for the case that the root system of $\mathfrak{g}$ is simple, are given in (2.6). Their proofs rely heavily on the explicit knowledge of the simple root systems. We need, for example, for the exceptional simple types $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$, $\mathbf{F}_4$, tables giving the positive roots when expressed in the simple ones (these tables are given in an appendix). We also need some properties of the integral structure constants N_{rs} of a semi-simple Lie algebra. From (2.6) we derive various characterizations of the " bad " primes for $\mathfrak{g}$, i.e. (in the simple case) those which divide the coefficients of the highest root of $\mathfrak{g}$. The results are given in (2.11). It would be interesting to have *a priori* proofs of these characterizations, the proofs of the present paper are by " checking cases ". In § 3 we make some remarks about the torsion of compact, semi-simple, simply connected Lie groups. The results are obtained by comparing those of § 2 with results which are proved in topology.

§ 4 contains results about regular unipotent elements in semi-simple algebraic groups over algebraically closed ground fields. Their existence has been proved meanwhile by Steinberg (in [17]), without restrictions on p, by a different method. Our method leads to some further results about the structure of the centralizer of a regular unipotent element (see (4.11) and (4.12)).

Finally in § 5, the discussion of § 4 is partly carried over to the corresponding problem for the Lie algebra of a semi-simple algebraic group.

0. Preliminaries.

(0.1) Let E and F be two free abelian groups of finite rank; let t be a homomorphism of E into F. We define, as usual, the *rank* of t to be the rank of $t(\mathrm{E})$. We call *elementary divisors* of t the elementary divisors of the module $\mathrm{F}/t(\mathrm{E})$ ([7], Chap. VII, § 4, n° 7). These are the prime powers which occur as orders of direct summands in the decomposition of the torsion-group $\mathrm{Tors}(\mathrm{F}/t(\mathrm{E}))$ as a direct sum of indecomposable groups. An elementary divisor p^n has a certain *multiplicity*, which is the number of indecomposable summands of order p^n.

We say that *t has no elementary divisors* if $\mathrm{F}/t(\mathrm{E})$ is torsion free (in particular, if t is surjective).

Choosing bases in E and F, we can describe t by an integral matrix M. Then the elementary divisors of M are by definition those of t. It is known that the elementary divisors of the transposed matrix ${}^tM$ and their multiplicities are the same as those of M.

(0.2) With the same notation, let E_1 be a submodule of E. We call E_1 *primitive* if E/E_1 is torsion free or, equivalently, if E_1 is a direct summand. E_1 being primitive, let t_1 be the homomorphism $\mathrm{E}/\mathrm{E}_1 \rightarrow \mathrm{F}/t(\mathrm{E}_1)$ induced by t.

We then have the following simple lemma, the proof of which is left to the reader.

(0.3) *Lemma. — If $t(\mathrm{E}_1)$ is primitive in* F, *then the elementary divisors of t and their multiplicities are the same as those of t_1.*

1. Results about semi-simple Lie algebras.

In this section we recall a number of results about semi-simple Lie algebras and their root systems, which we have to use. References are [9], [14] (exposés 14, 19).

(1.1) We start with a *root system* R in an l-dimensional vector space V over $\mathbf{R}$, with an Euclidean metric (given by a symmetric bilinear form (x, y)). This is a finite set of nonzero vectors, called roots, with the following properties:

a) R *contains a basis of* V ;

b) *if* $r \in \mathrm{R}$, *then* $-r \in \mathrm{R}$, *no other multiples of* r *lie in* R ;

c) *if* $r \in \mathrm{R}$, *then* $\mathrm{T}_r(\mathrm{R}) = \mathrm{R}$, *where* T_r *is the reflection in* V *defined by*

$$\mathrm{T}_r(x) = x - 2(r, r)^{-1}(x, r)r;$$

d) *for* $r, s \in \mathrm{R}$, $c_{rs} = 2(r, r)^{-1}(r, s)$ *is an integer.*

$l = \dim \mathrm{V}$ is called the *rank* of R. The root system R is called *simple* if it cannot be decomposed into two mutually orthogonal subsets. The simple root systems R can be classified. The classification gives the simple types $\mathbf{A}_l$ ($l\geq 1$), $\mathbf{B}_l$ ($l\geq 2$), $\mathbf{C}_l$ ($l\geq 3$), $\mathbf{D}_l$ ($l\geq 4$), $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$, $\mathbf{F}_4$, $\mathbf{G}_2$. We do not enter into the classification here; in n° 2 we shall have to use extensively the explicit description of the simple root systems.

(1.2) In a simple system R one defines the *length* of a root r as the ratio $(r,r)(r_0,r_0)^{-1}$, where r_0 is a fixed root in R such that (r_0,r_0) is smallest. The length of a root is 1 in the simple types $\mathbf{A}_l$, $\mathbf{D}_l$, $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$, 1 or 2 in the types $\mathbf{B}_l$, $\mathbf{C}_l$, $\mathbf{F}_l$, 1 or 3 in the type $\mathbf{G}_2$. If all roots have length 1, then for $r\neq s$ the integers c_{rs} are 0 or ± 1.

(1.3) There exist sets of *simple* roots S in R. These are subsets S of R consisting of l roots, whose characteristic property is the following one: any $r\in\mathrm{R}$ is a linear combination

$$r=\sum_{s\in\mathrm{S}} n_s s,$$

with integral coefficients n_s, all having the same sign. $h(r)=\sum_{s\in\mathrm{S}} n_s$ is then called the *height* of r. The root r is called *positive* if $h(r)>0$, *negative* if $h(r)<0$ (all this depends on S). If S and S′ are two sets of simple roots, then there exists a unique element w of the *Weyl group* W of R, the group generated by the reflections T_r of (1.1) *c)*, such that $\mathrm{S}'=w(\mathrm{S})$. The Weyl group W is also the group generated by the T_s ($s\in\mathrm{S}$).

Let us recall too that, if R is simple, there is exactly one root r with maximal height; we call it the *highest root.*

(1.4) Let Γ be the lattice in V spanned by the vectors $2(r,r)^{-1}r$ ($r\in\mathrm{R}$). Let Γ' be the lattice in V formed by the $x\in\mathrm{V}$ such that

$$(x,r)\in\mathbf{Z} \qquad \text{for all } r\in\mathrm{R}.$$

By (1.1) *d)* we have $\Gamma'\supset\Gamma$. The quotient Γ'/Γ is a finite abelian group, the *fundamental group* of R. It is isomorphic to $\mathbf{Z}/(l+1)\mathbf{Z}$ for type $\mathbf{A}_l$, to $\mathbf{Z}/2\mathbf{Z}$ for types $\mathbf{B}_l$, $\mathbf{C}_l$ and $\mathbf{E}_7$, to $(\mathbf{Z}/2\mathbf{Z})^2$ for type $\mathbf{D}_l$ (l even), to $\mathbf{Z}/4\mathbf{Z}$ for type $\mathbf{D}_l$ (l odd), to $\mathbf{Z}/3\mathbf{Z}$ for type $\mathbf{E}_6$, and is reduced to the identity in the other cases of a simple root system.

(1.5) Take any lattice Δ in V such that $\Gamma\subset\Delta\subset\Gamma'$ (hence (x,r) takes integral values if $x\in\Delta$).

We now define a Lie algebra $\mathfrak{g}$ over $\mathbf{Z}$ [1]. Put

$$\mathfrak{g}=\Delta+\sum_{r\in\mathrm{R}}\mathbf{Z}e_r,$$

where the Lie algebra product is as follows:

$$(1)\qquad \begin{cases} [h,e_r] &=(r,h)e_r \quad (h\in\Delta),\\ [e_r,e_{-r}] &=2(r,r)^{-1}r,\\ [e_r,e_s] &=\mathrm{N}_{rs}e_{r+s} \qquad (r,s\in\mathrm{R},\ r+s\neq 0),\\ [h,h'] &=0 \qquad\qquad (h,h'\in\Delta).\end{cases}$$

[1] The Lie algebra $\mathfrak{g}$ over $\mathbf{Z}$ which we define here is somewhat more general than that discussed in [9], p. 32 where only the case $\Delta=\Gamma$ is considered. We also have identified here V with its dual, by means of the inner product.

Here the N_{rs} are certain integers, 0 if $r+s\notin R$. They are discussed in Chevalley's fundamental paper [9]. Below we shall review the results which we shall need. We call the N_{rs} the *structure constants* of $\mathfrak{g}$.

(1.6) Some comments on the structure constants must be made. In the first place, in order for (1) to define a Lie algebra, Jacobi's identity must hold. This gives that the structure constants have to satisfy the following relations

$$(2)\qquad \begin{cases} N_{rs}=-N_{sr}, \\ N_{-r,s}N_{r,-r+s}+N_{sr}N_{-r,r+s}=c_{rs}, \\ N_{rs}N_{r+s,t}+N_{st}N_{s+t,r}+N_{tr}N_{t+r,s}=0 \end{cases}$$

(it being understood here that $N_{rs}=0$ if r, s or $r+s$ is not a root).

That complex structure constants N_{rs} exist, is a nontrivial classical result, due to É. Cartan, proved usually by " checking cases ". In Cartan's thesis ([8], Chap. V) one already finds explicit *integral* solutions of (2). More detailed results are given in [9]. We collect those which we need in lemmas.

(1.7) *Lemma. — Suppose* $r, s, r+s\in R$. *The* $i\in\mathbf{Z}$ *such that* $s+ir\in R$ *form a closed interval* $[-p, q]$ *in* $\mathbf{Z}$ *with* $p, q\geq 0$.

a) *For any solution of* (2) *we have* $N_{rs}N_{-r,-s}=-(p+1)^2$;

b) *There exists a solution of* (2) *such that for all* $r, s, r+s\in R$ *we have* $N_{rs}=\pm(p+1)$, *where p is the integer defined above*;

c) *If* (N_{rs}) *and* (N'_{rs}) *are two solutions of* (2) *satisfying* b), *then there exists a function* $\varepsilon: R\rightarrow\{1,-1\}$ *with* $\varepsilon(r)=\varepsilon(-r)$ *such that* $N'_{rs}=\varepsilon(r)\varepsilon(s)\varepsilon(r+s)N_{rs}$.

For the proofs of these statements see [9], p. 22-23. In the next lemma (N_{rs}) is any solution of (2).

(1.8) *Lemma. — Suppose that* $r, s, r+s\in R$.

a) $N_{-r,r+s}(N_{-s,r+s})^{-1}$ *is a negative rational number*;

b) *If* $\pm r$, $\pm s$, $\pm(r+s)$ *are the only linear combinations of r and s which are roots, then* $N_{-r,r+s}=-N_{-s,r+s}$.

