J. DIFFERENTIAL GEOMETRY
3 (1969) 481-492

DISCRETE NILPOTENT SUBGROUPS OF LIE GROUPS

HSIEN-CHUNG WANG

1. Introduction

C. L. Siegel [5] has shown that the area of the fundamental domain of a totally discontinuous group of motions of the hyperbolic plane is at least $\pi/21$. Recently D. A. Kazhdan and G. A. Margulis [4] proved that every semisimple Lie group without compact factor has a neighborhood U of the identity e such that, given any discrete subgroup Γ of G, there exists $g \in G$ with the property that $g\Gamma g^{-1} \cap U = \{e\}$. This implies that the volume of the fundamental domain of discrete subgroups of G (when considered as a group of left translations of G, or as the group of isometries on the symmetric space associated with G) has a positive lower bound. It is the aim of this paper to give a *quantitative* study of the neighborhood U. Two properties of discrete nilpotent subgroups of Lie groups will be established; they lead directly to an estimate of the size of U. One of the properties is a sharpening of a theorem of Zassenhaus [8]. We note that, whereas Kazhdan-Margulis used results on algebraic groups, our proof here consists in some elementary geometrical arguments.

Let G be a semisimple Lie group, $\mathfrak{G}$ its Lie algebra, k the Killing form over $\mathfrak{G}$, and $\sigma: \mathfrak{G} \to \mathfrak{G}$ a Cartan involution. Define an inner product $\langle\ \rangle$ by putting $\langle X, Y\rangle = -k(X, \sigma Y), X, Y \in \mathfrak{G}$; it gives a left invariant Riemannian metric, and hence a distance function ρ, over the group space G. This distance function ρ is not unique, but any two of such differ only by an inner automorphism of G. With the semisimple Lie algebra $\mathfrak{G}$, we associate a positive real number R_G which can be computed from the root system. For example, $R_{SL(n,R)} = c\sqrt{n}$, $R_{SU(p,q)} = c(p+q)^{1/2}$ where c is approximately $277/1000$. Using these notations, we can describe our main results as follows:

I. *For every discrete subgroup Γ of a semisimple Lie group G, the set $\{g \in \Gamma: \rho(e, g) \leq R_G\}$ generates a nilpotent subgroup.*

II. *Suppose G to be a semisimple Lie group without compact factor. Let $\mathfrak{G}_\pi$ be the totality of elements X in the Lie algebra of G such that all the eigenvalues of* $\operatorname{ad} X$ *have their imaginary parts lying in the open interval $(-\pi, \pi)$, and $G_\pi = \{\exp X: X \in \mathfrak{G}_\pi\}$. Then, given any nilpotent discrete subgroup Γ of G and any compact neighborhood C of e with $C \subset G_\pi$, there exists $g \in G$ such that $g\Gamma g^{-1} \cap C = \{e\}$.*

Received February 17, 1969. This work was supported in part by the National Science Foundation under contracts GP-6948.

As consequences of I and II, we have

III. *Suppose G to be a semisimple Lie group without compact factor. Let B be the closed ball $\{g \in G: \rho(e, g) \leq R_G\}$. Given any discrete subgroup Γ of G, there exsits g in G such that $g\Gamma g^{-1} \cap B = \{e\}$. Hence the volume of the fundamental domains of Γ is larger than the volume of the ρ-sphere with radius $R_G/2$.*

IV. *Let G be a semisimple Lie group without compact factor and having a finite center. There exist integers n, m with the following properties: Given any nilpotent discrete subgroups Γ of G, and any compact neighborhood C of e, we can find $g \in G$ such that* (i) *each element in $C \cap g\Gamma g^{-1}$ is periodic and of period less than n, and* (ii) *the intersection $C \cap g\Gamma g^{-1}$ contains less than m elements.* (These n and m depend on G and not at all on C and Γ.)

2. Canonical distance

Let G be a semisimple Lie group, and $\mathfrak{G}$ its Lie algebra. Choose a Cartan decomposition $\mathfrak{G} = \mathfrak{K} + \mathfrak{P}$, and denote by $\sigma: \mathfrak{G} \to \mathfrak{G}$ the involution such that $\sigma(U) = U, \sigma(Y) = -Y$ for $U \in \mathfrak{K}, Y \in \mathfrak{P}$. Let k be the Cartan Killing form of $\mathfrak{G}$. Then the bilinear form $\langle\ \rangle$ defined by $\langle X, Y\rangle = -k(X, \sigma Y)$, for $X, Y \in \mathfrak{G}$, is an inner product. Since k is invariant under automorphisms of G, we have

$$(2.1) \qquad \langle X, [Y, Z]\rangle + \langle[\sigma Y, X], Z\rangle = 0\,, \qquad \text{for } X, Y, Z \in \mathfrak{G}\,.$$

By $\|X\|$, we shall always mean $\langle X, X\rangle^{1/2}$. This inner product depends on the choice of the Cartan decomposition, but any two of such differ only by an inner automorphism.

For each endomorphism $f: \mathfrak{G} \to \mathfrak{G}$, we denote by $N(f)$ the norm of f, or in other words, $N(f) = \sup\{\|f(X)\|: X \in \mathfrak{G}, \|X\| = 1\}$. The following two constants: $C_1 = \sup\{N(\operatorname{ad} Y): Y \in \mathfrak{P}, \|Y\| = 1\}$, $C_2 = \sup\{N(\operatorname{ad} U): U \in \mathfrak{K}, \|U\| = 1\}$ play important roles in our later discussions. Suppose $Y \in \mathfrak{P}, U \in \mathfrak{K}$. Let $\lambda_1, \lambda_2, \cdots, \lambda_n$ and $\mu_1, \mu_2, \cdots, \mu_n$ ($n = \dim. G$) be, respectively, the eigenvalues of $\operatorname{ad} Y$ and $\operatorname{ad} U$. Since, for $X, Z \in \mathfrak{G}$,

$$\langle(\operatorname{ad} Y)X, Z\rangle = \langle X, (\operatorname{ad} Y)Z\rangle\,, \qquad \langle(\operatorname{ad} U)X, Z\rangle = -\langle X, (\operatorname{ad} U)Z\rangle\,,$$

we have

$$\|Y\|^2 = \sum \lambda_j^2, \quad \|U\|^2 = -\sum \mu_j^2\,, \quad N(\operatorname{ad} Y) = \max. |\lambda_j|\,, \quad N(\operatorname{ad} U) = \max. |\mu_j|\,.$$

