J. Math. Soc. Japan
Vol. 29, No. 2, 1977

Surjectivity of exponential map on semisimple Lie groups

By Heng-Lung LAI[1]

(Received June 4, 1976)

§ 1. Introduction.

Let $\mathfrak{G}$ be a connected (real or complex) Lie group with Lie algebra G. In general, the exponential map $\exp: G \to \mathfrak{G}$ is not onto. But, as is well known, for any element g in $SL(n, \boldsymbol{R})$, g^2 lies on some 1-parameter subgroup. We want to consider the analogous problem for an arbitrary connected Lie group $\mathfrak{G}$: Does there exist some positive integer p such that for any g in $\mathfrak{G}$, g^p lies on some 1-parameter subgroup of $\mathfrak{G}$? As was shown by an example in Markus [6], this may not be true for some (even simply connected) solvable Lie groups. The main result we will prove in this paper is the following theorem.

THEOREM. *Let $\mathfrak{G}$ be a connected (real or complex) semisimple Lie group with finite center. Then we can find a positive integer p such that $g^p \in \exp G$ for any $g \in \mathfrak{G}$.*

This result has been generalized by M. Goto (see [4]) for any algebraic groups over algebraically closed fields.

In section 2, we will consider the complex cases. First, we will prove the main theorem for a connected complex semisimple Lie group with trivial center; the general case can then be proved from this one as a corollary. Then we will find the smallest such numbers for some complex simple Lie groups. The results can be listed as follows. The first row indicates the type of Lie algebras, the second row gives the smallest numbers for the corresponding adjoint groups, and the third row gives the smallest numbers for the corresponding classical simple Lie groups.

A_l	B_l	C_l	D_l	G_2	F_4
1	2	2	2	6	12
$l+1$	2	2	2		

[1] This paper is a portion of the author's Ph. D. thesis. The thesis was written under the direction of Professor Morikuni Goto at the University of Pennsylvania. The author would like to take this opportunity to thank Professor Goto for his help and guidance.

For cases E_6, E_7, E_8, my method becomes too complicated to compute the best possible numbers, but we will give some lower bounds.

In section 3, we will prove the main theorem for a connected real semisimple Lie group without center. For the adjoint groups of real noncompact semisimple Lie algebras of the first category (in the sense of Gantmacher [2]), the number we need is the same as that for the corresponding complex case. For those in the second category, twice the number for the corresponding complex case is enough. Also, we will prove that this number is the best possible for AI_n. Whether it is also best possible for other cases remains an open question.

At the end of section 3, we will give an example in which $\mathfrak{G}$ has infinite center and such a positive integer does not exist.

§ 2. Complex cases.

Let G be a complex semisimple Lie algebra with a (fixed) Cartan subalgebra H. Let $G=H+\sum_{\alpha\in\Delta} Ce_\alpha$ be the corresponding root space decomposition, where Δ is the root system of G with respect to H. Let $\Pi=\{\alpha_1, \cdots, \alpha_l\}$ be a fundamental root system of Δ.

Denote by H_0^* the subspace generated by Δ (over the field $\boldsymbol{Q}$ of rational numbers) in the space H^* dual to H. Let B be the Killing form on G. As was shown in Goto & Grosshans [3], we can find $h_\alpha\in H$ ($\alpha\in\Delta$) such that $B(h, h_\alpha)=\alpha(h)$ for all $h\in H$, and such that h_α, e_α's satisfy the following:

$$[h, e_\alpha]=\alpha(h)e_\alpha,\quad [e_\alpha, e_\beta]=N_{\alpha,\beta}e_{\alpha+\beta} \text{ if } \alpha+\beta\neq 0 \text{ is in } \Delta,$$

$$[e_\alpha, e_{-\alpha}]=-h_\alpha,\quad [e_\alpha, e_\beta]=0 \text{ if } \alpha+\beta\notin\Delta.$$

Since $\Pi\subset H_0^*$ is linearly independent, we can choose $h_1, \cdots, h_l\in H$, such that $\alpha_i(h_j)=\delta_{ij}$, $1\leqq i, j\leqq l$. The lattice $\Omega=\boldsymbol{Z}2\pi\sqrt{-1}\,h_1+\cdots+\boldsymbol{Z}2\pi\sqrt{-1}\,h_l$ is the kernel of $\exp|_H: H\to \mathrm{Ad}\, G$.

THEOREM 1. *Let $\mathfrak{G}$ be a connected complex semisimple Lie group with Lie algebra G. Assume that the center $Z(\mathfrak{G})$ of $\mathfrak{G}$ is trivial. Then there exists a positive integer p, such that for any $g\in\mathfrak{G}$, g^p lies on some 1-parameter subgroup.*

PROOF. Any element $g\in\mathfrak{G}$ can be written uniquely as $g=g_0\cdot\exp N$, such that $g_0\cdot\exp N=\exp N\cdot g_0$, and where g_0 is semisimple and N is nilpotent. By Gantmacher [1], any semisimple element is conjugate to some element in $\exp H$. Therefore it suffices to consider elements g such that $g_0\in\exp H$.

For $g_0=\exp h_0$, $h_0\in H$. The choice of h_0 is not unique. In fact, $\exp(h_0+\Omega)=g_0$. Our problem is: given g_0 and N as above, is it possible to choose some h in $h_0+\Omega$, such that $[h, N]=0$?

Assume $h_0=x_1h_1+\cdots+x_lh_l$. The 1-eigenspace $G(1, \mathrm{Ad}\, g_0)$ of $\mathrm{Ad}\, g_0$ is a subalgebra of G. $G(1, \mathrm{Ad}\, g_0)=H+\sum_{\alpha\in\Delta_1} \boldsymbol{C}e_\alpha$, where $\Delta_1\subset\Delta\subset H_0^*$. Since Δ_1 generates an r-dimensional subspace of H_0^*, we may choose a generating system $\beta_1, \cdots, \beta_r\in\Delta_1$ for this subspace. In other words, $G(1, \mathrm{Ad}\, g_0)$ is generated (as an algebra) by H and $e_{\pm\beta_j}$, $j=1, \cdots, r$. The linearly independent subset $\{\beta_1, \cdots, \beta_r\}\subset\Delta$ can be extended to a maximal linearly independent subset, i. e. we can find $\beta_{r+1}, \cdots, \beta_l\in\Delta$ such that $\{\beta_1, \cdots, \beta_l\}$ is a linearly independent subset (over $\boldsymbol{Q}$). Clearly, we may assume all β_i's are positive roots. There exists nonnegative integers m_{ij} $(1\leqq i, j\leqq l)$ such that

$$\beta_i=m_{i1}\alpha_1+\cdots+m_{il}\alpha_l \qquad i=1, \cdots, l.$$

By assumption, $e_{\beta_i}\in G(1, \mathrm{Ad}\, g_0)$ for $i=1, \cdots, r$ implies $\beta_i(h_0)\in 2\pi\sqrt{-1}\,\boldsymbol{Z}$, i.e.

$$m_{i1}x_1+\cdots+m_{il}x_l=2\pi\sqrt{-1}\,k_i \qquad (1\leqq i\leqq r)$$

for some integer k_i. The problem is to choose $2\pi\sqrt{-1}\,(n_1h_1+\cdots+n_lh_l)\in\Omega$ $(n_1, \cdots, n_l\in\boldsymbol{Z})$ such that

$$m_{i1}(x_1+2\pi\sqrt{-1}\,n_1)+\cdots+m_{il}(x_l+2\pi\sqrt{-1}\,n_l)=0,$$

i. e.

$$m_{i1}n_1+\cdots+m_{il}n_l=-k_i \qquad i=1, \cdots, r.$$

The problem is thus reduced to solving the following system of linear equations for $(n_1, \cdots, n_l)$:

$$m_{i1}n_1+\cdots+m_{il}n_l=-k_i \qquad i=1, \cdots, r.$$

$$m_{i1}n_1+\cdots+m_{il}n_l=0 \qquad i=r+1, \cdots, l.$$

This is a linearly independent system with integral coefficients, so we can find a rational solution for $(n_1, \cdots, n_l)$. If $d=|\det(m_{ij})|$, which is nonzero, then we can find integral solutions for the following:

$$m_{i1}n_1+\cdots+m_{il}n_l=-dk_i \qquad i=1, \cdots, r.$$

$$m_{i1}n_1+\cdots+m_{il}n_l=0 \qquad i=r+1, \cdots, l.$$

This means, we can find $h\in dh_0+\Omega$ such that $[h, G(1, \mathrm{Ad}\, g_0)]=0$. In particular, $[h, N]=0$ because the fact that $g_0\cdot\exp N=\exp N\cdot g_0$ implies that $N\in G(1, \mathrm{Ad}\, g_0)$. Therefore

$$g^d=(g_0\cdot\exp N)^d=(\exp h_0\cdot\exp N)^d=\exp dh_0\cdot\exp dN$$
$$=\exp(h+dN)\in\exp G.$$

Since Δ is a finite set, there can be only finitely many choices of the

linearly independent subsets $\{\beta_1, \cdots, \beta_l\} \subset \Delta$. So the positive integer p defined to be the least common multiple of the set $\{|\det(m_{ij})| : \beta_i = \sum_j m_{ij}\alpha_j \ (1 \leqq i \leqq l)$ form a linearly independent subset in $\Delta\}$ is finite, and clearly, for any $g \in \mathfrak{G}$, g^p lies on some 1-parameter subgroup. Q. E. D.

COROLLARY. *The theorem is true without the assumption* $Z(\mathfrak{G})=1$.

PROOF. Note that $Z(\mathfrak{G})$ is finite, consider $\mathrm{Ad}\,\mathfrak{G}$, which has trivial center. By Theorem, we can find q such that for any $g \in \mathfrak{G}$, $(\mathrm{Ad}\, g)^q = \mathrm{Ad}\exp x$, for some $x \in G$. This means $g^q = \exp x \cdot c$ for some $c \in Z(\mathfrak{G})$. Let r be the smallest number such that $c^r = 1$ for any $c \in Z(\mathfrak{G})$. Then $p = qr$ satisfies the requirement. Q. E. D.

In the following, we want to find the smallest such numbers for certain complex simple Lie groups. We choose a root space decomposition for each classical simple Lie algebra as in Goto & Grosshans [3].

As usual, denote by E_{ij} the matrix with 1 for the (ij)th entry and 0 elsewhere, let 1_k be the k by k identity matrix, and denote by ${}^tX$ the transpose of matrix X.

2.1. *The special linear Lie algebra:* $sl(n+1, \boldsymbol{C}) = A_n$, $n \geqq 1$.

Recall that $sl(n+1, \boldsymbol{C}) = \{X \in gl(n+1, \boldsymbol{C}) : \mathrm{trace}\, X = 0\}$. We choose a Cartan subalgebra : $H = \{\Sigma_j x_j E_{jj} : \Sigma x_j = 0\}$, and we define weights $\lambda_i \in H^*$ by $\lambda_i(\Sigma_j x_j E_{jj}) = x_i$, $i = 1, \cdots, n+1$. Then the root system is $\Delta = \{\lambda_i - \lambda_j : i \neq j\}$, and we have a fundamental root system

$$\Pi = \{\alpha_i = \lambda_i - \lambda_{i+1} : i = 1, \cdots, n\} .$$

Note that any positive root $\lambda_i - \lambda_j$ $(i<j)$ can be written as $\alpha_i + \cdots + \alpha_{j-1}$.

(2.1.1) $\qquad \exp : G = sl(n+1, \boldsymbol{C}) \longrightarrow \mathrm{Ad}\, G$ is surjective.