With the notations of (1.7) Jacobi's identity implies

$$N_{rs}N_{-r,r+s}=q(p+1)$$

(see [6], p. 22). A similar formula is true with r and s interchanged. Since $N_{rs}=-N_{sr}$, *a)* follows. Under the hypothesis of *b)* the right hand sides in these relations are 1, which proves the assertion of *b)*.

(1.9) *Lemma. — Suppose that all roots have the same length. Assume that a set* S *of simple roots has been fixed. Then there exist structure constants* N_{rs} *such that* $N_{rs}=0$ *or* 1 *if s is simple and* $h(r)\geq 2$ [1].

Suppose that the following assertion has been proved: (*) there exist structure constants such that $N_{rs}=0$ or 1 if s is simple and $h(r)\geq i+1$.

[1] I owe this lemma to H. de Vries. It replaces a more complicated lemma and it led to some simplifications in the discussion of (2.9).

We shall show below that if $i \geq 2$, (*) holds too with $i+1$ replaced by i. Since (*) is obviously true for large i, (1.9) follows.

Since all roots have the same length, we may assume that $(r, r)=2$ for all $r \in \mathrm{R}$. It is known then, that if r and r' are linearly independent roots, we have $(r, r')=0$ or ± 1 and moreover that $(r, r')=-1$ if and only if $r+r'$ is a root.

Fix r with $h(r)=i$ and assume that $\mathrm{N}_{rs} \neq 0$ where s and t are simple and $s \neq t$. By our previous remarks we have $(r, s)=(r, t)=-1$. Now if $(s, t)=1$, $s-t$ would be a root, which is impossible. Hence $(s, t) \leq 0$. If $(s, t)=-1$, we would have $(r+s, t)=-2$, which is also impossible. So $(s, t)=0$, and $(r+s, t)=-1$. Hence $r+s+t$ is a root. Then Jacobi's identity implies that

$$\mathrm{N}_{r+s, t}\mathrm{N}_{rs}=\mathrm{N}_{r+t, s}\mathrm{N}_{rt}.$$

By (*) we have $\mathrm{N}_{r+s, t}=\mathrm{N}_{r+t, s}=1$. It follows that $\mathrm{N}_{rs}=\mathrm{N}_{rt}$. Changing the structure constants according to (1.7) *c)*, with $\varepsilon(r')=1$ if $r' \neq \pm r$, we may assume that $\mathrm{N}_{rs}=0$ or 1 for our fixed root r with height i and for all simple s. If $i \geq 2$, we can deal separately with each r, proving that (*) is true with i instead of $i+1$.

Remark. — The same argument shows the following. Let $\mathrm{S}=\mathrm{S}_1 \cup \mathrm{S}_2$, where S_i consists of orthogonal roots. Then structure constants exist which have, besides (1.9), also the following property:

$$\mathrm{N}_{st}=1 \quad \text{if} \quad s \in \mathrm{S}_1, \ t \in \mathrm{S}_2.$$

(1.10) We now define on our Lie algebra $\mathfrak{g}$ a grading as follows. Take a set S of simple roots, let h denote the height as in (1.3). Define

$$\mathfrak{g}^0=\Delta$$
$$\mathfrak{g}_i=\sum_{h(r)=i} \mathbf{Z}e_r \quad (i \neq 0).$$

We put $l_i=\operatorname{rank} \mathfrak{g}^i$ (= number of roots r with height i if $i \neq 0$). It is easily verified that

$$[\mathfrak{g}^i, \mathfrak{g}^j] \subset \mathfrak{g}^{i+j},$$

so that we have made $\mathfrak{g}$ into *a graded Lie algebra over* **Z**.

The grading depends on the choice of the simple roots. However, if we take another set S' of simple roots, there exists $w \in \mathrm{W}$ such that $w(\mathrm{S})=\mathrm{S}'$. Moreover, by (1.7) *c)* we have

$$\mathrm{N}_{w(r), w(s)}=\varepsilon(r)\varepsilon(s)\varepsilon(r+s)\mathrm{N}_{rs},$$

where ε is a function $\mathrm{R} \rightarrow \{1, -1\}$. Define an endomorphism Φ of $\mathfrak{g}$ by

$$\Phi(h)=w(h) \quad (h \in \Delta),$$
$$\Phi(e_r)=\varepsilon(r)e_{w(r)}.$$

It is easily seen that Φ is an automorphism of the Lie algebra $\mathfrak{g}$. Let

$$\mathfrak{g}=\Sigma(\mathfrak{g}^i)'$$

be the grading defined (as above) by S′. Then

$$\Phi(\mathfrak{g}^i)=(\mathfrak{g}^i)',$$

This shows that the graded Lie algebra structure on $\mathfrak{g}$ is unique up to isomorphism.

(**1.11**) Fix a set S of simple roots. Define then an element $n\in\mathfrak{g}$ by

$$n=\sum_{r\in S} e_r.$$

It is clear that n is a nilpotent element of $\mathfrak{g}$, i.e. such that ad $n : x\mapsto[n, x]$ is a nilpotent endomorphism of $\mathfrak{g}$. We call n a *principal nilpotent element* of $\mathfrak{g}$ (such elements have been investigated by Kostant ([12], [13]) for the case of semi-simple Lie algebras over the complex field).

One may prove by an argument like that used in (1.10) that if n and n' are two principal nilpotents, defined by sets S and S′ of simple roots, we have $n'=\Phi(n)$ where Φ is an automorphism of $\mathfrak{g}$.

In the next section we shall investigate in detail the action of ad n in $\mathfrak{g}$.

Remark. — Our definition of a principal nilpotent is unsatisfactory in that it depends on the choice of a particular basis in $\mathfrak{g}$. In Kostant's paper [12] cited above, intrinsic characterizations are given of principal nilpotent elements of a complex semi-simple Lie algebra. For instance, they are those nilpotent elements whose centralizer has least possible dimension. The author does not know similar characterizations for the algebras over **Z**. Because it is not necessary for the purpose of this paper, we don't want to pursue this matter further here.

2. The action of a principal nilpotent element.

(**2.1**) In this section $\mathfrak{g}$ is a Lie algebra over **Z** of the type considered in § 1. The root system R is assumed to be *simple*, the structure constants N_{rs} are assumed to have the properties of (1.7) *b)* and (1.9). A set S of simple roots is fixed, the grading of $\mathfrak{g}$ is that defined by S. If n denotes the principal nilpotent element, we define homomorphisms (of abelian groups)

$$t_i : \mathfrak{g}^i\rightarrow\mathfrak{g}^{i+1}$$

by

$$t_i(x)=[n, x].$$

It is the purpose of this section to investigate the elementary divisors of the t_i.

But first we want to recall a known result about the ranks of the t_i.

(**2.2**) *Proposition.* — t_i *is injective for* $i\leq 0$, rank $t_i=l_{i+1}(=\text{rank } \mathfrak{g}^{i+1})$ *for* $i\geq 0$.

A proof of (2.2) is contained in [12]. For the convenience of the reader we indicate one here.

Consider the Lie algebra $\mathfrak{g}_{\mathbf{Q}}=\mathfrak{g}\otimes_{\mathbf{Z}}\mathbf{Q}$. We imbed $\mathfrak{g}$ in $\mathfrak{g}_{\mathbf{Q}}$ in the obvious way. We choose

$$a=\sum_{s\in S}(2(s, s)^{-1}s)\otimes\xi_s$$

in $\mathfrak{g}^0 \otimes \mathbf{Q}$ such that

$$(3) \qquad [a, e_r] = e_r.$$

That such a choice is possible follows from the definitions (1) in (1.5) of the product in $\mathfrak{g}$: the ξ_s have to satisfy

$$(4) \qquad \sum_{s \in S} \xi_s c_{sr} = 1 \qquad (r \in S).$$

(4) can be solved in rational numbers, for the Cartan-matrix $(c_{rs})_{r,s \in S}$ is nonsingular.

Moreover it follows from (4), that for all $r \in R$ we have

$$(5) \qquad [a, e_r] = h(r) e_r,$$

where h denotes the height (defined in (1.3)).

Now let n be as above (identified with $n \otimes 1 \in \mathfrak{g}_{\mathbf{Q}}$), put $n' = \sum_{s \in S} e_{-s} \otimes \xi_s$. Then

$$[n, n'] = a, \qquad [a, n] = n, \qquad [a, n'] = -n'$$

a, n, n' span a three-dimensional simple subalgebra $\mathfrak{s}$ of $\mathfrak{g}_{\mathbf{Q}}$. Moreover 0 is the only element of $\mathfrak{g}_{\mathbf{Q}}$ annihilated by ad a, ad n, ad n'. For such an element must lie in $\mathfrak{g}^0_{\mathbf{Q}}$ (by (5)) and there both ad n and ad n' act injectively, because of the non-singularity of the Cartan-matrix. Also by (5), the eigenvalues of ad a are integral. It then follows from the representation theory of $\mathfrak{s}$ (see [11], p. 85) that there exist elements $x_1, \ldots, x_h$ in $\mathfrak{g}_{\mathbf{Q}}$ and odd positive integers $2k_1 + 1, \ldots, 2k_h + 1$ with the following properties:

a) $x_i \in \mathfrak{g}_{\mathbf{Q}}^{-k_i}$, $(\mathrm{ad}\, n)^{2k_i+1} x_i = 0$;

b) $(\mathrm{ad}\, n)^j x_i$ $(1 \leq i \leq h,\ 0 \leq j \leq 2k_i)$ is a basis of $\mathfrak{g}_{\mathbf{Q}}$.

It now follows that $(\mathrm{ad}\, n) x = 0$ implies that x is a linear combination of the $(\mathrm{ad}\, n)^{2k_i} x_i$ $(1 \leq i \leq h)$, which implies the first assertion of (2.2). The second one is obtained by observing that from *b)* it follows that $(\mathrm{ad}\, n) \mathfrak{g}^i_{\mathbf{Q}} = \mathfrak{g}^{i+1}_{\mathbf{Q}}$ for $i \geq 0$. Moreover, observing that rank $\mathfrak{g}^1_{\mathbf{Q}} = l$, we find that $h = l$.

(2.3) *Corollary.* — a) *If* $i < 0$ *we have* $l_i \leq l_{i+1}$, *if* $i > 0$ *we have* $l_{i+1} \leq l_i$;

b) *Let the positive integers* $(k_i)_{1 \leq i \leq h}$ *be such that* $k_1 < k_2 < \ldots < k_h$ *and that for* $i > 0$ *we have* $l_i > l_{i+1}$ *if and only if* $i = k_j$ *for some* j. *Then* $h = l$; *moreover for* $i < 0$ *we have* $l_i < l_{i+1}$ *if and only if* $i = -k_j - 1$ *for some* j.