This shows that C_1, C_2 depend only on the root system of $\mathfrak{G}$. The eigenvalues of $\operatorname{ad} Y$ ($\operatorname{ad} U$) occur in pairs $\pm\lambda$ ($\pm\mu$), and so $C_1 \leq 1/\sqrt{2}$ ($C_2 \leq 1/\sqrt{2}$). A table of these two constants for non-compact and non-exceptional simple Lie groups is given at the end of this paper.

By identifying $\mathfrak{G}$ with the tangent space $T_e(G)$ of G at the identity, we can extend the inner product to a left invariant Riemannian metric over the group manifold G. Such a metric will be called a *canonical Riemannian metric*. It is complete and invariant under $\mathrm{Ad}\,u$ with $u \in K = \exp \mathfrak{K}$ and under all left translations. The induced distance function will be denoted by ρ, and called a *canonical distance* or *canonical metric*.

Let G/K be the symmetric space, and $\pi: G \to G/K$ the projection. G/K has a G-invariant Riemannian metric such that the differential $d\pi$ of π carries $\mathfrak{P}$ (considered as a subspace of $T_e(G)$) isometrically onto the tangent space $T_{\pi(e)}(G/K)$ of G/K at $\pi(e)$. Therefore, for each tangent vector X of G, the length of $d\pi(X)$ cannot be greater than the length of X. Let $P = \exp \mathfrak{P}$, $K = \exp \mathfrak{K}$, $k \in K$, $Y \in \mathfrak{P}$, $p = \exp Y$, $x = pk$, and f: $[0,1] \to G$ a minimizing geodesic joining e to x. Denote by L the arc length of a curve, and by $\bar{\rho}$ the distance function on G/K. Since $\pi(x) = \pi(p)$ and $d\pi$ does not increase the length of vectors, we have

$$\rho(e, pk) = L(f) \geq L(\pi \circ f) \geq \bar{\rho}(\pi(e), \pi(p)) .$$

The curve $t \to \pi(\exp tY)$ is a minimizing geodesic in G/K, and so $\bar{\rho}(\pi(e), \pi(p)) = \|Y\|$, whence $\rho(e, pk) \geq \|Y\|$. In particular, $\rho(e, p) \geq \|Y\|$. On the other hand, $t \to \exp tY$ is a curve in G joining e to p with arc length $\|Y\|$. Therefore,

$$\rho(e, P) = \|Y\| , \qquad \rho(e, pk) \geq \rho(e, p) . \tag{2.2}$$

Unlike the compact case, a 1-parameter subgroup is, in general, not a geodesic with respect to our canonical metric. Nevertheless, by using the standard method, we can see easily [7] that every geodesic through the identity e takes the form $t \to \exp t(Y_0 - U_0) \exp 2tU_0$ where Y_0 is an element of $\mathfrak{P}$ and U_0 an element of $\mathfrak{K}$. The length of the tangent vectors of this geodesic is equal to $\|Y_0 + U_0\|$. From the method of first variations, we can deduce directly

(2.3) *Suppose an element x of G has the property that $\rho(e, x) \leq \rho(e, gxg^{-1})$ for all g in a neighborhood of the identity. Then there exist $Y_0 \in \mathfrak{P}$, $U_0 \in \mathfrak{K}$ such that $\rho(e, x) = \| U_0 = \| U_0 + Y_0 \|$, $x = \exp (Y_0 - U_0) \exp 2U_0$, $\exp (2 \,\mathrm{ad}\, U_0) Y_0 = Y_0$.*

The proof consists in straightforward computation, and the details can be found in [7].

3. A neighborhood of the identity

As before, G denotes a semisimple Lie group. It is the aim of this section to construct a neighborhood Q of the identity such that the subgroup generated by any subset of Q is either non-discrete or nilpotent. The existence of such a neighborhood for an arbitrary Lie group follows from an old result of Zassenhaus [8]. But here our concern is the size of Q. The method, though more complicated, is the same as that used by W. Boothby and the author in [1].

(3.1) *Let x, z be elements of G, $\rho(e, z) = r$, and*

$$N(\operatorname{Ad} x - I) < C_1 r/(\exp C_1 r - 1)\,.$$

Then $\rho(e, xzx^{-1}z^{-1}) < \rho(e, z)$.

Proof. Let $s \to u(s)$ be a minimizing geodesic with s as its arc length and $u(0) = e, u(r) = z$. Because of the completeness of the canonical Riemannian metric, such a geodesic always exists. Define $w(s) = u(s)x^{-1}u(s)^{-1}$. Then w is a curve joining x^{-1} to $zx^{-1}z^{-1}$. Denoting by M the arc length of w, we have $\rho(e, xzx^{-1}z^{-1}) = \rho(x^{-1}, zx^{-1}z^{-1}) \leq M$. For each $g \in G$, let us use L_g and R_g to denote, respectively, the left and right translations induced by g. For simplicity, we use the same letters to denote their respective differentials. Then

$$(L_w)^{-1}dw/ds = (\operatorname{Ad} u)(\operatorname{Ad} x - I)(L_u)^{-1}du/ds\,.$$