PROOF. If $\beta_i = m_{i1}\alpha_1 + \cdots + m_{in}\alpha_n$ $(1 \leqq i \leqq n)$ is a linearly independent subset in Δ, then the matrix $(m_{ij})_{1 \leqq i,j \leqq n}$ has row vectors of the form $(0, \cdots, 0, 1, \cdots, 1, 0, \cdots, 0)$. We want to prove $\det(m_{ij}) = \pm 1$ by induction on n.

When $n=1$, it is trivial.

In general, since (m_{ij}) is non-singular, there must be at least one 1 in each column, i. e. each α_j appears in some β_i. Choose the biggest root among β_i's which involve α_1. By changing the ordering if necessary, we may assume that this root is $\beta_1 = \alpha_1 + \cdots + \alpha_k$. Then, if $\beta_2 = \alpha_1 + \cdots + \alpha_r$ $(r<k)$, say, we may replace β_2 by $\beta_1 - \beta_2 = \alpha_{r+1} + \cdots + \alpha_k$. Continuing this process will reduce the matrix (m_{ij}) to

$$\begin{pmatrix} 1 & * \\ 0 & \\ \vdots & m'_{ij} \\ 0 & \end{pmatrix}$$

where $(m'_{ij})_{1\leqq i,j\leqq n-1}$ is an $(n-1)$ by $(n-1)$ matrix which is of the same form as (m_{ij}). So $\det(m_{ij})=\pm\det(m'_{ij})=\pm 1$ by induction. Hence, $\exp: G\to \mathrm{Ad}\, G$ is onto. Q. E. D.

For the simply connected Lie group $\mathfrak{G}=SL(n+1, \boldsymbol{C})$, we have $Z(\mathfrak{G})=\{aI: a\in\boldsymbol{C}, a^{n+1}=1\}$ which is cyclic of order $n+1$, so (2.1.1) implies that for any $g\in\mathfrak{G}$, g^{n+1} lies on some 1-parameter subgroup of $\mathfrak{G}$.

(2.1.2) $p=n+1$ is the smallest number such that, for all $g\in SL(n+1, \boldsymbol{C})$, g^p lies on some 1-parameter subgroup.

PROOF. It suffices to prove $p=n+1$ is necessary by considering the following example (which is also given in Markus [6]).

EXAMPLE. Let $N_1=\sum_{i=1}^{n} E_{ii+1}\in sl(n+1, \boldsymbol{C})$. Then the centralizer $c(N_1)$ of N_1 in $sl(n+1, \boldsymbol{C})$ is $\{a_1N_1+\cdots+a_nN_n: a_j\in\boldsymbol{C}\}$, where $N_j=\sum_{i=1}^{n-j+1} E_{ii+j}$. Let a be an $(n+1)^{st}$ primitive root of 1. Let $g_0=aI$, $g=g_0\cdot\exp N_1$. Suppose that $g_0^r\cdot\exp N_1=\exp x$ for some $x\in sl(n+1, \boldsymbol{C})$. Gantmacher [1] has shown that in the decomposition of any element in a semisimple Lie algebra, the semisimple and nilpotent parts commute with each other. Since the exponential map is injective on the nilpotent part, x can be decomposed as $x=x_0+N_1$, where $[x_0, N_1]=0$ and x_0 is semisimple. But the only semisimple element in $c(N_1)$ is 0. This implies that $I=g_0^r$, so $a^r=1$, which is impossible if $r<n+1$. Therefore g^r does not lie on any 1-parameter subgroup of $SL(n+1, \boldsymbol{C})$ if $r<n+1$. Q. E. D.

COROLLARY. *Suppose $\mathfrak{G}$ is a connected complex simple Lie group with Lie algebra $G=sl(n+1, \boldsymbol{C})$. Let $r=$order of the center $Z(\mathfrak{G})$. Then $p=r$ is the smallest number such that, for any $g\in\mathfrak{G}$, $g^p\in\exp G$.*

PROOF. By (2.1.1.) g^r lies on some 1-parameter subgroup of $\mathfrak{G}$, for any $g\in\mathfrak{G}$. On the other hand, $SL(n+1, \boldsymbol{C})$ is the universal covering group of $\mathfrak{G}$. It is easy to see that this is a $n+1/r$-fold covering. If $g^p\in\exp G$ for any $g\in\mathfrak{G}$, then $p(n+1)/r$ will be a sufficiently large number for $SL(n+1, \boldsymbol{C})$. By (2.1.2) $p(n+1)/r$ is at least $n+1$, so p must be multiple of r. Q. E. D.

2.2. *The symplectic Lie algebra:* $sp(n, \boldsymbol{C})=C_n$, $n\geqq 3$.

Recall that

$$sp(n, \boldsymbol{C})=\left\{X\in gl(2n, \boldsymbol{C}): {}^tX\begin{pmatrix}0 & 1_n\\ -1_n & 0\end{pmatrix}+\begin{pmatrix}0 & 1_n\\ -1_n & 0\end{pmatrix}X=0\right\}$$

$$=\left\{\begin{pmatrix}A & B\\ C & -{}^tA\end{pmatrix}: A, B, C\in gl(n, \boldsymbol{C}),\ B, C \text{ symmetric}\right\}.$$

Choose a Cartan subalgebra

$$H=\{(x_1, \cdots, x_n)=\sum_{1}^{n} x_i(E_{ii}-E_{n+i\, n+i}): x_i\in\boldsymbol{C}\},$$

and let weights $\lambda_i \in H^*$ be defined by $\lambda_i(x_1, \cdots, x_n)=x_i$, $1 \leqq i \leqq n$. The root system will be $\Delta=\{\lambda_i-\lambda_j\ (i\neq j),\ \pm(\lambda_i+\lambda_j)\ (i \leqq j)\}$, and we have a fundamental root system

$$\Pi=\{\alpha_i=\lambda_i-\lambda_{i+1}\ (1 \leqq i \leqq n-1),\ \alpha_n=2\lambda_n\}\ .$$

The root vector corresponding to $\alpha=\lambda_i-\lambda_j$ $(i<j)$ is $e_\alpha=E_{ij}-E_{n+j\ n+i}$, that corresponding to $\alpha=\lambda_i+\lambda_j$ $(i \leqq j)$ is $e_\alpha=E_{i\ n+j}+E_{j\ n+i}$.

Recall that the symplectic Lie group $Sp(n, \boldsymbol{C})$ is simply connected with center $\boldsymbol{Z}_2$.

(2.2.1) Let $g \in Sp(n, \boldsymbol{C})$, then g^2 lies on some 1-parameter subgroup.

PROOF. In this case, $\exp H=\{\mathrm{diag}\,(\beta_1, \cdots, \beta_n, \beta_1^{-1}, \cdots, \beta_n^{-1}) : \beta_i \neq 0 \text{ in } \boldsymbol{C}\}$. For $g_0=\mathrm{diag}\,(\beta_1, \cdots, \beta_n, \beta_1^{-1}, \cdots, \beta_n^{-1})$, choose $x_i \in \boldsymbol{C}$ such that $e^{x_i}=\beta_i$ and $-\pi<\mathrm{Im}\, x_i \leqq \pi$. Then $x=(x_1, \cdots, x_n) \in H$ and clearly $\exp x=g_0$. For $\alpha=\lambda_i-\lambda_j$ $(i<j)$

$$\mathrm{Ad}\, g_0 \cdot e_\alpha=\beta_i\beta_j^{-1}E_{ij}-(\beta_j^{-1})(\beta_i^{-1})^{-1}E_{n+j\ n+i}=\beta_i\beta_j^{-1}e_\alpha\,,$$

so $\mathrm{Ad}\, g_0 \cdot e_\alpha=e_\alpha$ if and only if $\beta_i=\beta_j$. By choice of x_i's, this is true if and only if $x_i=x_j$, in which case $\alpha(x)=0$.

On the other hand, for $\alpha=\lambda_i+\lambda_j$ $(i \leqq j)$,

$$\mathrm{Ad}\, g_0 \cdot e_\alpha=\beta_i(\beta_j^{-1})^{-1}E_{i\ n+j}+\beta_j(\beta_i^{-1})^{-1}E_{j\ n+i}=\beta_i\beta_j e_\alpha\,,$$

so $\mathrm{Ad}\, g_0 \cdot e_\alpha=e_\alpha$ if and only if $\beta_i\beta_j=1$, $\beta_i\beta_j=1$ if and only if $e^{x_i+x_j}=1$, and this happens when and only when either $x_i+x_j=0$ or $x_i+x_j=2\pi\sqrt{-1}$. In the first case, $\alpha(x)=0$, and we are done. So suppose $x_i+x_j=2\pi\sqrt{-1}$. This will happen only if $x_i=x_j=\pi\sqrt{-1}$.

Define $y=(y_1, \cdots, y_n) \in H$ as: $y_i=2x_i$ if $x_i \neq \pi\sqrt{-1}$, $y_i=0$ if $x_i=\pi\sqrt{-1}$. Then $\exp y=\exp 2x=g_0^2$, and $\mathrm{Ad}\, g_0 \cdot e_\alpha=e_\alpha$ when and only when $\alpha(y)=0$, because in case $\beta_i=\beta_j=-1$ we have $\alpha(y)=0$, while otherwise $\alpha(y)=2\alpha(x)=0$. In particular, given $g=g_0 \cdot \exp N \in Sp(n, \boldsymbol{C})$ as usual, choose y for g_0 as above, then we have $[y, N]=0$. So

$$g^2=\exp 2x \cdot \exp 2N=\exp y \cdot \exp 2N=\exp(y+2N)\,.$$

Hence, for any $g \in Sp(n, \boldsymbol{C})$, g^2 lies on some 1-parameter subgroup. Q. E. D.

Next, we want to prove $p=2$ is necessary for the adjoint group. This will imply $p=2$ is the smallest number which works for both the adjoint group and $Sp(n, \boldsymbol{C})$. We will prove this by proving

(2.2.2) $\exp : G=sp(n, \boldsymbol{C}) \longrightarrow \mathrm{Ad}\, G$ is not onto.

PROOF. Put $h_0=h_1+\cdots+h_{n-2}+\pi\sqrt{-1}\,h_{n-1} \in H$ (h_i has the same meaning as in the beginning of section 2), $g_0=\exp h_0$, and $N=e_{\alpha_n}+e_\beta$ where $\beta=2\alpha_{n-1}+\alpha_n$

$=2\lambda_{n-1}$. It is easy to prove $G(1, \mathrm{Ad}\, g_0)$ is generated by H, e_{α_n}, $e_{-\alpha_n}$, e_β, $e_{-\beta}$.

If $x=h+c_{\alpha_n}e_{\alpha_n}+c_{-\alpha_n}e_{-\alpha_n}+c_\beta e_\beta+c_{-\beta}e_{-\beta}\in G(1, \mathrm{Ad}\, g_0)$ commutes with N, then

$$0=[x, N]=[x, e_{\alpha_n}]+[x, e_\beta]$$

$$=\alpha_n(h)e_{\alpha_n}+c_{-\alpha_n}h_{\alpha_n}+\beta(h)e_\beta+c_{-\beta}h_\beta,$$

so that $c_{-\alpha_n}=c_{-\beta}=0$ (because h_{α_n} and h_β are linearly independent) and $\alpha_n(h)=\beta(h)=0$, i. e. $[h, c_{\alpha_n}e_{\alpha_n}+c_\beta e_\beta]=0$. This means that any $x\in G(1, \mathrm{Ad}\, g_0)$ which commutes with N can be written as $x=h+c_{\alpha_n}e_{\alpha_n}+c_\beta e_\beta$ with $[h, c_{\alpha_n}e_{\alpha_n}+c_\beta e_\beta]=0$. Therefore, if we decompose any element in G as the sum of its semisimple part and its nilpotent part, then any $x\in G(1, \mathrm{Ad}\, g_0)$ which commutes with N has its semisimple part in H. In particular, the only such semisimple element lies in H.

