GENERATION OF SOME DISCRETE SUBGROUPS OF SIMPLE ALGEBRAIC GROUPS

EIICHI ABE

(Received March 10, 1965)

1. Let G be a connected semi-simple algebraic group over the field C of complex numbers such that defined over the field Q of rational numbers and of Chevalley type (i.e. whose Lie algebra is anti-compact). Then G has a uniquely determined Z-structure (i.e. the structure of group scheme over the ring Z of rational integers) satisfying a proper condition (cf. C. Chevalley [2]). Denote by G_Z the group consisting of the Z-rational elements of G with respect to the structure. Suppose G is simply connected and simple. Let Σ be the system of roots of G with respect to a Cartan subgroup of G. Then G is isomorphic to the algebraic group generated by the symbols $x(r,t)$ ($r \in \Sigma$, $t \in C$) (as an abstract group) with the following relations (A), (B) and (C) when the rank of G is >1 and (A), (B′) and (C) when the rank of G is $=1$ (cf. R. Steinberg [5]).

(A) $$x(r,t)\,x(r,u) = x(r,t+u) \quad (r \in \Sigma\,;\ t,u \in C),$$

(B) $$(x(r,t), x(s,u)) = \prod_{i,j} x(ir+js, c_{i,j;r,s}\,t^i u^j) \quad (r,s \in \Sigma\,;\ r+s \neq 0),$$

where (x,y) is the commutator $xyx^{-1}y^{-1}$, the product is taken over all pairs (i,j) of positive integers such that $ir+js$ is a root, the pairs being arranged so that the roots $ir+js$ form an increasing sequence with respect to a fixed order in Σ, and where $c_{i,j;r,s}$ are integral constants depending only on Σ. We define $w(r,t) = x(r,t)\,x(-r,-t^{-1})\,x(r,t)$ and $h(r,t) = w(r,t)\,w(r,-1)$ where t is an element of the multiplicative group C^* of C. Then

(B′) $$w(r,t)\,x(r,u)\,w(r,t)^{-1} = x(-r,-t^2u) \quad (r \in \Sigma\,;\ t \in C^*,\ u \in C),$$

(C) $$h(r,t)\,h(r,u) = h(r,tu) \quad (r \in \Sigma\,;\ t,u \in C^*).$$

We shall identify the group with G. Then we see that the group G_Z is the subgroup of G generated by $x(r,t)$ for $r \in \Sigma$ and $t \in Z$ (cf. C. Chevalley [2]). If G is of type A_n or C_n, then $G_Z \cong SL(n+1,Z)$ or $G_Z \cong Sp(2n,Z)$ and it is known that $SL(n+1,Z)$ $(n \geqq 1)$ and $Sp(2n,Z)$ $(n > 3)$ are generated by two elements (cf. P. Stanek [3]). In this note we improve it and prove in 2 the following

THEOREM. *Let G be a connected, simply connected simple algebraic group defined over Q of Chevalley type. If G is of type A_n ($n \geqq 1$) or the rank of G is >3, then G_Z is generated by two elements. For other cases, G_Z is generated by at most three elements.*

Further, we give in 3 an application to the adjoint groups of complex simple Lie algebras.

2. For $r, s \in \Sigma$, define the integer $a(r, s) = p-q$ where q (resp. $-p$) is the maximum (resp. minimum) integer i such that $s+ir$ is a root. Let $\Pi = \{a_1, \cdots, a_n\}$ be the fundamental system of roots with respect to a fixed order of Σ. Denote $a(i,j) = a(a_i, a_j)$ and $a_1, \cdots, a_n$ are so labelled once for all that $a(i,i) = 2$, $a(i, i\pm 1) = -1$ and $a(i,j) = 0$ for all other pairs (i,j) with the following exceptions: $a(n-1, n) = -2$ for type B_n, $a(n, n-1) = -2$ for type C_n, $a(n-1, n) = a(n, n-1) = 0$ and $a(n-2, n) = a(n, n-2) = -1$ for type D_n ($n \geqq 4$), $a(n, n-1) = a(n-1, n) = 0$ and $a(n-1, n-3) = a(n-3, n-1) = -1$ for type E_n ($n=6, 7$ and 8), $a(2,3) = -2$ for type F_4 and $a(1,2) = -3$ for type G_2. The symmetry σ_r with respect to $r \in \Sigma$ is the permutation of Σ defined by $\sigma_r(s) = s - a(r, s)r$. The Weyl group W of Σ is the group generated by all σ_r, $r \in \Sigma$. Denote by σ_i the symmetry with respect to a_i ($1 \leqq i \leqq n$). Then W is generated by σ_i ($1 \leqq i \leqq n$). We shall use the following relations between generators where ε and η are 1 or -1 which are uniquely determined by the roots r and s (cf. R. Steinberg [5], 7.2 and 7.3).