Since our Riemannian metric is left invariant, and s is the arc length of the curve u, we have $\|(L_u)^{-1}du/ds\| = \|du/ds\| = 1$, and so

$$\|dw/ds\| = \|(L_w)^{-1}dw/ds\| \leq N(\operatorname{Ad} u)N(\operatorname{Ad} x - I)\,.$$

For each fixed s, let us write $u(s) = (\exp Y)k$ where $Y = Y(s) \in \mathfrak{P}$ and $k = k(s) \in K$. Since $\operatorname{Ad} k$ is an isometry and $\operatorname{ad} Y$ is self-adjoint with respect to the inner product $\langle\ \rangle$, we have

$$N(\operatorname{Ad} u(s)) = N(\operatorname{Ad}(\exp Y)) = \exp N(\operatorname{ad} Y) \leq \exp C_1\|Y\|\,.$$

From (2.2), $\|Y\| \leq \rho(e, u(s)) = s$. It follows $N(\operatorname{Ad} u(s)) \leq \exp C_1 s$, and then $\|dw/ds\| \leq N(\operatorname{Ad} x - I)\exp C_1 s$, whence

$$\rho(e, xzx^{-1}z^{-1}) \leq M = \int_0^r \|dw/ds\|\,ds \leq N(\operatorname{Ad} x - I)(\exp C_1 r - 1)/C_1 < r\,,$$

and our proposition is proved.

Let us consider the function

$$F(t) = \exp C_1 t - 1 + 2\sin C_2 t - C_1 t/(\exp C_1 t - 1)$$

of one real variable t. We find that $F(0) = 0, F(t) < 0$ when t is sufficiently small, and $\lim F(t) = \infty$ as t goes to infinity. Therefore, it has a positive zero. Let R_G denote the least positive zero of $F(t)$. It depends only on C_1 and C_2, and hence only on the Lie algebra $\mathfrak{G}$ of G. For non-compact, non-exceptional simple Lie groups G, we find that either $C_2 = C_1$ or $C_2 = \sqrt{2}C_1$. The number R_G is approximately $277/1000C_1$ in the first case, and $228/1000C_1$ in the second case. For example, $R_G = 277\sqrt{2}/1000$ when $G = SO(2, 1)$ and $R_G = 228\sqrt{2(p-1)}/1000$ when $G = SO(p, 1)$ with $p \geq 4$.

(3.2) Theorem. *Let G be a semisimple Lie group, ρ a canonical distance function, and R_G the constant defined above. Then, for any discrete subgroup Γ of G, the set $\Theta = \{g \in \Gamma : \rho(e, g) \leq R_G\}$ generates a nilpotent subgroup.*

Proof. Let $\mathfrak{G} = \mathfrak{P} + \mathfrak{K}$ be the Cartan decomposition of the Lie algebra $\mathfrak{G}$ based on which the canonical distance function is defined. Suppose $x, z \in \Theta$ and $x \neq e, z \neq e$. We write $x = pk$ where $p = \exp Y, k = \exp U, Y \in \mathfrak{P}, U \in \mathfrak{K}$. Here U is so chosen that $\rho(e, k) = \|U\|$. We have

$$N(\operatorname{Ad} x - I) = N(\operatorname{Ad} p - \operatorname{Ad} k^{-1}) \leq N(\operatorname{Ad} p - I) + N(I - \operatorname{Ad} k^{-1}) .$$

By (2.2), $\|Y\| \leq \rho(e, x)$. It follows then

$$N(\operatorname{ad} Y) \leq C_1\rho(e, x) , \qquad N(\operatorname{Ad} p - I) \leq \exp C_1\rho(e, x) - 1 .$$

Since the eigenvalues of ad U are all purely imaginary, we find that

$$N(I - \operatorname{Ad} k^{-1}) = N(\operatorname{Ad} k - I) \leq 2 \sin (C_2\rho(e, k)/2) .$$

But

$$\rho(e, k) \leq \rho(e, x) + \rho(e, p) < 2\rho(e, x) \leq 2R_G ,$$

and so

$$N(I - \operatorname{Ad} k^{-1}) < 2 \sin C_2R_G .$$

Therefore we have

$$\begin{aligned} N(\operatorname{Ad} x - I) &< \exp C_1R_G - 1 + 2 \sin C_2R_G \\ &= C_1R_G/(\exp C_1R_G - 1) \leq C_1\rho(e, z)/(\exp C_1\rho(e, z) - 1) . \end{aligned}$$

It follows from (3.1) that $\rho(e, xzx^{-1}z^{-1}) < \rho(e, z)$. Since

$$\rho(e, zxz^{-1}x^{-1}) = \rho(e, xzx^{-1}z^{-1}) ,$$

the roles of x and z can be interchanged, and so $\rho(e, xzx^{-1}z^{-1})$ is also less than $\rho(e, x)$.

Define Θ_m inductively by putting $\Theta_0 = \Theta, \Theta_j = \{aba^{-1}b^{-1}: a \in \Theta, b \in \Theta_{j-1}\}$. The above discussion on commutators $xzx^{-1}z^{-1}$ tells us that the sequence $\Theta = \Theta_0 \supset \Theta_1 \supset \Theta_2 \supset \cdots$ is strictly decreasing. On the other hand, since Γ is discrete, Θ contains only a finite number of elements. Therefore, $\Theta_m = \{e\}$ for large m. By a theorem of Zassenhaus [8], Θ generates a nilpotent group.

When G is not simple, a little better result can be obtained. In fact, we have

(3.3) Theorem. *Let $G = G_1 \cdot G_2 \cdots G_n$ be a local direct product of simple Lie groups G_i. Let ρ_i be a canonical distance of G_i, $Q_i = \{x \in G_i: \rho_i(e, x) \leq R_{G_i}\}$, and $Q = Q_1 \cdot Q_2 \cdots Q_n$. Then, for any discrete subgroup Γ of G, the intersection $\Gamma \cap Q$ generates a nilpotent group.*

This can be proved in the same way as above with obvious modification.