Remarks. — *a)* It is known that the real cohomology algebra of the compact, semi-simple, simply connected Lie group whose complexified Lie algebra is $\mathfrak{g} \otimes_{\mathbf{Z}} \mathbf{C}$ is an exterior algebra on l generators of degrees $2k_i + 1$ $(1 \leq i \leq l)$ (see e.g. [12], where the Betti numbers are discussed).

b) The property *b)* mentioned in the course of the proof of (2.2) can also be stated in the following way: the Jordan normal form of ad n in $g_{\mathbf{Q}}$ is a direct sum of l Jordan matrices, with $2k_1 + 1, \ldots, 2k_l + 1$ rows, respectively.

We now want to investigate the elementary divisors of the homomorphisms t_i. First an easy special case.

(2.4) *Proposition.* — *We have* $\mathfrak{g}^0 / t_{-1}(\mathfrak{g}^{-1}) \simeq \Delta / \Gamma$, $\quad \mathfrak{g}^1 / t_0(\mathfrak{g}^0) \simeq \Gamma' / \Delta$.

$\mathfrak{g}^{-1}$ has as a basis the $(e_{-s})_{s \in S}$ and we have $t_{-1}(e_{-s}) = 2(s, s)^{-1} s$, which implies the first assertion, taking into account the fact that Γ is generated by the $2(s, s)^{-1}s$ with $s\in S$ (this follows from the remark in [9], p. 16, lines 10-11 from below). Γ' has a basis $(f_s)_{s\in S}$ where $(r, f_s)=\delta_{rs}$ $(r, s\in S)$. Let $g_r=\sum_{s\in S}\alpha_{rs}f_s$ be basis vectors of $\mathfrak{g}^0=\Delta$ (where $\alpha_{rs}\in\mathbf{Z}$). Then $t_0(g_r)=-\sum_{s\in S}\alpha_{rs}e_r$. This implies that $\mathfrak{g}^1/t^0(\mathfrak{g}^0)\cong\Gamma'/\Delta$.

(2.5) *Corollary. — If* $\Delta=\Gamma$ *then* t_{-1} *has no elementary divisors and those of* t_0 *are: the prime powers occurring in the decomposition of* $l+1$ *for type* $\mathbf{A}_l$, 2 *for the types* $\mathbf{B}_l$, $\mathbf{D}_l$ *(*l *even),* $\mathbf{E}_7$, 3 *for type* $\mathbf{E}_6$, 4 *for type* $\mathbf{D}_l$ *(*l *odd). If* $\Delta=\Gamma'$ *then* t_0 *and* t_{-1} *are to be interchanged in the preceding statement.*

This follows from the structure of Γ'/Γ, given in (1.4).

We now come to the main result of this section.

(2.6) *Theorem. — For* $i>0$ *and* $i<-1$ t_i *has at most one elementary divisor. It is a prime* p *and its multiplicity is* 1. *This occurs in the following cases*

type $\mathbf{B}_l$ $(l\geq 2)$: $p=2,\ i=2, 4, \dots, 2\left[\frac{l}{2}\right], -3, -5, \dots, -2\left[\frac{l-1}{2}\right]-1;$

type $\mathbf{C}_l$ $(l\geq 3)$: $p=2,\ i=2, 4, \dots, 2l-2;$

type $\mathbf{D}_l$ $(l\geq 4)$: $p=2,\ i=2, 4, \dots, 2\left[\frac{l}{2}\right]-2, -3, -5, \dots, -2\left[\frac{l}{2}\right]+1;$

type $\mathbf{E}_6$: $p=2,\ i=2, -3;\ p=3,\ i=3, -4;$

type $\mathbf{E}_7$: $p=2,\ i=2, 4, 8, -3, -5, -9;\ p=3,\ i=3, -4;$

type $\mathbf{E}_8$: $p=2,\ i=2, 4, 8, 14, -3, -5, -9, -15;\ p=3,\ i=3, 9, -4, -10;$
$p=5,\ i=5, -6;$

type $\mathbf{F}_4$: $p=2,\ i=2, 4, 8, -3;\ p=3,\ i=3, -4;$

type $\mathbf{G}_2$: $p=2,\ i=2, -3;\ p=3,\ i=3.$

We shall prove (2.6) by " checking cases ". Before indicating how this can be done, we give a few facts of a more general nature, which are used in the proof. First observe that for $i=0, -1$ the matrix of t_i with respect to the bases of $\mathfrak{g}^i$, $\mathfrak{g}^{i+1}$ formed by the appropriate e_r is

$$M_i=(\mathrm{N}_{s-r,r})_{h(s)=i+1, h(r)=i} \tag{6}$$

(the roots of height i and $i+1$ are supposed to be ordered in some way).

We assume that the structure constants N_{rs} satisfy (1.7) *b)* and (1.9) (if applicable).

(2.7) *Lemma. — If all roots of* R *have the same length, then the elementary divisors of* t_i *and their multiplicities are the same as those of* $t_{-(i+1)}$ $(i>0)$.

If all roots have the same length, the condition of (1.8) *b)* is satisfied for all r, s. It then follows from (1.8) *b)* that

$$^tM_i=-M_{-(i+1)} \qquad (i>0),$$

which implies the assertion of (2.7).

(2.8) A method which we shall often use is the following one. Let $s_0\in S$ be a fixed simple root. Decompose $\mathfrak{g}^i=\mathfrak{m}_0^i+\mathfrak{m}_1^i$, where $\mathfrak{m}_0^i$ is spanned by the e_r such that r

contains s_0, i.e. that in $r=\sum_{s\in S} n_s s$ we have $n_{s_0}\neq 0$, and where $\mathfrak{m}_1^i$ is spanned by the other e_r. Decompose $\mathfrak{g}^{i+1}$ in the same manner. Let $t_{i,0}$ denote the restriction of t_i to $\mathfrak{m}_0^i$, let $t_{i,1}$ denote the induced homomorphism of $\mathfrak{m}_1^i$ into $\mathfrak{g}^{i+1}/\mathfrak{m}_0^{i+1}\cong\mathfrak{m}_1^{i+1}$. Suppose first that $t_{i,0}$ is an isomorphism of $\mathfrak{m}_0^i$ onto $\mathfrak{m}_0^{i+1}$. Then by (0.3) the elementary divisors of t_i can be found from those of $t_{i,1}$. The way in which $t_{i,1}$ is constructed shows that it is a mapping of the same kind as t_i, but for a root system R_1 of lower rank, whose roots are those of R which do not contain s_0. In this way we can use induction with respect to the rank l. This is one method which we shall use. A second one applies when $t_{i,1}$ is an isomorphism. In that case we know by (0.3) that the elementary divisors of t_i can be found from those of $t_{i,0}$.

(2.9) We now turn to the proof of (2.6), for which we shall discuss the simple types. These are described in [14] (exposé 19), we use the same description here. We denote in all cases a set of simple roots by $(r_i)_{1\leq i\leq l}$.

Type $\mathbf{A}_l$ $(l\geq 1)$:

The roots are the vectors $\pm(r_i+\ldots+r_j)$ $(1\leq i\leq j\leq l)$. There are $l-|i|+1$ roots with height i, the highest root is $r_1+\ldots+r_l$. All roots have the same length, all N_{rs} are ± 1.

We have to prove that the t_i $(i\neq 0,-1)$ have no elementary divisors. By (2.7) we need only to prove this for $i>0$.

For every height $i>0$ there is exactly one root s_i which contains r_1 (viz. $s_i=r_1+\ldots+r_i$). It follows immediately that $t_i(e_{s_i})=\pm e_{s_{i+1}}$. Moreover if $l\geq 2$ the roots which do not contain r_1 form a system of type $\mathbf{A}_{l-1}$.

We can now apply the first method of (2.8). It is clear that induction with respect to l gives the result which has to be proved. The starting point $l=1$ is easy.

Type $\mathbf{B}_l$ $(l\geq 2)$:

The roots are $\pm r_{ij}$, $\pm r'_{ij}$ with

$$r_{ij}=r_i+\ldots+r_j \qquad (1\leq i\leq j\leq l),$$
$$r'_{ij}=r_i+\ldots+r_{j-1}+2r_j+\ldots+2r_l \qquad (1\leq i<j\leq l).$$

We have

$$h(r_{ij})=j-i+1, \qquad h(r'_{ij})=2l-i-j+2.$$

There are $l-i$ roots with height $2i$ or $2i+1$. The highest root is $r_1+2r_2+\ldots+2r_l$.

Not all roots have the same length, $N_{rs}=\pm 1$ or ± 2.

Again, for each height $i\neq 0$ there is exactly one root s_i which contains r_1. We have $s_i=r_{1,i}$ $(1\leq i\leq l)$, $s_i=r'_{1,i}$ $(l+1\leq i\leq 2l-1)$, and $s_{-i}=-s_i$.

Moreover, for $l\geq 3$ the roots which do not contain r_1 form a root-system of type $\mathbf{B}_{l-1}$.

We prove the statement for type $\mathbf{B}_l$ contained in (2.6) by induction with respect to l. We start with $l=2$. In this case we have to prove that t_2 has an elementary divisor 2 with multiplicity 1 and that the other t_i $(i \neq 0, -1)$ do not have elementary divisors. This is an easy check. Suppose that $l>2$ and that we have already proved the assertion for type $\mathbf{B}_{l-1}$. Now we have $t_i(e_{s_i}) = \pm e_{s_{i+1}}$ if $i \neq l$, $t_i(e_{s_l}) = \pm 2 e_{s_{l+1}}$.

The first method of (2.8) establishes the assertion for $i \neq l$. If l is even the second method of (2.8) gives the desired result for $i=l$. Now let l be odd. Then the roots of height l are $r_{1,l}, r'_{2,l}, \ldots, r'_{\frac{1}{2}(l+1), \frac{1}{2}(l+3)}$, those with height $(l+1)$ are $r'_{1,l}, r'_{2,l-1}, \ldots, r'_{\frac{1}{2}(l-1), \frac{1}{2}(l+3)}$. Put $e_{r_{ij}} = e_{ij}$, $e_{r'_{ij}} = e'_{ij}$. We then have

$$\begin{cases} t_l(e_{1l}) = \pm 2 e'_{1l}, \qquad t_l(e'_{i,l-i+2}) = \pm e'_{i-1,l-i+2} \pm e'_{i,l-i+1} \qquad (i < \frac{1}{2}(l+1)), \\ t_l(e'_{\frac{1}{2}(l+1), \frac{1}{2}(l+3)}) = \pm e'_{\frac{1}{2}(l-1), \frac{1}{2}(l+3)}. \end{cases}$$

It is now easy to check that t_l has no elementary divisors. This settles the case $i>0$.

For $i<0$ we put $\mathfrak{g}^i = \mathfrak{m}_0^i + \mathfrak{m}_1^i$ as in (2.8), where $\mathfrak{m}_0^i = \mathbf{Z} e_{s_i}$. We have

$$t_i(e_{s_i}) = \pm e_{s_{i+1}} (\text{mod } \mathfrak{m}^{i+1})$$

if $i \neq -1$.