Consider $g=g_0\cdot\exp N$ (g_0, N as above). If $g=\exp x$ for some x, then $\mathrm{Ad}\, g\cdot x=x$, so $x\in G(1, \mathrm{Ad}\, g)=G(1, \mathrm{Ad}\, g_0)$. Now, Gantmacher [**1**] has shown that in the decomposition of any element in a semisimple Lie algebra, the semisimple and nilpotent parts commute with each other. Since the exponential map is injective on the nilpotent part, x can be decomposed as $x=x_0+N$, where $[x_0, N]=0$, x_0 is semisimple, and x_0 lies in $G(1, \mathrm{Ad}\, g_0)$ (because N does). The above argument implies that $x_0\in H$. Since $g_0=\exp x_0$, then $x_0\in h_0+\Omega$. But $\alpha_n(x_0)=0$, which forces x_0 to be independent from h_n. For such x_0, $\beta(x_0)=\beta(h_0)+4\pi\sqrt{-1}k\neq 0$. Thus such x_0 and x do not exist, i. e. exp is not surjective. Q. E. D.

COROLLARY. *For any connected complex simple Lie group* $\mathfrak{G}$ *with Lie algebra* G *of type* C, $p=2$ *is the smallest number such that* $g^p\in\exp G$ *for any* $g\in\mathfrak{G}$.

2.3. *The orthogonal Lie algebra:* $o(2n, \boldsymbol{C})=D_n$ $n\geqq 4$.

Recall that $o(2n, \boldsymbol{C})=\{X\in gl(2n, \boldsymbol{C}) : X+{}^tX=0\}$. In the following, we write $A\in gl(2n, \boldsymbol{C})$ as $A=(A_{ij})_{1\leqq i,j\leqq n}$, where each A_{ij} is a 2 by 2 matrix. Choose a Cartan subalgebra

$$H=\left\{(A_{ij}) : A_{ij}=\delta_{ij}\begin{pmatrix}0 & x_i\\ -x_i & 0\end{pmatrix};\ x_i\in\boldsymbol{C}\right\}$$

$$=\{(x_1, \cdots, x_n) : x_i\in\boldsymbol{C}\};$$

define weights $\lambda_i\in H^*$ by $\lambda_i(x_1, \cdots, x_n)=x_i$. The root system is $\Delta=\{\pm\sqrt{-1}(\lambda_i\pm\lambda_j) : i<j\}$, and a fundamental root system will be $\Pi=\{\alpha_i=\sqrt{-1}(\lambda_i-\lambda_{i+1})$ with $1\leqq i\leqq n-1$ and $\alpha_n=\sqrt{-1}(\lambda_{n-1}+\lambda_n)\}$. For a root vector corresponding to $\alpha=\sqrt{-1}(\lambda_i-\lambda_j)$ $(i<j)$, we take the matrix e_α defined by $(e_\alpha)_{ij}=\begin{pmatrix}1 & -\sqrt{-1}\\ \sqrt{-1} & 1\end{pmatrix}$ $(i<j)$, $(e_\alpha)_{ji}=\begin{pmatrix}-1 & -\sqrt{-1}\\ \sqrt{-1} & -1\end{pmatrix}$, 0 elsewhere; for that corresponding to $\alpha=\sqrt{-1}(\lambda_i+\lambda_j)$ $(i<j)$, we take the matrix e_α defined by

$(e_\alpha)_{ij}=-(e_\alpha)_{ji}=\begin{pmatrix} 1 & \sqrt{-1} \\ \sqrt{-1} & 1 \end{pmatrix}$, 0 elsewhere.

Recall that the special orthogonal Lie group $SO(2n, \boldsymbol{C})$ has center $\boldsymbol{Z}_2$.

(2.3.1) $p=2$ is sufficient for $SO(2n, \boldsymbol{C})$.

PROOF. In this case,

$$\exp H=\left\{(A_{ij})_{1\leqq i,j\leqq n}:\ A_{ij}=\delta_{ij}\begin{pmatrix} \cos x_i & \sin x_i \\ -\sin x_i & \cos x_i \end{pmatrix},\ x_i\in \boldsymbol{C}\right\},$$

where

$$\cos x_i=(e^{\sqrt{-1}x_i}+e^{-\sqrt{-1}x_i})/2,\ \sin x_i=(e^{\sqrt{-1}x_i}-e^{-\sqrt{-1}x_i})/2\sqrt{-1}.$$

Note that exp maps the subset $\{(x_1, \cdots, x_n):\ -\pi<\mathrm{Re}\, x_i\leqq\pi\}\subset H$ onto $\exp H$. So any $g_0\in\exp H$ can be written as $g_0=\exp x$ with x lying in this subset.

For $\alpha=\sqrt{-1}(\lambda_i-\lambda_j)$, $\mathrm{Ad}\, g_0\cdot e_\alpha=(A_{rs})_{1\leqq r,s\leqq n}$, where

$$A_{ij}=-A_{ji}=\begin{pmatrix} \cos(x_i-x_j)+\sqrt{-1}\sin(x_i-x_j) & \sin(x_i-x_j)-\sqrt{-1}\cos(x_i-x_j) \\ -\sin(x_i-x_j)+\sqrt{-1}\cos(x_i-x_j) & \cos(x_i-x_j)+\sqrt{-1}\sin(x_i-x_j) \end{pmatrix},$$

and 0 elsewhere.

So, $\mathrm{Ad}\, g_0\cdot e_\alpha=e_\alpha$ if and only if $\cos(x_i-x_j)+\sqrt{-1}\sin(x_i-x_j)=1$, this is true when and only when $e^{\sqrt{-1}(x_i-x_j)}=1$. By our choice of x_i's, $e^{\sqrt{-1}(x_i-x_j)}=1$ if and only if $x_i-x_j=0$, and this happens if and only if $\alpha(x)=0$.

Similarly, for $\alpha=\sqrt{-1}(\lambda_i+\lambda_j)$, $\mathrm{Ad}\, g_0\cdot e_\alpha=e_\alpha$ if and only if $\cos(x_i+x_j)+\sqrt{-1}\sin(x_i+x_j)=1$, and this condition is equivalent to $e^{\sqrt{-1}(x_i+x_j)}=1$; hence either $x_i+x_j=0$ or $x_i+x_j=2\pi$. In the first case, $x_i+x_j=0$, so $\alpha(x)=0$ and we are done. In the second case, the only possibility is $x_i=x_j=\pi$, so $\alpha(x)=2\pi\sqrt{-1}$.

Consider $g_0^2=\exp 2x$, and define $y=(y_1, \cdots, y_n)\in H$ as $y_i=2x_i$ if $x_i\neq\pi$, and $y_i=0$ if $x_i=\pi$. Then $\cos y_i=\cos 2x_i$, and $\sin y_i=\sin 2x_i$. So $\exp y=\exp 2x$. Moreover, $\mathrm{Ad}\, g_0\cdot e_\alpha=e_\alpha$ if and only if $\alpha(y)=0$.

If we consider $g=g_0\cdot\exp N\in\mathfrak{G}$ as usual and choose y for g_0 as above, then $[y, N]=0$. So $g^2=\exp y\cdot\exp 2N=\exp(y+2N)$. This proves (2.3.1). Q. E. D.

(2.3.2) $p=2$ is necessary for the adjoint group $\mathrm{Ad}\, G$, where $G=o(2n, \boldsymbol{C})$.

REMARK. (2.3.1) and (2.3.2) imply that $p=2$ is the smallest number which works for both $\mathrm{Ad}\, G$ and $SO(2n, \boldsymbol{C})$.

PROOF. It suffices to prove exp is not onto for $\mathrm{Ad}\, G$.

Let $h_0=h_1+\cdots+h_{n-4}+\pi\sqrt{-1}\, h_{n-2}\in H$, $g_0=\exp h_0$, $N=e_{\alpha_{n-3}}+e_{\alpha_{n-1}}+e_{\alpha_n}+e_\beta$, where $\beta=2\alpha_{n-2}+\alpha_{n-1}+\alpha_n$. It is not hard to prove that $G(1, \mathrm{Ad}\, g_0)$ is spanned by H together with $e_{\pm\alpha_{n-3}}$, $e_{\pm\alpha_{n-1}}$, $e_{\pm\alpha_n}$ and $e_{\pm\beta}$.

If $x=h+c_{\alpha_{n-3}}e_{\alpha_{n-3}}+\cdots\in G(1, \mathrm{Ad}\, g_0)$ commutes with N, then

$$0=[x, N]=[x, e_{\alpha_{n-3}}]+[x, e_{\alpha_{n-1}}]+[x, e_{\alpha_n}]+[x, e_\beta]$$
$$=\alpha_{n-3}(h)e_{\alpha_{n-3}}+c_{-\alpha_{n-3}}h_{\alpha_{n-3}}+\alpha_{n-1}(h)e_{\alpha_{n-1}}+c_{-\alpha_{n-1}}h_{\alpha_{n-1}}$$
$$+\alpha_n(h)e_{\alpha_n}+c_{-\alpha_n}h_{\alpha_n}+\beta(h)e_\beta+c_{-\beta}h_\beta$$

which implies that $c_{-\alpha_{n-3}}=c_{-\alpha_{n-1}}=c_{-\alpha_n}=c_{-\beta}=0$ and that $\alpha_{n-3}(h)=\alpha_{n-1}(h)=\alpha_n(h)=\beta(h)=0$, i.e. any $x\in G(1, \mathrm{Ad}\, g_0)$ which commutes with N can be written as $x=h+c_{\alpha_{n-3}}e_{\alpha_{n-3}}+c_{\alpha_{n-1}}e_{\alpha_{n-1}}+c_{\alpha_n}e_{\alpha_n}+c_\beta e_\beta$ with $[h, c_{\alpha_{n-3}}e_{\alpha_{n-3}}+c_{\alpha_{n-1}}e_{\alpha_{n-1}}+c_{\alpha_n}e_{\alpha_n}+c_\beta e_\beta]=0$.

Consider $g=g_0\cdot\exp N$ (g_0, N as above). If $g=\exp x$ for some x, then x can be written as $x=x_0+N$, where $[x_0, N]=0$ and x_0 is semisimple. Clearly, both x and x_0 lie in $G(1, \mathrm{Ad}\, g_0)$. The above argument implies that $x_0\in H$ and $\alpha_{n-3}(x_0)=\cdots=\beta(x_0)=0$. Since $g_0=\exp x_0$, we have $x_0\in h_0+\Omega$. But $\alpha_{n-3}(x_0)=\alpha_{n-1}(x_0)=\alpha_n(x_0)=0$, which forces x_0 to be independent from h_{α_j}'s ($j=n-3$, $n-1$, n). For such x_0, $\beta(x_0)=\beta(h_0)+4\pi\sqrt{-1}\,k\neq 0$. Thus such x_0 and x do not exist, i.e. exp is not onto. Q. E. D.

2.4. *The orthogonal Lie algebra:* $o(2n+1, \boldsymbol{C})=B_n$ $n\geqq 2$.