4. Nilpotent discrete subgroups

Let H be an arbitrary Lie group, and $\mathfrak{H}$ its Lie algebra. Consider the totality $\mathfrak{H}_\pi$ of elements X in $\mathfrak{H}$ such that the imaginary parts of all the eigenvalues of $\operatorname{ad} X$ lie in the open interval $(-\pi, \pi)$. Restricted to $\mathfrak{H}_\pi$, the exponential map exp is injective [6]. Since the differential of exp at a point X_0 of $\mathfrak{H}$ is given by $L_{\exp X_0} \circ \sum_{n=1}^{\infty} (-1)^{n-1}(\operatorname{ad} X_0)^{n-1}/n!$, where $L_{\exp X_0}$ denotes the left translation, it follows that the exponential map is regular at all X_0 in $\mathfrak{H}_\pi$. Therefore, exp carries $\mathfrak{H}_\pi$ diffeomorphically onto $H_\pi = \{\exp X \colon X \in \mathfrak{H}_\pi\}$. We note that H_π is a large open neighborhood of the identity, and is invariant under automorphisms of H. Let β be any endomorphism of $\mathfrak{H}$. For every X in $\mathfrak{H}_\pi$, if β commutes with $\operatorname{Ad}(\exp X)$, then β must also commute with $\operatorname{ad} X$ [6, p. 125].

(4.1) *Let $\mathfrak{J}$ be a subset of $\mathfrak{H}_\pi$. If the set $J = \{\exp X \colon X \in \mathfrak{J}\}$ generates a nilpotent subgroup M of H, then $\mathfrak{J}$ generates a nilpotent subalgebra.*

Proof. Since J as well as M belongs to the identity component of H, we can simply assume H to be connected. Let Z be the center of H, and $H' = H/Z$. We can see immediately the following: (A) *Either* $\dim H' < \dim H$, *or H' has a trivial center.* (B) *If* (4.1) *is valid for H', than* (4.1) *is also valid for H.* We note that in (A) the connectedness of H is needed.

Now let us prove (4.1) by induction, and suppose it to be valid for all Lie groups of lower dimension than H. From (A) and (B), we can assume that H has a trivial center. Select an element x in the center of M, with $x \neq e$, and let F be the identity component of the centralizer of x in H. Then $\dim F < \dim H$. Since $\operatorname{Ad} x$ centralizes $\operatorname{Ad} J$, it also centralizes $\operatorname{ad} \mathfrak{J}$ because of the particular property of $\mathfrak{H}_\pi$ mentioned above. But H has a trivial center so $\operatorname{Ad} x$ must leave J pointwise invariant. In other words, $\mathfrak{J}$ is contained in the Lie algebra of F. From the induction hypothesis, $\mathfrak{J}$ generates a nilpotent subalgebra. (4.1) is thus proved.

Now let us come back to a semisimple Lie group G. As before, we choose a Cartan decomposition $\mathfrak{G} = \mathfrak{K} + \mathfrak{P}$ of the Lie algebra $\mathfrak{G}$ of G, and denote by $\sigma \colon \mathfrak{G} \to \mathfrak{G}$ the corresponding Cartan involution. Suppose that the inner product $\langle\,\rangle$ and the norm $\|\ \|$ have the same meaning as in §2. We shall discuss the variation of the norm of vectors in a nilpotent subalgebra under the adjoint transformations. Suppose $X \in \mathfrak{G}$, $B \in \mathfrak{P}$ and $b(t) = \exp tB$. Then $(\operatorname{Ad} b(t))X = X + t[B, X] + t^2[B, [B, X]]/2 + 0(t^3)$. If follows then, from (2.1),

$$
\begin{aligned}
\|(\operatorname{Ad} b(t))X\|^2 &= \|X\|^2 + 2t\langle X, [B, X]\rangle \\
&\quad + t^2(\|[B, X]\|^2 + \langle X, [B, [B, X]]\rangle) + 0(t^3) \qquad (4.2)\\
&= \|X\|^2 + 2t\langle [\sigma X, X], B\rangle + 2t^2(\|[B, X]\|^2) + 0(t^3)\,.
\end{aligned}
$$

With this formula, let us prove the following:

(4.3) *Let $\{X_1, X_2, \cdots, X_m\}$ be a finite subset of $\mathfrak{G}$ which generates a nilpotent subalgebra $\mathfrak{N}$. If G has no compact factor, then there exists $g \in \exp P$*

such that $\|(\mathrm{Ad}\, g)X_i\| \geq \|X_i\|$ *for all* i, *and the strict inequality holds for at least one* i. *Moreover*, g *can be chosen arbitrarily close to the identity.*

Proof. Let $\mathfrak{Z}$ be the center of $\mathfrak{N}$. Two cases arise and we discuss them separately.

Case 1. Suppose there exists Z in $\mathfrak{Z}$ with $[\sigma Z, Z] \neq 0$. Putting $B = [\sigma Z, Z]$, we find $\sigma B = -B$ and so $B \in \mathfrak{P}$. For any X in $\mathfrak{N}$, $[X, Z] = 0$. It follows then from (2.1) that $\langle [\sigma X, X], B\rangle = \|[X, \sigma Z]\|^2 \geq 0$. From our choice of Z, $[\mathfrak{N}, \sigma Z] \neq 0$, and hence $[X_i, \sigma Z]$ cannot be all zero. By a change of indices, we can assume $[X_i, \sigma Z] \neq 0$ for $i = 1, 2, \cdots, n$ and $[X_j, \sigma Z] = 0$ for $j > n$. On account of (4.2), we know that, for small positive t, $\|(\mathrm{Ad}\,(\exp tB))X_i\| > \|X_i\|$ for $i \leq n$. As for $j > n$, we have $[X_j, \sigma Z] = 0$, and hence $[X_j, B] = 0$ and $\mathrm{Ad}\,(\exp tB)X_j = X_j$. Therefore, for small positive t, the element $g = \exp tB$ has the required properties.

