Reproduced (with corrections) from
The Punjab University
Journal of Mathematics
Vol. XVI (1983), pp. 9–30.

THE JACOBI IDENTITY

H. Azad

Introduction

The aim of this paper is to outline an alternative approach to Chevalley groups which is suggested by results of R. Steinberg, especially § 11 of [6], and by [1]. The approach we have in mind works with a system of axioms which involve only a root system and a commutative ring, and in a sense avoids Chevalley bases. Needless to say, this would have been impossible without knowing the contents of [2] and [6]. An advantage of this approach is that problems like those mentioned in [2, p. 64] vanish automatically. This paper is organized as follows: In § 1 we prove an analogue of [1] for a class of Lie algebras. Then, in § 2, by simply reversing a procedure given in the proof of Proposition (1.1), we construct, for a given root system which has no multiple bonds, a function N, defined on pairs of independent roots (u, v) such that $N_{u,v}$ is ± 1 if and only if $u+v$ is a root, and verify the Jacobi identity for N. That such a function exists is nothing new; see, for example [2, p. 24], [8] or [5, p. 285], which also gives the briefest solution to date of this problem. We have thought doing this worthwhile as the function N arises naturally from the root system. The construction of a Lie algebra for a given root system is then immediate. This construction may also interest those who do machine computation as Definition (2.3) can be translated into an algorithm which will produce positive roots and structure constants one after the other.

In the final section we give a system of axioms for Chevalley groups over commutative rings, and making use of results of R. Steinberg together with those of the previous sections, we outline a proof of existence of these groups.

The arguments of this paper are of an elementary character and in essence involve only the Jacobi identity and some technicalities on root systems.

Our references for root systems and Chevalley groups are [2, 4, 6].

1 A Uniqueness Theorem

Let R be an irreducible root system with no multiple bonds, R^+ a positive system of roots, S the corresponding simple system of roots and A a commutative ring. In this section we consider Lie algebras $(L, [\ ,\ ])$ over A with the following properties:

(a) L is generated by elements $X_r \ \ (r \in R)$ such that $aX_r \neq 0$ for all nonzero $a \in A$.

(b) $[X_r, X_s] = N_{r,s}X_{r+s}$, if $r + s \in R$, $N_{r,s}$ being an element of A, and $[X_r, X_s] = 0$ if $r + s \neq 0$ and $r + s \notin R$.

(c) $[X_s, X_{-s}; X_r] = \langle r, s\rangle X_{r,s}$, s being a *simple* and r an *arbitrary* root: here $\langle r, s\rangle$ is the Cartan integer corresponding to the pair of roots (r, s).

Proposition 1.1 *There exist units c_r $(r \in R)$ such that if we set $X'_r = c_r X_r$, $[X'_r, X'_s] = N'_{r,s}X'_{r+r}$ $\ (r + s \neq 0)$ and $H_r = [X'_r, X'_{-r}]$ for all $r, s \in R$, then*

(i) $[H'_r, X'_s] = \langle s, r\rangle X'_s \ \ (r, s \in R)$.

(ii) $N'_{r,s} = \pm 1$, *if* $r + s \in R$.

(iii) $N'_{r,s}$ *is completely determined once an ordering on* S *has been fixed.*

(iv) If $[X_a, X_{-a}]$ $\ (a \in S)$ *and* X_r $\ (r \in R)$ *form a basis of* L*, then every automorphism of* R *extends to an automorphism of* L*.*

(v) In any case, every automorphism of R *extends to an automorphism of the Lie algebra with generators* Y_a $\ (a \in R)$ *and relations* $[Y_a, Y_b] = N'_{a,b}Y_{a+b}$ $\ (a, b$ *being independent roots).*

Proof. (After [1]). Fix an ordering on S. Let $\sigma \in R^+$ be a non-simple root and let α be the first simple root such that $(\sigma, \alpha) > 0$. Then $\sigma - \alpha$ is a root but $\sigma + \alpha$ is not a root.

(A) Applying the Jacobi identity to $X_\alpha, X_{-\alpha}, X_\sigma$ we find that $N_{\alpha,\sigma-\alpha} N_{\sigma,-\alpha} = -1$. Hence $N_{\alpha,\sigma-\alpha}$ is a unit; likewise $N_{-\alpha,-\sigma+\alpha}$ is also a unit, so scaling X_σ and $X_{-\sigma}$ we can assume that $N_{\alpha,\sigma-\alpha} N_{-\alpha,-\sigma+\alpha} = -1$: this is the normalization which (i) requires, as we will soon see.

We next show that with this normalization we always have $N_{u,v} N_{-u,-v} = -1$, u, v being positive roots such that

$$u + v \text{ is a root.} \qquad (*)$$

Let $\sigma = u+v$, let α be the first simple root such that $(\sigma, \alpha) > 0$ and let $R_{uv\alpha}$ denote the integral closure of u, v, and α in R. If $R_{uv\alpha}$ is of type A_2 then u, v form a basis of $R_{uv\alpha}$, so u or v is α, and $(*)$ holds by definition, and therefore also when height of σ is 2. So suppose $R_{uv\alpha}$ is of type A_3. Choose a simple system of roots, say a, b, c corresponding to the positive system $R_{uv\alpha} \cap R^+$. We may assume that $\langle a, b \rangle = \langle b, c \rangle = -1$ and $\langle a, c \rangle = 0$. Then σ must be the sum of these simple roots. But σ has only two decompositions as sums of two roots in $R_{uv\alpha} \cap R^+$, namely $\sigma = a + (b+c) = (a+b) + c$ and α is a or c (so $N_{a,b+c} N_{-a,-b-c} = -1$ or $N_{c,a+b} N_{-c,-a-b} = -1$).