Choose a Cartan subalgebra $H=\{(x_1, \cdots, x_n): x_i\in\boldsymbol{C}\}$ where $(x_1, \cdots, x_n)$ is a matrix $\begin{pmatrix} A & \begin{matrix}0\\ \vdots\\ 0\end{matrix} \\ \begin{matrix}0 & \cdots & 0\end{matrix} & \end{pmatrix}\in gl(2n+1, \boldsymbol{C})$, with $A=(A_{ij})\in gl(2n, \boldsymbol{C})$, $A_{ij}=\delta_{ij}\begin{pmatrix}0 & x_i\\ -x_i & 0\end{pmatrix}$. Weights are defined, as before by $\lambda_i(x_1, \cdots, x_n)=x_i$. Then the root system is $\Delta=\{\pm\sqrt{-1}\,(\lambda_i\pm\lambda_j),\ (i<j)\ \text{and}\ \pm\sqrt{-1}\lambda_i\}$. A fundamental root system will be

$$\Pi=\{\alpha_i=\sqrt{-1}(\lambda_i-\lambda_{i+1}),\ (1\leqq i\leqq n-1)\ \text{and}\ \alpha_n=\sqrt{-1}\lambda_n\}.$$

Root vectors corresponding to $\sqrt{-1}(\lambda_i\pm\lambda_j)$ $(i<j)$ will be the same as those in the D_n case; the root vector corresponding to $\alpha=\sqrt{-1}\lambda_i$ is the matrix

$$e_\alpha=(E_{2i-1\ 2n+1}-E_{2n+1\ 2i-1})+\sqrt{-1}(E_{2i\ 2n+1}-E_{2n+1\ 2i}),$$

(2.4.1) $p=2$ is sufficient for the special orthogonal Lie group $SO(2n+1, \boldsymbol{C})$, which has trivial center.

PROOF. $\exp H$ is similar to that in the D_n case, so we can choose a subset of H as before. If $g_0=\exp(x_1, \cdots, x_n)\in\exp H$, then, for $\alpha=\sqrt{-1}\lambda_i$, we have $\mathrm{Ad}\, g_0\cdot e_\alpha=e_\alpha$ if and only if $\cos x_i+\sqrt{-1}\sin x_i=1$, which is the same as saying $e^{\sqrt{-1}x_i}=1$. By choice of the x_i's, this happens if and only if $x_i=0$. In the other two cases, $\mathrm{Ad}\, g_0\cdot e_\alpha=e_\alpha$ when and only when $\alpha(y)=0$, where y is gotten from $2x$ as before. Therefore $(g_0\cdot\exp N)^2=\exp(y+2N)$. Q. E. D.

(2.4.2) $p=2$ is necessary for the adjoint group.

REMARK. This and (2.4.1) imply $p=2$ is the smallest number which works for the adjoint group (which is isomorphic to $SO(2n+1, \boldsymbol{C})$). (Note that $n\geqq 2$.)

PROOF. Again, if suffices to show that exp is not onto.

Put $h_0=h_1+\cdots+h_{n-2}+\pi\sqrt{-1}\,h_n\in H$, $g_0=\exp h_0$, and $N=e_{\alpha_{n-1}}+e_\beta$ where $\beta=\alpha_{n-1}+2\alpha_n$. It is easy to see that $G(1, \mathrm{Ad}\, g_0)$ is generated by H, $e_{\alpha_{n-1}}$, $e_{-\alpha_{n-1}}$, e_β, $e_{-\beta}$.

If $x=h+c_{\alpha_{n-1}}e_{\alpha_{n-1}}+\cdots\in G(1, \mathrm{Ad}\, g_0)$ commutes with N, then

$$0=[x, N]=[x, e_{\alpha_{n-1}}]+[x, e_\beta]$$
$$=\alpha_{n-1}(h)e_{\alpha_{n-1}}+c_{-\alpha_{n-1}}h_{\alpha_{n-1}}+\beta(h)e_\beta+c_{-\beta}h_\beta$$

so that $c_{-\alpha_{n-1}}=c_{-\beta}=0$ and $\alpha_{n-1}(h)=\beta(h)=0$. Therefore any element in $G(1, \mathrm{Ad}\, g_0)$ which commutes with N has its semisimple part in H.

Consider $g=g_0\cdot\exp N$ (g_0, N as above). If $g=\exp x$ for some x, then $x=x_0+N$ with $[x_0, N]=0$ and x_0 semisimple, x_0 lies in $G(1, \mathrm{Ad}\, g_0)$. The above argument implies that $x_0\in H$. Since $g_0=\exp x_0$, this implies that $x_0\in h_0+\Omega$. But $\alpha_{n-1}(x_0)=0$ forces x_0 to be independent from h_{n-1}. For such x_0, clearly $\beta(x_0)\neq 0$. Thus x_0 and x do not exist, exp is not onto. Q. E. D.

2.5. *The simple Lie algebra of type G_2.*

Let G be of type G_2; then the corresponding simply connected Lie group $\mathfrak{G}$ has trivial center. We know (Jacobson [**5**]) that G has a subalgebra $G_0\cong sl(3, \boldsymbol{C})$. Moreover, a Cartan subalgebra H of G_0 is a Cartan subalgebra of G. Let $H=\{(x_1, x_2): x_1, x_2\in\boldsymbol{C}\}$. Weights are defined by $\lambda_i(x_1, x_2)=x_i$ ($i=1, 2$). The root system is

$$\Delta=\{\pm\lambda_1, \pm\lambda_2, \pm(\lambda_1\pm\lambda_2), \pm(2\lambda_1+\lambda_2), \pm(\lambda_1+2\lambda_2)\}.$$

We have a fundamental root system

$$\Pi=\{\alpha_1=\lambda_1-\lambda_2,\ \alpha_2=\lambda_2\}.$$

In the following, we put

$$\beta=\alpha_1+3\alpha_2=\lambda_1+2\lambda_2,\quad \gamma=\beta+\alpha_1=2\lambda_1+\lambda_2.$$

Computation shows that $h_1=(1, 0)$, $h_2=(1, 1)$. Thus

$$\Omega=\boldsymbol{Z}2\pi\sqrt{-1}h_1+\boldsymbol{Z}2\pi\sqrt{-1}h_2=2\pi\sqrt{-1}(\boldsymbol{Z}\times\boldsymbol{Z}).$$

(2.5.1) Notice that for $g_0\in\exp H$, we can choose $h_0=(x_1, x_2)$ with $-\pi<\mathrm{Im}\, x_1, x_2\leqq\pi$ such that $g_0=\exp h_0$. Therefore:

(i) If $\mathrm{Ad}\, g_0\cdot e_{\lambda_j}=e_{\lambda_j}$, then $\lambda_j(h_0)=0$ by choice of x_j, $j=1, 2$.

(ii) $\mathrm{Ad}\, g_0\cdot e_{\lambda_1-\lambda_2}=e_{\lambda_1-\lambda_2}$ implies $(\lambda_1-\lambda_2)(h_0)=x_1-x_2=0$.

(iii) $\mathrm{Ad}\, g_0\cdot e_{\lambda_1+\lambda_2}=e_{\lambda_1+\lambda_2}$ implies that either $x_1+x_2=0$ or $x_1+x_2=2\pi\sqrt{-1}$. In the second case, $(\lambda_1+\lambda_2)(2h_0-2\pi\sqrt{-1}h_2)=0$.

(iv) $\mathrm{Ad}\, g_0\cdot e_\beta=e_\beta$ implies $x_1+2x_2=0$ or $2\pi\sqrt{-1}$.

(v) $\mathrm{Ad}\, g_0\cdot e_\gamma=e_\gamma$ implies $2x_1+x_2=0$ or $2\pi\sqrt{-1}$.

Suppose that $G(1, \mathrm{Ad}\, g_0)$ contains e_β (with $\beta(x)=x_1+2x_2=2\pi\sqrt{-1}$) but not e_γ. Then it is not hard to prove there are only two cases:

Case 1. $G(1, \mathrm{Ad}\, g_0)$ contains only e_{λ_1} and e_β. In this case, $x_1=0$ and $x_2=\pi\sqrt{-1}$, so $\beta(2h_0-2\pi\sqrt{-1}(0, 1))=0$.

Case 2. $G(1, \mathrm{Ad}\, g_0)$ contains only e_β. In this case, we have $\beta(h_0-2\pi\sqrt{-1}h_1)=0$.

If $G(1, \mathrm{Ad}\, g_0)$ contains e_γ but not e_β, then we have similar results.

Finally, if e_β, $e_\gamma \in G(1, \mathrm{Ad}\, g_0)$, then $x_1=x_2=\frac{2\pi}{3}\sqrt{-1}$, and $e_{\alpha_1}\in G(1, \mathrm{Ad}\, g_0)$ as well. In this case, for $h=3h_0-2\pi\sqrt{-1}h_2$, we have $\beta(h)=\gamma(h)=\alpha_1(h)=0$.

From the above discussion, it follows that $p=6=2\times 3$ is sufficient for $\mathfrak{G}$.

Q. E. D.

(2.5.2) p must be a multiple of 2.

PROOF. Let $h_0=(\pi\sqrt{-1}, \pi\sqrt{-1})$, $g_0=\exp h_0$, and $N=e_{\alpha_1}+e_{\alpha_1+2\alpha_2}$. Then $G(1, \mathrm{Ad}\, g_0)$ is spanned by H, $e_{\pm\alpha_1}$, $e_{\pm(\alpha_1+2\alpha_2)}$.

If $x=h+c_{\alpha_1}e_{\alpha_1}+\cdots \in G(1, \mathrm{Ad}\, g_0)$ commutes with N, then

$$0=\alpha_1(h)e_{\alpha_1}+c_{-\alpha_1}h_{\alpha_1}+(\alpha_1+2\alpha_2)(h)e_{\alpha_1+2\alpha_2}+c_{-(\alpha_1+2\alpha_2)}h_{\alpha_1+2\alpha_2},$$

so that $c_{-\alpha_1}=c_{-(\alpha_1+2\alpha_2)}=0$ and $\alpha_1(h)=\alpha_1+2\alpha_2(h)=0$. It follows that the only such semisimple element lies in H.

If $g=g_0\cdot\exp N=\exp x$ for some x, then $x=x_0+N$ with $x_0\in H$, and therefore $x_0\in h_0+\Omega$. Any $x_0\in h_0+\Omega$ clearly cannot satisfy $\alpha_1(x_0)=0$ and $\alpha_1+2\alpha_2(x_0)=0$ simultaneously. But clearly $g_0^2=1$.

Therefore p must be a multiple of 2. Q. E. D.

(2.5.3) p must be a multiple of 3.

PROOF. Let $h_0=\frac{2\pi}{3}\sqrt{-1}(1, 1)$, $g_0=\exp h_0$, and $N=e_{\alpha_1}+e_\beta$. Then

$$G(1, \mathrm{Ad}\, g_0)=H+\boldsymbol{C}e_{\pm\alpha_1}+\boldsymbol{C}e_{\pm\beta}+\boldsymbol{C}e_{\pm\gamma}.$$

If $x=h+c_{\alpha_1}e_{\alpha_1}+\cdots \in G(1, \mathrm{Ad}\, g_0)$ commutes with N, then

$$\begin{aligned}0=&\alpha_1(h)e_{\alpha_1}+c_{-\alpha_1}h_{\alpha_1}+c_\beta N_{\alpha_1,\beta}e_\gamma+c_{-\gamma}N_{\alpha_1,-\gamma}e_{-\beta}\\&+\beta(h)e_\beta+c_{-\beta}h_\beta+c_{\alpha_1}N_{\beta,\alpha_1}e_\gamma+c_{-\gamma}N_{\beta,-\gamma}e_{-\alpha_1},\end{aligned}$$

so that $c_{-\alpha_1}=c_{-\beta}=c_{-\gamma}=0$ and $\alpha_1(h)=\beta(h)=0$ (so $\gamma(h)=0$ also). Thus the only such semisimple element lies in H.

Let $\mathfrak{G}_1$ be the connected subgroup of $\mathrm{Ad}\, G$ with Lie algebra $G(1, \mathrm{Ad}\, g_0)$, then g_0, $\exp N\in\mathfrak{G}_1$. Hence $g=g_0\cdot\exp N$ and g^2 lie in $\mathfrak{G}_1$. If $g^m=\exp y$, then $y\in G(1, \mathrm{Ad}\, g_0)$.

