ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 12, Number 3, Summer 1982

# ON LIE GROUPS WITH MINIMAL GENERATING SETS OF ORDER EQUAL TO THEIR DIMENSION

RICHARD M. KOCH AND FRANKLIN LOWENTHAL

ABSTRACT. Let $G$ be a connected Lie group with Lie algebra $g$, $\{X_1, \ldots, X_\ell\}$ a minimal generating set for $g$. The order of generation of $G$ with respect to $\{X_1, \ldots, X_\ell\}$ is the smallest integer $M$ such that every element of $G$ can be written as a product of $M$ elements taken from $\exp(tX_1), \ldots, \exp(tX_\ell)$. We find all $G$ which admit minimal generating sets $\{X_1, \ldots, X_n\}$ with $n = \dim G$; for each such set we construct an algorithm for computing the order of generation of $G$.

**I. Introduction.** A connected Lie group $G$ is generated by one-parameter subgroups $\exp(tX_1), \ldots, \exp(tX_\ell)$ if every element of $G$ can be written as a finite product of elements chosen from these subgroups. In this case, define the order of generation of $G$ to be the least positive integer $M$ such that every element of $G$ possesses such a representation of length at most $M$; if no such integer exists let the order of generation of $G$ be infinity. The order of generation will, of course, depend upon the one-parameter subgroups. Computation of the order of generation of $G$ for given $X_1, \ldots, X_\ell$ is analogous to finding the greatest wordlength needed to write each element of a finite group in terms of generators $g_1, \ldots, g_\ell$.

The subgroups $\exp(tX_1), \ldots, \exp(tX_\ell)$ generate $G$ just in case $X_1, \ldots, X_\ell$ generate the Lie algebra $g$ of $G$. Indeed the set of all finite products of elements from $\exp(tX_1), \ldots, \exp(tX_\ell)$ is an arcwise connected subgroup of $G$ and so a Lie subgroup by Yamabe's theorem **[10]**; clearly the Lie algebra of this subgroup is the subalgebra of $g$ generated by $X_1, \ldots, X_\ell$.

It is natural to restrict attention to minimal generating sets; from now on, then, suppose that no subset of $\{X_1, \ldots, X_\ell\}$ generates $g$. Call two generating sets $\{X_1, \ldots, X_\ell\}$ and $\{Y_1, \ldots, Y_\ell\}$ *equivalent* if it is possible to find an automorphism $\sigma$ of $G$, a permutation $\tau$ of $\{1, \ldots, \ell\}$, and non-zero constants $\lambda_1, \ldots, \lambda_\ell$ such that $X_i = \lambda_i \sigma_*(Y_{\tau(i)})$. The order of generation of $G$ depends only on the equivalence class of the generating set.

If $\{X_1, \ldots, X_\ell\}$ is a minimal generating set for $G$ and $\dim G > 1, 2 \leqq \ell$

Received by the editors on October 19, 1979.

$\leqq$ dim $G$. In this paper we consider the case $\ell =$ dim $G$. We classify all connected Lie groups $G$ whose Lie algebras admit such generating sets; for each $G$ on our list, we find all minimal generating sets with dim $G$ elements. Finally, we produce an algorithm for computing the order of generation of $G$ with respect to each minimal generating set obtained.

When $\{X_1, \ldots, X_n\}$ is a minimal generating set for $G$ and $n =$ dim $G$, it is easy to show that the map $\exp(t_1X_1) \circ \cdots \circ \exp(t_nX_n)$ from $R^n$ to $G$ is a local diffeomorphism near 0. Our calculations show that this map is rarely onto.

In a series of papers [**3**, **4**, **5**, **6**, **7**, **8**], the order of generation problem was completely solved for all two and three dimensional Lie groups. In particular, groups locally isomorphic to $SL(2, R)$ were discussed in [**4**]. It turns out that $sl(2, R)$ is the only simple Lie algebra which admits minimal generating sets with order equal to the dimension of the algebra, so the techniques used in [**4**] reappear here.

**II. Classification of Lie algebras.**

THEOREM 1. *Let $g$ be a real semisimple Lie algebra,* dim $g = n$. *Let $\{X_1, \ldots, X_n\}$ be a minimal generating set for $g$. There is an isomorphism carrying $g$ to $sl(2, R) \times \cdots \times sl(2, R)$ and $X_1, \ldots, X_n$ to real scalar multiples of*

$$\ldots, 0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0,$$

$$0 \times \cdots \times \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0,$$

$$0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \times \cdots \times 0, \ldots.$$

PROOF. Since the $X_i$ form a minimal generating set for $g$, $[X_i, X_j] = A_{ij}X_i + B_{ij}X_j$, $A_{ij}$, $B_{ij} \in R$. Let $g_C = g \otimes C$, $Y_i = X_i \otimes 1$. Of course $g \cong \{\sum \lambda_i Y_i \mid \lambda_i \in R\}$.

LEMMA 1. *If $[Y_i, Y_j] = A_{ij}Y_i + B_{ij}Y_j$, either $A_{ij} = B_{ij} = 0$ or $A_{ij} \neq 0$ and $B_{ij} \neq 0$.*

PROOF. Suppose, for example, $[Y_1, Y_2] = AY_1$, $A \neq 0$. If $i \geqq 3$, $0 = [[Y_1, Y_2], Y_i] + [[Y_i, Y_1], Y_2] + [[Y_2, Y_i], Y_1] = AA_{1i}Y_1 + AB_{1i}Y_i - AA_{1i}Y_1 + B_{1i}A_{2i}Y_2 + B_{1i}B_{2i}Y_i - AA_{2i}Y_2 - A_{1i}B_{2i}Y_1 - B_{1i}B_{2i}Y_i$, so the coefficient of $Y_i$, $AB_{1i}$, vanishes and $B_{1i} = 0$. In short, $[Y_1, Y_i] = A_{1i}Y_1$ for all $i$ and $Y_1$ generates a solvable ideal in $g_C$; contradiction.

LEMMA 2. *Each* ad $Y_i$ *is diagonalizable.*

PROOF. Since $[Y_i, Y_j] = A_{ij}Y_i + B_{ij}Y_j$, $(\text{ad } Y_i)(A_{ij}Y_i + B_{ij}Y_j) = B_{ij}(A_{ij}Y_i + B_{ij}Y_j)$. Therefore, ad $Y_i$ is diagonal with respect to the basis obtained from $\{Y_1, \ldots, Y_n\}$ by replacing $Y_j$ with $A_{ij}Y_i + B_{ij}Y_j$ whenever $B_{ij} \neq 0$.

REMARK. Let $\{Y_1, \ldots, Y_k\}$ be a maximal commuting subset of $\{Y_1, \ldots, Y_n\}$. Recall that an abelian subalgebra $a$ of a complex Lie algebra $g_C$ is contained in a Cartan subalgebra of $g_C$ if and only if ad $X$ is diagonalizable whenever $X \in a$ (see, for instance, exercise 21 on page 105 of Jacobson's book [2]). By the above lemma, then, there is a Cartan subalgebra $\mathscr{H}$ of $g_C$ containing $Y_1, \ldots, Y_k$. Let $g_C = \mathscr{H} \oplus \sum_\alpha Ce_\alpha$ be the corresponding decomposition of $g_C$. If $\langle\ ,\ \rangle$ is the Killing form of $g_C$ and $h \in \mathscr{H}$, recall that $[h, e_\alpha] = \langle h, \alpha\rangle e_\alpha$.

For each $j > k$, write $Y_j = h_j + \sum r_{\alpha, j}e_\alpha$ where $h_j \in \mathscr{H}$ and $r_{\alpha, j} \in C$.

LEMMA 3. *$Y_1, \ldots, Y_k$ generate $\mathscr{H}$.*

PROOF. If $j > k$, there is an $i \leqq k$ such that $[Y_i, Y_j] \neq 0$; thus $[Y_i, Y_j] = A_{ij}Y_i + B_{ij}Y_j = (A_{ij}Y_i + B_{ij}h_j) + \sum_\alpha B_{ij}r_{\alpha, j}e_\alpha = \sum r_{\alpha, j} \langle Y_i, \alpha\rangle e_\alpha$. By Lemma 1, $B_{ij} \neq 0$, so $h_j = -(A_{ij}/B_{ij})Y_i$. The lemma follows.

LEMMA 4. *If $j > k$, $r_{\alpha, j} \neq 0$ for exactly one root $\alpha$.*

PROOF. By the previous calculation, $r_{\alpha, j} \neq 0$ implies $B_{ij} = \langle Y_i, \alpha\rangle$. If $r_{\alpha, j} \neq 0$ and $r_{\beta, j} \neq 0$, $\langle Y_i, \alpha\rangle = \langle Y_i, \beta\rangle$ for all $i$, so $\langle h, \alpha - \beta\rangle = 0$ when $h = Y_1, \ldots, Y_k$ and thus whenever $h \in \mathscr{H}$ by Lemma 3. Since the Killing form is nondegenerate on $\mathscr{H}$, $\alpha = \beta$.

REMARK. Let $\alpha$ be the root corresponding to $j$; from now on write $Y_\alpha$ instead of $Y_j$. We can replace $e_\alpha$ by the equivalent eigenvector $r_{\alpha, j}e_\alpha$ and thus assume $Y_\alpha = h_\alpha + e_\alpha$.

LEMMA 5. *If $\alpha \neq \pm \beta$, then $[e_\alpha, e_\beta] = 0$.*

PROOF. $[h_\alpha + e_\alpha, h_\beta + e_\beta] = A_{\alpha\beta}(h_\alpha + e_\alpha) + B_{\alpha\beta}(h_\beta + e_\beta) = \langle h_\alpha, \beta\rangle e_\beta - \langle h_\beta, \alpha\rangle e_\alpha + [e_\alpha, e_\beta]$; since $\alpha \neq \pm \beta$, $[e_\alpha, e_\beta]$ is not a linear combination of $e_\alpha$, $e_\beta$, and elements of $\mathscr{H}$ unless it is zero.

LEMMA 6. *$Ce_\alpha \oplus Ce_{-\alpha} \oplus C[e_\alpha, e_{-\alpha}]$ is an ideal in $g_C$.*

PROOF. This subspace is clearly invariant under ad $\mathscr{H}$, ad $e_\alpha$, and ad $e_{-\alpha}$; if $\beta \neq \pm\alpha$, it is invariant under ad $e_\beta$ by the equation $[e_\beta, [e_\alpha, e_{-\alpha}]] = [[e_\beta, e_\alpha], e_{-\alpha}] + [e_\alpha, [e_\beta, e_{-\alpha}]]$ and Lemma 5.

REMARK. Write $g_C$ as a direct sum $g_1 \oplus \cdots \oplus g_\ell$ of simple ideals. Every ideal in $g_C$ has the form $g_{i_1} \oplus \cdots \oplus g_{i_r}$ for some choice of $1 \leqq i_1 < i_2 < \cdots < i_r \leqq \ell$. Since the dimension of the ideal $Ce_\alpha \oplus Ce_{-\alpha} \oplus C[e_\alpha, e_{-\alpha}]$ is three, it is one of the $g_i$; therefore $\sum_{\alpha>0}[Ce_\alpha \oplus Ce_{-\alpha} \oplus C[e_\alpha, e_{-\alpha}]]$ is a direct sum. This ideal contains all the $e_\alpha$, so $g_C = \sum_{\alpha>0} \oplus \{Ce_\alpha \oplus Ce_{-\alpha} \oplus C[e_\alpha, e_{-\alpha}]\}$. Notice that $\mathscr{H} = \sum_{\alpha>0} \oplus \{C[e_\alpha, e_{-\alpha}]\}$.