By the Jacobi identity we have

$$\begin{aligned} N_{b,c} N_{b+c,a} &= N_{a,b} N_{c,a+b}, \\ N_{-b,-c} N_{-b-c,-a} &= N_{-a,-b} N_{-c,-a-b}. \end{aligned}$$

By induction on heights we also have $N_{a,b} N_{-a,-b} = N_{b,c} N_{-b,-c} = -1$, so multiplying the previous two equations and using the parenthetical remark above we find that $N_{u,v} N_{-u,-v} = -1$.

Let $H_r = [X_r, X_{-r}]$ $(r \in R)$, with the X_r normalized as above. By assumption, when r is simple, we have $[H_r, X_s] = \langle r, s \rangle X_s$ and $[H_{-r}, X_s] = \langle -r, s \rangle X_s$. Assume this is true for all roots of height less than N and that r is a root of height N. Let $r = \alpha+\beta$, where $\alpha \in S$ and $(r, \alpha) > 0$.

Applying the Jacobi identity to $X_\alpha, X_\beta, X_{-\alpha-\beta}$ we find that

$$N_{\alpha\beta} H_{\alpha+\beta} = N_{\beta,-\alpha-\beta} H_\alpha + N_{-\alpha-\beta,\alpha} H_\beta. \qquad (**)$$

As $[H_\alpha, X_\beta] = \langle\beta, \alpha\rangle X_\beta$ as well as $N_{\alpha,\beta} N_{\alpha+\beta,-\alpha}, X_\beta$, we have $\langle\alpha, \beta\rangle = N_{\beta,\alpha} N_{\alpha+\beta,-\beta}$. Similarly, $\langle -\alpha, -\beta\rangle = N_{-\beta,-\alpha} N_{-\alpha-\beta,\beta}$. By induction on heights we have $[H_\beta, X_\alpha] = \langle\alpha, \beta\rangle X_\alpha$, so $\langle -\beta, -\alpha\rangle = N_{-\alpha,-\beta} N_{-\alpha-\beta,\alpha}$. Multiplying (**) by $N_{-\alpha,-\beta}$ and using $N_{\alpha,\beta} N_{-\alpha,-\beta} = -1$ we have:

$$\begin{aligned} -H_{\alpha+\beta} &= N_{-\alpha,-\beta} N_{\beta,-\alpha-\beta} H_\alpha + N_{-\alpha,-\beta} N_{-\alpha-\beta,\alpha} H_\beta \\ &= \langle\alpha, \beta\rangle H_\alpha + \langle\beta, \alpha\rangle H_\beta. \end{aligned}$$

Hence $H_{\alpha+\beta} = H_\alpha + H_\beta$, and therefore $[H_r, X_s] = \langle r, s\rangle X_s$ for all $s \in R$. This proves (i).

(B) To achieve (ii) we normalize X_σ and $X_{-\sigma}$ ($ht\sigma \geq 2$) so that $N_{\alpha,\sigma-\alpha} = 1$, and $N_{-\alpha,-\sigma+\alpha} = -1$. Arguing as in (A) we find that this normalization determines all the constants $N_{u,v}$ if $u + v$ is a root and u, v are both positive or both negative. Moreover, $N_{u,v} N_{-u,-v}$ is still -1 so $[H_r, X_s] = \langle r, s\rangle X_s$ for all $r, s \in R$. This implies that $\langle u, v\rangle = N_{v,u} N_{v+u,-v}$. By considering the roots in the integral closure of u and v we find that remaining structure constants are also completely determined.

(C) The proof of the remaining assertions is implicit in steps (A) and (B) and is left to the reader. ■

The following corollary has been known for some time: See [8, p. 51].

Corollary 1.2 [Steinberg]. *The existence problem for semi-simple Lie algebras is equivalent to the existence problem for Lie algebras whose root systems have no multiple bonds.*

Proof. Given a root system R with multiple bonds there exists a root system $\widetilde{R}$ with no multiple bonds and an automorphism ρ of $\widetilde{R}$ such that twisting $\widetilde{R}$ according to ρ one obtains R: see [6, p. 175] for details.

As a semisimple Lie algebra corresponding to the root system $\widetilde{R}$ is of the type considered above, we can extend the automorphism to an automorphism of this Lie algebra and consider its fixed points: this will be a Lie algebra with root system R. All of this follows from (1.1) and [7, p. 873–877]*. ■

Corollary 1.3 [3, p. 147]. *Let R be a root system with no multiple bonds, L a semisimple Lie algebra whose root system is R, S a simple system of roots and ρ an automorphism of R which maps S into itself. If L_α $(\alpha \in R)$ are the root spaces of L then there is an automorphism σ which maps L_α into $L_{-\alpha}$ $(\alpha \in R)$ and which commutes with ρ.*

Proof. We can choose a system of generators X_α $(\alpha \in R)$ such that $[X_\alpha, X_\beta] = N_{\alpha,\beta} X_{\alpha+\beta} (\alpha + \beta \neq 0)$ and $[X_\alpha, X_{-\alpha}; X_\beta] = \langle \beta, \alpha \rangle X_\beta$ [4, p. VI-2]. The automorphisms $\alpha \to -\alpha$ $(\alpha \in R)$ and σ commute and by (1.1) extend to commuting automorphisms of L. ■

2 A Construction

Let R, R^+ and S be as in § 1. Denote $R_{ab\ldots}$ the integral closure of the roots $a, b, \ldots$ in R. We wish to reverse the procedure given in the proof of (1.1) to construct a function N, defined on pairs of positive roots such that:

$$\left.\begin{array}{ll} \text{(a)} & N_{u,v} = -N_{v,u}; \\ \text{(b)} & N_{u,v} = 0 \text{ if } u+v \text{ is not a root and } N_{u,v} = \pm 1 \text{ otherwise;} \\ \text{(c)} & N_{u,v}N_{u+v,w} + N_{v,w}N_{v+w,u} + N_{w,u}N_{w+u,v} = 0, \text{ for all } u,v,w \in R^+ \end{array}\right\}. \qquad (2.1)$$

*See appendix

We first record some properties of R which we require:

Lemma 2.1 *Let u, v, w be distinct positive roots with $u + v$ a root and $w \neq u + v$:*

(i) If $\langle u + v, w\rangle > 0$ then either $\langle u, w\rangle = 1$ and $\langle v, w\rangle = 0$, or $\langle u, w\rangle = 0$ and $\langle v, w\rangle = 1$.