Since any element x_0 in $h_0+\Omega$ or in $2h_0+\Omega$ cannot satisfy $\alpha_1(x_0)=0$ and

$\beta(x_0)=0$ simultaneously, we conclude that $g=g_0\cdot\exp N$ and that g^2 cannot lie on any 1-parameter subgroups. So p must be a multiple of 3. Q. E. D.

CONCLUSION: $p=6$ is the smallest number which works for the connected complex Lie group with Lie algebra of type G_2.

REMARK. From the discussion in (2.5.1), it is immediate that, although 6 is the smallest number which works at once for *all* $g\in\mathfrak{G}$, nevertheless, for any *fixed* $g\notin\exp G$, either $g^2\in\exp G$ or $g^3\in\exp G$.

2.6. *The simple Lie algebra of type* F_4.

Let G be of type F_4. Then the corresponding simply connected Lie group $\mathfrak{G}$ has trivial center.

From [5], we know that G has a Cartan subalgebra

$$H=\{(x_1, x_2, x_3, x_4): x_i\in\boldsymbol{C}\}$$

such that if $\lambda_i(x_1, x_2, x_3, x_4)=x_i$ $(i=1, 2, 3, 4)$, then the root system Δ has a fundamental system of roots

$$\Pi=\left\{\alpha_1=\frac{1}{2}(\lambda_1-\lambda_2-\lambda_3-\lambda_4),\ \alpha_2=\lambda_4,\ \alpha_3=\lambda_3-\lambda_4,\ \alpha_4=\lambda_2-\lambda_3\right\}.$$

The positive roots can be expressed as $n_1\alpha_1+n_2\alpha_2+n_3\alpha_3+n_4\alpha_4$, where (n_1, n_2, n_3, n_4) are ranged from the following:

(0, 0, 0, 1)	(0, 0, 1, 0)	(0, 0, 1, 1)	(0, 1, 0, 0)	(0, 1, 1, 0)	(0, 1, 1, 1)
(0, 2, 1, 0)	(0, 2, 1, 1)	(0, 2, 2, 1)	(1, 0, 0, 0)	(1, 1, 0, 0)	(1, 1, 1, 0)
(1, 1, 1, 1)	(1, 2, 1, 0)	(1, 2, 1, 1)	(1, 2, 2, 1)	(1, 3, 2, 1)	(2, 2, 1, 0)
(2, 2, 1, 1)	(2, 2, 2, 1)	(2, 3, 2, 1)	(2, 4, 2, 1)	(2, 4, 3, 1)	(2, 4, 3, 2)

(2.6.1) Finding a sufficiently large p such that g^p lies in $\exp G$ for any g in $\mathfrak{G}$.

We cannot attack this case as we did the previous cases, but we can do the following. As in the proof of Theorem 1, choose any four linearly independent positive roots and compute the determinant of the coefficient matrix. Then the least common multiple over all possible such choices of all these determinants is a sufficiently large power. We used a computer to compute all these determinants; the values obtained were ±1, ±2, ±3, ±4 or ±8. Moreover, we get a determinant of ±8 only in the following three cases:

(a) $\alpha_3+\alpha_4,\ 2\alpha_2+\alpha_3+\alpha_4,\ 2\alpha_1+2\alpha_2+\alpha_3+\alpha_4,\ 2\alpha_1+4\alpha_2+3\alpha_3+\alpha_4$.

(b) $\alpha_3,\ 2\alpha_2+\alpha_3,\ 2\alpha_1+2\alpha_2+\alpha_3,\ 2\alpha_1+4\alpha_2+3\alpha_3+2\alpha_4$.

(c) $\alpha_4,\ 2\alpha_2+2\alpha_3+\alpha_4,\ 2\alpha_1+2\alpha_2+2\alpha_3+\alpha_4,\ 2\alpha_1+4\alpha_2+2\alpha_3+\alpha_4$.

In the notation in the proof of Theorem 1, given any integers k_1, k_2, k_3, k_4, the rational solutions (n_1, n_2, n_3, n_4) of the equations $\sum_{j=1}^{4} m_{ij}n_j=-k_i$ $(1\leqq i\leqq 4)$ for these three cases are:

(a) $n_1=\frac{k_2-k_3}{2}$, $n_2=\frac{k_1-k_2}{2}$, $n_3=\frac{k_2+k_3-k_1-k_4}{2}$, $n_4=\frac{k_4-k_1-k_2-k_3}{2}$.

(b) $n_1=\frac{k_2-k_3}{2}$, $n_2=\frac{k_1-k_2}{2}$, $n_3=-k_1$, $n_4=\frac{k_1+k_2+k_3-k_4}{2}$.

(c) $n_1=\frac{k_2-k_3}{2}$, $n_2=\frac{k_3-k_4}{2}$, $n_3=\frac{k_1+k_4-k_2-k_3}{2}$, $n_4=-k_1$.

This shows that we can find integral solutions for $\sum_{j=1}^{4} m_{ij}n_j=-2k_i$ in these cases. The least common multiple of $\{1, 2, 3, 4\}$ is 12. We conclude that $p=12$ is a sufficiently large number for our purpose.

(2.6.2) $p=12$ is best possible.

PROOF. We divide the proof into two steps, which together will imply that p must be a multiple of 12.

(a) p must be a multiple of 3.

Let $h_0=\frac{2\pi}{3}\sqrt{-1}h_2$, and consider $g_0=\exp h_0$. It is not hard to prove that $G(1, \mathrm{Ad}\, g_0)$ is spanned by H, $e_{\pm\alpha_1}$, $e_{\pm\alpha_3}$, $e_{\pm\alpha_4}$, $e_{\pm(\alpha_3+\alpha_4)}$, $e_{\pm\beta}$, $e_{\pm(\alpha_1+\beta)}$, where $\beta=\alpha_1+3\alpha_2+2\alpha_3+\alpha_4$.

Let $N=e_{\alpha_1}+e_{\alpha_3}+e_{\alpha_4}+e_{\beta}$. If $x=h+c_{\alpha_1}e_{\alpha_1}+\cdots$ is an element in $G(1, \mathrm{Ad}\, g_0)$ which commutes with N, then

$$\begin{aligned}0=&\alpha_1(h)e_{\alpha_1}+c_{-\alpha_1}h_{\alpha_1}+c_{\beta}N*e_{\alpha_1+\beta}+c_{-(\beta+\alpha_1)}N*e_{-\beta}\\&+\alpha_3(h)e_{\alpha_3}+c_{-\alpha_3}h_{\alpha_3}+c_{\alpha_4}N*e_{\alpha_3+\alpha_4}+c_{-(\alpha_3+\alpha_4)}N*e_{-\alpha_4}\\&+\alpha_4(h)e_{\alpha_4}+c_{-\alpha_4}h_{\alpha_4}+c_{\alpha_3}N*e_{\alpha_3+\alpha_4}+c_{-(\alpha_3+\alpha_4)}N*e_{-\alpha_3}\\&+\beta(h)e_{\beta}+c_{-\beta}h_{\beta}+c_{\alpha_1}N*e_{\alpha_1+\beta}+c_{-(\alpha_1+\beta)}N*e_{-\alpha_1}.\end{aligned}$$

Since α_1, α_3, α_4 and β are linearly independent in H^*, then $c_{-\alpha_1}=c_{-\alpha_3}=c_{-\alpha_4}=c_{-\beta}=0$; and $c_{-(\alpha_3+\alpha_4)}=c_{-(\beta+\alpha_1)}=0$ because $e_{-\alpha_1}$, $e_{-\alpha_3}$, $e_{-\alpha_4}$, $e_{-\beta}$ are linearly independent. Similarly, $\alpha_1(h)=\alpha_3(h)=\alpha_4(h)=\beta(h)=0$, and so $(\alpha_3+\alpha_4)(h)=(\alpha_1+\beta)(h)=0$. Thus the only semisimple elements in $G(1, \mathrm{Ad}\, g_0)$ which commute with N are in H.

Since any element h in $h_0+\Omega$ or in $2h_0+\Omega$ cannot satisfy $\alpha_1(h)=\alpha_3(h)=\alpha_4(h)=\beta(h)=0$, we by the same discussion as in (2.5.3), conclude that for $g=g_0\cdot\exp N$, g^2 and g^3 do not lie on any 1-parameter subgroups. Since $3h_0\in\Omega$, $\exp 3h_0=1$, so $(g_0\cdot\exp N)^3=\exp 3N$.

Thus p must be divisible by 3.

(b) p must be a multiple of 4.

Let $h_0=\frac{1}{2}\pi\sqrt{-1}h_2$, $g_0=\exp h_0$. It is not hard to prove that $G(1, \mathrm{Ad}\, g_0)$ is generated by H and by $e_{\pm\alpha}$ as α ranges over

$$S=\{\alpha_1, \alpha_3, \alpha_4, \alpha_3+\alpha_4, \beta, \beta+\alpha_3, \beta+\alpha_3+\alpha_4\},$$

where $\beta=2\alpha_1+4\alpha_2+2\alpha_3+\alpha_4$.

Let $N=e_{\alpha_1}+e_{\alpha_3}+e_{\alpha_4}+e_{\beta}$.

If $x=h+c_{\alpha_1}e_{\alpha_1}+\cdots\in G(1, \mathrm{Ad}\, g_0)$ commutes with N, then

$$\begin{aligned}0=&\alpha_1(h)e_{\alpha_1}+c_{-\alpha_1}h_{\alpha_1}\\&+\alpha_3(h)e_{\alpha_3}+c_{-\alpha_3}h_{\alpha_3}+c_{\alpha_4}N_*e_{\alpha_3+\alpha_4}+c_{-(\alpha_3+\alpha_4)}N_*e_{-\alpha_4}\\&\qquad+c_{\beta}N_*e_{\beta+\alpha_3}+c_{-(\beta+\alpha_3)}N_*e_{-\beta}\\&+\alpha_4(h)e_{\alpha_4}+c_{-\alpha_4}h_{\alpha_4}+c_{\alpha_3}N_*e_{\alpha_3+\alpha_4}+c_{-(\alpha_3+\alpha_4)}N_*e_{-\alpha_3}\\&\qquad+c_{\beta+\alpha_3}N_*e_{\beta+\alpha_3+\alpha_4}+c_{-(\beta+\alpha_3+\alpha_4)}N_*e_{-(\beta+\alpha_3)}\\&+\beta(h)e_{\beta}+c_{-\beta}h_{\beta}+c_{\alpha_3}N_*e_{\beta+\alpha_3}+c_{\alpha_3+\alpha_4}N_*e_{\beta+\alpha_3+\alpha_4}\\&\qquad+c_{-(\beta+\alpha_3)}N_*e_{-\alpha_3}+c_{-(\beta+\alpha_3+\alpha_4)}N_*e_{-(\alpha_3+\alpha_4)}.\end{aligned}$$

We then have:

(i) The coefficients of h_α's being zero implies $c_{-\alpha_1}=c_{-\alpha_3}=c_{-\alpha_4}=c_{-\beta}=0$;
(ii) The coefficient of $e_{-\alpha_4}$ being zero implies $c_{-(\alpha_3+\alpha_4)}=0$;
(iii) The coefficient of $e_{-\beta}$ being zero implies $c_{-(\beta+\alpha_3)}=0$;
(iv) The coefficient of $e_{-(\beta+\alpha_3)}$ being zero implies $c_{-(\beta+\alpha_3+\alpha_4)}=0$;
(v) Similarly $\alpha_1(h)=\alpha_3(h)=\alpha_4(h)=\beta(h)=0$, and so $\alpha_3+\alpha_4(h)=0$ etc.

It follows that the only semisimple elements in $G(1, \mathrm{Ad}\, g_0)$ which commute with N are in H.

Using again the argument used in (2.5.3) and in (a), we can prove that for $g=g_0\cdot\exp N$; g, g^2, $g^3\notin\exp G$ because any element h in $h_0+\Omega$ or in $2h_0+\Omega$ or in $3h_0+\Omega$ cannot satisfy $\alpha_1(h)=\alpha_3(h)=\alpha_4(h)=\beta(h)=0$. But clearly, $g^4=\exp 4N$.