Applying (0.3) with $E = \mathfrak{g}^i$, $E_1 = \mathbf{Z} e_{s_i}$ we get from the induction assumption the assertion about t_i for $i<0$, $i \neq -l$. The case $i=-l$ is dealt with as in the case that $i>0$.

Type $\mathbf{C}_l$ $(l \geq 3)$:

The roots are $\pm r_{ij}$, $\pm r'_{ij}$, where

$$\begin{aligned} r_{ij} &= r_i + \ldots + r_j && (1 \leq i \leq j \leq l), \\ r'_{ij} &= r_i + \ldots + r_{j-1} + 2r_j + \ldots + 2r_{l-1} + r_l && (1 \leq i \leq j \leq l). \end{aligned}$$

We have

$$h(r_{ij}) = j - i + 1, \qquad h(r'_{ij}) = 2l - i - j + 1.$$

There are $l-i$ roots with height $2i$ or $2i+1$. The highest root is $2r_1 + \ldots + 2r_{l-1} + r_l$.

Not all roots have the same length, $N_{rs} = \pm 1$ or ± 2.

For each height $i \neq 0$ there is exactly one root s_i which contains r_1, viz. $s_i = r_{1i}$ $(1 \leq i \leq l)$, $s_i = r'_{1i}$ $(l+1 \leq i \leq 2l-1)$ and $s_{-i} = -s_i$.

The statement regarding type $\mathbf{C}_l$ is proved in the same way as that for type $\mathbf{B}_l$, we leave the details to the reader.

Type $\mathbf{D}_l (l \geq 4)$:

The roots are $\pm r_{ij}$, $\pm r'_{ij}$, $\pm r'_i$, where

$$\begin{aligned} r_{ij} &= r_i + \ldots + r_j && (1 \leq i \leq j \leq l-1), \\ r'_{ij} &= r_i + \ldots + r_{j-1} + 2r_j + \ldots + 2r_{l-2} + r_{l-1} + r_l && (1 \leq i < j \leq l-1), \\ r'_i &= r_i + \ldots + r_{l-2} + r_l && (1 \leq i \leq l-1). \end{aligned}$$

We have

$$h(r_{ij}) = j - i + 1, \qquad h(r'_{ij}) = 2l - i - j, \qquad h(r'_i) = l - i.$$

There are $l-i$ roots with height $2i<l$ and $2i+1<l$, there are $l-i-1$ roots with height $2i\geq l$ and $2i+1\geq l$. The highest root is $r_1+2r_2+\ldots+2r_{l-2}+r_{l-1}+r_l$, its height is $2l-3$. All roots have the same length, $N_{rs}=\pm 1$. So by lemma (2.7) it suffices to prove the part of (2.6) about $\mathbf{D}_l$ only for positive heights i.

For each height $i>0$, $i\neq l-1$ there is exactly one root s_i containing r_1, for $i=l-1$ there are 2 such roots, which we call s_{l-1} and s'_{l-1}. We have $s_i=r_{1i}\,(1\leq i<l)$, $s_i=r'_{1i}\,(l\leq i\leq 2l-3)$, $s'_{l-1}=r'_l$. The roots which are linear combinations of $r_2, \ldots, r_l$ form a root system of type $\mathbf{D}_{l-1}$ (of type $\mathbf{A}_3$ if $l=4$).

We have

$$t_i(e_{s_i})=\pm e_{s_{i+1}} \qquad \text{for } i\neq l-2,$$

and

$$t_{l-1}(e_{s'_{l-1}})=\pm e_{s_l}.$$

Using the first method explained in (2.8) we see that the elementary divisors of t_i for type $\mathbf{D}_l$ are the same as those of t_i for type $\mathbf{D}_{l-1}$ ($\mathbf{A}_3$ for $l=4$), if $i\neq l-2$.

So it remains to consider the case $i=l-2$. In that case the assertion of (2.6) is: t_{l-2} has the elementary divisor 2 with multiplicity 1 if l is even and does not have elementary divisors if l is odd.

Let $l\geq 4$. The roots of height $l-2$ are $r_{1,l-2}, r_{2,l-1}, r'_2, r'_{i,l+2-i}\,(3\leq i<\frac{1}{2}(l+1))$, those of height $l-1$ are $r_{1,l-1}, r'_1, r_{i,l+1-i}\,(2\leq i<\frac{1}{2}(l+1))$. Put $e_{ij}=e_{r_{ij}}$, $e'_i=e_{r'_i}$, $e'_{ij}=e_{r'_{ij}}$, we define $e'_{ij}=0$ if $i\geq j$.

Assuming (1.9) for the structure constants, we have

$$\begin{aligned}
t_{l-2}(e_{1,l-2}) &= -e_{1,l-1}-e'_1,\\
t_{l-2}(e_{2,l-1}) &= -e_{1,l-1}-e'_{2,l-1},\\
t_{l-2}(e'_2) &= -e'_1-e'_{2,l-1},\\
t_{l-2}(e'_{i,l+2-i}) &= -e'_{i-1,l+2-i}-e'_{i,l+1-i}.
\end{aligned}$$

If l is odd, $t_{l-2}(e'_{\frac{1}{2}(l+1),\frac{1}{2}(l+3)})=-e_{\frac{1}{2}(l-1),\frac{1}{2}(l+3)}$, which is readily seen to imply that t_{l-2} is *surjective*; hence has no elementary divisors.

If l is even, t_{l-2} maps $e'_{i,l+2-i}\,(i\geq 3)$ in $-e'_{i,l+1-i}$ modulo the sublattice of $\mathfrak{g}_{l-1}$ generated by $r_{1,l-1}, r'_1, r_{j,l+1-j}\,(2\leq j<i)$. From this one infers that the elementary divisors of t_{l-2} are the same as those of t_2 for type $\mathbf{D}_4$. In this case the preceding formulas are easily seen to imply that there is only an elementary divisor 2, with multiplicity 1.

Type $\mathbf{E}_6$:

There is a basis $(x_i)_{1\leq i\leq 6}$ of V such that the roots are $x_i-x_j\,(i\neq j)$, $\pm(x_i+x_j+x_k-s)$ (i, j, k distinct) and $\pm s$, where $s=(1/3)\sum_{i=1}^{6} x_i$. The simple roots are then $r_i=x_i-x_{i+1}\,(1\leq i\leq 5)$, $r_6=x_4+x_5+x_6-s$. One can now write down all positive roots, expressed as linear combinations of the simple ones. The result is given in table I (appendix). The highest root is $r_1+2r_2+3r_3+2r_4+r_5+2r_6$.

All N_{rs} are ± 1, the roots have the same length. So by lemma (2.7) it is sufficient to consider positive heights.

One sees by inspection of table I that, except for $i=2, 3,$ the following situation prevails: the bases (e_r) of $\mathfrak{g}^i$ and $\mathfrak{g}^{i+1}$ can be numbered such (say $e_1, \ldots, e_s, f_1, \ldots, f_t$) that we have $t_i(e_k)=\pm f_k+$ a linear combination of $f_1, \ldots, f_{k-1}$.

It is then obvious that t_i has no elementary divisors. So only $i=2,3$ remain. If $i=2$ we apply the first method of (2.8), with $s=r_1$. There is only one root of height 2 or 3 containing r_1, and the roots not containing r_1 form a root system of type $\mathbf{D}_5$. Hence the case of height 2 for type $\mathbf{E}_6$ can be reduced to height 2 for type $\mathbf{D}_5$, which has already been dealt with.

In the remaining case $i=3$ we must make a computation. Making use of table I, it is easy to write down the matrix M_3 for this case (which has 5 rows and columns). Its entries are 0 or -1 (by (1.9)). There is no difficulty in finding its determinant, it turns out to be ± 3. This implies that t_3 has an elementary divisor 3 with multiplicity 1, which proves the assertion about $\mathbf{E}_6$. For $\mathbf{E}_7$ and $\mathbf{E}_8$ the argument is of the same nature.

Type $\mathbf{E}_7$:

There is a basis $(x_i)_{1\leq i\leq 7}$ of V such that the roots are $x_i-x_j\ (i\neq j)$, $\pm(x_i+x_j+x_k-s)$ $(i, j, k$ distinct), $\pm(s-x_i)$, where $s=(1/3)\sum_{i=1}^{7} x_i$. The simple roots are then $r_i=x_i-x_{i+1}$ $(1\leq i\leq 6)$, $r_7=x_5+x_6+x_7-s$. In table II the reader will find the positive roots, expressed in the simple ones.

The highest root is $r_1+2r_2+3r_3+4r_4+3r_5+2r_6+2r_7$. All roots have the same length, the N_{rs} are ± 1. So we need only consider positive heights.

Again, as for $\mathbf{E}_6$, a verification based on the use of table II shows that one only needs to consider the cases $i=2, 3, 4, 8$. The cases $i=2, 3$ are reduced to the corresponding cases for type $\mathbf{E}_6$ (there is only one root of height 2 or 3 containing r_1 and the roots not containing r_1 correspond to those of a system of type $\mathbf{E}_6$). For $i=4$ we apply the first method of (2.8) with $s=r_6$. The roots not containing r_6 form a system of type $\mathbf{D}_6$, we may then reduce the case $i=4$ for $\mathbf{E}_7$ to the corresponding case for $\mathbf{D}_6$, which has been dealt with. In the remaining case $i=8$ a simple computation shows that $\det M_8=\pm 2$. This settles type $\mathbf{E}_7$.

Type $\mathbf{E}_8$:

V is generated by vectors $(x_i)_{1\leq i\leq 9}$ with sum zero, such that the roots are $x_i-x_j\,(i\neq j)$, $\pm(x_i+x_j+x_k)$ $(i, j, k$ distinct). The simple roots are $r_i=x_i-x_{i+1}$ $(1\leq i\leq 7)$, $r_8=x_6+x_7+x_8$. In table III we have given the positive roots, expressed in the simple ones.

The highest root is $2r_1+3r_2+4r_3+5r_4+6r_5+4r_6+2r_7+3r_8$. All roots have the same length, $\mathrm{N}_{rs}=\pm 1$. We need only consider positive heights.

For $i \neq 2, 3, 4, 5, 8, 9, 14$ a verification using table III shows that t_i has no elementary divisors.

In the cases $i=2, 3, 4, 8$ we can reduce, considering the roots containing r_1, type $\mathbf{E}_8$ to type $\mathbf{E}_7$.

In the remaining cases $i=5, 9, 14$ one has to calculate the determinant of M_i. The method is the same as in the previous cases. The result is that in these cases $\det(M_i)$ is, in absolute value, 5, 3, 2, respectively. This settles type $\mathbf{E}_8$.