LEMMA 7. *If* $i \leqq k$ *and* $\langle Y_i, \alpha\rangle \neq 0$, $h_\alpha$ *is a non-zero real multiple of* $Y_i$ (*and consequently* $Y_i$ *is a non-zero real multiple of* $h_\alpha$). *Moreover*, $\langle Y_i, \alpha\rangle$ *is real.*

PROOF. $[Y_i, h_\alpha + e_\alpha] = \langle Y_i, \alpha\rangle e_\alpha = AY_i + B(h_\alpha + e_\alpha)$; thus $B = \langle Y_i, \alpha\rangle$ and $AY_i = -\langle Y_i, \alpha\rangle h_\alpha$. By Lemma 1, $B \neq 0$ implies $A \neq 0$.

LEMMA 8. *If* $i \leqq k$, *there is an* $\alpha$ *such that* $Y_i \in C[e_\alpha, e_{-\alpha}]$. *Conversely, each* $C[e_\alpha, e_{-\alpha}]$ *contains a unique* $Y_i$.

PROOF. For each $\alpha$, there is exactly one $i$ such that $\langle Y_i, \alpha\rangle \neq 0$. Indeed there is at least one such $i$ because $Y_1, \ldots, Y_k$ generate $\mathscr{H}$; if $\langle Y_i, \alpha\rangle \neq 0$ and $\langle Y_j, \alpha\rangle \neq 0$, $Y_i$ and $Y_j$ are non-zero multiples of $h_\alpha$ by the previous lemma, but $Y_i$ and $Y_j$ are linearly independent.

Let $\mathscr{S}$ be the set of all pairs $\{\alpha, -\alpha\}$ and consider the map $\mathscr{S} \to \{1, 2, \ldots, k\}$ defined by mapping $\{\alpha, -\alpha\}$ to the unique $i$ such that $\langle Y_i, \alpha\rangle \neq 0$. The decomposition $\mathscr{H} = \sum_{\alpha>0} \oplus C[e_\alpha, e_{-\alpha}]$ shows that $|\mathscr{S}| = k$; since the map just defined is clearly onto, it is one-to-one. Thus each $Y_i$ is associated with a unique pair $\{\alpha, -\alpha\}$ such that $\langle Y_i, \alpha\rangle \neq 0$. But $Y_i \in \mathscr{H} = \sum_{\beta>0} \oplus C[e_\beta, e_{-\beta}]$ and $\langle \beta, [e_\nu, e_{-\nu}]\rangle \neq 0$ if and only if $\beta = \pm \nu$, so $Y_i \in C[e_\alpha, e_{-\alpha}]$.

Finally $Y_1, \ldots, Y_k$ generate $\mathscr{H} = \sum_{\beta>0} \oplus C[e_\beta, e_{-\beta}]$ so each $C[e_\beta, e_{-\beta}]$ must contain a $Y_i$.

LEMMA 9. *If* $Y_\alpha = h_\alpha + e_\alpha$, *then* $h_\alpha \in C[e_\alpha, e_{-\alpha}]$.

PROOF. Let $Y_i \in C[e_\alpha, e_{-\alpha}]$. Since $\langle Y_i, \alpha\rangle \neq 0$, $h_\alpha$ is a non-zero multiple of $Y_i$ by Lemma 7.

REMARK. From now on, call the $Y_i$ associated with the pair $\{\alpha, -\alpha\}$ "$H_\alpha$". Notice that $H_\alpha$, $Y_\alpha$, $Y_{-\alpha}$ generate $Ce_\alpha \oplus Ce_{-\alpha} \oplus C[e_\alpha, e_{-\alpha}]$ and that $g$ is the set of real multiples of $\{H_\alpha, Y_\alpha, Y_{-\alpha}\}_{\alpha>0}$.

By Lemma 7, $\langle H_\alpha, \alpha\rangle$ is real; after multiplying $H_\alpha$ by a suitable non-zero real constant we can suppose $\langle H_\alpha, \alpha\rangle = 2$. By Lemma 7, $Y_\alpha = \lambda_\alpha H_\alpha + e_\alpha$ for $\lambda_\alpha$ real and non-zero. After multiplying $Y_\alpha$ by a suitable non-zero real constant (and choosing a new $e_\alpha$) we can suppose $Y_\alpha = H_\alpha + e_\alpha$. Similarly we can suppose $Y_{-\alpha} = H_\alpha + e_{-\alpha}$.

LEMMA 10. $[H_\alpha, e_\alpha] = 2e_\alpha$, $[H_\alpha, e_{-\alpha}] = -2e_{-\alpha}$, $[e_\alpha, e_{-\alpha}] = -4H_\alpha$.

PROOF. $[H_\alpha, e_\alpha] = \langle H_\alpha, \alpha\rangle e_\alpha = 2e_\alpha$; $[H_\alpha, e_{-\alpha}] = -\langle H_\alpha, \alpha\rangle e_{-\alpha} = -2e_{-\alpha}$. Finally $[H_\alpha + e_\alpha, H_\alpha + e_{-\alpha}] = -\langle H_\alpha, \alpha\rangle e_{-\alpha} - \langle H_\alpha, \alpha\rangle e_\alpha + [e_\alpha, e_{-\alpha}] = -2e_\alpha - 2e_{-\alpha} + [e_\alpha, e_{-\alpha}] = A(H_\alpha + e_\alpha) + B(H_\alpha + e_{-\alpha})$, so $A = B = -2$ and $[e_\alpha, e_{-\alpha}] = -4H_\alpha$.

REMARK. This completes the proof of Theorem 1 because

$$H_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; e_\alpha = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \text{and } e_{-\alpha} = \begin{pmatrix} 0 & 0 \\ -2 & 0 \end{pmatrix}$$

satisfy these commutation relations and $RH_\alpha \oplus Re_\alpha \oplus Re_{-\alpha} = sl(2, R)$.

THEOREM 2. *Let $g$ be a real Lie algebra with dimension $n$, $\mathscr{R}$ the radical of $g$. Let $\{X_1, \ldots, X_n\}$ be a minimal generating set for $g$. There is an isomorphism carrying $g$ to $sl(2, R) \times \cdots \times sl(2, R) \times \mathscr{R}$ and $X_1, \ldots, X_n$ to real scalar multiples of*

$$\cdots, 0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0,$$

$$0 \times \cdots \times \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0,$$

$$0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \times \cdots \times 0,$$

$$\cdots, 0 \times \cdots \times 0 \times v_i$$

*where $\{v_1, \ldots, v_\ell\}$ is a minimal generating set for $\mathscr{R}$ and $\ell = \dim \mathscr{R}$.*

PROOF. As before, real constants $A_{ij}$, $B_{ij}$ exist such that $[X_i, X_j] = A_{ij}X_i + B_{ij}X_j$. After renumbering if necessary, we can suppose that the elements $\bar{X}_1 \ldots, \bar{X}_{n-\ell}$ in $g/\mathscr{R}$ induced by $X_1, \ldots, X_{n-\ell}$ form a basis for $g/\mathscr{R}$. Since $[\bar{X}_i, \bar{X}_j] = A_{ij}\bar{X}_i + B_{ij}\bar{X}_j$, the subspace of $g$ generated by $X_1, \ldots, X_{n-\ell}$ is a subalgebra isomorphic to the semisimple algebra $g/\mathscr{R}$ and $X_1, \ldots, X_{n-\ell}$ is a minimal generating set for this subalgebra. By theorem 1, then, $g = sl(2, R) \oplus \cdots \oplus sl(2, R) \oplus \mathscr{R}$ and $X_1, \ldots, X_{n-\ell}$ are, up to scalar multiples,

$$\cdots, 0 \oplus \cdots \oplus \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \oplus \cdots \oplus 0 \oplus 0,$$

$$0 \oplus \cdots \oplus \begin{pmatrix} 1 & 2 \\ 0 & -0 \end{pmatrix} \oplus \cdots \oplus 0 \oplus 0,$$

$$0 \oplus \cdots \oplus \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \oplus \cdots \oplus 0 \oplus 0.$$

LEMMA 11. *$sl(2, R) \oplus \cdots \oplus sl(2, R)$ is an ideal in $g$.*

PROOF. If $j > n - \ell$, write $X_j = Y_j + Z_j$ where $Y_j \in sl(2, R) \oplus \cdots \oplus sl(2, R)$ and $Z_j \in \mathscr{R}$. Whenever $i < n - \ell$, $[X_i, Y_j + Z_j] = [X_i, Y_j] + [X_i, Z_j] = (A_{ij}X_i + B_{ij}Y_j) + B_{ij}Z_j$; since $\mathscr{R}$ is an ideal, $[X_i, Y_j] = A_{ij}X_i + B_{ij}Y_j$ and $[X_i, Z_j] = B_{ij}Z_j$. Look at this last equation carefully; it implies that whenever $X$ belongs to $sl(2, R) \oplus \cdots \oplus sl(2, R)$, there is a constant $\lambda(X)$ such that $[X, Z_j] = \lambda(X)Z_j$. The map $\lambda$: $sl(2, R) \oplus \cdots \oplus sl(2, R) \to R$ is clearly linear; by the Jacobi identity it vanishes on brackets. Since $sl(2, R) \oplus \cdots \oplus sl(2, R)$ is generated by such brackets, $\lambda$ is identically zero and $[sl(2, R) \oplus \cdots \oplus sl(2, R), Z_j] = 0$. But the $Z_j$ generate $\mathscr{R}$.

LEMMA 12. *If $j > n - \ell$, then $X_j \in \mathscr{R}$. Consequently $X_{n-\ell+1}, \ldots, X_n$ is a minimal generating set for $\mathscr{R}$.*

PROOF. Consider the equation in the second sentence of the previous proof; since $B_{ij} = 0$, $[X_i, X_j] = A_{ij}X_i$. In particular, the component of $Y_j$ in the *r-th* $sl(2, R)$ must be a matrix $U$ such that

$$\left[U, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] = \alpha \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \left[U, \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}\right] = \beta \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}, \left[U, \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix}\right] = \nu \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix}.$$

It is easy to show that $U = 0$.

REMARK. The affine algebra $a(m)$ is by definition $\{\langle A \mid v\rangle \mid A$ is an $m \times m$ matrix, $v \in R^m\}$; the Lie bracket is given by $[\langle A|v\rangle, \langle B|w\rangle] = \langle [A, B], Aw - Bv\rangle$.