Case 2. Suppose $[Y, \sigma Y] = 0$, for all $Y \in \mathfrak{Z}$. Since $Y + \sigma Y \in \mathfrak{K}$, $Y - \sigma Y \in \mathfrak{P}$, the endomorphisms $\mathrm{ad}\,(Y + \sigma Y)$ and $\mathrm{ad}\,(Y - \sigma Y)$ are semisimple and commute with each other. Therefore $\mathrm{ad}\, Y$ is semisimple. Now $\mathrm{ad}\,\mathfrak{Z}$ contains only semisimple elements. It follows that $\mathfrak{N}$ is abelian and $\mathfrak{N} = \mathfrak{Z}$. Since G has no compact factor, the centralizer or $\mathfrak{P}$ in $\mathfrak{G}$ is zero, so we can find $B \in \mathfrak{P}$ such that $[X_1, B] \neq 0$. The equality (4.2) for the elements X_i takes the form

$$\|(\mathrm{Ad}\,(\exp tB)X_i)\|^2 = \|X_i\|^2 + 2t^2(\|[B, X_i]\|^2) + 0(t^3)\,.$$

When $[B, X_i] = 0$, $\mathrm{Ad}\,(\exp tB)X_i = X_i$. Therefore, the element $g = \exp tB$, for small non-zero t, has all the required properties. (4.3) is thus proved.

For any subset $\mathfrak{F}$ of $\mathfrak{G}$, let us put $r(\mathfrak{F}) = \inf\{\|X\| : X \in \mathfrak{F}, X \neq 0\}$. Then we have

(4.4) *Let* $\mathfrak{F}$ *be a closed discrete subset of a nilpotent subalgebra of* $\mathfrak{G}$ *containing at least one non-zero element. If* G *has no compact factor, then there exists an element* h *such that* $r(\mathfrak{F}) < r((\mathrm{Ad}\, h)\mathfrak{F})$. *Moreover*, h *can be chosen arbitrarily close to the identity* e.

Proof. Since $\mathfrak{F}$ is discrete and closed in $\mathfrak{G}$, there are only a finite number of elements $X_1, X_2, \cdots, X_m$ in $\mathfrak{F}$ with length equal to $r(\mathfrak{F})$. For other elements Y of $\mathfrak{F}$, either $Y = 0$, or $\|Y\| > r(\mathfrak{F})P + \varepsilon$ where ε is a fixed positive number. Apply (4.3) to the set $\{X_1, X_2, \cdots, X_m\}$ and choose g *sufficiently close to identity*. We have the following two alternatives: (I) $r((\mathrm{Ad}\, g)\mathfrak{F}) = r(\mathfrak{F})$ and $(\mathrm{Ad}\, g)\mathfrak{F}$ contains less than m elements with length equal to $r(F)$; or (II) $r((\mathrm{Ad}\, g)\mathfrak{F}) > r(\mathfrak{F})$. Thus if we repeatedly use this procedure (not more than m times), we get the required element h.

(4.5) Theorem. *Let* Γ *be a discrete nilpotent subgroup of a semisimple Lie group* G *without compact factor. Then, given any compact neighborhood* Q *of the identity* e *with* $Q \subset G_\pi$, *there exists* $g \in G$ *such that* $Q \cap g\Gamma g^{-1} = \{e\}$.

Proof. For each $h \in G$, let $\mathfrak{F}(h) = \{X \in \mathfrak{G}_\pi : \exp X \in h\Gamma h^{-1}\}$, and consider the set $\{r(\mathfrak{F}(h)) : h \in G\}$ of real numbers. Suppose that this set has a finite least upper bound, say b. Then there exist $h_i \in G$, $i = 1, 2, \cdots$, such that

$r(\mathfrak{F}(h_1)) \leq r(\mathfrak{F}(h_2)) \leq r(\mathfrak{F}(h_3)) \leq \cdots$, and $\lim_{i\to\infty} r(\mathfrak{F}(h_i)) = b$. Let

$$W = \{\exp X : X \in \mathfrak{G}_\pi, \|X\| < r(\mathfrak{F}(h_1))\} .$$

Obviously, $W \cap h_i \Gamma h_i^{-1} = \{e\}$ for all i, or in other words, the sequence $\{h_i \Gamma h_i^{-1}\}$ of subgroups is uniformly discrete. By a Theorem of Chabauty [2], this sequence has a convergent subsequence, and so we can assume that $\{h_i \Gamma h_i^{-1}\}$ is already convergent and approaches Γ' as a limit. Γ' is evidently discrete and nilpotent. Let $\mathfrak{F}' = \{X \in \mathfrak{G}_\pi : \exp X \in \Gamma'\}$. We see immediately that $r(\mathfrak{F}') = b$. By (4.4), there exists $k \in G$ such that $r((\mathrm{Ad}\, k)F') > r((F') = b$. It follows that $\lim_{i\to\infty} r(\mathfrak{F}(kh_i)) = r((\mathrm{Ad}\, k)\mathfrak{F}') > b$ which contradicts the definition of b. Therefore, the set $\{r(\mathfrak{F}(h)) : h \in G\}$ is not bounded.

Now let Q be a compact neighborhood of e with $Q \in G_\pi$. There exists a large number q such that $Q \subset \{\exp X : X \in \mathfrak{G}_\pi, \|X\| \leq q\}$. By the preceeding discussions, we can find $g \in G$ with $r(\mathfrak{F}(g)) > q$. It follows then that $Q \cap g\Gamma g^{-1} = \{e\}$, and thus our theorem is proved.

5. An application

In this section, we shall combine (3.2) and (4.5) to give a quantitative version of a theorem of Kazhdan and Margulis.