$$w(r, 1)\, w(s, 1)\, w(r, -1) = w(\sigma_r(s), \varepsilon), \tag{1}$$

$$w(r, 1)\, x(s, t)\, w(r, -1) = x(\sigma_r(s), \varepsilon). \tag{2}$$

Suppose G is not of type G_2 and let r, s and $r+s \in \Sigma$, then the possible relations (B) are the following (cf. C. Chevalley [1], p. 36): If r, s generate a system of type A_2, then $r-s$ is not a root and

$$(x(r, t), x(s, u)) = x(r+s, \varepsilon tu). \tag{3}$$

If r, s generate a system of type B_2, when $r-s$ is not a root,

$$(x(r, t), x(s, u)) = x(r+s, \varepsilon tu)\, x(r+2s, \eta tu^2) \text{ or } x(r+s, \varepsilon tu)\, x(2r+s, \eta t^2 u) \tag{4}$$

and when $r-s$ is a root,

$$(5) \qquad (x(r,t), x(s,u)) = x(r+s, \varepsilon 2tu).$$

LEMMA 1. *G_Z is generated by $x(\pm a_i, 1)$ for $1 \leqq i \leqq n$.*

Let H be the subgroup of G_Z generated by $x(\pm a_i, 1)$ $(1 \leqq i \leqq n)$. Then H contains $w(a_i, 1)$ $(1 \leqq i \leqq n)$ by definition. Since W is generated by σ_i $(1 \leqq i \leqq n)$ and for any root r, there exists an element σ of W such that $\sigma(r) = \pm a_i$ for some i, (1) and (2) show that H contains $x(r, 1)$ for all $r \in \Sigma$.

LEMMA 2. (R. Steinberg [4], 2.1) *If W is not of type A_n $(n \geqq 2)$, D_n (n odd) or E_6, then W contains the central reflexion -1 defined by $r \to -r$ $(r \in \Sigma)$ and it is a power of $\sigma = \sigma_1 \sigma_2 \cdots \sigma_n$ (operations from right to left).*

N.B. The order of the operations σ_i of σ is some what different from that of [4], however we have the assertion in the same way.

Now we define $w = w(a_1, 1)\, w(a_2, 1) \cdots w(a_n, 1)$, then we have

PROPOSITION 1. *If G is of type A_n $(n \geqq 1)$, then G_Z is generated by w and $u = x(a_1, 1)$. For other cases, G_Z is generated by w, $x(a_1, 1)$ and $x(a_n, 1)$.*

Let H be the subgroup generated by two or three elements stated in the proposition. By Lemma 1, it is sufficient to show that H contains $x(\pm a_i, 1)$ for $1 \leqq i \leqq n$. First, we notice that if $a_1, \cdots, a_k$ $(k \leqq n)$ form a system of type A_k and a_j is orthogonal to a_i $(1 \leqq i \leqq k-1)$ for all $j > k$, then

$$(6) \qquad w^i x(a_1, 1)\, w^{-i} = x(a_{i+1}, \varepsilon) \quad (1 \leqq i \leqq k-1).$$