Therefore p must be divisible by 4. Q. E. D.

REMARKS. (1) Clearly (2.6.1) and (2.6.2) prove that $p=12$ is the smallest number such that $g^p\in\exp G$ for any $g\in\mathfrak{G}$.

(2) From the discussions in (2.6.1), given any four positive roots with coefficient matrix (m_{ij}), the linear equations $\sum_{j=1}^{4}m_{ij}n_j=-pk_i$ $(i=1, 2, 3, 4)$ has an integral solution for some $p\in\{1, 2, 3, 4\}$. Therefore, given any (fixed) element g in $\mathrm{Ad}\, G$, $g^p\in\exp G$ for some $p\in\{1, 2, 3, 4\}$.

2.7. *The simple Lie algebra of type E_n $(n=6, 7, 8)$.*

For the adjoint group, as in the F_4 case, we could use a computer to com-

pute the determinants of the coefficient matrices of all possible maximal linearly independent system of positive roots, the least common multiple of all these determinants, as we have seen, is a sufficiently large number for our purposes. However, this computation is too complicated even for a computer.

To find a lower bound for the adjoint group in E case, we need some more notation:

Let G be any semisimple (complex) Lie algebra, H be a Cartan subalgebra, $-\alpha_0=m_1\alpha_1+\cdots+m_l\alpha_l$ be the maximal root expressed in terms of a simple root system $\{\alpha_1, \cdots, \alpha_l\}$, $\tilde{\Pi}=\Pi\cup\{\alpha_0\}$ the extended simple root system.

Consider $h_0=2\pi\sqrt{-1}h_j/m_j\in H$, then $G(1, \mathrm{Ad}\exp h_0)=H+\sum_{\alpha\in\Delta(h_0)} \boldsymbol{C}e_\alpha$. It is not hard to prove that the subsystem $\Delta(h_0)$ is generated by $\tilde{\Pi}-\{\alpha_j\}$. To simplify the notation, we denote by $\mathrm{ind}\,(g)$ the smallest integer p for which $g^p\in\exp G$ ($g\in\mathrm{Ad}\,G$).

LEMMA. *Let $h_0=2\pi\sqrt{-1}\,h_j/m_j$ (for some j) be such that the Dynkin diagram of $\Pi(h_0)=\tilde{\Pi}-\{\alpha_j\}$ is a π-system consisting of several homogeneous chains.* (Cf. Goto-Grosshans [3].) *Assume that $\pi(h_0)=\{\gamma_1, \cdots, \gamma_l\}$ with Dynkin diagram*

$$\underset{\gamma_1}{\circ}\!-\!\underset{}{\circ}\!-\cdots-\!\underset{\gamma_p}{\circ}\qquad \underset{}{\circ}\!-\!\underset{}{\circ}\!-\cdots-\!\underset{}{\circ}\cdots\underset{}{\circ}\!-\!\underset{}{\circ}\!-\cdots-\!\underset{\gamma_l}{\circ}$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \gamma_{q+1}$$

Let $N=\sum_{j=1}^{l} e_{\gamma_j}$, $g=\exp h_0\cdot\exp N$. Then $\mathrm{ind}\,(g)=m_j$.

PROOF. In the following, for any root $\beta=b_1\alpha_1+\cdots+b_l\alpha_l$, we denote by $|\beta|=|b_1+\cdots+b_l|$ the length of β.

We have $G(1, \mathrm{Ad}\exp h_0)=H+\sum_{\delta\in\Delta(h_0)} \boldsymbol{C}e_\delta$. Assume that $X=h+\sum_{\delta\in\Sigma(h_0)} c_\delta e_\delta\in G(1, \mathrm{Ad}\exp h_0)$ commutes with N, then

$$(*)\qquad 0=\sum_{i=1}^{l}-(\gamma_i(h)e_{\gamma_i}+c_{-\gamma_i}h_{-\gamma_i})+\sum_{i=1}^{l}\sum_{\delta\in\Sigma(h_0)} c_\delta N_{\gamma_i,\delta}e_{\gamma_i+\delta}\,.$$

By linear independence, $\gamma_i(h)=0$ and $c_{-\gamma_i}=0$ for all $i=1, \cdots, l$. We want to prove that $c_\delta=0$ for all negative δ in $\Delta(h_0)$.

From the diagram, γ_1 can only connect with γ_2, so the coefficient of $e_{-\gamma_1}$ term in (*) is $c_{-\gamma_1-\gamma_2}N_{\gamma_2,-\gamma_1-\gamma_2}$, therefore $c_{-(\gamma_1+\gamma_2)}=0$.

γ_2 can only connect with γ_1 and γ_3, so the coefficient of $e_{-\gamma_2}$ in (*) will be $c_{-\gamma_1-\gamma_2}N_{\gamma_1,-\gamma_1-\gamma_2}+c_{-\gamma_2-\gamma_3}N_{\gamma_3,-\gamma_2-\gamma_3}$, which has to be zero by linear independence, so $c_{-(\gamma_2+\gamma_3)}=0$ because $c_{-(\gamma_1+\gamma_2)}=0$.

Continuing this process, we get $c_\delta=0$ for all negative δ with $|\delta|=2$.

Next, note that all positive root must have the form $\gamma_i+\gamma_{i+1}+\cdots+\gamma_{i+r}$ such that $\{\gamma_i, \gamma_{i+1}, \cdots, \gamma_{i+r}\}$ is a connected subset of the Dynkin diagram. Let $\gamma=\gamma_i+\cdots+\gamma_{i+r}$, consider $\{\gamma_1, \cdots, \gamma_{i-1}, \gamma, \gamma_{i+r+1}, \cdots, \gamma_l\}$ where γ_{i-1} is connected with γ in case γ_{i-1} is connected with γ_i, and γ_{i+r+1} is connected with γ in case γ_{i+r+1} is connected with γ_{i+r}. Clearly, $\{\gamma_1, \cdots, \gamma_{i-1}, \gamma, \gamma_{i+r+1}, \cdots, \gamma_l\}$ forms a π-

system consisting of several homogeneous chains (cf. section 2.5 of Goto-Grosshans [3]), so the only possible positive roots containing γ will be $\gamma_{i-1}+\gamma$, $\gamma+\gamma_{i+r+1}$. If we start with $i=1$, this say that the coefficient of $e_{-\gamma}$ will either be 0 or $c_{-\gamma-\gamma_{r+2}}N_{\gamma_{r+2},-\gamma-\gamma_{r+2}}$, so $c_{-\gamma-\gamma_{r+2}}=0$, i. e. $c_{-\gamma_1-\cdots-\gamma_{r+2}}=0$. Consider $i=2$, using the same argument as in case $i=1$, we will get $c_{-\gamma_2-\cdots-\gamma_{r+3}}=0$. Continuing this process, we can prove that $c_\delta=0$ for all negative δ with length $r+2$. Therefore $c_\delta=0$ for all negative δ.

In particular, the only element in $G(1, \mathrm{Ad}\exp h_0)$ which commutes with N has its semisimple part lying in H and $\gamma_i(h)=0$ for all i.

Assume that $g=\exp X$, then the above implies that $X=h+N$ with $\gamma_i(h)=0$ for all i, but this will imply that $h\in\Omega$. On the other hand, $\exp h=\exp h_0\neq 1$, so $h_0\notin\Omega$, this contradiction shows that $g\notin\exp G$.

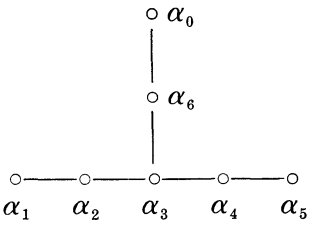
Let $\mathfrak{G}_1$ be the connected subgroup of Ad G with Lie algebra $G(1, \mathrm{Ad}\exp h_0)$. Then $g\in\mathfrak{G}_1$, so that $g^p\in\mathfrak{G}_1$ for any positive integer p. If $g^p=\exp y$, then $y\in G(1, \mathrm{Ad}\exp h_0)$. So the above argument implies that $g^p\notin\exp G$ if $p<m_j$.

Therefore, $\mathrm{ind}\,(g)=m_j$. Q. E. D.

Now we consider E cases.

(a) G is of type E_6.

The extended Dynkin diagram has the following form



The maximal root is $-\alpha_0=\alpha_1+2\alpha_2+3\alpha_3+2\alpha_4+\alpha_5+2\alpha_6$.

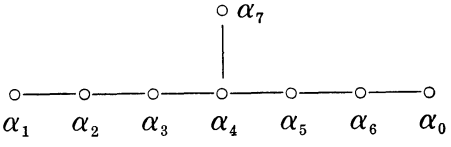
Considering $j=2$ or 3 and applying the above lemma, we can get

$$g_2=\exp(2\pi\sqrt{-1}\,h_2/2)\cdot\exp\Big(\sum_{j\neq 2}e_{\alpha_j}\Big)\quad (j \text{ runs from 0 to 6}) \text{ with } \mathrm{ind}\,(g_2)=2;$$

$$g_3=\exp(2\pi\sqrt{-1}\,h_3/3)\cdot\exp\Big(\sum_{j\neq 3}e_{\alpha_j}\Big)\quad (j \text{ runs from 0 to 6}) \text{ with } \mathrm{ind}\,(g_3)=3.$$

(b) G is of type E_7.

The extended Dynkin diagram has the form



The maximal root is $-\alpha_0=\alpha_1+2\alpha_2+3\alpha_3+4\alpha_4+3\alpha_5+2\alpha_6+2\alpha_7$.

Considering $j=3, 4, 7$, applying the above lemma for each case, we can get the following elements (where j runs from 0 to 7).

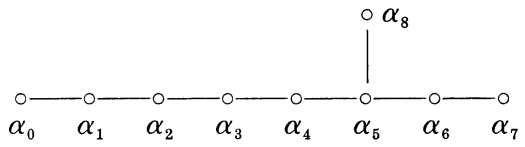
$$g_3=\exp(2\pi\sqrt{-1}\,h_3/3)\cdot\exp(\sum_{j\neq 3}e_{\alpha_j}) \quad \text{with} \quad \operatorname{ind}(g_3)=3;$$

$$g_4=\exp(2\pi\sqrt{-1}\,h_4/4)\cdot\exp(\sum_{j\neq 4}e_{\alpha_j}) \quad \text{with} \quad \operatorname{ind}(g_4)=4;$$

$$g_7=\exp(2\pi\sqrt{-1}\,h_7/2)\cdot\exp(\sum_{j\neq 7}e_{\alpha_j}) \quad \text{with} \quad \operatorname{ind}(g_7)=2.$$

(c) G is of type E_8.

The extended Dynkin diagram has the following form



The maximal root is $-\alpha_0=2\alpha_1+3\alpha_2+4\alpha_3+5\alpha_4+6\alpha_5+4\alpha_6+2\alpha_7+3\alpha_8$.

Considering $j=4, 5, 6, 8$ and applying the above lemma, we can get

$$g_4=\exp(2\pi\sqrt{-1}\,h_4/5)\cdot\exp(\sum_{j\neq 4}e_{\alpha_j}) \quad \text{with} \quad \operatorname{ind}(g_4)=5;$$

$$g_5=\exp(2\pi\sqrt{-1}\,h_5/6)\cdot\exp(\sum_{j\neq 5}e_{\alpha_j}) \quad \text{with} \quad \operatorname{ind}(g_5)=6;$$

$$g_6=\exp(2\pi\sqrt{-1}\,h_6/4)\cdot\exp(\sum_{j\neq 6}e_{\alpha_j}) \quad \text{with} \quad \operatorname{ind}(g_6)=4;$$

$$g_8=\exp(2\pi\sqrt{-1}\,h_8/3)\cdot\exp(\sum_{j\neq 8}e_{\alpha_j}) \quad \text{with} \quad \operatorname{ind}(g_8)=3.$$

(In the above four equations, j runs from 0 to 8.)

