GENERATING SETS FOR COMPACT SEMISIMPLE LIE GROUPS

MICHAEL FIELD

(Communicated by Roe W. Goodman)

Abstract. Let \( \Gamma \) be a compact connected semisimple Lie group. We prove that the subset of \( \Gamma^2 \) consisting of pairs \((g, h)\) which topologically generate \( \Gamma \) is Zariski open.

1. Introduction

Suppose that \( \Gamma \) is a compact connected Lie group of dimension \( n \). Let \( \langle \gamma_1, \ldots, \gamma_N \rangle \) denote the closure (in \( \Gamma \)) of the group generated by \( \gamma_1, \ldots, \gamma_N \in \Gamma \). If \( \langle \gamma_1, \ldots, \gamma_N \rangle = \Gamma \), we say \( \gamma_1, \ldots, \gamma_N \) are topological generators of \( \Gamma \).

If \( \Gamma \) is abelian, then \( \Gamma \) is isomorphic to a torus \( T^n \). It follows from Kronecker’s theorem that \( \Gamma \) may be topologically generated by one element of \( \Gamma \) (see [1, 3]). Indeed, Kronecker’s theorem gives necessary and sufficient conditions for an element of \( T^n \) to generate \( T^n \) topologically. It follows from these conditions that the topological generators of \( T^n \) form a dense (full-measure) subset of \( \Gamma \) with no interior points.

Since a single element of \( \Gamma \) always generates an abelian subgroup of \( \Gamma \), it follows that if \( \Gamma \) is not abelian, then we need at least two group elements to generate \( \Gamma \) topologically. Somewhat surprisingly, basic results for the non-abelian case appear not to be very well known. In fact, Auerbach showed in 1934 [2] that a compact connected (linear) Lie group \( \Gamma \) could be generated by two elements and that the set of generating pairs had full measure in \( \Gamma^2 \). Subsequently, in 1935, Schreier & Ulam [11] showed that for compact connected metrizable topological groups \( \Gamma \) the set of pairs generating \( \Gamma \) was dense in \( \Gamma^2 \). We refer to the article by Hoffman and Morris [7] for more recent results on the minimal number of generators needed for locally compact groups.

We recall that \( \Gamma \) is semisimple if the center \( Z(\Gamma) \) of \( \Gamma \) is finite. In 1949, Kuranishi showed that connected semisimple Lie groups could be generated by two elements [8]. Later, in 1951, Kuranishi showed that if \( \Gamma \) was a perfect Lie group, then the set of pairs generating \( \Gamma \) was open and dense in \( \Gamma^2 \) [9]. It follows from a result of Goto [6] that every compact connected semisimple Lie group is perfect and so the set of pairs generating a compact connected semisimple Lie group is open and dense.
The proof of Kuranishi’s theorem uses the Hausdorff topology on compact subsets of \( \Gamma \). In particular, the proof gives little insight into the structure of the pairs which do not generate \( \Gamma \).

In this note we give an elementary proof of the following result.

**Theorem 1.1.** Let \( \Gamma \) be a compact connected semisimple Lie group. The set of pairs topologically generating \( \Gamma \) is a non-empty Zariski open subset of \( \Gamma^2 \).

Elsewhere, we use openness results of this type to prove results on the stable ergodicity of Hölder continuous skew-extensions by compact Lie groups [5].

2. **Preliminaries**

In this section we recall some basic definitions and results on compact connected Lie groups and Lie algebras. Details of proofs may be found in standard references (for example [1, 3]). Henceforth, we always assume that the Lie group \( \Gamma \) is compact and connected. Since \( \Gamma \) admits a faithful representation on some \( \mathbb{R}^m \) by matrices of determinant one, it is no loss of generality to assume that \( \Gamma \subset \text{SO}(m) \), for some \( m \in \mathbb{N} \).

We use the term *Zariski open* for subsets whose complement is a closed algebraic variety. Since every compact Lie group may be given the (unique) structure of a real algebraic variety by embedding in some \( \text{SO}(m) \), we may refer, without ambiguity, to Zariski open subsets of a compact Lie group (for uniqueness of algebraic structure, see [10, pg 247]).

If \( H \) is a closed subgroup of \( \Gamma \), we let \( H_0 \) denote the identity component of \( H \).

Let \( \mathfrak{g} \) denote the Lie algebra of \( \Gamma \). The group \( \Gamma \) is semisimple if and only if \( \mathfrak{g} \) is semisimple (as a Lie algebra). The structure of a semisimple group is given in terms of simple groups by the following well-known result.

**Theorem 2.1.** If \( \Gamma \) is semisimple, there exist compact simple groups \( \Gamma_1, \ldots, \Gamma_p \) and a finite covering homomorphism

\[
\phi : \Gamma \rightarrow \Gamma_1 \times \ldots \times \Gamma_p.
\]

Up to order and isomorphism, the \( \Gamma_i \) are uniquely determined by \( \Gamma \).