THEOREM 3. *Let $g$ be a solvable real Lie algebra with dimension $n$, $\{X_1, \ldots, X_n\}$ a minimal generating set for $g$. There is an integer $m$, a linear subspace $\mathscr{D}$ of the set of all $m \times m$ diagonal matrics, and an isomorphism carrying $g$ to $\{\langle A \mid v\rangle \in a(m) | A \in \mathscr{D}\}$ and $X_1, \ldots, X_n$ to real scalar multiples of $\langle A_1 | 0\rangle, \ldots, \langle A_r | 0\rangle, \langle B_1 | e_1\rangle, \ldots, \langle B_m | e_m\rangle$ where $\{A_1, \ldots, A_r\}$ is a basis of $\mathscr{D}$, $\{e_1, \ldots, e_m\}$ is the canonical basis of $R^m$, and $B_1, \ldots, B_m$ belong to $\mathscr{D}$.*

The following lemmas supply the proof of this theorem.

LEMMA 13. *If $g$ is a solvable Lie algebra of dimension $n$ which admits a minimal generating set with $n$ elements, there is a basis $Z_1, \ldots, Z_n$ of $g$ such that whenever $i < j$, $[Z_i, Z_j] = A_{ij}Z_i$.*

PROOF. We work by induction on dim $g$. Since $g$ is solvable, there is an ideal $g_1 \subseteqq g$ with dim $g_1 = n - 1$. Let $X_1, \ldots, X_n$ minimally generate $g$ and suppose $X_n \notin g_1$. For each $i < n$ choose $\lambda_i$ so $\tilde{X}_i = X_i - \lambda_i X_n$ belongs to $g_1$; then $\{\tilde{X}_1, \ldots, \tilde{X}_{n-1}, X_n\}$ is a basis for $g$. Moreover, $\{\tilde{X}_1, \ldots, \tilde{X}_{n-1}, X_n\}$ is a minimal generating set, for $[\tilde{X}_i, X_n]$ can be written as a linear combination of $X_i$ and $X_n$ and thus as a linear combination of $\tilde{X}_i, X_n$; $[\tilde{X}_i, \tilde{X}_j]$ can be written as a linear combination of $\tilde{X}_i$, $\tilde{X}_j$, and $X_n$, but $g_1$ is a subalgebra, so the component of $X_n$ in this linear expression must vanish. Notice that $[\tilde{X}_i, X_n] = A_{in} \tilde{X}_i$ because $g_1$ is an ideal.

Separate the $\tilde{X}_i$ into two classes, those that do not commute with $X_n$ and those that do. Call the elements of the first class $Y_1, \ldots, Y_{m-1}$; let $Y_m = X_n$; call the elements of the second class $Y_{m+1}, \ldots, Y_n$. In short, $g$

has a minimal generating set $\{Y_1, \ldots, Y_{m-1}, Y_m, Y_{m-1}, \ldots, Y_n\}$ where whenever $i < m$, $[Y_i, Y_m] = \lambda_i Y_i$, $\lambda_i \neq 0$, and whenever $m < i$, $[Y_m, Y_i] = 0$.

Let $i < j < m$; $[[Y_i, Y_j], Y_m] = [[Y_i, Y_m], Y_j] + [Y_i, [Y_j, Y_m]]$ so $A_{ij}\lambda_i Y_i + B_{ij}\lambda_j Y_j = \lambda_i(A_{ij}Y_i + B_{ij}Y_j) + \lambda_j(A_{ij}Y_i + B_{ij}Y_j)$ and $\lambda_j A_{ij} = \lambda_i B_{ij} = 0$. Since $\lambda_i \neq 0$, and $\lambda_j \neq 0$, $A_{ij} = B_{ij} = 0$ and $[Y_i, Y_j] = 0$.

Let $i < m < j$; $[[Y_i, Y_j], Y_m] = [[Y_i, Y_m], Y_j] + [Y_i, [Y_j, Y_m]]$ so $A_{ij}\lambda_i Y_i = \lambda_i(A_{ij}Y_i + B_{ij}Y_j)$ and $\lambda_i B_{ij} = 0$. Since $\lambda_i \neq 0$, $B_{ij} = 0$ and $[Y_i, Y_j] = A_{ij}Y_i$.

The subalgebea of $g$ generated by $Y_{m+1}, \ldots, Y_n$ is solvable and has dimension less than $n$; by induction it has a basis $Z_{m+1}, \ldots, Z_n$ such that $[Z_i, Z_j] = A_{ij}Z_i$ whenever $i < j$. Clearly $Y_1, \ldots, Y_m, Z_{m+1}, \ldots, Z_n$ is the desired basis for $g$.

LEMMA 14. *If $g$ is a solvable Lie algebra of dimension $n$ which admits a minimal generating set with $n$ elements, there is a basis $Y_1, \ldots, Y_m, Y_{m+1}, \ldots, Y_n$ for $g$ such that*

a) *when $i < j$, $[Y_i, Y_j] = A_{ij}Y_i$,*

b) *when $1 \leqq i, j \leqq m$, $[Y_i, Y_j] = 0$,*

c) *when $m + 1 \leqq i, j \leqq n$, $[Y_i, Y_j] = 0$, and*

d) *no non-trivial linear combination of $Y_{m+1}, \ldots, Y_n$ acts trivially on the space generated by $Y_1, \ldots, Y_m$.*

PROOF. By Lemma 13, there is a basis satisfying a). For each such basis, there is an $m$ such that the first $m$ elements commute and the first $m + 1$ elements do not commute. Choose a basis maximizing this $m$. This basis satisfies a) and b); we show it also satisfies c) and d).

If $i < j < k$, $[[Y_i, Y_j], Y_k] = [[Y_i, Y_k], Y_j] + [Y_i, [Y_j, Y_k]]$ so $A_{ij}A_{ik}Y_i = A_{ik}A_{ij}Y_i + A_{jk}A_{ij}Y_i$ and $A_{ij}A_{jk} = 0$. In short, $[Y_i, Y_j] = 0$ or $[Y_j, Y_k] = 0$.

Suppose $m + 1 < j < k \leqq n$ and $[Y_j, Y_k] \neq 0$. It is easy to see, using the calculation just concluded, that $Y_1, \ldots, Y_m, Y_j, Y_{m+1}, \ldots, \hat{Y}_j, \ldots, Y_n$ is a new basis satisfying a); at least the first $m + 1$ elements of this new basis commute, contradiction.

Suppose $\sum_{i=m+1}^{n} \lambda_i Y_i$ acts trivially on the subspace generated by $Y_1, \ldots, Y_m$ and $\lambda_j \neq 0$. Then $\sum_{i=m+1}^{n} \lambda_i Y_i, Y_1, \ldots, Y_m, Y_{m+1}, \ldots, \hat{Y}_j, \ldots, Y_n$ is a new basis satisfying a), and at least the first $m + 1$ elements of this new basis commute, contradiction.

REMARK. Let $Y_1, \ldots, Y_n$ be a basis with the properties described in the previous lemma. Notice that ad $Y_{m+1}, \ldots,$ ad $Y_n$ act on the space generated by $Y_1, \ldots, Y_m$. Consider the associated $m \times m$ matrices; each is diagonal. If $\mathscr{D}$ is the space spanned by these matrices, clearly $g \cong \{\langle A \mid v\rangle \in a(m) \mid A \in \mathscr{D}\}$.

LEMMA 15. *Let $A_1, \ldots, A_r$ be a basis for $\mathscr{D}$. Let $X_1 = \langle A_1 \mid v_1 \rangle, \ldots, X_r = \langle A_r | v_r \rangle$ belong to $g = \{\langle A | v \rangle \in a(m) \mid A \in \mathscr{D}\}$ and suppose $[X_i, X_j] = A_{ij}X_i + B_{ij}X_j$. There is an automorphism of $g$ taking $X_1, \ldots, X_r$ to $\langle A_1 | 0 \rangle, \ldots, \langle A_r | 0 \rangle$.*

PROOF. Since $[\langle A_i | v_i \rangle, \langle A_j | v_j \rangle] = \langle 0 | A_i v_j - A_j v_i \rangle = A_{ij} \langle A_i | v_i \rangle + B_{ij} \langle A_j | v_j \rangle$, $A_i v_j = A_j v_i$.

Consider the map $\phi(\langle \sum_i r A_i | v \rangle) = \langle \sum r_i A_i | v - \sum r_i v_i \rangle$. This map carries $\langle A_i | v_i \rangle$ to $\langle A_i | 0 \rangle$; it is an automorphism precisely because $A_i v_j = A_j v_i$.

REMARK. Clearly, Lemma 15 implies that any minimal generating set of $\{\langle A \mid v \rangle \in a(m) \mid A \in \mathscr{D}\}$ with $n$ elements is equivalent to $\{\langle A_1 \mid 0 \rangle, \ldots, \langle A_r \mid 0 \rangle, \langle B_1 \mid v_1 \rangle, \ldots, \langle B_m, v_m \rangle\}$ where $\{A_1, \ldots, A_r\}$ is a basis of $\mathscr{D}$ and $\{v_1, \ldots, v_m\}$ is a basis of $R^m$. Notice that $[\langle A_1 \mid 0 \rangle, \langle B_j \mid v_j \rangle] = \langle 0 \mid A_i v_j \rangle = A_{ij} \langle A_i | 0 \rangle + B_{ij} \langle B_j | v_j \rangle$, so each $A_i$ acts diagonally with respect to the basis $v_1, \ldots, v_m$. Let $e_1, \ldots, e_m$ be the standard basis of $R^m$ and choose a matrix $M$ such that $M v_i = e_i$; then $\phi \langle A \mid v \rangle = \langle MAM^{-1} | Mv \rangle$ maps $g$ to $\{\langle A \mid v \rangle \in a(m) \mid A \in M \mathscr{D} M^{-1} = \tilde{\mathscr{D}}\}$, $\langle A_i | 0 \rangle$ to $\langle MA_i M^{-1} \mid 0 \rangle$ and $\langle B_i \mid v_i \rangle$ to $\langle MB_i M^{-1} \mid e_i \rangle$.

THEOREM 4. *A Lie algebra $g$ of dimension $n$ admits a minimal generating set with $n$ elements if and only if it is isomorphic to $sl(2, R) \times \cdots \times sl(2, R) \times \{\langle A \mid v \rangle \in a(m) \mid A \in \mathscr{D}\}$ where $\mathscr{D}$ is a linear subspace of the set of all $m \times m$ diagonal matrices. If $X_1, \ldots, X_n$ is a minimal generating set for $g$ with $n$ elements, it is possible to choose the isomorphism so that $X_1, \ldots, X_n$ are taken to real scalar multiples of*

$$\cdots, 0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0 \times \langle 0 | 0 \rangle,$$

$$0 \times \cdots \times \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0 \times \langle 0 | 0 \rangle,$$

$$0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \times \cdots \times 0 \times \langle 0 | 0 \rangle,$$

*$0 \times \cdots \times 0 \times \langle A_1 | 0 \rangle, \cdots, 0 \times \cdots \times 0 \times \langle A_r \mid 0 \rangle, 0 \times \cdots \times 0 \times \langle B_1 \mid e_1 \rangle, \cdots, 0 \times \cdots \times 0 \times \langle B_m, e_m \rangle$ where $\{A_1, \ldots, A_r\}$ is a basis for $\mathscr{D}$, $\{e_1, \ldots, e_m\}$ is the canonical basis of $R^m$, and $B_j \in \mathscr{D}$.*

*This last set is a minimal generating set just in case $B_j = 0$ whenever two or more $A_i$ are non-zero on $e_j$, $B_j = \lambda_j A_{\sigma(j)}$ whenever exactly one $A_i$, say $A_{\sigma(j)}$, is non-zero on $e_j$, and $\tau B_j = \mu B_k$ whenever $B_k e_j = \tau e_j$ and $B_j e_k = \mu e_k$.*

PROOF. This is a summary of our previous results; the proof of the last claim is straightforward.