Case of type A_n $(n \geqq 1)$: (6) holds for $1 \leqq i \leqq n-1$. Therefore $x(a_i, 1) \in H$ for $1 \leqq i \leqq n$. From relations $w^n x(a_1, 1)\, w^{-n} = x(-(a_1 + \cdots a_n), \varepsilon)$ and $x(a_i, 1)\, x(-(a_i + \cdots + a_n), 1)\, x(a_i, -1) = x(-(a_{i+1} + \cdots + a_n), \varepsilon)$ $(1 \leqq i \leqq n-1)$, we have $x(-a_n, 1) \in H$. Then $w^i x(-a_n, 1)\, w^{-i} = x(-a_{i-1}, \varepsilon)$ $(2 \leqq i \leqq n)$ shows that $x(-a_i, 1) \in H$ for $1 \leqq i \leqq n$. Case of type B_n or C_n $(n \geqq 2)$: (6) holds for $1 \leqq i \leqq n-2$. Therefore, from Lemma 2, we have $x(\pm a_i, 1) \in H$ for $1 \leqq i \leqq n-1$ and also we have $x(\pm a_n, 1) \in H$. *Case of type D_n ($n \geqq 4$, even)*: (6) holds for $1 \leqq i \leqq n-3$. Therefore, from Lemma 2, we have $x(\pm a_i, 1) \in H$ for $1 \leqq i \leqq n-2$. Since $w^{n-2} x(a_n, 1)\, w^{-n+2} = x(-(a_{n-2} + a_{n-1}), \varepsilon)$, the relation (3) for $r = a_{n-1}$ and $s = -(a_{n-2} + a_{n-1})$ shows that $x(-a_{n-1}, 1) \in H$. Thus $x(\pm a_{n-1}, 1)$ and $x(\pm a_n, 1)$ are also contained in H. *Case of type D_n ($n > 4$,* odd): (6) holds for $1 \leqq i \leqq n-3$. Therefore from $w^{n-1}x(a_1, 1)w^{-n+1} = x(-a_1, \varepsilon)$, we have $x(\pm a_i, 1) \in H$ for $1 \leqq i \leqq n-2$. From the relations $w^{n-2}x(a_n, 1) w^{-n+2} = x(-(a_{n-2}+a_n), \varepsilon)$, $w^{n-2}x(a_1, 1)w^{-n+2} = x(-(a_1+\cdots+a_n), \varepsilon)$ and (3), we see that $x(\pm a_n, 1)$ and $x(\pm a_{n-1}, 1)$ are contained in H. *Case of type E_6*: (6) holds for $i = 1, 2$. Therefore $x(a_i, 1) \in H$ for $i = 1, 2$ and 3. $wx(a_1, 1)w^{-1} = x(-(a_1+a_2+a_3+a_6), \varepsilon)$ and (3) show that $x(\pm a_i, 1) \in H$ for $i = 1, 2, 3$ and 6. From $w^2x(\pm a_6, 1)w^{-2} = x(\mp(a_2+a_3+a_4), \varepsilon)$, $w^5x(\pm a_6, 1)w^{-5} = x(\mp(a_3+a_4+a_5), \varepsilon)$, we have $x(\pm a_4, 1)$ and $x(\pm a_5, 1)$ are contained in H. Case of type E_n $(n=7, 8)$: (6) holds for $1 \leqq i \leqq n-4$. Therefore, from Lemma 2, we have $x(\pm a_i, 1) \in H$ for $1 \leqq i \leqq n-3$. Since $w^{n-3}x(a_1, 1)w^{-n+3} = x(a_1+\cdots+a_{n-2}+a_n, \varepsilon)$ and $w^{n-2}x(a_1, 1)w^{-n+2} = x(a_2+\cdots+a_{n-1}, \varepsilon)$, using (3), we have $x(\pm a_{n-2}, 1)$ and $x(\pm a_{n-1}, 1)$ are contained in H. *Case of type F_4*: From $wx(a_1\, 1)w^{-1} = x(a_2, \varepsilon)$, $wx(a_4, 1)w^{-1} = x(-(a_1+\cdots+a_4), \varepsilon)$ and Lemma 2, we have $x(\pm a_i, 1) \in H$ for $1 \leqq i \leqq 4$. Case of type G_2: From Lemma 2, we have $x(\pm a_i, 1) \in H$ for $i = 1, 2$.