(ii) If $u + v + w$ is a root then exactly two of $u + v, v + w, w + u$ are roots.

This is a consequence of the assumptions on R, namely, if a, b are distinct roots and $a + b \neq 0$ then the Cartan integer $\langle a, b\rangle$ is 0, 1 or -1.

The following definition is more or less dictated by (2.1) and the Jacobi identity.

Definition 2.2 Fix an ordering on S. Let u, v be positive roots such that $\sigma = u+v$ is a root. Let α be the first simple root such that $(\sigma, \alpha) > 0$. Set $N_{\alpha,\sigma-\alpha} = 1,\ N_{\sigma-\alpha,\alpha} = -1$.

If u, v are distinct from α define $N_{u,v}$ and $N_{v,u}$, by induction on height of $(u + v)$, by the identities:

$$N_{u-\alpha,\alpha} N_{u,v} + N_{v,u-\alpha} N_{\sigma-\alpha,\alpha} = 0, \qquad (*)$$

$N_{v,u} = -N_{u,v}$, in case $(u, \alpha) = 1,\ (v, \alpha) = 0$, and

$$N_{u,v-\alpha} N_{\sigma-\alpha,\alpha} + N_{v-\alpha,\alpha} N_{v,u} = 0, \qquad (**)$$

$N_{u,v} = -N_{v,u}$, in case $(u, \alpha) = 0, (v, \alpha) = 1$. If $u + v$ is not a root, set $N_{u,v} = 0$.

Proposition 2.3 *Let u, v, w be positive roots and let N be as in (2.2). Then*

$$N_{u,v} N_{u+v,w} + N_{v,w} N_{v+w,u} + N_{w,u} N_{w+u,v} = 0. \qquad (*)$$

Proof. If $\sigma = u+v+w$ is not a root then there is nothing to prove. So let σ be a root. We may assume that $u + v, v + w$ are roots but $u + w$ is not a root (2.2): call such a triple (u, v, w) an A_3-triple. Denote the left-hand side of $(*)$ by $J(u, v, w)$. Let α be the first simple root such that $\langle \sigma, \alpha\rangle > 0$. If α is one of u, v or w then $(*)$ follows from the definition of N. So assume α is distinct from u, v and w. Then, by (2.2), we have $\langle u+v, \alpha\rangle = 1$ and $\langle w, \alpha\rangle = 0$ or $\langle u+v, \alpha\rangle = 0$ and $\langle w, \alpha\rangle = 1$. Now we express, using (2.3), $J(u, v, w)$ as a linear combination of $J(u', v', w')$ with height of $(u'+v'+w')$ less than height of $(u+v+w)$ and apply induction. The details are as follows:

(A) Suppose $\langle u+v, \alpha\rangle = 1$ (and $\langle w, \alpha\rangle = 0$). Then $\langle u, \alpha\rangle = 1$ and $\langle v, \alpha\rangle = 0$ or $\langle v, \alpha\rangle = 1$ and $\langle u, \alpha\rangle = 0$. In the first case $J(u, v, w)$ is, by definition of N,

$$N_{u,v}N_{u+v-\alpha,w}(N_{\alpha,u+v-\alpha})^{-1} + N_{v,w}N_{v+w,u-\alpha}(N_{\alpha,u-\alpha})^{-1}.$$

Hence

$$(N_{\alpha,u-\alpha})J(u, v, w) \equiv J(u-\alpha, v, w) \quad \text{(using (2.3 (*)).}$$

In case $(u, \alpha) = 0, (v, \alpha) = 1, (w, \alpha) = 0$ we have

$$J(u, v, w) \equiv J(u, v-\alpha, w).$$

(B) Suppose $\langle u+v, \alpha\rangle = 0$ and $\langle w, \alpha\rangle = 1$. Then $\langle u, \alpha\rangle = \langle v, \alpha\rangle = 0$ or $\langle u, \alpha\rangle = 1$, $\langle v, \alpha\rangle = -1$: $\langle v, \alpha\rangle$ cannot be 1, else $\langle v+w, \alpha\rangle$ would be 2, i.e., $v+w$ would be a simple root.

The first case follows by symmetry from (A). So suppose $\langle u, \alpha\rangle = 1, \langle v, \alpha\rangle = -1$. Then $(u-\alpha, w, v)$ and $(w-\alpha, u, v)$ are A_3-triples. In this case

$$J(u, v, w) = N_{u,v}N_{u+v,w-\alpha}(N_{\alpha,w-\alpha})^{-1} + N_{v,w}N_{v+w,u-\alpha}(N_{\alpha,u-\alpha})^{-1}.$$

Now

$$\begin{aligned} 0 &= J(u-\alpha, w, v) = N_{u-\alpha,w}N_{u+w-\alpha,v} + N_{w,v}N_{w+v,u-\alpha} \\ 0 &= J(w-\alpha, u, v) = N_{w-\alpha,u}N_{w-\alpha+u,v} + N_{u,v}N_{u+v,w-\alpha}. \end{aligned}$$

Dividing the second equation by $N_{\alpha,w-\alpha}$, the first by $N_{\alpha,u-\alpha}$, setting $c = N_{u+w-\alpha,v}$ and subtracting we see that

$$0 = [(N_{w-\alpha,u}(N_{\alpha,w-\alpha})^{-1} - N_{u-\alpha,w}(N_{\alpha,u-\alpha})^{-1}]c + J(u, v, w),$$

i.e.,

$$0 = J(\alpha, u-\alpha, w-\alpha)c + N_{\alpha,u-\alpha}N_{\alpha,w-\alpha}J(u,v,w).$$

Since $J(\alpha, u-\alpha, w-\alpha) = 0$ we see that $J(u,v,w) = 0$. This completes the proof of (2.4).