Type $\mathbf{F}_4$:

There is a basis $(x_i)_{1\leq i\leq 4}$ such that the roots are $x_i-x_j\ (i\neq j)$, $\pm x_i$, $\pm(x_i+x_j)\ (i\neq j)$, $(1/2)\sum_{i=1}^{4}\varepsilon_i x_i$, where $\varepsilon_i=\pm 1$. The simple roots are $r_1=x_1-x_2$, $r_2=x_2-x_3$, $r_3=x_3$, $r_4=(1/2)(x_4-x_1-x_2-x_3)$.

The positive roots, expressed in the simple ones, are given in table IV. The highest root is $2r_1+3r_2+4r_3+2r_4$.

The roots do not have all the same length, $\mathrm{N}_{rs}=\pm 1$ or ± 2. For $i>0$ one checks, using table IV, that except for $i=3$, we may take bases $e_1, \ldots, e_s$ and $f_1, \ldots, f_t$ of $\mathfrak{g}^i$ and $\mathfrak{g}^{i+1}$ such that

$$t_i(e_k)=\alpha f_k+\text{a linear combination of } f_1, \ldots, f_{k-1},$$

where $\alpha=\pm 1$ or ± 2.

One checks that $\alpha=\pm 2$ can only happen if $i=2, 4, 8$. It is easily verified in these cases that the assertion of (2.6) holds. For $i<-1$ a similar argument gives the desired result if $i\neq -4$. There remain the cases $i=3, -4$. There again we calculate a determinant. In this case we have to use a more complicated argument, because the $|\mathrm{N}_{rs}|$ may have different values.

First let $i=3$. We then find without difficulty that

$$\pm\det M_3=\mathrm{N}_{r+r_1,r_3}\mathrm{N}_{r+r_3,r_4}\mathrm{N}_{r+r_4,r_1}+\mathrm{N}_{r+r_1,r_4}\mathrm{N}_{r+r_4,r_3}\mathrm{N}_{r+r_3,r_1},$$

where $r=r_2+r_3$ (which is a root).

Now by Jacobi's identity (viz. the last formula (2)) we have

$$(8)\qquad \begin{cases} \mathrm{N}_{r+r_1,r_3}\mathrm{N}_{r,r_1}=\mathrm{N}_{r+r_3,r_1}\mathrm{N}_{r,r_3} \\ \mathrm{N}_{r+r_4,r_1}\mathrm{N}_{r,r_4}=\mathrm{N}_{r+r_1,r_4}\mathrm{N}_{r,r_1} \\ \mathrm{N}_{r+r_3,r_4}\mathrm{N}_{r,r_3}-\mathrm{N}_{r+r_4,r_3}\mathrm{N}_{r,r_4}+\mathrm{N}_{sr}\mathrm{N}_{r_3,r_4}=0, \end{cases}$$

where $s=r_3+r_4$.

Now it follows from lemma (1.7) *b)* that $\mathrm{N}_{r,r_4}=\pm 1$. Then the first 2 formulas (8) give

$$\mathrm{N}_{r+r_1,r_3}\mathrm{N}_{r+r_3,r_4}\mathrm{N}_{r+r_4,r_1}=\mathrm{N}_{r+r_1,r_4}\mathrm{N}_{r+r_3,r_1}\mathrm{N}_{r+r_3,r_4}\mathrm{N}_{r,r_3}\mathrm{N}_{r,r_4}.$$

It follows that

$$\pm\det M_3 = N_{r+r_1,r_4} N_{r+r_3,r_1} (N_{r+r_3,r_4} N_{r,r_3} N_{r,r_4} + N_{r+r_4,r_3}),$$

which (using again lemma (1.7) *b)*) yields

$$\pm\det M_3 = N_{r+r_4,r_3} N_{r,r_4} + N_{r+r_3,r_4} N_{r,r_3} = 2N_{r+r_4,r_3} N_{r,r_4} - N_{sr} N_{r_3,r_4},$$

by the last formula (8).

Another application of Jacobi's identity gives

$$N_{r+r_4,r_3} N_{s,r_2} = N_{sr} N_{r_2,r_3}.$$

Since $N_{s,r_2} = \pm 1$, we have

$$\begin{aligned}\pm\det M_3 &= 2N_{r+r_4,r_3} N_{s,r_2} N_{r,r_4} - N_{sr} N_{r_3,r_4} N_{sr_2}\\ &= N_{sr}(2N_{r,r_4} N_{r_2,r_3} - N_{r_3,r_4} N_{sr_2}).\end{aligned}$$

Now $N_{r,r_4} N_{r_2,r_3} = -N_{r_3,r_4} N_{sr_2}$ (again by Jacobi's identity), and these integers as well as N_{sr}, are ± 1 (by lemma (1.7) *b)*). So $\det M_3 = \pm 3$, which settles the case $i=3$.

Finally for $i=-4$, we find an expression for $\det M_{-4}$ like the one for $\det M_3$ with which we started. Using lemma (1.8) *a)* one gets

$$(9) \qquad N_{r,s-r}(N_{-s,s-r})^{-1} = -|N_{r,s-r}|\,|N_{-s,s-r}|^{-1},$$

if r and s are positive roots (such that $s-r$ is one). By lemma (1.7) *b)* one knows $|N_{rs}|$. Now (9) allows one to compare the expression which one finds for $\det M_{-4}$ with the above one for $\det M_3$, the result is that both have the same absolute value, which has been found to be 3.

Type $\mathbf{G}_2$:

The roots are $\pm r_1$, $\pm r_2$, $\pm(r_1+r_2)$, $\pm(r_1+2r_2)$, $\pm(r_1+3r_2)$, $\pm(2r_1+3r_2)$.

The highest root is $2r_1+3r_2$. We have $N_{rs}=0, \pm 1, \pm 2, \pm 3$. There is no difficulty, using lemma (1.7) *b)*, to verify the assertion of theorem (2.6). This finishes the proof of theorem (2.6).

(2.10) We shall say that p is a *bad prime* for the simple root system R or for the corresponding Lie algebra $\mathfrak{g}$ if p divides a coefficient of the highest root of R (this obviously does not depend on Δ).

If R is not simple, then we say that p is a bad prime if it is one for one of the simple components of R. Otherwise p is called a *good prime.* In the course of the proof of (2.6) we have indicated the highest roots of the various types. From this it follows that the bad primes are for the simples types:

$\mathbf{A}_l$: none; $\mathbf{B}_l, \mathbf{C}_l, \mathbf{D}_l : p=2$; $\mathbf{E}_6, \mathbf{E}_7, \mathbf{F}_4, \mathbf{G}_2 : p=2, 3$; $\mathbf{E}_8 : p=2, 3, 5$.

From (2.6) and its proof we can now extract various characterizations of the bad primes (R is supposed to be simple).

(2.11) *Theorem. — p is a bad prime for $\mathfrak{g}$ if and only if one of the following conditions holds*:

(i) t_i *has an elementary divisor p for some* $i>0$;

(ii) t_p *has an elementary divisor* (*which is then p with multiplicity* 1);

(iii) $l_p = l_{p+1}$;

(iv) $l_i = l-1$ *if* $2 \leq i \leq p+1$.

(As in (1.10), l_i denotes the number of roots with height i).

(i) and (ii) are read off from the statement of theorem (2.6). (iii) and (iv) are read off from the explicit structure of the root systems of the simple types. This is an entirely straightforward verification (using tables I, II, III, IV for types $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$, $\mathbf{F}_4$ and the results cited in (2.9) for the other types).

(2.12) *Proposition. — If t_i ($i>0$) has an elementary divisor, then* $l_i = l_{i+1}$.

This is also proved by using (2.6) and checking the possible cases.

It would be interesting to have a priori proofs of (2.11) and (2.12).

3. On the torsion of compact Lie groups.

(3.1) In this paragraph we denote by G a compact, semi-simple, simply connected Lie group. We denote by $\mathfrak{g}$ the Lie-algebra over $\mathbf{Z}$ defined in § 1, defined by the root system of G. For definiteness we assume $\mathfrak{g}$ to be of " simply connected " type ($\Delta = \Gamma'$). It is known (see [6]) that if R is simple, G has a p-torsion exactly in the following cases:

$p=2$, types $\mathbf{B}_l$, $\mathbf{D}_l$, $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$, $\mathbf{F}_4$, $\mathbf{G}_2$;

$p=3$, types $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$, $\mathbf{F}_4$;

$p=5$, type $\mathbf{E}_8$.

Combining this information with that given by theorem (2.6) one obtains the following result (in which we use for $\mathfrak{g}$ the notations of § 2).

(3.2) *Theorem. — Let* G *be a compact, semi-simple, simply connected Lie group. Then* G *has p-torsion if and only if $t_{-(p+1)}$ has an elementary divisor.*

For the simple types this is checked at once; the extension to the general case is then immediate.

(3.3) (3.2) indicates that there is a connection between the topology of G and the structure of $\mathfrak{g}$. We shall give now a few more results which point in the same direction. All these results are obtained by " checking cases ". We first recall some facts about the structure of the cohomology algebra $H^*(G, k)$ for a field k. It is known that this algebra is a Hopf algebra. The structure theory of Hopf algebras (see e.g. [4]) then implies that

$$H^*(G, k) = k[X_1, \ldots, X_m]/(X_1^{d(1)}, \ldots, X_m^{d(m)}),$$

where $k[X_1, \ldots, X_m]$ is a graded anticommutative polynomial algebra with generators X_i of degree $h(i)$ ($1 \leq i \leq m$). The $d(i)$ are 2 if $\mathrm{char}(k)=0$ and are either 2 or a power of $\mathrm{char}(k)$ if $\mathrm{char}(k) \neq 0$. We now list some known results.

a) If $\mathrm{char}(k)=0$, then $H^*(G, k)$ is an exterior algebra on l generators (where $l=\mathrm{rank}\, G$). These generators have degrees $h(i)=2k_i+1$, where the k_i the integers defined in (2.3). They can be read off from the root system R, as follows from (2.3). These matters are dealt with in [12].

b) Take now $k=\mathbf{F}_p$, the prime field with p elements. If G has p-torsion, then we assume the X_i to be numbered such that $d(1), \ldots, d(a)$ are >2 and $d(a+1)=\ldots=d(m)=2$. We call

$$k[X_1, \ldots, X_a]/(X_1^{d(1)}, \ldots, X_a^{d(a)})$$

the *extraordinary part* of the cohomology algebra $H^*(G, \mathbf{F}_p)$.

First let p be odd. Let G be simple. In the cases where p-torsion occurs (which are enumerated above) the extraordinary part of $H^*(G, \mathbf{F}_p)$ is known (see [5] for $\mathbf{F}_4$, [2] and [6] for $\mathbf{E}_6, \mathbf{E}_7, \mathbf{E}_8$), the following holds: all $d(i)$ $(1\leq i\leq a)$ are equal to p, the $h(i)$ are respectively,

8 if $p=3$, for types $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{F}_4$,
8,20 if $p=3$, for type $\mathbf{E}_8$,
12 if $p=5$, for type $\mathbf{E}_8$.