(5.1) *Let G be a semisimple Lie group, R_G the constant associated to G as in § 3, and ρ the canonical metric based on a Cartan decomposition $\mathfrak{G} = \mathfrak{K} + \mathfrak{P}$ of the Lie algebra $\mathfrak{G}$ of G. Then the closed ball $B = \{x \in G : \rho(e, x) \leq R_G\}$ is contained in G_π.*

Proof. Let us first show that, for every y in B, $\mathrm{Ad}\, y$ cannot have any eigenvalue equal to -1. Suppose that -1 is an eigenvalue of $\mathrm{Ad}\, y$. Then there exists $Z \in \mathfrak{G}$ with $(\mathrm{Ad}\, y)Z = -Z$, and we can choose $\|Z\|$ so small that $q = \exp Z \in B$. Let $q_0 = q$, and $q_i = yq_{i-1}y^{-1}q_{i-1}^{-1}$ for $i = 1, 2, \cdots$. Then, by the proof of (3.2), the distance $\rho(e, q_i)$ approaches zero as i goes to infinity. On the other hand, we have $q_m = \exp(-2)^m Z$, $m = 1, 2, \cdots$. A contradiction is thus obtained. In other words, -1 cannot be the eigenvalue of $\mathrm{Ad}\, y$ for any element y of B.

Now let us come to the proof of our proposition. Suppose (5.1) to be false. Then the difference set $B - G_\pi$ is compact and non-empty, and so we can find $x \in B - G_\pi$ with $\rho(e, x) = \rho(e, B - G_\pi)$. If $g \in G$ and $\rho(e, gxg^{-1}) < \rho(e, x)$, then $gxg^{-1} \in B - gG_\pi g^{-1} = B - G_\pi$, and $\rho(e, B - G_\pi) < \rho(e, x)$ which is impossible. Therefore $\rho(e, gxg^{-1}) \geq \rho(e, x)$ for all g of G. By (2.3), we can find $Y_0 \in \mathfrak{P}$, $U_0 \in \mathfrak{K}$ such that $\rho(e, x) = \|Y_0 + U_0\|$, $x = \exp(Y_0 - U_0)\exp 2U_0$ and $\exp(2\,\mathrm{ad}\, U_0)Y_0 = Y_0$. Let $\{\theta_1 i, \theta_2 i, \cdots\}$ be the set of eigenvalues of $\mathrm{ad}\, U_0$. For any real number s, put $u(s) = \exp sU_0$. When $0 \leq s \leq 1$, $\rho(e, u(s)) \leq s\|U_0\| \leq \|U_0\| \leq \rho(e, x) \leq R_G$. Therefore, $u(s) \in B$ and -1 is not an eigenvalue of $\mathrm{Ad}\, u(s)$. It follows that $|s\theta_j| < \pi$, and whence $|\theta_j| < \pi$. The equality $\exp(2\,\mathrm{ad}\, U_0)Y_0 = Y_0$ then implies that $[U_0, Y_0] = 0$. Thus we have $x = \exp(U_0 + Y_0)$, $U_0 + Y_0 \in \mathfrak{G}_\pi$, and $x \in G_\pi$. A contradiction is obtained; in other words, $B \subset G_\pi$.

(5.2) Therem. *Let G be a semisimple Lie group without compact factor, and $B = \{x \in G\colon \rho(e, x) \leq R_G\}$ the closed ball as before. Then, given any discrete subgroup Γ of G, there exists $g \in G$ such that $B \cap g\Gamma g^{-1} = \{e\}$.*

Proof. From (5.1), for any x of B, there exists a unique $X \in \mathfrak{G}_\pi$ with $\exp X = x$. Let H be any subset of G, and denote

$$\Phi(H) = \inf\{\|X\|\colon X \in \mathfrak{G}_\pi, X \neq 0, \exp X \in B \cap H\}\,.$$

Therefore, $\Phi(H) = \infty$ when $B \cap H = \{e\}$, and $\Phi(H) \leq q < \infty$ when otherwise where $q = \max\{\|X\|\colon X \in \mathfrak{G}_\pi, \exp X \in B\}$. Hence, to prove our theorem, it suffices to show that the set $\Theta = \{\Phi(g\Gamma g^{-1})\colon g \in G\}$ is not bounded. Suppose that Θ has a finite least upper bound, say b. There exist $h_n \in G$ $(n = 1, 2, \cdots)$ such that $\lim_n \Phi(h_n\Gamma h_n^{-1}) = b$, and $\Phi(h_{n-1}\Gamma h_{n-1}^{-1}) \leq \Phi(h_n\Gamma h_n^{-1})$. The sequence $\{h_i\Gamma h_i^{-1}\}$ $i=1,2,\cdots$ is uniformly discrete, and so by Mahler-Chabauty theorem [2], we can assume it to be convergent. Let $\Gamma' = \lim h_n\Gamma h_n^{-1}$. Then Γ' is discrete, nilpotent and $\Phi(\Gamma') = b$. The set B is compact and so $\Gamma' \cap B$ contains only a finite number of elements, say $x_1, x_2, \cdots, x_m$. There exists unique $X_j \in \mathfrak{G}_\pi$ with $x_j = \exp X_j$ for each j. From (3.2), $\{x_1, x_2, \cdots, x_m\}$ generates a nilpotent subgroup, and then from (4.1), $\{X_1, X_2, \cdots, X_m\}$ generates a nilpotent subalgebra. Obviously, $\min\{\|X_1\|, \|X_2\|, \cdots, \|X_m\|\} = b$. On account of (4.4), we can find $h \in G$ such that $\|(\operatorname{Ad} h)X_j\| > b$ for all j. Since B is compact and $\Gamma' - B$ is closed in G, we can choose h so close to the identity that $(\operatorname{Ad} h)(\Gamma' - B)$ does not intersect B. Therefore, $\Phi(h\Gamma'h^{-1}) > b$. But $\lim(hh_n\Gamma h_n^{-1}h^{-1}) = h\Gamma'h^{-1}$, which contradicts the fact that $\Phi(hh_n\Gamma h_n^{-1}h^{-1}) \leq b$. In other words, the set Θ cannot be bounded, and thus our theorem is proved.