PROPOSITION 2. *If G is not of type A_n and the rank of G is >3, then G_Z is generated by $w = w(a_1, 1)\cdots w(a_n, 1)$ and $u = x(a_1, 1)x(-a_n, 1)$.*

Denote by H the subgroup of G_Z generated by w and u. It is sufficient to show that $x(a_1, 1)$ and $x(a_n, 1)$ are contained in H. If $\sigma^k = -1$ (cf. Lemma 2), denote by $x^* = w^kxw^{-k}$ for $x \in G_Z$. *Case of type B_n $(n > 3)$*: We have $v_1 = wuw^{-1} = x(a_2, \varepsilon)x(a_1+\cdots+a_n, \eta)$, $v_2 = w^2uw^{-2} = x(a_3, \varepsilon)x(a_2+\cdots+a_n, \eta)$ and $v_3 = (u, v_1) = x(a_1+a_2, \varepsilon)x(a_1+\cdots+a_{n-1}, 2\eta)$, $v_4 = (v_2, v_3) = x(a_1+a_2+a_3, \varepsilon)$. Since, by Lemma 2, v_2^* and $u^* \in H$, we have $((v_2, v_3), v_2^*) = x(a_1+a_2, \varepsilon)$ and $(x(a_1+a_2, 1), u^*) = x(a_2, \varepsilon)$ are contained in H. Therefore, from (6), $x(a_1, 1) \in H$ and also we have $x(a_n, 1) \in H$. Case of type C_n $(n > 3)$: We have $v_1 = wuw^{-1} = x(a_2, \varepsilon)x(2a_1+\cdots+2a_{n-1}+a_n, \eta)$, $(u, v_1) = x(a_1+a_2, \varepsilon)$. Since, by Lemma 2, $u^* \in H$, $(v_1, u^*) = x(a_2, \varepsilon) \in H$. From (6), $x(a_1, 1) \in H$ and also we have $x(a_n, 1) \in H$. Case of type D_n $(n \geqq 4)$: We have $v_1 = wuw^{-1} = x(a_2, \varepsilon) x(a_1+\cdots+a_{n-2}+a_n, \eta)$, $v_2 = w^2uw^{-2} = x(a_3, \varepsilon)x(a_2+\cdots+a_{n-2}+a_{n-1}, \eta)$ and $v_3 = (u, v_2) = x(a_1+\cdots+a_{n-1}, \varepsilon)$. If n is odd, $w^{n-2}v_3w^{-n+2} = x(a_n, \varepsilon)$ and $v_4 = (v_3, x(a_n, 1)) = x(a_1+\cdots+a_n, \varepsilon)$. If n is even, $w^{n-2}v_3w^{-n+2} = x(a_{n-1}, \varepsilon)$ and $v_4 = (v_1, x(a_{n-1}, 1)) = x(a_1+\cdots+a_n, \varepsilon)$. Therefore $wv_4w^{-1} = x(-a_1, 1)$ and we have $w^{n-1}x(-a_1, 1)w^{-n+1} = x(a_1, \varepsilon)$ is contained in H. *Case of type E_n $(n = 6, 7$ and $8)$*: We have $v_1 = wuw^{-1} = x(a_2, \varepsilon)x(a_1+\cdots+a_{n-3}+a_n, \eta)$, $v_2 = w^2uw^{-2} = x(a_3, \varepsilon)x(a_2+\cdots+a_{n-2}, \eta)$, $v_3 = (u, v_1) = x(a_1+a_2, \varepsilon)x(a_1+\cdots+a_{n-3}, \eta)$ and $v_4 = (v_2, v_3) = x(a_1+a_2+a_3, \varepsilon)$. If $n = 6$, $v_5 = w^7uw^{-7} = x(a_5, \varepsilon) x(-(a_1+a_2+a_3+a_6), \eta)$, $(v_4, v_5) = x(-a_6, \varepsilon)$. Therefore $x(a_1, 1)$ and $x(a_6, 1) \in H$. If $n = 7, 8$, since $u^*, v_1^* \in H$, $(v_4, u^*) = x(a_2+a_3, \varepsilon)$ and $(x(a_2+a_3, 1), v_1^*) = x(a_3, \varepsilon) \in H$. Therefore from (6), we have $x(a_1, 1) \in H$ and also $x(a_n, 1) \in H$. *Case* *of type* F_4: We have $v_1 = wuw^{-1} = x(a_2, \varepsilon) x(-(a_1 + \cdots + a_4), \eta)$, $v_2 = (u, v_1) = x(a_1 + a_2, \varepsilon)$. Since $v_2^* \in H$, $(u, v_2^*) = x(-a_2, \varepsilon) \in H$. Thus we have $x(a_1, 1)$, $x(a_4, 1) \in H$.