**III. The order of generation problem for solvable groups.**

THEOREM 5. *Let $G$ be a connected solvable $n$-dimensional Lie group, $\{X_1, \ldots, X_n\}$ a minimal generating set for $G$. The order of generation of $G$ with respect to $\{X_1, \ldots, X_n\}$ is $n$. Every element of $G$ can be written in the form* $\exp(t_1X_1) \circ \cdots \circ \exp(t_nX_n)$ *if and only if (in the notation of Theorem* 4) each $\lambda_j = 0$.

PROOF. By Theorem 3, the Lie algebra of $G$ is isomorphic to $\{\langle A \mid v\rangle \in a(m) \mid A \in \mathscr{D}\}$ where $\mathscr{D}$ is a linear subspace of the set of diagonal matrices. Let $A(m)$ be the affine group $\{\langle A, v\rangle \mid A \in GL(m, R), v \in R^m\}$; recall that $\langle A, v\rangle \circ \langle B, w\rangle = \langle AB, Aw + v\rangle$. Consider the group $\tilde{G} = \{\langle A, v\rangle \in A(m) \mid A \in \exp(\mathscr{D})\}$. Its Lie algebra is clearly $\{\langle A \mid v\rangle \in a(m) \mid A \in \mathscr{D}\}$. Since each element of $\mathscr{D}$ is diagonal, $\exp\colon \mathscr{D} \to \exp(\mathscr{D}) \subseteqq GL(m, R)$ is a homeomorphism, so $\{\langle A, v\rangle \in A(m) \mid A \in \exp \mathscr{D}\}$ is homeomorphic to $R^{\dim \mathscr{D}+m}$ and thus simple connected. Consequently $\tilde{G}$ must be the universal covering group of $G$. The center of $\tilde{G}$ is easily seen to be $\{\langle I, v\rangle \in A(m) \mid \mathscr{D}v = 0\}$; by general Lie theory, there is a discrete subgroup $N \subseteqq \{\langle I, v\rangle \mid \mathscr{D}v = 0\}$ such that $G \cong \tilde{G}/N$.

The generators of $g$ have the form $\langle A_i | 0\rangle$ or $\langle B_j | e_j\rangle$ where $B_j(e_j) = \mu_j e_j$. A short calculation shows that $\exp t\langle A_i \mid 0\rangle = \langle e^{tA_i}, 0\rangle$, $\exp t\langle B_j|e_j\rangle = \langle e^{tB_j}, te_j\rangle$ if $\mu_j = 0$, and $\exp t\langle B_j \mid e_j\rangle = \langle e^{tB_j}, (1/\mu_j)(e^{t\mu_j} - 1)\, e_j\rangle$ if $\mu_j \neq 0$.

By Sard's theorem [9], the order of generation of a Lie group of dimension $n$ with respect to any $\{X_1, \ldots, X_\ell\}$ is at least $n$. Consider a typical expression of length $n$ in $\tilde{G}$ involving all the generators; it has the form

$$\begin{aligned}\langle e^{t_1D_1}, \phi_1(t_1)\, e_{i_1}\rangle &\circ \cdots \circ \langle e^{t_nD_n}, \phi_n(t_n)\, e_{i_n}\rangle \\ &= \langle e^{\Sigma t_iD_i}, \phi_1(t_1)\, e_{i_1} + e^{t_1D_1}\phi_2(t_2)\, e_{i_2} + \cdots \\ &\qquad + e^{t_1D_1+\cdots+t_{n-1}D_{n-1}}\phi_n(t_n)\, e_{i_n}\rangle\end{aligned}$$

where each $D_i$ is one of $A_1, \ldots, A_r, B_1, \ldots, B_m$, each $e_{i_j}$ is one of $0, e_1, \ldots, e_m$, and each $\phi_i(t_i)$ is $t_i$ or $(1/\mu)(e^{t_i\mu} - 1)$. Moreover, $e_j$ occurs exactly once, say in the $\nu(j)$-th term. We want to make this expression equal $\langle \exp(\sum \varepsilon_i A_i), \sum \theta_j e_j\rangle$ by correctly choosing $t_1, \ldots, t_n$. This will be done as follows. First we shall choose $t$'s for the terms $\langle B_j \mid e_j\rangle$ where $\mathscr{D}e_j = 0$. Next we shall choose $t$'s for the terms $\langle B_j \mid e_j\rangle$ where $B_j = \lambda_j A_{\sigma(j)}$, $\lambda_j \neq 0$, $A_{\sigma(j)}(e_j) \neq 0$. Simultaneously we choose $t$'s for the terms $\langle A_i | 0\rangle$. Finally we shall choose $t$'s for the remaining $\langle B_j \mid e_j\rangle$, $B_j = 0$.

Consider first those $e_j$ for which $\mathscr{D}e_j = 0$. Then $\mu_j = 0$, $\phi_{\nu(j)}(t_{\nu(j)}) = t_{\nu(j)}$ and

$$\exp(\sum_{i=1}^{\nu(j)-1} t_iD_i)\, e_j = e_j.$$

In short, $e_j$ enters into the final product in the form $t_{\nu(j)}e_j$ and we are forced to choose $t_{\nu(j)} = \theta_j$; let this be done.

Leaving the difficult case until last, suppose $t$'s have been chosen for all terms except those of the form $\langle B_j \mid e_j \rangle$, $B_j = 0$. Consider a typical $\langle 0 \mid e_j \rangle$. The choice of $t_{\nu(j)}$ does not affect any of the terms of the form $\exp(\sum t_i D_i)$ and $e_j$ enters into the final product as $t_{\nu(j)}\exp(\sum r_i D_i)e_j$. Since $\exp(\sum t_i D_i)\, e_j$ is a non-zero multiple of $e_j$, there is a unique $t_{\nu(j)}$ such that $t_{\nu(j)} \exp(\sum t_i D_i)\, e_j$ equals $\theta_j e_j$.

It remains to choose $t$'s for $\langle A_i \mid 0 \rangle$ and $\langle B_j \mid e_j \rangle$. For each such $j$, there is exactly one $A_i$, $A_{\sigma(j)}$, such that $A_{\sigma(j)}e_j \neq 0$; $B_j = \lambda_j A_{\sigma(j)}$, $\lambda_j \neq 0$. Let us concentrate on a fixed $A_{\sigma(j)}$; call it $A$. Let $f_1, \ldots, f_s$ be the $\{e_j\}$ corresponding to this $A$; order the $f$'s so that $f_1$ occurs furthest to the left in the product being considered, $f_2$ occurs next, etc. Then $Af_i = \eta_i f_i$ where $\eta_i$ is a non-zero constant. Call the generator corresponding to $f_i$ $\langle \lambda_i A | f_i \rangle$, $\lambda_i \neq 0$; this involves an abuse of notation, since the subscript $i$ on $\lambda_i$ is supposed to refer to the $i$-th $e$ rather than the $i$-th $f$, but it will not matter.

If $\langle B_j | e_j \rangle$ is a generator and $B_j f_i \neq 0$, $e_j$ is one of the $f$'s. Indeed, $B_j$ is not zero, so $\mathscr{D} e_j = 0$ or else exactly one $A_k$ is non-zero on $e_j$ and $B_j$ is a multiple of that $A_k$; in this last case $A_k$ is clearly $A$ and $e_j$ is one of the $f$'s. If $\mathscr{D} e_j = 0$, apply the condition at the end of Theorem 4 to $\langle B_j | e_j \rangle$ and $\langle \lambda_i A \mid f_i \rangle$; $B_j f_i = \tau f_i$ so $\tau \lambda_i A = 0$, so $\tau = 0$.

Suppose the term corresponding to $\langle A \mid 0 \rangle$ occurs between the $r$-th and the $(r - 1)$-st $f_i$. Call the $t$ corresponding to $\langle \lambda_i A \mid f_i \rangle$ "$u_i$" and the $t$ corresponding to $\langle A \mid 0 \rangle$ "$u$". Consider the product $\langle \exp(\sum t_i D_i), \psi(t_1)\, e_{i_i} + \cdots \rangle$; the coefficient of $A$ in $\sum t_i D_i$ is $\lambda_1 u_1 + \cdots + \lambda_s u_s + u$, $f_1$ occurs as

$$\frac{1}{\lambda_1 \eta_1}(e^{u_1 \lambda_1 \eta_1} - 1) f_1,$$

$f_2$ as

$$\frac{1}{\lambda_2 \eta_2}(e^{u_2 \lambda_2 \eta_2} - 1) e^{\lambda_1 u_1 A} f_2,$$

$f_3$ as

$$\frac{1}{\lambda_3 \eta_3}(e^{u_3 \lambda_3 \eta_3} - 1) e^{(\lambda_1 u_1 + \lambda_2 u_2) A} f_3,$$

etc., up to $f_r$; $f_{r+1}$ occurs as

$$\frac{1}{\lambda_{r+1} \eta_{r+1}}(e^{u_{r+1} \lambda_{r+1} \eta_{r+1}} - 1) e^{(\lambda_1 u_1 + \cdots + \lambda_r u_r + u) A} f_{r+1},$$

etc. Consequently we must choose $u_1, \ldots, u_s, u$ so that (if $f_i = e_{\tau(i)}$)

$$\lambda_1 u_1 + \cdots + \lambda_s u_s + u = \varepsilon_{\sigma(j)},$$

$$\frac{1}{\lambda_1\eta_1}(e^{u_1\lambda_1\eta_1} - 1) = \theta_{\tau(1)}$$

$$\frac{1}{\lambda_2\eta_2}(e^{u_2\lambda_2\eta_2} - 1)e^{\lambda_1 u_1\eta_2} = \theta_{\tau(2)}$$

$$\vdots$$

$$\frac{1}{\lambda_r\eta_r}(e^{u_r\lambda_r\eta_r} - 1)e^{(\lambda_1u_1+\cdots+\lambda_{r-1}u_{r-1})\eta_r} = \theta_{\tau(r)}$$

$$\frac{1}{\lambda_{r+1}\eta_{r+1}}(e^{u_{r+1}\lambda_{r+1}\eta_{r+1}} - 1)e^{(\lambda_1u_1+\cdots+\lambda_ru_r+u)\eta_{r+1}} = \theta_{\tau(r+1)}$$

$$\vdots$$

$$\frac{1}{\lambda_s\eta_s}(e^{\mu_s\lambda_s\eta_s} - 1)e^{(\lambda_1u_1+\cdots+\lambda_{s-1}u_{s-1}+u)\eta_s} = \theta_{\tau(s)}$$