Remark. If G is not simple, then (5.2) can be slightly improved. In fact, suppose that $G = G_1 \cdot G_2 \cdots G_q$ is a local direct product of noncompact simple Lie groups G_i. For each i, let $R_i = R_{G_i}$ be the constant associated with G_i, and put $Q_i = \{x \in G_i\colon \rho_i(e, x) \leq R_i\}$ where ρ_i is a canonical metric over G_i. The product $Q = Q_1 \cdot Q_2 \cdots Q_q$ is a compact neighborhood of e in G, and $Q \subset G_\pi$. When $q > 1$, this Q is actually larger than the spherical ball B in (5.2). On account of (3.3) we have

Given any discrete subgroup Γ of G, there exists $g \in G$ such that $Q \cap g\Gamma g^{-1} = \{e\}$.

The proof is the same as that of (5.2).

6. A corollary of (4.5)

When G is a semisimple Lie group with a finite center, we can say more about the set G_π. It is the aim of this section to see what we can get from Theorem (4.5) under this further assumption.

Let φ be an invertible real matrix. There exist real matrices α and β such that (i) $\varphi = \alpha \cdot \exp\beta$, (ii) $\alpha\beta = \beta\alpha$. (iii) α is semisimple and all its eigenvalues are of modulus 1, and (iv) the eigenvalues of β are all real numbers. We can verify that α, β are uniquely determined and that β belongs to the Lie algebra of the least algebraic group of real matrices containing φ. This decomposition $\varphi = \alpha \cdot \exp \beta$ is usually called the *polar decomposition* of φ.

Now let us consider a semisimple Lie group G and an element g of G. Suppose $\operatorname{Ad} g = \alpha(\exp \beta)$ to be the polar decomposition. Since G is semisimple, $\operatorname{ad} \mathfrak{G}$ is the Lie algebra of the least algebraic group of real matrices containing $\operatorname{Ad} G$. Therefore, $\beta = \operatorname{ad} Y$ where $Y \in \mathfrak{G}$. The element $u = g \cdot \exp(-Y)$ will be called the *elliptic part* of the element g. We note that the elements u of G and Y of $\mathfrak{G}$ are uniquely determined by the following four properties: (a) $g = u \cdot \exp Y$, (b) $(\operatorname{Ad} u)Y = Y$, (c) $\operatorname{Ad} u$ is semisimple and all its eigenvalues are of modulus 1, and (d) all the eigenvalues of $\operatorname{ad} Y$ are real numbers.

(6.1) *For any positive number r with $r \leq \pi$, let $\mathfrak{G}_r$ denote the totality of elements X of $\mathfrak{G}$ such that the imaginary parts of the eigenvalues of* $\operatorname{ad} X$ *are all contained in the open interval $(-r, r)$, and let $G_r = \{\exp X : X \in \mathfrak{G}_r\}$. Then $g \in G_r$ if and only if the elliptic part of g belongs to G_r.*

Proof. We write $g = u \cdot \exp Y$ as above. Suppose $g \in G_r$. Then $g = \exp Z$, $Z \in \mathfrak{G}_r$. Since $\exp Y$ commutes with $\exp Z$, and $Y, Z \in \mathfrak{G}_\pi$. it follows that $\operatorname{ad} Y$ commutes with $\operatorname{ad} Z$, whence $[Y, Z] = 0$. We know that $\operatorname{ad} Y$ has only real eigenvalues, and therefore, the set of the imaginary parts of the eigenvalues of $\operatorname{ad} Z$ coincides with that of $\operatorname{ad}(Z - Y)$. Hence $u = \exp(Z - Y) \in G_r$, and we have proved that if $g \in G_r$, then $u \in G_r$. The converse can be proved in a similar manner.

From now on, we assume G to be a semisimple Lie group with a finite center. Choose a real number a with $0 < a < \pi$, and denote by $\bar{G}_a$ the closure of G_a in G. Let H be a maximal compact, connected, abelian subgroup of G. There exists a positive integer n such that, for every element h of H, the set $\{h, h^2, \cdots, h^n\}$ intersects $\bar{G}_a$. Let us assume n to be the least positive integer with this property. Since $\bar{G}_a$ is invariant under inner automorphisms of G, and any two maximal compact, connected abelian subgroups are conjugate, the integer $n = n(G, a)$ depends only on G and a, but not on the choice of H.

Let K be a maximal compact subgroup of G. Since G_a is a neighborhood of the identity, there exists positive integers m such that, given any m elements $k_1, k_2, \cdots, k_m$ of K, we can find i, j with $k_i^{-1}k_j \in \bar{G}_a$ and $i \neq j$. We assume m to be the least positive integer with this property. Just as above, this integer $m = m(G, a)$ depends on G and a, but not on the choice of K.

(6.2) *Suppose that G is a semisimple Lie group with a finite center, and $n = n(G, a)$ has the same meaning as above. Then, for every element g of G, the set $\{g, g^2, \cdots, g^n\}$ interesects $\bar{G}_a$.*

Proof. Let u be the elliptic part of g. Then u^p is the elliptic part of g^p for any integer p. Since $\bar{G}_a = \bigcap_{r>a} G_r$, we know from (6.1) that $g^p \in \bar{G}_a$ if and only if $u^p \in \bar{G}_a$. Therefore, it suffices to show that $\{u, u^2, \cdots, u^n\}$ intersects $\bar{G}_a$. We know that all the eigenvalues of $\mathrm{Ad}\, u$ are of modulus 1, and the center of G is finite. It follows that u belongs to a compact subgroup of G. Hence u is contained in a maximal compact, connected abelian subgroup of G, say H. From the definition of n, the set $\{u, u^2, \cdots, u^n\}$ intersects $\bar{G}_a$, and Proposition (6.2) is thus proved.