From Propositions 1 and 2, we have the theorem. As a special case of the theorem, we have

COROLLARY 1. (cf. P. Stanek [3]) $SL(n+1, Z)$ $(n \geqq 1)$ *and* $Sp(2n, Z)$ $(n > 3)$ *are generated by two elements.*

For $G = SL(n+1, C)$ $(n \geqq 1)$, let $\Sigma = \{\lambda_i - \lambda_j,\ i \neq j,\ 1 \leqq i,\ j \leqq n+1\}$ be the root system of type A_n. Then the set of matrices $x(\lambda_i - \lambda_j, t) = I + tE_{ij}$ $(\lambda_i - \lambda_j \in \Sigma,\ t \in C)$ where E_{ij} is the $(n+1, n+1)$ matrix whose (i,j) component is 1 and all other components are 0, is a system of generators of G which satisfy (A), (B) (or (B′)) and (C). We have $G_Z = SL(n+1, Z)$ and also our assertion. For $G = Sp(2n, C)$ $(n > 3)$, let $\Sigma = \{\lambda_i \pm \lambda_j,\ \pm 2\lambda_i : i \neq j,\ 1 \leqq i,\ j \leqq n\}$ be the root system of type C_n. Then the following matrices are generators of G satisfying (A), (B) and (C): $x(\lambda_i - \lambda_j, t) = I + t(E_{ij} - E_{j+n, i+n})$, $x(\lambda_i + \lambda_j, t) = I + t(E_{i, j+n} + E_{j, i+n})$, $x(-(\lambda_i + \lambda_j), t) = I + t(E_{j+n, i} + E_{i+n, j})$, $x(2\lambda_i, t) = I + tE_{i, i+n}$, $x(-2\lambda_i, t) = I + tE_{i+n, i}$. We see that $G_Z = Sp(2n, Z)$ and we have our assertion. Note that $x(\lambda_j - \lambda_i, t)$, $x(\lambda_i + \lambda_j, t)$ and w are the matrices denoted by $R_{ji}(t)$, $T_{ij}(t)$, $T_i(t)$ and D respectively in [3].

3. Let G be the adjoint group of a complex simple Lie algebra $\mathfrak{g}$ (i.e. the connected component of the identity of the group of all automorphisms of $\mathfrak{g}$. We fix a canonical base $(H_1, \cdots, H_n, X_r, r \in \Sigma)$ of $\mathfrak{g}$ defined by Chevalley (cf. [1], Th. 1). Then we may suppose that G is a linear algebraic group defined over Q in $GL(N, C)$ where N is the dimension of $\mathfrak{g}$. We denote by G_Z the subgroup of G consisting of the elements with integral coefficients and determinants $= 1$. Then we have

COROLLARY 2. *Let G be the adjoint group of a complex simple Lie algebra and suppose that G is a linear algebraic group with respect to a canonical base of* $\mathfrak{g}$. *If* $\mathfrak{g}$ *is not of type* D_n, $n \geqq 4$ *and even, then* G_Z *is generated by two elements.*