Comparing this with the results stated in (2.6) we obtain the following statement.

(3.4) *Proposition. — Let* G *be a compact, simple, simply connected Lie group. If p is odd, the extraordinary part of* $H^*(G, \mathbf{F}_p)$ *is* $k[X_1, \ldots, X_a]/(X_1^p, \ldots, X_a^p)$ *where $h(i)$ runs through the integers $2j$ such that t_{-j} has an elementary divisor p.*

(3.5) For $p=2$ a corresponding statement is not true. For then the $d(i)$ occurring in the extraordinary part of $H^*(G, \mathbf{F}_2)$ are not always equal (this is the case, for example, in type $\mathbf{E}_8$, as follows from the results of [3]). The known results (see [1], [3], [5]) show however that the following holds: *the degrees $h(i)$ $(1\leq i\leq a)$ occurring in the extraordinary part of* $H^*(G, \mathbf{F}_2)$ *are the integers j such that t_{-j} has an elementary divisor* 2.

4. The centralizer of a regular unipotent element of a semi-simple algebraic group.

(4.1) In this paragraph we shall give an application of the results of § 2 to a problem in the theory of algebraic groups over an algebraically closed ground field k.

We denote now by G an algebraic group over k (= smooth affine group scheme of finite type over k) which is connected and semi-simple. For the standard facts about such groups we refer to [14], to which we conform. We recall some notions. Let T be a maximal torus in G. With G there is associated a root-system R (in the sense of § 1), the $r\in R$ are rational characters of T. For any $r\in R$ there exists a unipotent subgroup X_r of G, which is isomorphic over k to the additive group G_a and which is normalized by T. Fixing a set of simple roots, let U be the subgroup of G generated by the X_r with $r>0$, let B be the group generated by T and U. The group B is then a Borel (= maximal connected solvable) subgroup of G, U is a maximal connected unipotent subgroup of G.

The Borel subgroups of G are conjugate, so are the maximal connected unipotent subgroups.

In the next result the structure constants N_{rs} will occur of a Lie algebra $\mathfrak{g}$ discussed in § 1, belonging to the root-system R of G. These structure constants are assumed to be integers satisfying (1.7) *b)*. We then have the following important result, due to Chevalley (see [9] and [10]).

(4.2) *Proposition. — There exist isomorphisms* $x_r : G_a \to X_r$ $(r \in R)$ *such that if* $r+s \neq 0$ *we have for* $\xi, \eta \in G_a$,

$$x_r(\xi)x_s(\eta)x_r(\xi)^{-1}x_s(\eta)^{-1} = \prod_{i,j>0} x_{ir+js}(C_{ijrs}\xi^i\eta^j),$$

where the product on the righthand side is over the integral linear combinations of r and s which are contained in R, *taken in a suitable order and where the* C_{ijrs} *are integers with* $C_{11rs} = N_{rs}$.

We shall apply this to obtain information about the structure of U. Henceforth the x_r will always denote isomorphisms $G_a \to X_r$ with the properties of (4.2).

(4.3) *Lemma. — Let* S *be the set of simple roots of* R *defining the ordering of* R. *Let* $x = \prod_{r>0} x_r(\xi_r)$ *(the product being taken in some order) be an element of* U *such that* $\xi_r \neq 0$ *for* $r \in S$. *Then x is contained in exactly one Borel subgroup of* G, *namely* B. *The centralizer* G_x *of x is the direct product of the center* C *of* G *and* U_x, *the centralizer of x in* U.

The first assertion is proved in [17] (lemma 3.2), for the convenience of the reader we indicate the proof. Suppose $gxg^{-1} \in B$ for $g \in G$. Applying Bruhat's lemma ([14], exposé 13, th. 3, Cor. 1) we see that we may take $g = \sigma_w b$, where $b \in B$ and where σ_w is a representative in G of the element $w \in W = N(T)/T$ (N(T) denoting the normalizer of T in G). If x satisfies the condition of (4.3) then (4.2) implies (together with the facts that $B = TU$ and that T normalizes all X_r) that bxb^{-1} satisfies the same conditions. It suffices then to take $g = \sigma_w$. However since $\sigma_w X_r \sigma_w^{-1} = X_{w(r)}$ it follows that $w(s) > 0$ for all $s \in S$. This is known to imply that $w = 1$. Hence $gxg^{-1} \in B$ implies $g \in B$, which proves the first assertion.

As to the second assertion, the preceding argument shows that $G_x \subset B$. Take $g \in G_x$ and write $g = tu$ $(t \in T, u \in U)$. It is well-known that

$$tx_r(\xi)t^{-1} = x_r(r(t)\xi).$$

Using this it follows that $s(t) = 1$ for all $s \in S$. This implies that $t \in C$.

Let X denote the set of all unipotent elements of G. Let l be the rank of G, i.e. the dimension of the maximal tori of G.

(4.4) *Proposition. —* X *is an irreducible Zariski-closed subset of* G *of dimension* $\dim G - l$.

Since every unipotent element of G is conjugate to an element of U, X is the union of the conjugates of U. Then (4.3) implies that the normalizer of U in G is the same as the normalizer of B in G, which is B itself. Application of a well-known result ([14], exposé 6, lemma 5, a more general version is in [15], exposé XIII), taking into account (4.3) and the fact that G/B is a complete variety, proves that X is closed and has the asserted dimension. The irreducibility of X follows easily from the proof of the cited result.

For $x \in G$, let G_x denote its centralizer in G.

(4.5) *Proposition. — For any* $x \in G$ *we have* $\dim G_x \geq l$.

If x is unipotent this follows from (4.4): then the orbit of x in X under the adjoint action of G has dimension $\leq \dim G - l$, hence $\dim G_x \geq l$.

If x is arbitrary, write $x = su$ (where s and u are the semi-simple and unipotent parts of x). Then the identity component G_s^0 of G_s is a reductive group (i.e. a connected algebraic group whose radical is a torus) and the centralizer of x in G coincides with that of u in G_s. Now $u \in G_0^s$ ([14], exp. 6, cor. 2 of Th. 6). We can then apply the statement for x unipotent to G_s^0 modulo its radical.

(4.6) We define an element x of G to be *regular* if its centralizer G_x has dimension l. The regular elements of a semi-simple group are the subject of [17], where various characterizations and properties are discussed. One of the crucial points of [17] is the proof of the existence of regular unipotent elements for any semi-simple G. We shall show that the results of § 2 of this paper enable one to give a different existence proof (however under some restrictions on the characteristic of k). Moreover with the results of § 2 one can get information about the connectedness of the centralizer G_x of a regular unipotent element x. The study of these connectedness questions is the main object of this paragraph.

(4.7) *Lemma. — Suppose that* G *contains a regular unipotent element. Then any element* $x \in U$ *with the property of* (4.3) *is regular. Two regular unipotent elements are conjugate.*

This follows from Theorem 3.3 of [17]. A direct proof is as follows: suppose that $y = \prod_{r>0} x_r(\xi_r) \in U$ is regular. The set Y of conjugates uyu^{-1} $(u \in U)$ of y in U is closed in U by a theorem of Rosenlicht (*Trans. Am. Math. Soc.*, 101 (1961), p. 221), moreover it is clear that $\dim Y \geq \dim U - l$. On the other hand it follows from (4.2) that if $z = \prod_{r>0} x_r(\eta_r) \in Y$, we have $\eta_s = \xi_s$ for $s \in S$. It follows that $\dim Y = \dim U - l$ and that Y is precisely the set of elements z satisfying this condition. In particular, $u = \prod_s x_s(\xi_s)$ lies in Y and hence is regular. Now if $\xi_{s_0} = 0$ for some $s_0 \in S$, there is a non-trivial subtorus of T which centralizes u, therefore $\dim G_u \geq l + 1$, which contradicts the regularity of u. Hence, all ξ_s are $\neq 0$ and the first assertion follows.

The second assertion can be derived from the first one. Another proof is as follows: let x and y be regular unipotents. Consider their orbits (under adjoint action of G) in the set X of unipotent elements. Because of dimensions, these orbits contain Zariski-open subsets of X. X being irreducible, these open sets have a non-empty intersection and the conjugacy of x and y follows.

(4.8) It follows from (4.7) that, if regular unipotents exist,

$$v = \prod_{s \in S} x_s(1) \tag{10}$$

(the product taken in some order) is a typical one.

From (4.3) it follows that v is contained in exactly one Borel subgroup, namely B and that $G_v = U_v C$. We shall now investigate, generally, the group U_v.

Denote by U_i the normal subgroup of U generated by the X_r with $h(r) \geq i$ $(i \geq 1)$. We have $U_i \supset U_{i+1}$, $U_1 = U$, $U_n = \{e\}$ for large n. U_i/U_{i+1} is an abelian algebraic group, isomorphic to $(G_a)^{l_i}$ (where, as in § 2, l_i is the number of positive roots r with height i). All this follows from (4.2).

Put for $i \geq 1$,

$$V_i = \{u \in U \mid vuv^{-1}u^{-1} \in U_{i+1}\},$$

this is a closed subgroup of U, containing U_i. Let W_i be the canonical image of V_i in U/U_i. W_i is a unipotent algebraic group over k. The canonical homomorphism $U/U_{i+1} \to U/U_i$ induces a homomorphism

$$f_i : W_{i+1} \to W_i.$$

W_1 is reduced to the identity, on the other hand for sufficiently large n we have $W_n = U_v$.

We now study $\operatorname{Ker} f_i$ and $\operatorname{Im} f_i$. Let $w \in \operatorname{Ker} f_i$. Then w is the coset of an element

$$u = \prod_{h(r)=i} x_r(\xi_r)$$

modulo U_{i+1}.

Using (4.2) one sees that for an u of this form one has

$$vuv^{-1}u^{-1} = \prod_{h(r)=i+1} x_r(\eta_r) \bmod U_{i+2},$$

where

$$\eta_r = \sum_{s \in S} N_{s,r-s}\xi_{r-s}. \tag{11}$$

Here s runs through the set S of simple roots, the $N_{s,r-s}$ are the structure constants of the Lie algebra $\mathfrak{g}$ belonging to R (with the convention that $N_{s,r-s} = 0$ if $r-s$ is not a root).

If $w \in W_{i+1}$, we have $vuv^{-1}u^{-1} \in U_{i+2}$, hence the ξ_r have to satisfy the linear equations obtained by putting the η_r in (11) equal to 0.

Next $\operatorname{Im} f_i$. Map V_i homomorphically into U_{i+1}/U_{i+2} by sending $u \in V_i$ into $vuv^{-1}u^{-1}$. Under this homomorphism U_i is mapped onto a subgroup U'_{i+1}/U_{i+2} of U_{i+1}/U_{i+2}, where U'_{i+1} denotes the group generated by U_{i+2} and the elements

$$\prod_{h(r)=i+1} x_r(\eta_r),$$

with η_r of the form (11).