Substituting the first equation in the last $s - r$ equations and reordering, we have

$$e^{u_1\lambda_1\eta_1} - 1 = \lambda_1\eta_1\theta_{\tau(1)}$$

$$e^{u_2\lambda_2\eta_2} - 1 = \lambda_2\eta_2\theta_{\tau(2)}e^{-\lambda_1u_1\eta_2}$$

$$\vdots$$

$$e^{u_r\lambda_r\eta_r} - 1 = \lambda_r\eta_r\theta_{\tau(r)}e^{-(\lambda_1u_1+\cdots+\lambda_{r-1}u_{r-1})\eta_r}$$

$$1 - e^{-u_s\lambda_s\eta_s} = \lambda_s\eta_s\theta_{\tau(s)}e^{-\varepsilon_{\sigma(j)}\eta_s}$$

$$1 - e^{-u_{s-1}\lambda_{s-1}\eta_{s-1}} = \lambda_{s-1}\eta_{s-1}\theta_{\tau(s-1)}e^{(\lambda_su_s-\varepsilon_{\sigma(j)})\eta_{s-1}}$$

$$\vdots$$

$$1 - e^{-u_{r+1}\lambda_{r+1}\eta_{r+1}} = \lambda_{r+1}\eta_{r+1}\theta_{\tau(r+1)}e^{(\lambda_su_s+\cdots+\lambda_{r+2}\eta_{r+2}-\varepsilon_{\sigma(j)})\eta_{r+1}}$$

$$u = \varepsilon_{\sigma(j)} - \lambda_1u_1 - \cdots - \lambda_su_s$$

These equations can be solved successively provided $\lambda_1\eta_1\theta_{\tau(1)} \geqq 0, \ldots, \lambda_r\eta_r\theta_{\tau(s)} \geqq 0$, $\lambda_s\eta_s\theta_{\tau(s)} \leqq 0, \ldots, \lambda_{r+1}\eta_{r+1}\theta_{\tau(r+1)} \leqq 0$. Consequently $\langle \exp(\sum\varepsilon_iA_i), \sum\theta_je_j\rangle$ can be written in terms of some expression of length $n$; the order of the terms in this expression must be carefully chosen. Since the order of generation of $\tilde{G}$ is thus $\leqq n$, the order of generation of $G$ is $\leqq n$.

Our calculation shows that every element of $\tilde{G}$ can be written in terms of the fixed expression $\exp(t_1X_1) \circ \cdots \circ \exp(t_nX_n)$ if each $\lambda_i = 0$. If some $\lambda_i$ is non-zero, the expression $\exp(t_1X_1) \circ \cdots \circ \exp(t_nX_n)$ cannot give every element of $\tilde{G}$, for $e^{u_i\lambda_i\eta_i} - 1 > -1$ and $1 - e^{-u_i\lambda_i\eta_i} < 1$.

It follows that the expression cannot give every element of $G = \tilde{G}/N$. Indeed $N \subseteqq \{\langle I, v\rangle \mid \mathscr{D}v = 0\}$; if $\mathscr{D}v = 0$ and $v$ is written as a linear combination of $e_1, \ldots, e_m$, the coefficient of $f_i$ is zero because $Av = 0$, $A$ acts diagonally, and $Af_i \neq 0$. Thus elements in $\tilde{G}$ equivalent modulo $N$ have the same $f_i$ components; if one cannot be written in the form $\exp(t_1X_1) \circ \cdots \circ \exp(t_nX_n)$, neither can the others.

**IV. Reduction of the general case to the semisimple case.** Let $\tilde{SL}(2, R)$ be the universal covering group of $SL(2, R)$, The simply connected Lie group corresponding to the Lie algebra $g = sl(2, R) \times \cdots \times sl(2, R) \times \{\langle A \mid v\rangle \in a(m) \mid A \in \mathscr{D}\}$ is clearly $\tilde{G} = \tilde{SL}(2, R) \times \cdots \times \tilde{SL}(2, R) \times \{\langle A, v\rangle \in A(m) \mid A \in \exp \mathscr{D}\}$. Recall that the center of $\tilde{SL}(2, R)$ is isomorphic to $Z$ [4]; the center $\mathscr{C}$ of $\tilde{G}$ is thus $Z \times \cdots \times Z \times \{\langle I, v\rangle \mid \mathscr{D}v = 0\}$. If $G$ is a connected Lie group with Lie algebra $g$, $G \cong \tilde{G}/N$ for some discrete subgroup $N$ of $\mathscr{C}$.

THEOREM 6. *Let $N$ be a discrete subgroup of $Z \times \cdots \times Z \times \{\langle I, v\rangle \mid \mathscr{D}v = 0\}$ and suppose $\{X_1, \ldots, X_n\}$ is a minimal generating set for $g$, as given in theorem 4. Let the order of generation of $\tilde{SL}(2, R) \times \cdots \times \tilde{SL}(2, R)/\tilde{N}$ with respect to*

$$\cdots, 0 \times \cdots \times \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \times \cdots \times 0,$$

$$0 \times \cdots \times \begin{pmatrix}1 & 2\\ 0 & -1\end{pmatrix} \times \cdots \times 0,$$

$$0 \times \cdots \times \begin{pmatrix}1 & 0\\ -2 & -1\end{pmatrix} \times \cdots \times 0,$$

*be $M$, where $\tilde{N}$ is the image of $N$ under the projection $Z \times \cdots \times Z \times \{\langle I, v\rangle \mid \mathscr{D}v = 0\} \to Z \times \cdots \times Z$. The order of generation of $G = \tilde{G}/N$ with respect to $X_1, \cdots, X_n$ is $N + m + \dim \mathscr{D}$. There is a fixed expression $\exp(t_1X_{i_1}) \circ \exp(t_2X_{i_2}) \circ \cdots$ of length $M + m + \dim \mathscr{D}$ giving each element of $G$ just in case there is a fixed expression of length $M$ giving each element of $\tilde{SL}(2, R) \times \cdots \times \tilde{SL}(2, R)/\tilde{N}$ and each $\lambda_i = 0$.*

REMARK. We will later show that no fixed expression of length $M$ gives each element of $\tilde{SL}(2, R) \times \cdots \times \tilde{SL}(2, R)/\tilde{N}$. Consequently, unless $G$ is solvable no fixed expression of length $M + m + \dim \mathscr{D}$ gives each element of $G$.

PROOF. Let $\mathscr{F}$ be a family of expressions of length $M$ giving the entire group $\tilde{SL}(2, R) \times \cdots \times \tilde{SL}(2, R)/\tilde{N}$. Let $\mathscr{G}$ be a family of expressions of length $m + \dim \mathscr{D}$ giving the entire group $\{\langle A, v\rangle \in A(m) \mid A \in \exp \mathscr{D}\}$; such a $\mathscr{G}$ exists by Theorem 5. Write $\mathscr{F} \times \mathscr{G}$ for the set of all expressions of length $M + m + \dim \mathscr{D}$ obtained by multiplying expressions in $\mathscr{F}$ by expressions in $\mathscr{G}$. We claim $\mathscr{F} \times \mathscr{G}$ generates $G$. Indeed let $a_1 \times a_2$ be a representative of an element of $G$, where $a_1 \in \widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)$ and $a_2 \in \{\langle A, v\rangle \mid A \in \exp \mathscr{D}\}$. We can find $n_1 \in \tilde{N}$ and an expression in $\mathscr{F}$ giving $a_1 n_1$. Let $n_1 \times n_2 \in N$. We can find an expression in $\mathscr{G}$ giving $a_2 n_2$. Consequently there is an expression in $\mathscr{F} \times \mathscr{G}$ giving $a_1 n_1 \times a_2 n_2 = (a_1 \times a_2)(n_1 \times n_2)$. Thus the order of generation of $G$ is at most $M + m + \dim \mathscr{D}$. In particular if a single expression generates $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/\tilde{N}$ and each $\lambda_i = 0$, $\mathscr{F}$ and $\mathscr{G}$ can be chosen containing a single expression each, so $G$ is generated by one fixed expression.

Conversely let $\mathscr{H}$ be a family of expressions of fixed length $\ell$ generating $G$. Each expression in $\mathscr{H}$ has the form $\exp(t_1 X_{i_1}) \circ \cdots \circ \exp(t_\ell X_{i_\ell})$. Let $\tilde{\mathscr{H}}$ be the set of all expressions in $\mathscr{H}$ which involve each of the $m + \dim \mathscr{D}$ generators of $\{\langle A \mid v\rangle \in a(m) \mid A \in \mathscr{D}\}$ at least once.

Since $\{\langle A_1 \mid 0\rangle, \ldots, \langle A_r \mid 0\rangle, \langle B_1 \mid e_1\rangle, \ldots, \langle B_m \mid e_m\rangle\}$ is a minimal generating set for $\{\langle A \mid v\rangle \mid A \in \mathscr{D}\}$, the subalgebra generated by any $m + \dim \mathscr{D} - 1$ of these terms has dimension $m + \dim \mathscr{D} - 1$. Let $R_1, \ldots, R_P$ be the subgroups of $\{\langle A, v\rangle \in A(m) \mid A \in \exp \mathscr{D}\}$ corresponding to all such subalgebras. Each $R_i$ is a set of measure zero in $\{\langle A, v\rangle \mid A \in \exp \mathscr{D}\}$. Let $\tilde{\tilde{N}}$ be the image of $N$ under the map $Z \times \cdots \times Z \times \{\langle I, v\rangle \mid \mathscr{D}v = 0\} \to \{\langle I, v\rangle \mid \mathscr{D}v = 0\}$. Since $\tilde{\tilde{N}}$ is countable, $\bigcup_{i=1}^{P} \bigcup_{n_j \in \tilde{\tilde{N}}} R_i n_j^{-1}$ is a set of measure zero and we can choose $a_2 \in \{\langle A, v\rangle \mid A \in \exp \mathscr{D}\}$ not in any $R_i n_j^{-1}$ If $a_1 \in \widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)$, $a_1 \times a_2$ represents an element in $G$, so there is an element $n_1 \times n_2 \in N$ and an expression in $\mathscr{H}$ giving $(a_1 \times a_2)(n_1 \times n_2)$. But $a_2 n_2$ can only be given by an expression involving all generators of $\{\langle A \mid v\rangle \mid A \in \mathscr{D}\}$, so $\tilde{\mathscr{H}}$ is not empty and indeed the $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)$ terms of the expressions in $\tilde{\mathscr{H}}$ generate $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/\tilde{N}$. Consequently some expression in $\tilde{\mathscr{H}}$ involves at least $M$ generators of $sl(2, R) \times \cdots \times sl(2, R)$; all expressions in $\tilde{\mathscr{H}}$ involve at least $m + \dim \mathscr{D}$ generators of $\{\langle A \mid v\rangle \mid A \in \mathscr{D}\}$ so $\ell \geqq M + m + \dim \mathscr{D}$.

Finally, suppose $\mathscr{H}$ contains only one expression and $\ell = M + m + \dim \mathscr{D}$. By the argument just concluded, the $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)$ part of this expression has length $M$ and generates $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/\tilde{N}$. The $\{\langle A, v\rangle \mid A \in \exp \mathscr{D}\}$ part of the expression has length $m + \dim \mathscr{D}$ and generates $\{\langle A, v\rangle \mid A \in \exp \mathscr{D}\}/\{\langle I, v\rangle \mid \mathscr{D}v = 0\}$. By the last step in the proof of theorem 5, each $\lambda_i$ is zero.