(6.3) Corollary. *Let G be a semisimple Lie group without compact factor, and $n = n(G, a)$ and $m = m(G, a)$ be the integers defined above. Suppose that the center of G is finite. Then, given any compact neighborhood C of the identity and any discrete nilpotent subgroup Γ of G, there exists $g \in G$ such that* (i) *each element in $C \cap g\Gamma g^{-1}$ is periodic and of period not greater than n, and* (ii) *the intersection $C \cap g\Gamma g^{-1}$ contains less than m elements.*

Proof. Let ρ be a fixed canonical metric over G. Choose a positive number b such that $\rho(e, x) < b$ for all x in C. Let $B = \{x \in G : \rho(e, x) \leq nb\}$ be the closed ball of radius nb, and $Q = B \cap \bar{G}_a$. Since a is a number less than π, Q is a compact subset of G_π. By (4.5), we can find $g \in G$ such that $Q \cap g\Gamma g^{-1} = \{e\}$. Now let us verify that this g has the required properties. Suppose $y \in C \cap g\Gamma g^{-1}$. From (6.2), there exists an integer p such that $y^p \in \bar{G}_a$ and $1 \leq p \leq n$. Since $\rho(e, y) < b, \rho(e, y^p) < pb \leq nb$, whence $y^p \in B \cap \bar{G}_a$. It follows then $y^p \in Q \cap g\Gamma g^{-1}$ and $y^p = e$. Property (i) is thus proved. To see (ii), suppose $y_1, y_2, \cdots, y_m \in C \cap g\Gamma g^{-1}$. We know that Γ is discrete and nilpotent. It must be finitely generated. Therefore, the totality of all the periodic elements of $g\Gamma g^{-1}$ forms a finite subgroup, say F. Choose a maximal compact subgroup K of G with $F \subset K$. Then $Y_1, y_2, \cdots, y_m \in K$. By definition of the integer m, there exist i, j such that $y_i^{-1} y_j \in \bar{G}_a$ and $i \neq j$. Since $\rho(e, y_i^{-1} y_j) \leq \rho(e, y_i) + \rho(e, y_j) \leq 2b \leq nb$, we have $y_i^{-1} y_j \in Q \cap g\Gamma g^{-1}$, and hence $y_i = y_j$. In other words, $C \cap g\Gamma g^{-1}$ contains less than m elements. This completes the proof.

7. Appendix

The following is a table of the constants C_1 and C_2 for non-compact classical simple Lie groups. For notations, cf. [3, Chap. IX].

Group	Cartan Type	Dimension	C_1	C_2/C_1
$SL(n, C)$	A	$2(n^2 - 1)$	$(1/2n)^{1/2}$	1
$SO(n, C)$	BD	$n(n - 1)$	$(1/4(n - 2))^{1/2}$	1
$Sp(n, C)$	C	$2n(2n + 1)$	$(1/2(n + 1))^{1/2}$	1
$SL(n, R)$	A I	$n^2 - 1$	$(1/n)^{1/2}$	1
$SU^*(2n)$	A II	$4n^2 - 1$	$(1/4n)^{1/2}$	$\sqrt{2}$
$SU(p, q)$	A III	$(p + q)^2 - 1$	$1/(p + q)^{1/2}$	1

Group	Cartan Type	Dimension	C_1	C_2/C_1
$SO(p, q)$ $(p > 2, p \geq q > 1)$	BD I	$(p+q)(p+q-1)/2$	$1/(p+q-2)^{1/2}$	1
$SO(p, 1)$ $(p > 3)$	BD II	$p(p+1)/2$	$1/(2(p-1))^{1/2}$	$\sqrt{2}$
$SO^*(2n)$ $(n > 2)$	D III	$n(2n-1)$	$1/(2n-2)^{1/2}$	1
$Sp(n, R)$	C I	$n(2n+1)$	$1/(n+1)^{1/2}$	1
$Sp(p, q)$	C II	$(p+q)(2p+2q-1)$	$1/(2(p+q+1))^{1/2}$	$\sqrt{2}$

From C_1 and C_2, the constant R_G can be computed. In fact the product $R_G C_1$ is approximately 288/1000 or 277/1000 according as $C_2 = C_1$ or $C_2 = \sqrt{2}C_1$.

Added in proof. A recent note of Armand Borel, *Sous-groupes discrets de groupes semi-simples*, Séminaire Bourbaki, 1968/69, Exp. 358, contains a detailed proof of the theorem of Kazhdan-Margulis mentioned in the Introduction of this paper.

References

[1] W. Boothby & H. C. Wang, *On the finite subgroups of connected Lie groups*, Comm. Math. Helv. **39** (1965) 281–294.

[2] C. Chabauty, *Limite d'ensembles et géométrie des nombres*, Bull. Soc. Math. France **78** (1950) 143–151.

[3] S. Helgason, *Differential geometry and symmetric spaces*, Academic Press, New York, 1962.

[4] D. A. Kazhdan & G. A. Margulis, *A proof of Selberg's hypothesis*, Mat. Sb. (N.S.) **75 (117)** (1968) 163–168.

[5] C. L. Siegel, *Some remarks on discontinuous groups*, Ann. of Math. **46** (1945) 708–718.

[6] H. C. Wang, *On a maximality property of discrete subgroups with fundamental domain of finite measure*, Amer. J. Math. **89** (1967) 124–132.

[7] ——, *On some geometrical invariants associated to a discrete subgroup of Lie groups*, to appear.

[8] H. Zassenhaus, *Beweis eines Satzes über diskrete Gruppen*, Adh. Math. Sem. Univ. Hamburg **12** (1938) 289–312.

CORNELL UNIVERSITY