We now extend the function N of (2.3) to a function $\widetilde{N}$, defined on all pairs of roots u, v such that $(u+v) \neq 0$, and having the properties (2.1) (a, b, c). This extension is again forced upon us by (1.1). ■

Definition 2.4 Let u be a positive root and v a root such that $u+v$ is a root. If v is positive, set $\widetilde{N}_{u,v} = N_{u,v}$ and define $\widetilde{N}_{-u,-v}$ by: $N_{u,v}\widetilde{N}_{-u,-v} = -1$. If v is negative define $\widetilde{N}_{u,v}$ by the equation:

$$\widetilde{N}_{u,v}N_{u+v,-v} + \langle v, u\rangle = 0,$$

in case $u+v$ is positive, and by:

$$\widetilde{N}_{u,v}\widetilde{N}_{u+v,-u} - \langle u, v\rangle = 0,$$

in case $u+v$ is negative.

Set $\widetilde{N}_{v,u} = -\widetilde{N}_{u,v}$. Finally, let $\widetilde{N}_{a,b} = 0$ if $a+b$ is not a root.

Corollary 2.5 *Let $\widetilde{N}$ be as in (2.5). If u, v, w are roots and $R_{u,v,w}$ is of rank 3 then*

$$\widetilde{N}_{u,v}\widetilde{N}_{u+v,w} + \widetilde{N}_{v,w}\widetilde{N}_{v+w,u} + \widetilde{N}_{w,u}\widetilde{N}_{w+u,v} = 0. \qquad (*)$$

Proof. For notational convenience, denote $\widetilde{N}$ by N. It suffices to assume that $\sigma = u+v+w$ is a root. As in (2.2), we may also assume that $u+v, v+w$ are roots but $u+w$ is not a root. Denote the left hand side of $(*)$ by $J(u,v,w)$.

Now $(*)$ is true when u, v, w are all positive or all negative, so we may assume that v is positive. As $N_{a,b} = N_{b,a}$ for all roots a, b we may also assume that $u \in R^+$ and $w \in R^-$. So we have the following possibilities:

(A) $v + w \in R^+$: Here $J(u, v, w) \equiv N_{u,v}N_{\sigma,-w} + N_{v+w,-w} \cdot N_{v+w,u} \cdot$ We have $J(u, v + w, -w) = 0$. Writing this out and multiplying by $N_{u,v+w}N_{v,u}$ we find that the relation so obtained is equivalent to $J(u, v, w)$ being 0.

(B) $v + w \in R^-$ and $u + (v + w) \in R^+$: Here the relation to be checked becomes $N_{u,v}N_{\sigma,-w} + N_{v,-v-w}N_{\sigma,-v-w} = 0$. Now $J(\sigma, -v - w, v) = 0$. We multiply this by $N_{\sigma,-w}N_{\sigma,-v-w}$ to get the desired result.

(C) $v + w \in R^-$, $u + (v + w) \in R^-$: In this case the relation $J(u, v, w) = 0$ is equivalent to

$$N_{u,v}N_{-\sigma,u+v} + N_{v,-v-w}N_{-\sigma,u} = 0,$$

the left hand side of which is $J(-\sigma, u, v)$. This completes the proof of (2.6). ■

3 The Lie Algebra $L_R(A)$

Let A be a commutative ring. Using (2.5), it is now easy to construct a Lie algebra $L_R(A)$ such that every automorphism of R extends to an automorphism of $L_R(A)$. We take $L_R(A)$ to be the free A-module with basis $H_a(a \in S), X_b(b \in R)$. For u, v both positive or negative let $[X_u, X_v] = \widetilde{N}_{u,v}X_{u+v}, \widetilde{N}$ being as in (2.5). If $a \in S$, set $H_a = [X_a, X_{-a}]$, and if $\sigma \in R^+$ and $(\sigma, a) > 0$, set $H_\sigma = H_a + H_{\sigma-a}$, and $[X_\sigma, X_{-\sigma}] = H_\sigma$. Defining, for a simple root a and an arbitrary root b $[H_a, X_b]$ to be $\langle b, a\rangle X_a$, requiring this operation to be bilinear and anti-symmetric (i.e., $[X, X] = 0$ for all $X \in L_R(A)$) the reader will find that $L_R(A)$ is now a Lie algebra over A with the stated properties. Clearly, $L_R(A) \cong L_R(Z) \bigotimes_Z A$. Moreover, ad $X_a^3 = 0 \quad (a \in R)$ and $\frac{1}{2}$ ad X_a^2 maps $L_R(Z)$ into itself. These remarks, which are trivial to check, will play an role in the following section.

4 The Functor $G_R(A)$

Let R be an irreducible root system of rank $\geqq 2$, A a commutative ring with unity and A^* the group of units of A. Let G be a group with generators $x_a(u) \quad (a \in R, u \in A)$

which satisfy the following relations:

(R1) $x_a(u+v) = x_a(u)x_a(v) \qquad (u, v \in A, a \in R)$.

(R2) If a, b are linearly independent roots then the commutator

$$(x_a(u), x_b(v)) = \prod_{\substack{ia+jb\in R\\ i,j>0}} x_{ia+jb}(N_{a,b,i,j}u^i v^j),$$

where $N_{a,b,i,j}$ are elements of A and the product on the right hand side is taken in some ordering of the roots $ia + jb \ (i, j > 0)$.