**V. The order of generation problem for semisimple groups.** Define integer-valued functions $h_1(x)$, $h_2(x)$, and $h_3(x) = h_2(-x)$ on $R$ as follows: $h_i(x) = [3 \mid x \mid] + 3$ if $x \notin Z$ ($[x]$ denotes, of course, the greatest integer less than or equal to $x$); $h_1(0) = 0$, $h_2(0) = h_3(0) = 2$; if $n$ is a positive integer, $h_1(n) = h_2(n) = h_3(-n) = 3n + 3$; if $n$ is a negative integer, $h_1(n) = 3|n| + 3$ and $h_2(n) = h_3(-n) = 3|n| + 2$.

THEOREM 7. *Let $N$ be a subgroup of $Z^p = Z \times \cdots \times Z$. The order of generation of $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/N$ with respect to*

$$\cdots, 0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0,$$

$$0 \times \cdots \times \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0,$$

$$0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \times \cdots \times 0, \cdots$$

*is the smallest integer $M$ such that whenever $1 \leqq i_j \leqq 3$,*

$$\{(x_1, \ldots, x_p) \mid h_{i_1}(s_1) + \cdots + h_{i_p}(x_p) \leqq M\}$$

*contains a representative of each element in $R^p/N$.*

PROOF. The group $PSL(2, R) = SL(2, R)/\{\pm I\} = \widetilde{SL}(2, R)/Z$ acts on the projective line $P^1 = R \cup \{\infty\}$ by

$$x \xrightarrow{\begin{pmatrix} ab \\ cd \end{pmatrix}} \frac{ax + b}{cx + d}.$$

Call an ordered triple $(x_1, x_2, x_3)$ in $P^1 \times P^1 \times P^1$ *oriented* if there is a cyclic permutation $\sigma$ such that $-\infty < x_{\sigma(1)} < x_{\sigma(2)} < x_{\sigma(3)} \leqq \infty$. If $(x_1, x_2, x_3)$ and $(y_1, y_2, y_3)$ are oriented triples, $PSL(2, R)$ contains a unique element mapping $x_i$ to $y_i$.

Let $L$ be the universal covering space of $P^1$, $\tau: L \to P^1$ the covering map. Of course $L$ is homeomorphic to $R$. Choose this homeomorphism so that $\tau(0) = \infty$, $\tau(1/3) = -1$, $\tau(2/3) = 0$ and $x \to x + n$ is a covering transformation for each integer $n$.

There is a natural map $\psi$: $\widetilde{SL}(2, R) \to \{(a_L, a, b, c) \in L \times P^1 \times P^1 \times P^1 \mid \tau(a_L) = a, (a, b, c) \text{ an oriented triple}\}$ defined as follows. Suppose $\tilde{g} \in \widetilde{SL}(2, R)$. Let $\pi$: $\widetilde{SL}(2, R) \to PSL(2, R)$ be the canonical projection; $\pi(\tilde{g})$ maps $(\infty, -1, 0)$ to an oriented triple $(a, b, c)$. Choose a path $\nu(t)$: $[0, 1] \to \widetilde{SL}(2, R)$ starting at the identity and ending at $\tilde{g}$; $(\pi\nu(t))(\infty)$ is a path in $P^1$ starting at $\infty$ and ending at $a$. This path uniquely lifts to a path in $L$ starting at 0 and ending at a point $a_L$ over $a$. Let $\psi(\tilde{g}) = (a_L, a, c, b)$. The map $\psi$ is one-to-one and onto; it carries the center of $\widetilde{SL}(2, R)$ to $\{(n, \infty, -1, 0) \mid n \in Z\}$. Moreover, if $\psi(\tilde{g}) = (a_L, a, b, c)$ and $\psi(\tilde{h}) = (n, \infty, -1, 0)$, $\psi(\tilde{g}\tilde{h}) = (a_L + n, a, b, c)$. For details, see [4].

LEMMA 16. *Whenever $\tilde{g} \in \widetilde{SL}(2, R)$ satisfies $\psi(\tilde{g}) = (a_L, a, b, c)$, $\tilde{g}$ can be represented by an expression of length* $[3|a_L|] + 3$. *For each $a \in P^1$ there is a triple $(a, b, c)$ such that no $\tilde{g}$ for which $\psi(\tilde{g}) = (a_L, a, b, c)$ and $a_L \neq 0$ can be represented by an expression of length* $[3|a_L|] + 2$.

PROOF. For convenience let $X$, $Y$, and $Z$ denote the one parameter groups

$$\exp t\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \exp t\begin{pmatrix}1 & 2\\ 0 & -1\end{pmatrix}, \text{ and } \exp t\begin{pmatrix}1 & 0\\ -2 & -1\end{pmatrix}$$

respectively. Notice that each element of $X$ leaves 0 and $\infty$ fixed; $X$ acts transitively on $(-\infty, 0)$ and $(0, \infty)$. Similarly the fixed points of $Y$ are $-1$, $\infty$ and those of $Z$ are $-1$, 0; $Y$ and $Z$ act transitively on the connected components of the complements of their fixed point sets. We shall think of $X$, $Y$, and $Z$ in four different ways: as one parameter groups in $\widetilde{SL}(2, R)$, as the corresponding one parameter groups in $PSL(2, R)$, as one parameter groups acting on $P^1$, and as one parameter groups acting on $L$. No confusion results (we hope)!

```
            <-------  ------->  <-------  ------->  <-------  ------->
exq(tX):—*——o———#——*——o———#——*——o———#——*—
        -4/3  -1   -2/3 -1/3  0    1/3  2/3   1    4/3  5/3
```

In $L$, $X$ leaves $0 + Z$ and $2/3 + Z$ fixed and acts transitively on $(-1/3 + n, 0 + n)$ and $(0 + n, 2/3 + n)$ (see figure). Similarly $Y$ leaves $0 + Z$ and $1/3 + Z$ fixed and acts transitively on $(0 + n, 1/3 + n)$ and $(1/3 + n, 1 + n)$; $Z$ leaves $1/3 + Z$ and $2/3 + Z$ fixed and acts transitively on $(-1/3 + n, 1/3 + n)$ and $(1/3 + n, 2/3 + n)$. During the arguments in the following pages the reader will often find it useful to draw orbit pictures in $L$.

Notice that $Z(0)$ can be any point in $[0, 1/3)$, $XZ(0)$ any point in $[0, 2/3)$, $YXZ(0)$ any point in $[0, 1)$, etc. Similarly, $Z(0)$ can be any point in $(-1/3, 0]$, $YZ(0)$ any point in $(-2/3, 0]$, $XYZ(0)$ any point in $(-1, 0]$, etc. In short, for each $a_L \in (-k/3, k/3)$ there is an expression $\ldots Z$ of length $k$ mapping 0 to $a_L$. The inverse of the projection of this expression to $PSL(2, R)$ maps $a$ to $\infty$ and so maps $(a, b, c)$ to $(\infty, \tilde{b}, \tilde{c})$.

If $-1 < \tilde{c}$, there is an element in $Y$ mapping 0 to $\tilde{c}$. If this expression maps $\tilde{\tilde{b}}$ to $\tilde{b}$, it maps $(\infty, \tilde{\tilde{b}}, 0)$ to $(\infty, \tilde{b}, \tilde{c})$; since all triples are oriented, $\tilde{\tilde{b}} < 0$ and there is an element in $X$ mapping $-1$ to $\tilde{\tilde{b}}$, so $\ldots ZYX$ maps $(\infty, -1, 0)$ to $(a, b, c)$ and $0 \in L$ to $a_L$.

If $\tilde{c} \leqq -1$, $\tilde{b} < \tilde{c} < 0$ and there is an element in $X$ mapping $-1$ to $\tilde{b}$. Let this expression map $\tilde{\tilde{c}}$ to $\tilde{c}$; then $(\infty, -1, \tilde{\tilde{c}})$ maps to $(\infty, \tilde{b}, \tilde{c})$, so $-1 < \tilde{\tilde{c}}$ and there is an element in $Y$ mapping 0 to $\tilde{\tilde{c}}$. Thus $\ldots ZXY$ maps $(\infty, -1, 0)$ to $(a, b, c)$ and $0 \in L$ to $a_L$.

Thus whenever $-k/3 < |a_L| < k/3$, the element in $\widetilde{SL}(2, R)$ corresponding to $(a_L, a, b, c)$ can be written as a product with $k + 2$ terms. The first part of the lemma follows.

As for the second part of the lemma, if $a \in [\infty, -1]$ let $b = -1$, $c = 0$. If $a \in [-1, 0)$, let $b = 0$, $c = \infty$. If $a \in [0, \infty)$, let $b = \infty$, $c = -1$. We shall discuss the case $a \in [\infty, -1]$, leaving all other cases to the reader.

Consider an expression in $X$, $Y$, $Z$ of length $k + 2$, where $k = [3|a_L|]$. One of $\infty$, $-1$, $0$ is left fixed by the first two terms in this expression. Let $\ell \in L$ be a point over this fixed element; $\ell$ is equivalent to 0, 1/3, or 2/3. The image of $\ell$ under the third term in the expression must belong to $(\ell - 1/3, \ell + 1/3)$, its image under the fourth term must belong to $(\ell - 2/3, \ell + 2/3)$, etc., and its final image must belong to $(\ell - k/3, \ell + k/3)$.

If the first two terms leave $\infty$ fixed, the image of 0 in $L$ belongs to $(-k/3, k/3)$ and so cannot equal $a_L$. Otherwise, suppose for a moment $a_L > 0$. Since $\tau(a_L) = a \in [\infty, -1)$, $a_L = m + \eta$, where $m$ is a non-negative integer and $0 \leqq \eta < 1/3$; $[3a_L] = 3m$, $k = 3m$. If the first two terms leave $-1$ fixed, the image of 1/3 in $L$ belongs to $(1/3 - m, 1/3 + m)$; since $-1$ is mapped to $-1$, this image must be equivalent to 1/3. Hence the image of 1/3 is at most $1/3 + m - 1$; since $0 < 1/3$, the image $a_L$ of 0 is smaller than the image of 1/3, and so smaller than $1/3 + m - 1$, contradiction. If the first two terms leave 0 fixed, the image of 2/3 in $L$ belongs to $(2/3 - m, 2/3 + m)$; since 0 is mapped to 0, this image must be equivalent to 2/3 and so must be at most $2/3 + m - 1$; as before, $a_L < 2/3 + m - 1$, contradiction.

If $a_L < 0$, let $a_L = -m + \eta$, where $m$ is a non-negative integer and $\eta \in [0, 1/3)$; then $[3|a_L|] = 3m - 1$ or 3m and at any rate $k \leqq 3m$. If the first two terms leave $-1$ fixed, the image of $-2/3$ in $L$ belongs to $(-2/3 - m, -2/3 + m)$ and is equivalent to $-2/3$, so it is greater than or equal to $-2/3 - m + 1$; since $-2/3 < 0$, the image $a_L$ of 0 is greater than the image of $-2/3$, so $-2/3 - m + 1 < a_L$, contradiction. If the first two terms leave 0 fixed, the image of $-1/3$ in $L$ belongs to $(-1/3 - m, 1/3 + m)$ and is equivalent to $-1/3$, so it is greater than or equal to $-1/3 - m + 1$; as before $-1/3 - m + 1 < a_L$, contradiction.