Clearly, $\operatorname{ind}(g_6^2)=2$. Q. E. D.

If we denote by p the smallest positive integer such that $g^p\in\exp G$ for any $g\in\operatorname{Ad}G$, then we have shown the following:

p must be a multiple of 6 if G is of type E_6.

p must be a multiple of 12 if G is of type E_7.

p must be a multiple of 60 if G is of type E_8.

It is my conjecture that these are the smallest numbers which works.

§ 3. Real cases.

Let G be a real semisimple Lie algebra, and let $G_c=G\otimes_R C$ be the complexification of G. For $z=x+\sqrt{-1}y\in G_c$ with $x, y\in G$, we denote $x-\sqrt{-1}y$ by $\bar{z}$.

Given any automorphism σ of G, we can consider σ as an automorphism on G_c. The decomposition of σ into semisimple part σ_0 and unipotent part σ_u

can be taken such that σ_0, $\sigma_u \in \mathrm{Aut}\, G$.

The eigenvalues of σ_0 are either real or appear in complex conjugate pairs $re^{\sqrt{-1}\theta}$, $re^{-\sqrt{-1}\theta}$, where $r>0$, $-\pi<\theta<\pi$ and $\theta\neq 0$. It is easy to see that

$$G_c(re^{-\sqrt{-1}\theta}, \sigma_0) = \{\bar{z} : z \in G_c(re^{\sqrt{-1}\theta}, \sigma_0)\} .$$

In fact, for $x+\sqrt{-1}y \in G_c(re^{\sqrt{-1}\theta}, \sigma_0)$ with x, $y \in G$, we have

$$\sigma_0 \cdot x = (r\cos\theta)x - (r\sin\theta)y , \qquad \sigma_0 \cdot y = (r\sin\theta)x + (r\cos\theta)y .$$

If $re^{\pm\sqrt{-1}\theta}$ is a pair of complex eigenvalues of σ_0, and if we denote by $G(r, \theta\,; \sigma_0)$ the subspace

$$\{x \in G : ((\sigma_0)^2 - (2r\cos\theta)\sigma_0 + r^2 \cdot 1)x = 0\}$$

of G, then $G(r, \theta\,; \sigma_0)_c = G_c(re^{\sqrt{-1}\theta}, \sigma_0) + G_c(re^{-\sqrt{-1}\theta}, \sigma_0)$. On the other hand, if s is a real eigenvalue of σ_0, then $G_c(s, \sigma_0) = G(s, \sigma_0)_c$.

Define the "real" part σ_1 of σ_0 as: $\sigma_1 x = |a|x$ whenever $x \in G_c(a, \sigma_0)$ (a is complex number).

LEMMA 1. *σ_1 is an inner automorphism on G.*

PROOF. For $x \in G_c(a, \sigma_0)$ and $y \in G_c(b, \sigma_0)$, we have $[x, y] \in G_c(ab, \sigma_0)$. So

$$[\sigma_1 \cdot x, \sigma_1 \cdot y] = [|a|x, |b|y] = |a|\,|b|[x, y] = |ab|[x, y] .$$

Hence $\sigma_1 \in \mathrm{Aut}\, G_c$. Moreover, if $re^{\sqrt{-1}\theta}$, $re^{-\sqrt{-1}\theta}$ are eigenvalues of σ_0 as above, then for $z \in G_c(re^{\sqrt{-1}\theta}, \sigma_0)$, we have $\sigma_1 \cdot z = |re^{\sqrt{-1}\theta}|\, z = rz$, and $\sigma_1 \cdot \bar{z} = |re^{\sqrt{-1}\theta}|\,\bar{z} = r\bar{z}$, i. e. σ_1 is just $r\cdot 1$ on $G(r, \theta\,; \sigma_0)_c$. In particular, σ_1 maps $G(r, \theta\,; \sigma_0)$ into itself. Clearly also, σ_1 maps $G(s, \sigma_0)$ into itself for any real eigenvalue s. Therefore, $\sigma_1 \in \mathrm{Aut}\, G$. But all of the eigenvalues of σ_1 are positive real. We can define $\delta_1 \cdot x = (\ln t)x$ whenever $x \in G(t, \sigma_1)$. Then δ_1 is a derivation on G because $[G(s, \sigma_1), G(t, \sigma_1)] \subset G(st, \sigma_1)$. By the semisimplicity of G, δ_1 must be an inner derivation. So $\sigma_1 = \mathrm{Exp}\, \delta_1$ is an inner automorphism on G. Q. E. D.

From the definition, it is easy to see that $\sigma_0\sigma_1 = \sigma_1\sigma_0$. If we define the "imaginary" part σ_2 of σ_0 to be $\sigma_2 = \sigma_0\sigma_1^{-1}$. Then σ_2 is also an automorphism of G, and σ_0, σ_1, σ_2 commute with each other. This proves

LEMMA 2. *The "real" and "imaginary" parts of any semisimple inner automorphism of a real semisimple Lie algebra G are again semisimple inner automorphisms of G.*

THEOREM 2. *Let $\mathfrak{G}$ be a connected real semisimple Lie group with trivial center. Then there exists a positive integer p such that for any $g \in \mathfrak{G}$, g^p lies on some 1-parameter subgroup of $\mathfrak{G}$.*

PROOF. If G is the Lie algebra of $\mathfrak{G}$, then $\mathfrak{G}$ can be identified with $\mathrm{Ad}\, G$. The decomposition of any element g: $g = g_0 \cdot \exp N$ has the property that $g_0 \in \mathfrak{G}$, $N \in G$. Define the real and imaginary parts σ_1, σ_2 of $\mathrm{Ad}\, g_0$ as above. By Lemma 2, both σ_1, σ_2 are semisimple inner automorphisms of G, i. e. $\sigma_1 = \mathrm{Ad}\, g_1$,

$\sigma_2=\mathrm{Ad}\,g_2$ for some semisimple elements g_1, g_2 of $\mathfrak{G}$. Since we assume $\mathfrak{G}$ has trivial center, $g_0=g_1g_2$, and g_0, g_1, g_2 all commute with each other.

The proof of Lemma 1 implies that $g_1=\exp x_1$ for some x_1 such that $[x_1, G(1, \mathrm{Ad}\,g_1)]=0$. In particular, $[x_1, G(1, \mathrm{Ad}\,g_0)]=0$ and $[x_1, N]=0$. Since $\mathrm{Ad}\,g_0$ is a semisimple inner automorphism, $G(1, \mathrm{Ad}\,g_0)$ contains a Cartan subalgebra of G. The semisimplicity of x_1 and the equation $[x_1, G(1, \mathrm{Ad}\,g_0)]=0$ imply that x_1 lies in that Cartan subalgebra. In particular, $x_1\in G(1, \mathrm{Ad}\,g_0)$.

Consider now the imaginary part $\sigma_2=\mathrm{Ad}\,g_2$ of $\mathrm{Ad}\,g_0$; clearly $G(1, \mathrm{Ad}\,g_0)\subset G(1, \mathrm{Ad}\,g_2)$, so the above discussion proves that x_1, $N\in G(1, \mathrm{Ad}\,g_2)$.

Since any eigenvalue of $\mathrm{Ad}\,g_2$ has absolute value 1, g_2 lies in some maximal compact subgroup $\mathfrak{K}$ of $\mathfrak{G}$. The compactness of $\mathfrak{K}$ guarantees that $g_2=\exp x_2$ for some $x_2\in K$ (=Lie subalgebra of G corresponding to the Lie subgroup $\mathfrak{K}$). Note that since x_2 is semisimple, we can choose a Cartan subalgebra H_c of G_c containing x_2 such that the corresponding root space decomposition $G_c=H_c+\sum_{\alpha\in\Delta} \boldsymbol{C}e_\alpha$ has the property that each e_α is an eigenvector of $\mathrm{Ad}\,g_2$.

For each $\alpha\in\Delta$, define $\bar{\alpha}$ as: $\bar{\alpha}(h)=\overline{\alpha(\bar{h})}$ for all $h\in H_c$, where $\overline{\alpha(\bar{h})}$ means the complex conjugate of $\alpha(\bar{h})$. Then $\bar{\alpha}$ is also a root in Δ. Furthermore, if $\Pi=\{\alpha_1, \cdots, \alpha_l\}$ is a fundamental root system, then $\bar{\Pi}=\{\bar{\alpha}_1, \cdots, \bar{\alpha}_l\}$ is also a fundamental root system (see for example, Goto & Grosshans [3]). For Π, we can choose $h_1, \cdots, h_l\in H_c$ such that $\alpha_i(h_j)=\delta_{ij}$, then $\bar{\alpha}_i(\bar{h}_j)=\overline{\alpha_i(h_j)}=\delta_{ij}$. Assume $G_c(1, \mathrm{Ad}\,g_2)=H_c+\sum_{\alpha\in\Delta_1} \boldsymbol{C}e_\alpha$ where Δ_1 is a subsystem of Δ. (We may assume this because $G_c(1, \mathrm{Ad}\,g_2)$ is a subalgebra of G_c.) Note that $\bar{\alpha}\in\Delta_1$ whenever $\alpha\in\Delta_1$. As in the proof of Theorem 1, choose $\beta_1, \cdots, \beta_r\in\Delta_1$ as generating system for the subspace in H_c^* spanned by Δ_1 and extend it to a maximal linearly independent subset $\{\beta_1, \cdots, \beta_r, \beta_{r+1}, \cdots, \beta_l\}$ of Δ. Then $\{\bar{\beta}_1, \cdots, \bar{\beta}_r\}\subset\Delta_1$ is also a generating system for the same subspace and $\{\bar{\beta}_1, \cdots, \bar{\beta}_l\}$ is a maximal linearly independent subset. The subalgebra $G_c(1, \mathrm{Ad}\,g_2)$ is generated (as an algebra) by H_c and $e_{\pm\beta_j}$ $(j=1, \cdots, r)$, as well as by H_c and $e_{\pm\bar{\beta}_j}$ $(j=1, \cdots, r)$.

If $\beta_i=\sum_{j=1}^{l} m_{ij}\alpha_j$, then clearly $\bar{\beta}_i=\sum_{j=1}^{l} m_{ij}\bar{\alpha}_j$ with $m_{ij}\in\boldsymbol{Z}$. Since we may assume that $\beta_i(x_2)=2\pi\sqrt{-1}k_i$ for $i=1, \cdots, r$, where $k_i\in\boldsymbol{Z}$, and since $x_2\in G$, we have $\bar{\beta}_i(x_2)=-2\pi\sqrt{-1}k_i$. As was proved in Theorem 1, if we let $d=|\det(m_{ij})|$, then we can find integers $n_1, \cdots, n_l$ such that

$$\beta_i(dx_2+\sum_{j=1}^{l} 2\pi\sqrt{-1}n_jh_j)=0 \qquad \text{for } i=1, \cdots, r.$$

This implies $\beta(dx_2+\sum_{j=1}^{l} 2\pi\sqrt{-1}n_jh_j)=0$ for all β in Δ_1. On the other hand,

$$\bar{\beta}_i(dx_2-\sum_{j=1}^{l} 2\pi\sqrt{-1}n_j\bar{h}_j)=\overline{\beta_i(dx_2+\sum_{j=1}^{l} 2\pi\sqrt{-1}n_jh_j)}=0,$$

so that $\beta(dx_2-\sum_{j=1}^{l}2\pi\sqrt{-1}n_j\bar{h}_j)=0$ for all β in Δ_1 (because $\bar{\beta}_1, \cdots, \bar{\beta}_r$ generate Δ_1).