Denote by $x(r, t) = \exp t \operatorname{ad} X_r$, $r \in \Sigma$, $t \in C$, and by G'_Z the subgroup of G generated by $x(r, 1)$, $r \in \Sigma$. Then G'_Z is also generated by two elements by the theorem. For G'_Z is the homomorphic image of $\widetilde{G}_Z$ where $\widetilde{G}$ is the universal covering group of G. G'_Z is a normal subgroup of G_Z and further we shall show the following

LEMMA 3. *If $\mathfrak{g}$ is of type A_n (n even), E_6, E_8, F_4 or G_2, then $G_Z = G'_Z$. If $\mathfrak{g}$ is of type A_n (n odd), B_n, C_n, D_n ($n \geqq 5$, odd) or E_7, then G_Z/G'_Z is the cyclic group of order 2. If $\mathfrak{g}$ is of type D_n ($n \geqq 4$, even), then G_Z/G'_Z is the direct product of two cyclic groups of order 2.*

Denote by H_Z the subgroup of G_Z generated by $h(\mathcal{X})$, where $h(\mathcal{X})$ is the automorphism of $\mathfrak{g}$ defined by $H_i \rightarrow H_i$, $X_r \rightarrow \mathcal{X}(r)X_r$, $\mathcal{X}$ being a homomorphism of the additive group P_r generated by the roots of $\mathfrak{g}$ into the multiplicative group $U=\{1, -1\}$, and by $H'_Z=H_Z \cap G'_Z$. Then H'_Z is the group generated by $h(\mathcal{X})$ such that $\mathcal{X}$ can be extended to a homomorphism of the additive group P of the weights of the representations of $\mathfrak{g}$ into U. We have $G_Z/G'_Z \cong H_Z/H'_Z$ (cf. Cvevalley [2]). Since $[H_Z : H'_Z]$ is equal to the order of $\mathrm{Hom}(P/P_r, U)$ (cf. Chevalley [1], p. 63), G_Z/G'_Z is the elementary abelian group of order 2^d where $d=n-\mathrm{rank}\ A$, A being the (n, n) matrix with coefficients in $Z/2Z$ whose (i, j) component is the image of $a(i, j)$ in $Z/2Z$. From this we have the lemma.

When $G_Z = G'_Z$, the corollary is trivial by theorem. When G_Z/G'_Z is the cyclic group of order 2, let w, u be the generators of G'_Z which are the canonical image of the generators of G_Z denoted by the same letters in 2, h be an element of H_Z not contained in H'_Z. Then wh and u generate the group G_Z.

In the case of type D_n, $n \geqq 4$ and even, we have not known whether the group G_Z may be generated by two elements or not, but from theorem, we have that G_Z is generated by three elements.

REMARK. Let G be the group consisting of the matrices x such that ${}^t xJx = J$, $\det x = 1$, where $J = \begin{pmatrix} & I \\ I & \end{pmatrix}$, I being the unit matrix of degree n and G_Z be the subgroup of G consisting of the matrices with integral coefficients. Since G_Z is the group of Z-rational elements with respect to an admissible Z-structure of G, we have, in the same way as the proof of corollaries 1 and 2, that if $n > 3$, G_Z is generated by two elements. (Note that in this case G_Z/G'_Z is a cyclic group of order 2.) The same reasoning doesn't hold for the classical group of type B_n.

REFERENCES

[1] C. CHEVALLEY, Sur certains groupes simples, Tôhoku Math. Journ., 7(1955), 14-66.
[2] C. CHEVALLEY, Certains schémas de groupes semi-simples, Séminaire Bourbaki, 13 (1960/61), No. 219.
[3] P. STANEK, Concerning a theorem of L. K. Hua and I. Reiner, Proc. Amer. Math. Soc., 14(1963), 751-753.

[4] R. STEINBERG, Generators for simple groups, Canad. Journ. Math., 14(1962), 277-283.
[5] R. STEINBERG, Générateurs, relations et revêtments de groupes algébriques, Coll. théorie des groupes algébriques, Bruxelles, (1962), 113-127.

TÔHOKU UNIVERSITY.