(R3) If J is an integrally closed irreducible subsystem of R of rank at most 3, J^+ a positive system of roots in J and an ordering of the roots in J^+ has been fixed, then every element x of the group generated by $x_r(u)(r \in J^+, u \in A)$ has a unique expression

$$x = \prod_{r\in J^+} x_r(u_r),$$

the product on the right hand side being taken in the chosen ordering of roots in J^+. [In case R has no multiple bonds we need only assume that $\mathrm{rank}(J) \leqq 2$].

(R4) If a, b are independent roots and $u \in A^*$ then

$$w_a(u)U_b w_a(u)^{-1} = U_{w_a(b)},$$

where $w_a(u) = x_a(u)x_{-a}(-u^{-1})x_a(u)$, w_a is the reflection along the root a and $U_r \ (r \in R)$ is the group generated by $x_r(u)(u \in A)$.

It is shown in [1] that every group with the above properties is homomorphic image of a single group $G_R(A)$, which is determined up to isomorphism by the system R and the ring A: in particular, every automorphism of R extends to an automorphism of $G_R(A)$ (see remarks following statement of the proposition in [1]*).

*For the case of G_2, see [9, p. 295]

To prove the existence of $G_R(A)$ we first assume that R has no multiple bonds. Let $L_R(A)$ be the Lie algebra as defined in (2.7). Recall that the Steinberg group $\mathrm{St}_R(A)$ is the group with generators $x'_a(u) \quad (a \in R, u \in A)$ subject to the relations

(A) $x'_a(u+u') = x'_a(u)x'_a(u') \quad (u, u \in A, a \in R)$

(B) $(x'_a(u), x'_b(v) = x'_{a+b}(N'_{ab}uv)$, if $u+v \in R$

$\qquad = 1 \qquad\qquad$, if $u+v \notin R$.

Here the N'_{ab} are as in Proposition (1.1).

This group has a representation in $\mathrm{Aut}(L_R(A))$, namely, map $x'_a(u)$ into the formal exponential

$$x_a(u) = 1 + (\mathrm{ad}\ X_a) \otimes u + \frac{\mathrm{ad}(X_a^2)}{2!} \otimes u^2.$$

Here x_a is a basis element of $L_R(A)$ as given in (2.7), and the formal exponential has only two terms because R has no multiple bonds.

Straightforward calculations show that the group $G_{\mathrm{ad},R}(A)$ generated by $x_a(u)(a \in R, u \in A)$ satisfies (R1), (R2) and (R4). In fact $w_a(u)x_b(v)w_a(u)^{-1} = x_{a+b}(N'_{a,b}uv)$ if $a+b$ is a root. To see that (R3) holds we need an auxiliary lemma.

Let $U_r(r \in R)$ be the group generated by $x_r(u)$ $(u \in A)$, let R^+ be a positive system of roots and let $a_1, \ldots, a_N$ be all the elements of R^+ listed so that $ht(a_i) \leqq ht(a_j)$ if $i \leqq j$. Let U^+ be the group generated by the subgroups $U_r(r \in R^+)$.

Lemma 4.1 [2, p. 39]. *Every element x of U^+ has a unique expression*

$$x = \prod_{i=1,\ldots,N} x_{a_i}(u_i).$$

Proof. The commutator formula (R2) implies that x has an expression of the above form. Let S be the simple system of roots which corresponds to R^+ and let $L_R(A)$ be the Lie algebra s defined in (2.7) with $H_a(a \in S, X_b(b \in R)$ as a basis. Let U^+ and U^- be the subalgebras generated by $X_r(r \in R^+)$ and $X'_r(r' \in R^-)$, respectively.

Now if u, v are positive roots and $ht(u) > ht(v)$ then either $u - v$ is not a root, or else it is a positive root; and if $ht(u) = ht(v)$ then $u - v$ is not a root. Moreover, if u and v are distinct then $x_u(t)X_{-v} = X_{-v} + tN_{u,-v}X_{u-v}$. Therefore if $x = \prod_{i=1,\ldots,N} x_{a_i}(u_i)$ then

$$\begin{aligned} x(X_{-a_1}) &\equiv x_{a_1}(u_1)(X_{a_1})(\text{mod } U^+) \\ &\equiv X_{-a_1} + u_1[X_{x_1}, X_{-a_1}](\text{mod } U^+) \\ &\equiv u_1 H_{a_1}(\text{mod}(U^+ + U^-)). \end{aligned}$$

As $L_R(A) = H + U^+ + U^-$, we see that $u_1 H_{a_1}$ is uniquely determined by x. As rank $R \geqq 2$, there exists some root b with $\langle b, a \rangle = 1$. This means that u_1 is uniquely determined by x. Therefore if $x = \prod x_{a_i}(u_i')$, then $u_1 = u_1'$. Canceling $x_{a_1}(u_1)$ we continue and conclude that $u_i = u_i'$ for all i.

From Proposition (1.1) it is clear that if σ is an automorphism of R then it extends to an automorphism $\widetilde{\sigma}$ of $L_R(A)$ as well as of $\mathrm{St}_R(A)$ and we have:

$$\widetilde{\sigma} X_a = c_a X_{\sigma(a)}, \widetilde{\sigma}(x_a'(u)) = x_{\sigma(a)}'(c_a u),\ c_a = \pm 1 \text{ and } c_a c_{-a} = 1$$

(because $H_a = [X_a, X_{-a}]$ and $\widetilde{\sigma}(H_a) = H_{\sigma(a)}$).

Moreover $\widetilde{\sigma}(\text{ad } X_a)(\widetilde{\sigma})^{-1} = \text{ad}(\widetilde{\sigma} X_a)$ and this means that $\widetilde{\sigma}$ normalizes $G_{\text{ad},R}(A)$. Suppose $\widetilde{\sigma}$ fixes a positive system of roots R^+ in R. It follows by using (1.1) and [6, p. 172–175] or [7, p. 875–877] that the fixed points of $\widetilde{\sigma}$ in $G_{\text{ad},R}(A)$ contain a group which satisfies the relations (R1), ..., (R4), with R replaced by the root system obtained by twisting R according to σ.* This proves the existence of the groups in question.