LEMMA 17. *Let* $(\infty, b, c)$ *be an oriented triple. There is an* $i$, $1 \leqq i \leqq 3$, *such that whenever* $\tilde{g} \in \widetilde{SL}(2, R)$ *and* $\psi(g) = (n, \infty, b, c)$, $\tilde{g}$ *can be represented by an expression of length* $h_i(n)$. *For each* $i$, *there is a triple* $(\infty, b, c)$ *such that no* $\tilde{g}$ *for which* $\psi(\tilde{g}) = (n, \infty, b, c)$ *can be represented by an expression of length* $h_i(n) - 1$.

PROOF. The element corresponding to $(n, \infty, -1, 0)$ can be represented by an expression of length $h_1(n)$, but not by an expression of length $h_1(n) - 1$. Indeed, if $n = 0$, this element is just the identity and the result is obvious. Otherwise Lemma 16 applies.

If $-1 < b$ or $0 < c$, the element corresponding to $(n, \infty, b, c)$ can be represented by an expression of length $h_2(n)$; if $-1 < b < 0$ and $0 < c$, this element cannot be represented by an expression of length $h_2(n) - 1$. Indeed suppose $-1 < b$. If $n > 0$, Lemma 16 shows that the element corresponding to $(n, \infty, b, c)$ can be written as a product of length $h_2(n)$. It is easy to see that $(0, \infty, b, c)$ can be written as a product of length 2. Suppose $n < 0$; then $h_2(n) = 3|n| + 2$. But $1/3$ in $L$ can be mapped to any point in $(0, 1/3)$ by a single term, to any point in $(-1/3, 1/3)$ by two terms, etc., and so to any point in $(-(3|n| - 1)/3, 1/3) = (-|n| + 1/3, 1/3)$ by an expression with $3|n|$ terms. In particular, it can be mapped by such an expression to the element $b_L$ in $(-|n| + 1/3, -|n| + 1)$ such that $\tau(b_L) = b$. As in the proof of Lemma 16, it is then easy to find an expression of length $3|n| + 2$ mapping $1/3$ to $b_L$ and $(\infty, -1, 0)$ to $(\infty, b, c)$. Since $0 < 1/3$, the image of 0 in $L$ must be smaller than the image of $1/3$ in $L$, so $a_L < b_L < -|n| + 1$. Since $a_L$ is an integer, $|a_L| \leqq -|n|$. But expressions of length $3|n| + 2$ carry 0 into $(-|n| - 2/3, |n| + 2/3)$, so $a_L = -|n|$ and the expression of length $3|n| + 2$ obtained yields the element in $\widetilde{SL}(2,R)$ corresponding to $(-|n|, \infty, b, c)$. A similar argument works when $c < 0$.

Suppose $-1 < b < 0$ and $0 < c$. No expression of length $h_2(n) - 1$ can represent $(n, \infty, b, c)$. Indeed if $n = 0$, $h_2(n) - 1 = 1$ and all expressions with one term leave $-1$ or 0 fixed. If $n > 0$, one of $\infty, -1, 0$ is left fixed by the first two terms of a given expression of length $h_2(n) - 1 = 3n + 2$. If this element is $\infty$, 0 in $L$ is mapped to $a_L < n$. If it is $-1$, $1/3$ in $L$ is mapped to an element less than $n + 1/3$ and equivalent to an element in $(1/3, 2/3)$ and consequently less than $n - 2/3$, so $a_L < n - 2/3$. If 0 is left fixed by the first two terms, $2/3$ in $L$ is mapped to an element less than $n + 2/3$ and equivalent to an element in $(2/3, 1)$ and consequently less than $n$, so $a_L < n$.

If $n < 0$, one of $\infty, -1, 0$ is left fixed by the first two terms of a given expression of length $h_2(n) - 1 = 3|n| + 1$. If this element is $\infty$, $-|n| - 1/3 < a_L$. If it is $-1$, $-2/3$ in $L$ is mapped to an element greater than $-|n| - 1/3$ and equivalent to an element in $(1/3, 2/3)$ and consequently greater than $-|n| + 1/3$, so $-|n| + 1/3 < a_L$. If 0 is left fixed by the first two terms, $-1/3$ in $L$ is mapped to an element greater than $-|n|$, so $-|n| < a_L$.

If $b < -1$ or $c < 0$, the element corresponding to $(n, \infty, b, c)$ can be represented by an expression of length $h_3(n)$; if $b < -1$ and $-1 < c < 0$, this element cannot be represented by an expression of length $h_3(n) - 1$. The proof is exactly as before.

The three statements just proved clearly imply Lemma 17.

CONCLUSION OF THE PROOF OF THEOREM 7. Let $\tilde{g}_1 \times \cdots \times \tilde{g}_p$ belong to $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)$, and suppose $\psi(\tilde{g}_j) = (a_{L,j}, a_j, b_j, c_j)$. By Lemmas 16 and 17, there is an $i_j$, $1 \leqq i_j \leqq 3$, such that whenever $n \in Z$, the element in $\widetilde{SL}(2, R)$ corresponding to $(a_{L,j} + n, a_j, b_j, c_j)$ can be written as a product of at most $h_{i_j}(a_{L,j} + n)$ terms. Since $(a_{L,1}, \ldots, a_{L,p})$ is equivalent modulo $N$ to an element of $\{(x_1, \ldots, x_p) \mid h_{i_1}(x_1) + \cdots + h_{i_p}(x_p) \leqq M\}$, there is an $n_1 \times \cdots \times n_p$ in $N$ such that $\tilde{g}_1 n_1 \times \cdots \times \tilde{g}_p n_p$ can be written as a product of length at most $M$.

Conversely suppose the order of generation of $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2,R)/N$ is $M$. Let $(x_1, \ldots, x_p) \in R^p$ and let $h_{i_1}, \ldots, h_{i_p}$ be given, $1 \leqq i_j \leqq 3$. By Lemmas 16 and 17, for each $j$ there is an oriented triple $(\tau(x_j), b_j, c_j)$ such that whenever $n \in Z$, the element $\tilde{g}_j$ in $\widetilde{SL}(2, R)$ corresponding to $(x_j + n, \tau(x_j), b_j, c_j)$ cannot be written as a product of fewer than $h_{i_j}(x_j + n)$ terms. But $\tilde{g}_1 \times \cdots \times \tilde{g}_p$ is equivalent to an element that can be written as a product of length at most $M$, so there is an element $n_1 \times \cdots \times n_p$ in $N$, depending on the $x_j$'s and the $i_j$'s, such that $h_{i_j}(x_1 + n_1) + \cdots + h_{i_p}(x_p + n_p) \leqq M$.

Corollary 1. *The order of generation of $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/N$ is finite if and only if $N$ has maximal rank.*

Proof. By the theorem, the order of generation is finite if and only if there exists a compact subset of $R^p$ containing a representative of each element of $R \times \cdots \times R/N$; it is well known that this happens just in case $N$ has maximal rank.

Corollary 2. *If $n > 0$, the order of generation of $\widetilde{SL}(2, R)/nZ$ is* $[(3n + 6)/2]$.

Proof. Notice that $\{x \mid h_1(x) \leqq M\} = (-(M - 2)/3, (M - 2)/3)$ whenever $M \geqq 3$. If $(M - 2)/3$ is not an integer, $\{x \mid h_2(x) \leqq M\} = (-(M - 2)/3, (M - 2)/3)$ and $\{x \mid h_3(x) \leqq M\} = (-(M - 2)/3, (M - 2)/3)$. If $(M - 2)/3$ is an integer, $\{x \mid h_2(x) \leqq M\} = [-(M - 2)/3, (M - 2)/3)$ and $\{x \mid h_3(x) \leqq M\} = (-(M - 2)/3, (M - 2)/3]$. The order of generation of $\widetilde{SL}(2, R)/nZ$ is thus the smallest $M$ such that $[-n/2, n/2] \subseteqq (-(M - 2)/3, (M - 2)/3)$; a little thought shows that $M = [3n + 6)/2]$.

Remark. Think of $P^1$ as a circle. Using our results, the reader can show that $\widetilde{SL}(2, R)/nZ$, $n$ even, contains a unique element of maximal length; this element turns the circle through $n/2$ revolutions. If $n$ is odd, $\widetilde{SL}(2, R)/nZ$ contains a family of elements of maximal length; each such element turns the circle through $(n - 1)/2$ revolutions and then twists it an extra half turn so that each fixed point goes into the open interval bounded by the other two fixed points.

Remark. When $N \subseteqq Z \times \cdots \times Z$ has maximal rank, routine algebra shows that $N$ can be generated by the row vectors of a triangular matrix

$$\begin{bmatrix} n_{11} & n_{12} & n_{13} & \cdots & n_{1p} \\ 0 & n_{22} & n_{23} & \cdots & n_{2p} \\ 0 & 0 & n_{33} & \cdots & n_{3p} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & n_{pp} \end{bmatrix}$$

THEOREM 8. a) *The order of generation of* $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/N$ *is less than or equal to* $[(3n_{11} + 6)/2] + \cdots + [(3n_{pp} + 6)/2]$.

b) *If the off-diagonal entries in the above matrix vanish, the order of generation of* $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/N$ *is exactly* $[(3n_{11} + 6)/2] + \cdots + [(3n_{pp} + 6)/2]$.

PROOF. Let $\tilde{g} = \tilde{g}_1 \times \cdots \times \tilde{g}_p$ belong to $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)$. The order of generation of $\widetilde{SL}(2, R)/n_{11}Z$ is $[(3n_{11} + 6)/2]$, so $\tilde{g}$ is equivalent via a multiple of $n_{11} \times n_{12} \times \cdots \times n_{1p}$ to $\tilde{h}_1 \times \tilde{g}_2^1 \times \cdots \times \tilde{g}_p^1$ where $\tilde{h}_1$ can be written as a product of $[(3n_{11} + 6)/2]$ terms. Similarly $\tilde{h}_1 \times \tilde{g}_2^1 \times \cdots \times \tilde{g}_p^1$ is equivalent via a multiple of $0 \times n_{22} \times \cdots \times n_{2p}$ to $\tilde{h}_1 \times \tilde{h}_2 \times \cdots \times \tilde{g}_p^{11}$ where $h_2$ can be written as a product of $[(3n_{22} + 6)/2]$ terms. Continue. Eventually $\tilde{g}$ is equivalent modulo $N$ to $\tilde{h}_1 \times \cdots \times \tilde{h}_p$ where each $\tilde{h}_i$ can be written as a product of $[(3n_{ii} + 6)/2]$ terms.