By passing to quotients one gets a homomorphism of W_i into U_{i+1}/U'_{i+1}. It follows at once that the kernel of this homomorphism is $\operatorname{Im} f_i$.

One gets in this way the following inequality

$$\dim \operatorname{Im} f_i \geq \dim W_i - \dim U_{i+1}/U'_{i+1}. \tag{12}$$

(4.9) (11) shows that the matrices M_i defined by (6) enter the picture here. We now tie up the problems considered here with the results of § 2. Let $\mathfrak{g}$ be the Lie-algebra of the type of § 2, whose root system is that of G (the choice of Δ is immaterial).

Put $\mathfrak{g}_k=\mathfrak{g}\otimes_{\mathbf{Z}}k$, $\mathfrak{g}_k^i=\mathfrak{g}^i\otimes_{\mathbf{Z}}k$, $t_{i,k}=t_i\otimes\mathrm{id}$. Let p be the characteristic of k. Define

$$l_{i,p}=\mathrm{rank}\ t_{i,k}$$

(this depends only on the characteristic of k), then

$$\dim_k(\mathrm{Ker}\ t_{i,k})=l_i-l_{i,p}.$$

(2.2) asserts that $l_{i,0}=l_{i+1}$, (2.11) asserts that $l_{i,p}=l_{i+1}$ is p is a good prime for g.

(4.10) *Proposition. — a)* $\mathrm{Ker} f_i$ *is isomorphic to* $(\mathrm{G}_a)^{l_i-l_{i,p}}$;

b) $\dim \mathrm{Im} f_i \geq \dim \mathrm{W}_i - l_{i+1}+l_{i,p}$.

In fact, both of these results are direct consequences of what was established in (4.8). For example, *b)* is another way of writing (12). (Actually, equality holds in *b)*, as follows from [17]. We will use this in the proof of (4.12).)

We can now prove the main results of this paragraph. We shall say that a prime is a good (or bad) prime for G if it is a good (or bad) prime for its root system R (see (2.10)). p always denotes the characteristic of k.

(4.11) *Theorem. — Let p be* 0 *or a good prime for* G. *Then there exist regular unipotent elements in* G. *The centralizer of a regular unipotent element is the direct product of the center of* G *and a connected unipotent subgroup.*

It has already been established in (4.7) that we only need to prove that the element v of (10) is regular. Our assumption about p implies by (2.11) that $l_{i,p}=l_{i+1}$, then (4.10) *b)* shows that f_i is surjective and (4.10) *a)* shows that $\dim \mathrm{U}_v=\sum_i(l_i-l_{i+1})=l$.

The connectedness statement also follows: assuming W_i to be connected, the surjectivity of f_i and the fact that $\mathrm{Ker} f_i$ is connected (it is a vector group) implies that W_{i+1} is connected. Since $\mathrm{W}_1=\{e\}$, $\mathrm{W}_n=\mathrm{U}_v$ for large n, U_v is connected.

The counterpart of (4.11) for bad primes is

(4.12) *Theorem. — Let p be a bad prime for* G. *Then there exist regular unipotent elements in* G. *A regular unipotent element is not contained in the identity component of its centralizer, hence the centralizer of a regular unipotent element is the direct product of the center of* G *and a non-connected unipotent subgroup.*

The fact that regular unipotent elements exist in all cases has been established by Steinberg ([17], § 4) by a different method. We will use this now, to prove the other statements of (4.12).

Let v be the element defined by (10). We know by (4.7) that v is regular, hence $\dim \mathrm{U}_v=l$. From (4.10) one infers that

$$\dim \mathrm{W}_{i+1}-\dim \mathrm{Ker} f_i \geq \dim \mathrm{W}_i - l_{i+1}+l_{i,p},$$

hence by (4.10) *a)*

$$\dim \mathrm{W}_{i+1}-\dim \mathrm{W}_i \geq l_i-l_{i+1},$$

whence

$$l = \dim U_v = \sum_i (\dim W_{i+1} - \dim W_i) \geq \sum_i (l_i - l_{i+1}) = l.$$

It follows that

$$(13) \qquad \dim \operatorname{Im} f_i = \dim W_i - l_{i+1} + l_{i,p}, \qquad \dim W_{i+1} - \dim W_i = l_i - l_{i+1}$$

for all $i \geq 1$.

If p is a bad prime we know from (2.11) that t_i has an elementary divisor for some i and then we read off from (2.6) that $l_{i,p} = l_{i+1} = l - 1$ for $i = 1, \ldots, p-1$ and $l_{p,p} = l_{p+1} - 1 = l - 2$ (where $l = \operatorname{rank} G$). Then (13) implies that $\dim W_i = 1$ for $2 \leq i \leq p$. Moreover it also follows from the first formula (13) that f_i is surjective for $i = 1, \ldots, p-1$.

We now obtain from the first formula (13)

$$\dim \operatorname{Im} f_p = 0,$$

so $f_p(W_{p+1})$ is a finite group. A fortiori the canonical image of U_v in U/U_p is a finite group. This image contains the coset of v modulo U_p, which is not the identity element (since $v \notin U_p$). It follows that v is not contained in the identity component U_v^0 of U_v. This proves (4.12)

(4.13) *Remarks.* — *a)* It would be interesting to know the exact order of U_v/U_v^0 in the case considered in (4.12). Of course this order is a p-power.

The only result in this direction which is known to the author (and which will be stated here without proof) is the following one. Suppose that there is exactly one $i > 0$ for which t_i has an elementary divisor p. Then U_v/U_v^0 has order p. This result covers the following cases of a simple G: $p = 2$, types $\mathbf{B}_2, \mathbf{B}_3, \mathbf{E}_6, \mathbf{G}_2$; $p = 3$, types $\mathbf{E}_6, \mathbf{E}_7, \mathbf{F}_4, \mathbf{G}_2$; $p = 5$, types $\mathbf{E}_8$.

b) That regular unipotent elements behave differently in low characteristics was first brought to the author's attention by J. Tits.

From (4.11) one can derive the following result about semi-simple groups over nonalgebraically closed ground fields.

(4.14) *Theorem.* — *Let k be a perfect field. Suppose that* G *is a semi-simple algebraic group of adjoint type, defined over k, suppose that the characteristic p of k is* 0 *or a good prime for* G. *Let* $G(k)$ *denote the group of k-rational points of* G. *Then any two regular unipotent elements in* $G(k)$ *are conjugate in* $G(k)$.

If $G(k)$ does not contain any regular unipotent element of G, the assertion is vacuous. Assume now that $x, y \in G(k)$ are regular unipotent elements of $G(k)$. By (4.11), the centralizer G_x of x is a *connected* unipotent subgroup of G. x being rational over the perfect field k, it is well-known that G_x is defined over k. Put

$$P = \{g \in G \mid gxg^{-1} = y\}$$

By (4.7) P is not empty. Hence P is a principal homogeneous space of G_x, which is defined over k. G_x being connected and unipotent and k being perfect, P contains a point $g \in G(k)$ (see [16], III-8, prop. 6). This proves our assertion.

(4.15) *Remarks.* — *a)* It seems likely that the condition for k to be perfect can be dropped from (4.14). Since the result about principal homogeneous spaces, used in the proof of (4.14), is false for non-perfect fields (counterexamples are in [16], III-16), the proof does not carry over.

b) From [17], Theorem 1.6, it follows that $G(k)$ contains regular unipotent elements either if G is split over k or if G contains a Borel subgroup over k (the quoted result gives the existence of regular unipotent elements if G contains a Borel subgroup over k only if G does not have a component of type $\mathbf{A}_n$ with n even; this restriction can however be removed).

c) If p is a bad prime for G the argument used in the proof of (4.13) shows that the number of conjugacy classes of regular unipotent elements of $G(k)$ is either 0 or the number of elements of $H^1(k, G_x/G_x^0)$. It can be shown that the number of elements of $H^1(k, G_x/G_x^0)$ is at least 2. Consequently, if k is a perfect field, the condition that p is a good prime is also necessary for the conjugacy statement of (4.14) (provided, of course, that $G(k)$ contains regular unipotent elements).

5. Regular nilpotent elements in the Lie algebra of a semi-simple algebraic group.

(5.1) As in § 4, let G denote a connected, semi-simple, linear algebraic group over the algebraically closed field k. We consider now the Lie algebra of G. It is known that this Lie algebra is isomorphic to $\mathfrak{g} \otimes_{\mathbf{Z}} k$, where $\mathfrak{g}$ is of the type discussed in § 2 (its root system R is that of G). However, to abbreviate notations, we write throughout this paragraph $\mathfrak{g}$ instead of $\mathfrak{g} \otimes_{\mathbf{Z}} k$.

Let T, U, B, X_r have the same meaning as in § 4. The structure of $\mathfrak{g}$ is then as follows. $\mathfrak{g}$ is a direct sum

$$\mathfrak{g} = \mathfrak{t} + \sum_{r \in R} k e_r$$

where $\mathfrak{t}$ is the Lie algebra of T and ke_r that of X_r (both identified with a subalgebra of $\mathfrak{g}$). With the notations of § 2, $\mathfrak{t}$ corresponds to $\Delta \otimes_{\mathbf{Z}} k$ and e_r to $e_r \otimes 1$.

The Lie algebra of B is

$$\mathfrak{b} = \mathfrak{t} + \sum_{r>0} k e_r,$$

that of U is

$$\mathfrak{u} = \sum_{r>0} e_r.$$

G acts on $\mathfrak{g}$ by means of the adjoint representation Ad. For $x \in \mathfrak{g}$, we denote by G_x the centralizer of x in G, i.e. the subgroup of G formed by the $g \in G$ with $\mathrm{Ad}(g)x = x$. We denote by $\mathfrak{g}_x$ the centralizer of x in $\mathfrak{g}$ (which contains the Lie algebra of G_x).

We shall say that $x \in \mathfrak{g}$ is *nilpotent* if x is contained in the Lie algebra of a connected unipotent subgroup H of G. Since H is conjugate to a subgroup of U, x is nilpotent if and only if $\mathrm{Ad}(g)x \in \mathfrak{u}$ for some $g \in \mathrm{G}$. We shall give presently some results about nilpotent elements in $\mathfrak{g}$, similar to those proved in § 4 for unipotent elements in groups.