Finally, let K be the normal subgroup of $\mathrm{St}_R(A)$ generated by

$$w_a'(t)x_a'(u)w_a'(t)^{-1}x_{-a}'(-t^{-2}u)$$

*See appendix, pp. 17–19.

and

$$h_a(tt')h_a(t')^{-1}h_a(t)^{-1} \quad (a \in R, t, t' \in A^*, u \in A),$$

where

$$w'_a(t) = x'_a(t)x'_{-a}(-t^{-1})x'_a(t) \text{ and } h_a(t) = w'_a(t)w'_a(-1):$$

note that $\widetilde{\sigma}(K) = K$.

It is shown in [6, p. 66] that when A is a field the group $\mathrm{St}_R(A)/K$ is isomorphic to the universal Chevalley group corresponding to the system R, and hence $(\mathrm{St}_R(A)/K)\widetilde{\sigma}$ is isomorphic to the universal Chevalley group corresponding to the system obtained by twisting R according to σ [cf. 6, p. 172].

Therefore the subgroups $(\mathrm{St}_R(A)/K)\widetilde{\sigma} - \sigma$ being any automorphism of $R-$are appropriate generalizations of Chevalley groups. For example, in this way, one obtains the maximal compact subgroups of some real Lie groups. In this connection, see also [2, p. 65]. ■

Remark 4.2 For some applications it is useful to replace the relations (R3) of § 3 by

(a) If J is an integrally closed irreducible subsystem of R of rank at most 2, J^+ a positive system of roots in J and an ordering of the roots J^+ has been fixed, then every element x of the group generated by $x_r(u)$ $(r \in J^+, u \in A)$ has a unique expression

$$x = \prod_{r \in J^+} x_r(u_r).$$

the product on the right hand side being taken in the chosen ordering of roots in J^+.

(b) If a, b, c are positive roots such that $a+b, b+c$ and $a+c$ are not roots then every element x of the group generated by $x_r(u)(r = a, b, c, u \in A)$ has a unique expression

$$x = x_a(u)x_b(v)x_c(w).$$

[In case R has no multiple bonds we need only assume (R3) (a)].

5 Appendix

Let L, R, S, A and $X_r (r \in R)$ be as in § 1. Assume that $[X_a, X_{-a}]$ $(a \in S)$ and $X_r (r \in R)$ form a basis of L over A. In view of (1.1) we may, after a suitable normalization of the generators, also assume that for all roots r and s

$$[[X_r, X_{-r}], X_s] = \langle s, r\rangle X_s. \qquad (**)$$

It then follows (cf. 1.1)) that if S' is any simple system of roots in R and σ an automorphism of R, then the mapping $X_a \to X_{\sigma(a)}$ $(a \in S' \cup -S')$ extends to an automorphism of L, and of the group $G_R(A)$ of § 3, and this extension is unique.

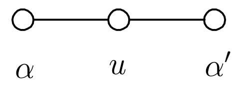
From now on, we assume that the generators of L have been chosen so as to satisfy $(*)$. Furthermore, that σ is an automorphism of R which maps S into itself (so σ is of order 2 or 3). The unique extension of the mapping $X_a \to X_{\sigma(a)} (a \in S \cup -S)$ will be denoted by $\widetilde{\sigma}$.

5.1

$\widetilde{\sigma}(X_r) = X_r$ whenever $\sigma(r) = r$, unless R is of type A_{2m}, in which case $\widetilde{\sigma}(X_r) = -X_r$ whenever $\sigma(r) = r$.

Proof. First, suppose that σ is of order 2 and R is not of type A_{2m}. Let r be a positive root fixed by σ. If r is simple then $\widetilde{\sigma}(X_r) = X_r$. So let $r = \alpha + \beta (\alpha \in S, \beta \in R^+)$. Denoting images under σ by primes, we have $r = r' = \alpha' + \beta'$, so $R_{\alpha\beta\alpha'}$ is an irreducible root system, with $R_{\alpha\beta\alpha'} \cap R^+$ as a positive system of roots, and α, α' remain simple roots of this subsystem.

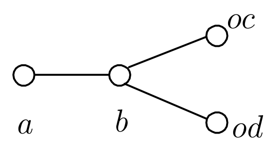
If $R_{\alpha\beta\alpha'}$ is of type A_2 then we must have $\alpha = \alpha'$, otherwise $\alpha + \alpha'$ would be root, and since α, α' are both simple, this is only possible if R is of type A_{2m}. Hence $\alpha = \alpha', \beta = \beta'$ and $\widetilde{\sigma}[X_\alpha, X_\beta] = [X_\alpha, X_\beta]$ (by induction on heights). If $R_{\alpha\beta\alpha'}$ is of type A_3 (so $\alpha \neq \alpha'$) then there is a root u of this subsystem such that



is its Dynkin diagram, and such that $r = \alpha + u + \alpha'$, As $u = u'$ we have $\widetilde{\sigma}(X_u) = X_u$, by induction on heights. Moreover $\widetilde{\sigma}[X_\alpha, X_u; X_{\alpha'}] = [X_{\alpha'} X_u; X_\alpha] = [X_\alpha, X_u; X_{\alpha'}]$ (by Jacobi), hence $\widetilde{\sigma}(X_r) = X_r$.

If R is of type A_{2m} and σ of order 2, then σ does not fix any simple root. There is a unique simple root α such that $\alpha + \alpha'$ is a root and so $\widetilde{\sigma}[X_\alpha X_{\alpha'}] = -[X_\alpha, X_{\alpha'}]$. An argument similar to the one just given shows that $\widetilde{\sigma}(X_r) = -X_r$ whenever $\sigma(r) = r$.