Therefore, for

$$y_2=(dx_2+\sum_{j=1}^{l}2\pi\sqrt{-1}n_jh_j)+(dx_2-\sum_{j=1}^{l}2\pi\sqrt{-1}n_j\bar{h}_j),$$

we have $\beta(y_2)=0$ for all β in Δ_1, i.e. $[y_2, G(1, \mathrm{Ad}\, g_2)]=0$. But

$$y_2=2dx_2+\sum_{j=1}^{l}(2\pi\sqrt{-1}n_jh_j-2\pi\sqrt{-1}n_j\bar{h}_j)$$

$$=2dx_2+\sum_{j=1}^{l}(2\pi\sqrt{-1}n_jh_j+\overline{2\pi\sqrt{-1}n_jh_j})$$

lies in G. Clearly $\exp y_2=\exp 2dx_2=g_2^{2d}$.

We have proved already that $x_1, N\in G(1, \mathrm{Ad}\, g_0)\subset G(1, \mathrm{Ad}\, g_2)$ and $[x_1, N]=0$. So $[y_2, x_1]=0$, $[y_2, N]=0$. Therefore

$$g^{2d}=g_0^{2d}\cdot\exp 2dN=g_1^{2d}\cdot g_2^{2d}\cdot\exp 2dN=\exp 2dx_1\cdot\exp 2dx_2\cdot\exp 2dN$$

$$=\exp 2dx_1\cdot\exp y_2\cdot\exp 2dN=\exp(2dx_1+y_2+2dN).$$

Again, if we let p be the least common multiple of all such $2d$, then for any $g\in\mathfrak{G}$, g^p lies on some 1-parameter subgroup. Q. E. D.

REMARK. In the above proof, the number obtained is twice the number we got for the corresponding complex case. The question arises: Is this number best possible? If the given real semisimple Lie algebra G is compact, then, as is well known, $\exp: G\to \mathrm{Ad}\, G$ is onto, and there is nothing need to discuss. If the given G is a non-compact real form of its complexification, then there are two cases:

1. G is of the first category in the sense of Gantmacher [2].

In this case, for the compact subalgebra K containing x_2 obtained in the above proof, we have a Cartan decomposition $G=K+P$. Then for the Cartan subalgebra H_c in the proof, we have: $\sqrt{-1}h_\alpha\in K$ for all α in Δ. (h_α is defined as usual by $B(h_\alpha, h)=\alpha(h)$, for all h in H_c.) Thus $\sqrt{-1}h_j\in K$ $(j=1, \cdots, l)$, $dx_2+\sum_{j=1}^{l}2\pi\sqrt{-1}n_jh_j\in K\subset G$, and for $d=|\det(m_{ij})|$, $g^d\in\exp G$. The smallest number which works is the same as that for the complexification. In particular, for each real simple Lie algebra of the first category, the smallest such number is the same as that in the corresponding complex case.

2. G is of the second category.

In this case, we may actually have to use twice the number we get for its complexification. For example, in case G_c is of type A_n, we know $\exp: G_c\to \mathrm{Ad}\, G_c$ is onto, but for real simple Lie algebra of type AI_n, as the

following example shows, we need $p=2$.

EXAMPLE. If n is an odd number, the $SL(n, \boldsymbol{R})$ has trivial center, so $SL(n, \boldsymbol{R}) \cong \mathrm{Ad}\, sl(n, \boldsymbol{R})$. In this case, we already know $\exp : sl(n, \boldsymbol{R}) \to SL(n, \boldsymbol{R})$ is not onto. For example, for $n=3$, let $g=\mathrm{diag}\left(-2, -\frac{1}{2}, 1\right)$. Then g is a semisimple regular element (in the Lie group sense, i.e. $G_c(1, \mathrm{Ad}\, g)$ has dimension 2, which is the same as the rank of G) in $\mathrm{Ad}\, G_c$. So if $g=\exp x$ for some x in G_c, then x must lie in the Cartan subalgebra containing $\mathrm{diag}\,(ln\, 2+\pi\sqrt{-1}, -ln\, 2-\pi\sqrt{-1}, 0)$, i.e. x must lie in the lattice

$$\{\mathrm{diag}(ln\, 2+(2k+1)\pi\sqrt{-1}, -ln\, 2+(2m-1)\pi\sqrt{-1}, -2(k+m)\pi\sqrt{-1}) : k, m \in \boldsymbol{Z}\},$$

but clearly, this lattice has no intersection with $sl(3, \boldsymbol{R})$.

If n is even, $SL(n, \boldsymbol{R})$ has center of order 2. In case $n=2$, $\exp : sl(2, \boldsymbol{R}) \to \mathrm{Ad}\, sl(2, \boldsymbol{R})$ is clearly onto. But when $n \geqq 4$, this is no longer true. We consider $n=4$ as an example, the discussion for general case is exactly the same.

Let $g=\mathrm{diag}\left(-2, -\frac{1}{2}, 2, \frac{1}{2}\right) \in SL(4, \boldsymbol{R})$, so that g is semisimple and regular in $SL(4, \boldsymbol{C})$. Let Ω be the lattice

$$\{\mathrm{diag}\,(2\pi\sqrt{-1}k, 2\pi\sqrt{-1}m, 2\pi\sqrt{-1}p, -2\pi\sqrt{-1}(k+m+p)) : k, m, p \in \boldsymbol{Z}\}.$$

If $g=\exp x$ for some x in $sl(4, \boldsymbol{C})$, then

$$x \in (ln\, 2+\pi\sqrt{-1}, -ln\, 2-\pi\sqrt{-1}, ln\, 2, -ln\, 2)+\Omega.$$

Clearly, then, if $\mathrm{Ad}\, g=\mathrm{Ad}\exp x$ for some x in $sl(4, \boldsymbol{C})$, then x lies either in

$$(ln\, 2+\pi\sqrt{-1}, -ln\, 2-\pi\sqrt{-1}, ln\, 2, -ln\, 2)+\Omega$$

or in

$$(ln\, 2, -ln\, 2, ln\, 2+\pi\sqrt{-1}, -ln\, 2-\pi\sqrt{-1})+\Omega.$$

Neither of these two lattices has any intersection with $sl(4, \boldsymbol{R})$. Thus $\mathrm{Ad}\, g$ does not lie on any 1-parameter subgroup of $\mathrm{Ad}\, sl(4, \boldsymbol{R})$.

This example shows that $p=2$ is the best possible number which works for $\mathrm{Ad}\, G$ when G is of type AI. We already know that $p=2$ (respectively, $p=4$) is a sufficiently large number for $\mathrm{Ad}\, G$ in case G is of type AII (respectively, of type BDI), but whether it is also best possible remains an open question. Finally if G is of type E (either of first category or of second category), we can only give some lower bounds, which is similar to those listed in 2.7.

The following is an immediate consequence of Theorem 2.

COROLLARY. *Let $\mathfrak{G}$ be a connected real semisimple Lie group with finite center. Then we can find a positive integer p such that g^p lies on some 1-parameter subgroup of $\mathfrak{G}$ for any g in $\mathfrak{G}$.*

REMARKS. (1) Let q be the smallest number which works for $\mathrm{Ad}\,\mathfrak{G}$, r be the smallest number such that $c^r=1$ for any $c\in Z(\mathfrak{G})$ (such a number r exists because we assume that $Z(\mathfrak{G})$ is finite), then $p=qr$ is a sufficiently large number which works for $\mathfrak{G}$, but it may not be the smallest such number. For example, when $\mathfrak{G}=SL(n, \boldsymbol{R})$ (n is even), then $q=2$, $r=2$, but $p=2$ works.

(2) When $\mathfrak{G}$ has infinite center, the following example shows that there may not exist such a p at all.

EXAMPLE. Let $\mathfrak{G}$ be the universal covering group of $SL(2, \boldsymbol{R})$, so that $G=sl(2, \boldsymbol{R})$; let $\pi: \mathfrak{G}\to SL(2, \boldsymbol{R})$ be the canonical map, so that $\pi\cdot\exp$ gives the exponential map on $SL(2, \boldsymbol{R})$. Choose a generator a of the center $Z(\mathfrak{G})\cong \boldsymbol{Z}$. First note that if A is a 1-parameter subgroup of $\mathfrak{G}$ passing through some nontrivial element in $\boldsymbol{Z}(\mathfrak{G})$, then $\boldsymbol{Z}(\mathfrak{G})\subset A$ (reason: $\pi(A)$ is compact, hence conjugate to $SO(2, \boldsymbol{R})$, i.e. A is the lifting of a maximal compact subgroup). In particular, then, since the lifting of $SO(2, \boldsymbol{R})$ is a 1-parameter subgroup which has intersection with $\boldsymbol{Z}(\mathfrak{G})$, we can choose $x_0\in G$ such that $a=\exp x_0$.

Let $N=\begin{pmatrix}0 & -1\\ 0 & 0\end{pmatrix}\in G$. Consider $g=a^r\cdot\exp N=\exp rx_0\cdot\exp N$, where r is a positive integer. Suppose then that we had $g=\exp y$ for some $y\in G$. Since y can be decomposed as $y=y_0+N$ such that $[y_0, N]=0$ and y_0 is semisimple, we would have $a^r=\exp y_0$. The previous remark implies that $a=\exp t_0y_0$ for some $t_0\in \boldsymbol{R}$. Therefore $a\cdot\exp N=\exp(t_0y_0+N)$. But it is easy to see that $\pi(a\cdot\exp N)=\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$ does not lie on any 1-parameter subgroup of $SL(2, \boldsymbol{R})$. This contradiction implies that, for $g_0=a\cdot\exp N$, g_0^r does not lie on any 1-parameter subgroup of $\mathfrak{G}$ for any positive integer r. Q. E. D.

§ 4. A generalization.

Let $\mathfrak{G}$ be a (not necessarily connected) real or complex linear group such that the connected component $\mathfrak{G}^0$ (containing the identity element) is a semisimple Lie group and $\mathfrak{G}/\mathfrak{G}^0$ is of finite order (for example, any real or complex semisimple algebraic group). Then the center $Z(\mathfrak{G}^0)$ of $\mathfrak{G}^0$ is finite. By the results of sections 2 and 3, there is a positive integer m such that for any $g\in\mathfrak{G}^0$, g^m lies on some 1-parameter subgroup. On the other hand, since $\mathfrak{G}/\mathfrak{G}^0$ is finite, we can find k such that $g^k\in\mathfrak{G}^0$ for any $g\in\mathfrak{G}$. For $p=mk$, then, we have: g^p lies on some 1-parameter subgroup of $\mathfrak{G}$ for any $g\in\mathfrak{G}$. This also follows immediately from Goto [4] when $\mathfrak{G}$ is a complex semisimple algebraic group.

Bibliography

[1] F. Gantmacher, Canonical representations of automorphisms of a complex semi-simple Lie group, Rec. Math., **5** (1939), 101-144.
[2] F. Gantmacher, On the classification of real simple Lie groups, Rec. Math., **5** (1939), 217-249.
[3] M. Goto and F. Grosshans, Lie Algebras, to be published by Marcel Dekker, New York, 1977.
[4] M. Goto, On an integer associated with an algebraic group, J. Math. Soc. Japan, **29** (1977), 161-163.
[5] N. Jacobson, Lie Algebras, Interscience, New York, 1962.
[6] L. Markus, Exponentials in algebraic matrix groups, Advances in Math., 11 (1973), 351-367.

Heng-Lung LAI
Department of Mathematics
National Central University
Chung-Li, Taiwan 320
Republic of China

Added in Proof: After this paper was submitted, the author found that the results in section 2 can be generalized and simplified, which will appear in a paper with title "Index of the exponential map on a complex simple Lie group."