(5.2) *Remarks.* — *a)* The definition of a nilpotent element, given above, is the most convenient one for our purposes here. However, because of the definition of semi-simple and unipotent elements in algebraic groups ([14], exposé 4, n° 4), another way of defining nilpotent elements in the Lie algebra $\mathfrak{g}$ of any connected linear algebraic group G (semi-simple or not) over the algebraically closed field k would be the following one: Suppose G is a subgroup of $\mathrm{GL}(n, k)$, then $\mathfrak{g}$ is a subalgebra of the Lie algebra $\mathfrak{gl}(n, k)$, in which the notion of nilpotent element is known. Define then $x \in \mathfrak{g}$ to be nilpotent if it is nilpotent as an element of $\mathfrak{gl}(n, k)$.

One can show that this definition is equivalent to the one given above.

b) One can define an element x of $\mathfrak{g}$ to be semi-simple if x is contained in the Lie algebra of a torus of G. The remarks made under *a)* hold too in that case.

It can be proved that if G is a connected linear algebraic group over k (algebraically closed) any element x of the Lie algebra $\mathfrak{g}$ of G can be written in the form $x = x_s + x_n$, where x_s (x_n) is a semi-simple (nilpotent) element of $\mathfrak{g}$, such that $[x_s, x_n] = 0$. Moreover such a decomposition is unique [1].

c) In the case that the characteristic of k is 0, the statements about nilpotent elements of $\mathfrak{g}$ to be given below can be derived easily from the corresponding ones about unipotent elements in G (e.g. using an " exponential mapping ").

(5.3) *Lemma. — Let* S *be the set of simple roots of* R, *defining the ordering of* R. *Let* $x = \sum_{r>0} \xi_r e_r$ *be an element of* $\mathfrak{u}$ *such that* $\xi_r \neq 0$ *if* $r \in \mathrm{S}$. *Then there is exactly one Borel subgroup of* G *whose Lie algebra contains* x, *viz.* B. G_x *is the direct product of the center of* G *and of* U_x, *the centralizer of* x *in* U.

The proof of this is completely analogous to that of (4.3), so we leave it to the reader.

Let X denote the set of all nilpotent elements of $\mathfrak{g}$, let l be the rank of G.

(5.4) *Proposition. —* X *is an irreducible Zariski-closed subset of the affine space* $\mathrm{W}(\mathfrak{g})$ *determined by* $\mathfrak{g}$, *whose dimension is* $\dim \mathrm{G} - l$.

This is proved like (4.4), using (5.3).

(5.5) *Remark.* — By a similar argument one derives from (5.3) the following result of Grothendieck: $\mathfrak{g}$ is the union of the Lie algebras of its Borel subgroups ([15], exposé XIV, th. 4.11, the proof given there is different).

(5.6) *Proposition. — Let x be a nilpotent element of* $\mathfrak{g}$, *then* $\dim \mathrm{G}_x \geq l$.

Because the orbit of x under the adjoint action of G is contained in X, we have $\dim \mathrm{G}/\mathrm{G}_x \leq \dim \mathrm{X}$, which implies (5.6).

[1] *(Added in proof.)* Proofs of these statements can be found in a note of A. Borel and the author in *Proc. Sympos. Pure Math.*, vol. 9 (Amer. Math. Soc., Providence, 1966).

Remark. — (5.6) is true for all $x \in \mathfrak{g}$.

(5.7) We now define $x \in \mathfrak{g}$ to be *regular* if $\dim G_x = l$ and *smoothly regular* if $\dim \mathfrak{g}_x = l$ [1]. Since $\dim G_x \leq \dim \mathfrak{g}_x$ it follows from (5.6) that a smoothly regular nilpotent element is regular (it will follow from (5.9) that the converse is not true).

(5.8) *Lemma.* — *Suppose that* $\mathfrak{g}$ *contains regular nilpotent elements. Then any* $x \in \mathfrak{g}$ *with the property of* (5.3) *is regular.*

The proof is like that of (4.7).

(5.9) *Theorem.* — a) *Smoothly regular milpotent elements exist in* $\mathfrak{g}$ *if and only if the characteristic of* k *is either* 0 *or a good prime for* G, *which does not divide the order of the fundamental group of* R.

b) *If* p *is either* 0 *or a good prime for* G *then regular nilpotent elements exist in* $\mathfrak{g}$, *the centralizer* G_x *of a regular nilpotent element* x *is then the direct product of the center of* G *and a connected unipotent subgroup of* G.

c) *The regular nilpotent elements of* $\mathfrak{g}$ *form one orbit of* G *under adjoint action.*

From (5.8) it follows that if $\mathfrak{g}$ contains regular nilpotent elements, then $x = \sum_{r \in S} e_r$ is one (S is the set of simple roots). So in order to prove *a)* it suffices to investigate when $\dim \mathfrak{g}_x = l$.

This one can read off from (2.5) and (2.6) (using (2.11)).

b) is proved in the same way as (4.11), the details may be left to the reader. The conjugacy statement of *c)* is proved as the corresponding statement of (4.7).

(5.10) *Remark.* — One can ask whether (4.12) has a counterpart for $\mathfrak{g}$. The proof of (4.12) depended on Steinberg's result that regular unipotent elements exist in all characteristics. The author does not know whether the corresponding result is true for Lie algebras.

Mathematisch Instituut der Rijksuniversiteit, Utrecht.

[1] The name smoothly regular has been chosen because the centralizer of a regular element x in the sense of group schemes is smooth over k if and only if x is smoothly regular.

Manuscrit reçu le 14 juin 1965.

APPENDIX

We give here tables for the positive roots of the root-systems of type $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$, $\mathbf{F}_4$, when expressed in the simple roots. Description of these root-systems are given in (2.9). We use an evident abbreviation in the tables: for example, in the case $\mathbf{E}_6$, 012211 denotes the root $r_2+2r_3+2r_4+r_5+r_6$, where the r_i are the simple roots given in (2.9).

TABLE I

Positive roots of $\mathbf{E}_6$

Height						
1......	100000	010000	001000	000100	000010	000001
2......	110000	011000	001100	001001	000110	
3......	111000	011100	011001	001110	001101	
4......	111100	111001	011110	011101	001111	
5......	111110	111101	012101	011111		
6......	112101	111111	012111			
7......	122101	112111	012211			
8......	122111	112211				
9......	122211					
10......	123211					
11......	123212					

TABLE II

Positive roots of $\mathbf{E}_7$

Height							
1......	1000000	0100000	0010000	0001000	0000100	0000010	0000001
2......	1100000	0110000	0011000	0001100	0001001	0000110	
3......	1110000	0111000	0011100	0011001	0001110	0001101	
4......	1111000	0111100	0111001	0011110	0011101	0001111	
5......	1111100	1111001	0111110	0111101	0012101	0011111	
6......	1111110	1111101	0112101	0111111	0012111		
7......	1112101	1111111	0122101	0112111	0012211		
8......	1122101	1112111	0122111	0112211			
9......	1222101	1122111	1112211	0122211			
10......	1222111	1122211	0123211				
11......	1222211	1123211	0123212				
12......	1223211	1123212					
13......	1233211	1223212					
14......	1233212						
15......	1234212						
16......	1234312						
17......	1234322						

TABLE III

Positive roots of $\mathbf{E}_8$

Height								
1......	10000000	01000000	00100000	00010000	00001000	00000100	00000010	00000001
2......	11000000	01100000	00110000	00011000	00001100	00001001	00000110	
3......	11100000	01110000	00111000	00011100	00011001	00001110	00001101	
4......	11110000	01111000	00111100	00111001	00011110	00011101	00001111	
5......	11111000	01111100	01111001	00111110	00111101	00012101	00011111	
6......	11111100	11111001	01111110	01111101	00112101	00111111	00012111	
7......	11111110	11111101	01112101	01111111	00122101	00112111	00012211	
8......	11112101	11111111	01122101	01112111	00122111	00112211		
9......	11122101	11112111	01222101	01122111	01112211	00122211		
10......	11222101	11122111	11112211	01222111	01122211	00123211		
11......	12222101	11222111	11122211	01222211	01123211	00123212		
12......	12222111	11222211	11123211	01223211	01123212			
13......	12222211	11223211	11123212	01223212	01233211			
14......	12223211	11233211	11223212	01233212				
15......	12233211	12223212	11233212	01234212				
16......	12333211	12233212	11234212	01234312				
17......	12333212	12234212	11234312	01234322				
18......	12334212	12234312	11234322					
19......	12344212	12334312	12234322					
20......	12344312	12334322						
21......	12345312	12344322						
22......	12345322	12345313						
23......	12345422	12345323						
24......	12345423							
25......	12346423							
26......	12356423							
27......	12456423							
28......	13456423							
29......	23456423							

TABLE IV

Positive roots of $\mathbf{F}_4$

Height				
1......	1000	0100	0010	0001
2......	1100	0110	0011	
3......	1110	0120	0111	
4......	1120	1111	0121	
5......	1220	1121	0122	
6......	1221	1122		
7......	1231	1222		
8......	1232			
9......	1242			
10......	1342			
11......	2342			

BIBLIOGRAPHY

[1] S. Araki, Cohomology modulo 2 of the compact exceptional groups E_6 and E_7, *Journal of Math. Osaka City Univ.* 12 (1961), 43-65.

[2] —, Differential Hopf algebras and the cohomology mod 3 of the compact exceptional groups E_7 and E_8, *Annals of Math.* 73 (1961), 404-436.

[3] — and Y. Shikata, Cohomology mod 2 of the compact exceptional group E_8, *Proc. Japan Acad.* 37 (1961), 619-622.

[4] A. Borel, Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts, *Annals of Math.* 57 (1953), 115-207.

[5] —, Sur l'homologie et la cohomologie des groupes de Lie, *American Journal of Math.* 76 (1954), 273-342.

[6] —, Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes, *Tôhoku Math. Journal*, 2nd Series 13 (1961), 216-240.

[7] N. Bourbaki, *Algèbre*, chap. VI et VII, Paris (1952).

[8] E. Cartan, Sur la structure des groupes de transformations finis et continus, *Œuvres* I 1, Paris (1952), 137-287.

[9] C. Chevalley, Sur certains groupes simples, *Tôhoku Math. Journal*, 2nd Series 7 (1955), 14-66.

[10] —, Certains schémas de groupes semi-simples, *Sém. Bourbaki*, exposé n° 219 (1960-61).

[11] N. Jacobson, *Lie algebras*, Interscience (1962).

[12] B. Kostant, The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group, *American Journal of Math.* 81 (1959), 973-1032.

[13] —, Lie group representations in polynomial rings, *ibid.*, 85 (1963), 327-404.

[14] Séminaire C. Chevalley, *Classification des groupes de Lie algébriques*, Paris (1956-58).

[15] Séminaire M. Demazure et A. Grothendieck, *Schémas en groupes* (1963-64).

[16] J.-P. Serre, Cohomologie galoisienne, *Lecture notes in mathematics*, n° 5, Springer-Verlag (1964).

[17] R. Steinberg, Regular elements of semi-simple algebraic groups, *Publications Math.*, I.H.E.S., n° 25 (1965).