There remains the case: R is of type D_4 and $\sigma^3 = 1, \sigma \neq 1$. Label the Dynkin diagram of D_4 as



The non-simple positive roots are $a+b, b+c, b+d, a+(b+c), a+(b+d), c+(b+d), a+(b+c+d), b+(a+b+c+d)$. Fixing the order $a < b < c < d$ on S and using (1.1) (B), we may assume that $N_{a,b} = N_{b,c} = N_{b,d} = 1$, $N_{a,b+c} = N_{a,b+d} = 1$, $N_{c,b+d} = 1$, $N_{a,b+c+d} = N_{b,a+b+c+d} = 1$; moreover if u, v are roots such that $N_{u,v} \neq 0$ then $N_{u,v} N_{-u,-v} = -1$. The non-simple positive roots left fixed by σ are $a+b+c+d$ and $a+2b+c+d$.

Now

$$\sigma[X_a, [X_c, [X_b, X_d]]] = N_{d,a+b} N_{b,a} N_{c,a+b+d} X_{a+b+c+d}$$

and

$$[X_a, [X_c, [X_b, X_d]]] = N_{a,c+b+d} N_{c,b+d} N_{b,d} X_{a+b+c+d}.$$

Using the above data, one can check that the right hand sides of the last two equations are equal. The verification for the root $b + (a+b+c+d)$, which is similar, completes the proof of (4.1).

The following lemma is well known: a version occurs in [2, pp. 19–20], and 4.2 (i) can also be extracted from [7, p. 877, line 14]. We need it in the following form.

5.2

Let R be not of type A_{2m} and let σ be of order 2. Denote images under σ by primes:

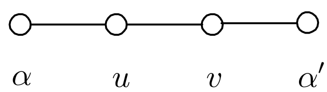
(i) For all roots r, we have $r + r'$ is not a root.

(ii) If $r = r', s \neq s', r$ and s are non-orthogonal, then $R_{rss'}$ is irreducible of rank 3 and σ acts as a non-trivial permutation on $R^+ \cap R_{rss'}$.

(iii) If $r \neq r'$, $s \neq s'$ are roots such that $r+\xi s \in R(\xi = \pm 1)$ then either $r+\xi s = r'+\xi s'$, in which case $R_{rsr's'}$ is irreducible of rank 3 and σ acts non-trivially or $R_{rsr's'} \cap R^+$, or else $\langle r, s' \rangle = \langle r', s \rangle = 0$.

■

Proof. We may assure that r is a positive root. As σ preserves heights, it is clear that $r - r'$ is not a root. Suppose $r + r'$ is a root. As R is not of type A_{2m}, r cannot be simple, so $r = \alpha + \beta$ $(\alpha \in S, \beta \in R^+)$. As $\alpha + \beta, \alpha' + \beta'$ and $r + r'$ are roots, we see that $R_{\alpha\beta\alpha'\beta'}$ is an irreducible root system of rank 4 at most hence is of type A_2, A_3, A_4 or D_4, and σ acts as a non-trivial permutation on $R^+ \cap R_{\alpha\beta\alpha'\beta'}$. One checks that if τ is an involutory automorphism of a system of type A_3 or D_4, fixing a positive system of roots, then there is no root r such that $(r + \tau r)$ is a root. Hence $R_{\alpha\beta\alpha'\beta'}$ must be of type A_2 or A_4, with α, α' occuring as distinct simple roots in $R_{\alpha\beta\alpha'\beta'} \cap R^+$. As R is not of type A_{2m} we see that $\alpha + \alpha'$ is not a root, hence the Dynkin diagram of $R_{\alpha\beta\alpha'\beta'} \cap R^+$ must be

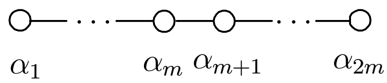


and r is then $\alpha + u$ or $v + \alpha'$. As σ must permute α, α' and u, v, respectively, we see that u is a root of lower height than r such that $(u+u')$ is a root. By induction on heights, it follows that $r+r'$ is not a root.

Let $r = r', s \neq s'$ be roots such that $r+\xi s$ is a root ($\xi = \pm 1$). Now $R_{rss'}$ is irreducible of rank 3 at most; its rank by (i) cannot be 2 as $R_{rss'} \cap R^+$ admits a permutation of order 2. This proves (ii).

Finally, let r and s be non-orthogonal roots such that $r \neq r', s \neq s'$. Let $r+\xi s$ be a root. As $r \pm r'$ and $s \pm s'$ are not roots, we see that $\langle r+\xi s, r'+\xi s'\rangle = 2\xi\langle r, s'\rangle$. Hence either $r+\xi s = r'+\xi s'$ or else $\langle r, s'\rangle = \langle r', s\rangle = 0$. This proves (iii).

Remark 5.1 The proof of (i) also shows that R is of type A_{2m} and



is its Dynkin diagram then the positive roots of R such that $r = r'$ are

$$\{\alpha_m+\alpha_{m+1}, \alpha_{m-1}+\alpha_m+\alpha_{m+1} + \alpha_{m+2}, \ldots, \alpha_1 + \\ + \alpha_m+\alpha_{m+1}+\cdots+\alpha_{2m}\}$$

Proposition 5.2 [7, p. 875–877]. *Let V denote the real span of R and fix a positive definite inner product on R relative to which elements of the Weyl group and σ become isometries. For $v \in V$, let $\widetilde{v}$ denote the orthogonal projection of V on V_σ, where $V_\sigma = \{v \in V | \sigma(v) = v\}$. Then $\widetilde{R} = \{\widetilde{r} : r \in R\}$ is an irreducible reduced root system in V_σ and the distinct elements of $\{\widetilde{\alpha} : \alpha \in S\}$ form a fundamental system of roots of $\widetilde{R}$, unless R is of type A_{2m} in which case it is of type BC_m.*