Suppose next that all off-diagonal entries are zero. There are elements $\tilde{g}_1, \ldots, \tilde{g}_p$ in $\widetilde{SL}(2, R)$ such that no element equivalent to $\tilde{g}_i$ via a multiple of $n_{ii}$ can be written using fewer than $[(3n_{ii} + 6)/2]$ terms. Consequently no element equivalent to $\tilde{g}_1 \times \cdots \times \tilde{g}_p$ via $N$ can be written with fewer than $[(3n_{11} + 6)/2] + \cdots + [(3n_{pp} + 6)/2]$ terms.

REMARK. One can calculate the order of generation of $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/N$ for a fixed $N$ in a finite number of steps. Indeed, $h_{i_1}(x_1) + \cdots + h_{i_p}(x_p)$ is constant on subsets of the form $S_1 \times \cdots \times S_p$ where $S_i = (\ell/3, \ell + 1/3)$ or $S_i = \{\ell/3\}$. Each such subset is entirely inside or entirely outside $\{(x_1, \ldots, x_p) \mid h_{i_1}(x_1) + \cdots + h_{i_p}(x_p) \leqq M\}$. Moreover $(S_1 \times \cdots \times S_p) \circ (n_1 \times \cdots \times n_p)$ is again a set of the form $\tilde{S}_1 \times \cdots \times \tilde{S}_p$. Each $(x_1, \ldots, x_p)$ is equivalent to some $(y_1, \ldots, y_p)$ such that $|y_i| \leqq n_{ii}/2$. Consequently each $S_1 \times \cdots \times S_p$ is equivalent to $\tilde{S}_1 \times \cdots \times \tilde{S}_p$ such that $\tilde{S}_i \subseteqq (-(3n_{ii} + 2)/6, (3n_{ii} + 2)/6)$. The set $\mathscr{C}$ of such $\tilde{S}_1 \times \cdots \times \tilde{S}_p$ is finite. The order of generation is less than or equal to $M$ if and only if whenever $1 \leqq i_j \leqq 3$, each element of $\mathscr{C}$ is equivalent modulo $N$ to an element of $\mathscr{C}$ inside $\{x_1, \ldots, x_p) \mid h_{i_1}(x_1) + \cdots + h_{i_p}(x_p) \leqq M\}$.

In practice, it pays to proceed in a less systematic manner.

EXAMPLE. Let $N$ be the subgroup of $Z \times Z$ generated by $1 \times 2$ and $0 \times 5$. By Theorem 8, the order of generation of $\widetilde{SL}(2, R) \times \widetilde{SL}(2, R)/N$ is at most $[(3 + 6)/2] + [(15 + 6)/2] = 14$. However the actual order of generation is 11.

Indeed any point in $R^2$ is equivalent to a point in $\{(x_1, x_2) \mid |x_1| \leqq 1/2, |x_2| \leqq 5/2\}$. If $3/2 \leqq x_2 \leqq 5/2$, $(x_1, x_2)$ is equivalent to $(x_1 - 1, x_2 - 2)$ and $-3/2 \leqq x_1 - 1 \leqq -1/2$, $-1/2 \leqq x_2 - 2 \leqq 1/2$. If $-5/2 \leqq x_2 \leqq -3/2$, $(x_1, x_2)$ is equivalent to $(x_1 + 1, x_2 + 2)$ and $1/2 \leqq x_1 + 1 \leqq 3/2$, $-1/2 \leqq x_2 + 2 \leqq 1/2$. Thus any point in $R^2$ is equivalent to a point in $\{(x_1, x_2) \mid |x_1| \leqq 3/2, |x_2| \leqq 1/2\} \cup \{(x_1, x_2) \mid |x_1| \leqq 1/2, |x_2| \leqq 3/2\}$ For any $i = 1, 2$, or $3$, $h_i(x) \leqq 4$ if $|x| \leqq 1/2$ and $h_i(x) \leqq 7$ if $|x| \leqq 3/2$ so every point is equivalent to a point $(x_1, x_2)$ such that $h_{i_1}(x_1) + h_{i_2}(x_2) \leqq 11$ and the order of generation is at most 11.

However consider $(-1/2, 3/2)$; it is easy to see that $h_1(-1/2 + n) + h_1(3/2 + 2n + 5m) \geqq 11$ for all $m$ and $n$, so the order of generation is at least 11.

THEOREM 9. *Suppose $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/N$ has order of generation $M$. No fixed expression of length $M$ generates $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/N$.*

PROOF. Pick $\tilde{g} \in \widetilde{SL}(2, R)$ covering

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

in $\widetilde{SL}(2, R)$. The map $g \to \tilde{g}g\tilde{g}^{-1}$ is an automorphism of $\widetilde{SL}(2, R)$ fixing the center $Z$ of $\widetilde{SL}(2, R)$ pointwise; the induced automorphism of $sl(2, R)$ takes

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ to } -\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \text{ to } \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \text{ to } -\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Consequently, any expression of length $M$ giving each element of $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/N$ can be carried by a suitable automorphism of $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)/N$ to a second such expression so that the first appearances of

$$0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0 \text{ and } 0 \times \cdots \times \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \times \cdots \times 0$$

appear to the right of the first appearance of

$$0 \times \cdots \times \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \times \cdots \times 0$$

in the new expression. From now on, fix such a hypothetical expression. An element $\tilde{g}_1 \times \cdots \times \tilde{g}_p$ in $\widetilde{SL}(2, R) \times \cdots \times \widetilde{SL}(2, R)$ for which

$\psi(\tilde{g}_i) = (a_{L,i}, a_i, b_i, c_i)$ can be written in terms of this expression only if $a_{L,1} \times \cdots \times a_{L,p}$ is in $A_1 \times \cdots \times A_p$ where $A_i \subseteqq L$ is the interval of images of 0 in $L$ under the induced action on $L$ of the terms affecting the $i$-th component of the above expression. Each element of $R^p$ must be equivalent modulo $N$ to an element in $A_1 \times \cdots \times A_p$.

Suppose $n_i$ terms in the expression affect the $i$-th $\tilde{SL}(2, R)$. By an argument that has become standard in this paper, $A_i \subseteqq (-(n_i - 2)/3, (n_i - 2)/3)$. Let $h(x) = [3|x|] + 3$; notice that $h(x) \geqq h_j(x)$ whenever $1 \leqq j \leqq 3$. Since $h \leqq n_i$ on $A_i$, $A_1 \times \cdots \times A_p \subseteqq \{(x_1, \ldots, x_p) \mid h(x_1) + \cdots + h(x_p) \leqq n_1 + \cdots + n_p = M\}$. We are going to show that each point in $A_1 \times \cdots \times A_p$ is equivalent to a point in $\{(x_1, \ldots, x_p) \mid h(x_1) + \cdots + h(x_p) \leqq M - 1\}$. It will follow that the order of generation of $\tilde{SL}(2, R) \times \cdots \times SL(2, R)/N$ is less than or equal to $M - 1$ and we will be done.

Consider a typical $A_i$. The first two terms affecting $A_i$ leave 0 fixed and the third term maps 0 into $(-1/3), 1/3)$. Since 1/2 is not equivalent modulo $Z$ to any point in $(-1/3, 1/3)$, there must be a fourth term. This term carries 0 into $(-1/3, 2/3)$ or $(-2/3, 1/3)$. From now on throughout the rest of the argument we shall suppose all fourth terms carry 0 into $(-1/3, 2/3)$; the reader will soon see that our argument carries over to the general case with only minor notational changes. The fifth term carries 0 into $(-2/3, 3/3)$, and the sixth term carries 0 into $(-3/3, 3/3)$ or $(-2/3, 4/3)$. However, if the sixth term carries 0 into $(-3/3, 3/3)$, $A_i \subseteqq (-(n_i - 3)/3, (n_i - 3)/3)$, $h(A_i) \leqq n_i - 1$, and $A_1 \times \cdots \times A_p \subseteqq \{x_1, \ldots, x_p \mid h(x_1) + \cdots + h(x_p) \leqq M - 1\}$. So the sixth term carries 0 into $(-2/3, 4/3)$.

In short, $n_i \geqq 4$; if $n_i = 4$, $A_i \subseteqq (-1/3, 2/3)$; if $n_i = 5$, $A_i \subseteqq (-2/3, 3/3)$; if $n_i \geqq 6$, $A_i \subseteqq (-(n_i - 4)/3, (n_i - 2)/3)$.

Since $h(a_i) < n_i$ on $(-(n_i - 3)/3), (n_i - 3)/3)$, every point in $A_1 \times \cdots \times A_p$ not in $[(n_1 - 3)/3, (n_1 - 2)/3) \times \cdots \times [(n_p - 3)/3, (n_p - 2)/3)$ already belongs to $\{(x_1, \ldots, x_p) \mid h(x_1) + \cdots + h(x_p) \leqq M - 1\}$. Consider the point $(n_1 - 2)/3 \times \cdots \times (n_p - 2)/3$; this point is equivalent modulo $N$ to a point in $A_1 \times \cdots \times A_p$, so there is an element $\ell_1 \times \cdots \times \ell_p$ in $N$ such that $(n_i - 2)/3 - \ell_i \in A_i$. If $n_i = 4$, $-1/3 < 2/3 - \ell_i < 2/3$; there is not such integer $\ell_i$. If $n_i = 5$, $-2/3 < 3/3 - \ell_i < 3/3$ and $\ell_i = 1$. If $n_i \geqq 6$, $-(n_i - 4)/3 < (n_i - 2)/3 - \ell_i < (n_i - 2)/3$. In each case, $[(n_i - 3)/3, (n_i - 2)/3) - \ell_i \subseteqq (-(n_i - 3)/3, (n_i - 3)/3)$, so each element of $[(n_1 - 3)/3, (n_1 - 2)/3) \times \cdots \times [(n_p - 3)/3, (n_p - 2)/3)$ is equivalent modulo $N$ to an element in $\{(n_1, \ldots, x_p) \mid h(x_1) + \cdots + h(x_p) \leqq M - 1\}$ and we are done.

## References


1. G. Hochschild, *The Structure of Lie Groups*, Holden-Day, San Francisco, 1965.
2. N. Jacobson, *Lie Algebras*, John Wiley, New York, 1962.

3. R. M. Koch and F. Lowenthal, *Uniform finite generation of three dimensional linear Lie groups*, Can. J. Math. **27** (1975), 396–417.

4. ———, *Uniform finite generation of Lie groups locally-isomorphic to SL(2, R)*, Rocky Mountain J. Math. **7** (1977), 707–724.

5. F. Lowenthal, *Uniform finite generation of the isometry groups of Euclidean and non-Euclidean geometry*, Can. J. Math. **23** (1971), 364–373.

6. ———, *Uniform finite generation of the rotation group*, Rocky Mountain J. Math. **1** (1971), 575–586.

7. ———, *Uniform finite generation of the affine group*, Pacific J. Math. **40** (1972), 341–348.

8. ———, *Uniform finite generation of SU(2) and SL(2, R)*, Can. J. Math. **24** (1972), 713-727.

9. S. Sternberg, *Lectures on Differential Geometry*, Prentice-Hall, Englewood Cliffs, N.J., 1964.

10. H. Yamabe, *On an arcwise connected subgroup of a Lie group*, Osaka J. Math. **2** (1950), 13–14.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OREGON, EUGENE, OR 97403

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY, HAYWARD, CA 94542