The reader is referred to [6, p. 172] or [7, pp. 875–877] for details. In the case which interests us here, namely R is not of type A_{2m}, this also follows, as we show presently, from (5.2), when $\sigma^2 = 1$, and by explicit computations as in (5.1) when $\sigma^3 = 1$. Let $\sigma^2 = 1 (\sigma \neq 1)$ and $\omega_{\widetilde{a}}$ denote the reflection in the hyplane orthogonal to $\widetilde{a}$. In view of (5.2), to see that $\omega_{\widetilde{a}}(\widetilde{R}) = \widetilde{R}$, we have only to verify this when R is of type A_3 or $A_2 \times A_2$ with σ interchanging the two components in the latter case: this verification is easy, using (5.2) (ii) and (iii), and will also show that $\langle \widetilde{a}, \widetilde{b} \rangle \in Z$. Therefore $\widetilde{R}$ is a root system in the sense of [4, p. V-3] and every element of $\widetilde{R}$ is an integral linear combination of elements of $\widetilde{S}$. Defining height with respect to $\widetilde{S}$ and using the integrality condition $\langle \widetilde{a}, \widetilde{b} \rangle \in Z$ we see that if r is a positive root and $2\widetilde{r} \in \widetilde{R}$ the $2\widetilde{a}$ $(a \in S)$ is also in $\widetilde{R}$, say $2\widetilde{a} = \widetilde{s}(s \in R^+)$. So s must be a linear combination of the transforms of a under σ. The condition $2\widetilde{a} = \widetilde{s}$ implies that $R_{aa'}$ is of type A_2 and $s = a + a'$. As a, a' are both simple, this is only possible when R is of type A_{2m}.

Now $\sigma \omega_{\widetilde{a}} \sigma^{-1} = \omega_{\widetilde{a}}(a \in R)$ so [2, p. 19, Lemma 1] or [5, p. 234, 11.1.4] implies that if $\widetilde{a}$ and $\widetilde{b}$ are linearly independent roots such that a is orthogonal to all transforms of b under σ then $\widetilde{R}_{\widetilde{a},\widetilde{b}}$ the integral closure of $\widetilde{a}, \widetilde{b}$ in $\widetilde{R}$, is of type $A_1 \times A_1$.

Let U^+ and U^- be the subalgebras of L generated by $X_r(r \in R^+)$ and $X_s(s \in R^-)$, respectively. Let H be the subalgebra generated by $H_a(a \in S)$. Clearly $L_{\widetilde{\sigma}} = U^+_{\widetilde{\sigma}} \oplus H_{\widetilde{\sigma}} \oplus U^-_{\widetilde{\sigma}}$. For each root $\alpha \in \widetilde{R}$ choose a root r such that $\alpha = \widetilde{r}$ and define X_α and H_α to be the sums of the distinct transforms of X_r and H_r, respectively, under $\widetilde{\sigma}$. Now using (5.2), and (5.1) in case σ is of order 3, the reader can check that $[X_\alpha, X_{-\alpha}] = H_\alpha$

$$[H_\alpha, X_\beta] = \langle \beta, \alpha \rangle X_\beta \text{ and } [X_\alpha, X_\beta] = \begin{cases} 0 & \text{if } \alpha + \beta \notin \widetilde{R} \\ N_{\alpha,\beta} X_{\alpha+\beta} & \text{if } \alpha + \beta \in \widetilde{R}, \end{cases}$$

$N_{\alpha,\beta}$ being some constants.

In particular, taking $A = \mathbb{C}$ and using the fact that the Cartan matrix $(\langle \widetilde{r}, \widetilde{s} \rangle)$ is non-singular, where r, s run through a set of representatives of the orbits of S under σ, we see that $L_R(C)_{\widetilde{\sigma}}$ is a semi-simple algebra whose root system is $\widetilde{R}$. This proves (1.2).

Finally, consider the group $G_{\mathrm{ad},R}(A)$ of § 3. The automorphism σ of R extends to an automorphism $\widetilde{\sigma}$ of $G_{\mathrm{ad},R}(A)$. For each root $\alpha \in \widetilde{R}$, choose a root $r \in R$ such that $\alpha = \widetilde{r}$. Define $x_\alpha(a)$ to be product of the distinct transforms of $x_r(a)$ under σ and let

U_α be the group generated by $x_\alpha(a)(a \in A)$. Using (5.2) and, in case σ is of order 3, the normalization of the structure constants of D_4 as given in (5.1), the reader can check that the group generated by $x_\alpha(a)(\alpha \in \widetilde{R},\ a \in A)$ satisfies the relations (R1), (R2) and (R4) of § 3. As the group generated by $U_\alpha(\alpha \in \widetilde{R}^+)$ is a subgroup of the group U_σ^+, the commutator formula and the lemma in § 3 implies that the generators $x_\alpha(a)$ satisfy the relations (R3) also: see [6, § 11, p. 180, Lemma 62] for details. ■

Acknowledgment

I thank Professor Dimitri Leites for suggesting that this paper be made more accessible. I have taken this opportunity to correct several misprints in the original version.

(Dhahran, December 24, 2004)

References

[1] H. Azad, Structure constants of algebraic groups, Journal of Algebra, vol. 75, 1982.

[2] C. Chevalley, Sur certains groupes simples, Tôhoku Math. Journal, 1955.

[3] N. Jacobson, Lie Algebras, Interscience, New York, 1962.

[4] J.P. Serre, Algebres de Lie semi-simples complexes, W.A. Benjamin, New York, 1966.

[5] T.A. Springer, Linear Algebraic Groups, Birkhauser, Boston, 1980.

[6] R. Steinberg, Lectures on Chevalley Grouops, Yale University, Lecture Notes, 1968.

[7] R. Steinberg, Variations on a theme of Chevalley, Pacific Journal of Mathematics, 1959.

[8] J. Tits, Sur les constantes de structure et le theoreme d'existgence des algebres de Lie semi-simples. Publ. Math. I. H.E.S., No. 31, 1966.

[9] M. Demazure, Schemas en Groups, Springer-Verlag, Berlin, 1970