**Lemma 2.2.** Let \( \phi : \Gamma \rightarrow G \) be a covering homomorphism of compact connected Lie groups. Let \( g, h \in \Gamma \). Then \( \langle g, h \rangle = \Gamma \) if and only if \( \langle \phi(g), \phi(h) \rangle = G \).

**Proof.** Since \( \Gamma \) is compact, \( \phi \) is a finite covering homomorphism. It follows that if \( \langle \phi(g), \phi(h) \rangle = G \), then \( \phi(\langle g, h \rangle) = G \). Hence, \( \dim(\langle g, h \rangle) = \dim(\Gamma) \) and so, since \( \Gamma \) connected, \( \langle g, h \rangle = \Gamma \). The converse is trivial. \( \square \)

3. **Infinite subgroups generated by two elements**

Regard \( \Gamma \) as embedded in \( \text{SO}(m) \). Let \( \langle , \rangle \) be the inner product defined on real \( m \times m \) matrices by

\[
(A, B) = \text{trace}(AB^t) .
\]

Let \( \| \| \) denote the associated norm. If \( A, B \in \text{SO}(n) \), let \([A, B]\) denote the commutator \( ABA^{-1}B^{-1} \). We recall, without proof, the following well-known result on commutators of orthogonal transformations.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Lemma 3.1 ([4, Lemmas 36.15, 36.16]). Let \( A, B \in SO(m) \) and set \( C = [A, B] \).

1. \(|I - C| \leq \sqrt{2}||I - A||||I - B||\).
2. If \( AC = CA \) and \(|I - B| < 2 \), then \( AB = BA \).

Let \( D \) denote the open disk, center \( I \), radius \( 1/\sqrt{2} \) in \( \Gamma \). Set \( D^* = D \setminus \{I\} \).

Lemma 3.2. If \( g, h \in D^* \) and \( gh \neq hg \), then \( \langle g, h \rangle \) is infinite.

Proof. Define the sequence \((g_n)\) inductively by \( g_0 = g \), \( g_n = [g_{n-1}, h] \), \( n \geq 1 \). Since \( g, h \in D^* \), it follows from Lemma 3.1 (1), that \( g_n \not\to I \). If \( \langle g, h \rangle \) is finite, it follows that there exists \( n \geq 1 \) such that \( g_n = I \). That is, \( g_{n-1}h = hg_{n-1} \). It follows from Lemma 3.1(2) that \( h \) must commute with \( g_{n-1} \). Proceeding inductively, it follows that \( gh = hg \), contradicting our assumption that \( g, h \) do not commute. Hence \( \langle g, h \rangle \) is infinite.

Remark 3.3. The proof of Lemma 3.2 is based on part of the proof of Jordan’s theorem given in [4, §36].

Lemma 3.4. Let \( m \geq 1 \). The set \( Z_m \) of pairs \((g, h)\) such that \( g^p h^q \neq h^q g^p \), \( 1 \leq p, q \leq m \), is a non-empty Zariski open subset of \( \Gamma^2 \).

Proof. It suffices to show that for all \( p, q \geq 1 \), the equation \( g^p h^q = h^q g^p \) defines a proper Zariski closed subset of \( \Gamma^2 \). For this, choose \( g, h \in \Gamma \) such that \( g, h \) generate distinct maximal tori.

The next result follows from the compactness of \( \Gamma \).

Lemma 3.5. There exists \( N \in \mathbb{N} \) such that for all \( g \in \Gamma \), there exists \( n, 1 \leq n \leq N \), such that \( g^n \in D \).

Lemma 3.6. If \((g, h) \in Z_N\), then \( \langle g, h \rangle \) is infinite.

Proof. If \((g, h) \in Z_N\), then there exist \( p, q \in \mathbb{N} \), \( 1 \leq p, q \leq N \), such that \( g^p h^q \in D \) and \( g^q h^p \neq h^q g^p \). Since \( g^p h^q \neq h^q g^p \), it follows that \( g^p, h^q \neq I \) and so \( g^p, h^q \in D^* \). The result follows from Lemma 3.2.

4. Generating semisimple groups

Lemma 4.1. Let \( \Gamma \) be a finite product of compact connected simple Lie groups. There is a non-empty Zariski open set \( S \subset \Gamma^2 \) such that if \((g, h) \in S \), then either \( \langle g, h \rangle \) is finite, or \( \langle g, h \rangle = \Gamma \).

Proof. Regard \( \Gamma \) as acting on \( \mathfrak{g} \) via the adjoint representation. Since \( \Gamma \) is a product of simple Lie groups, the adjoint representation is faithful and so we may and shall regard \( \Gamma \) as embedded in \( GL(\mathfrak{g}) \). It follows from Lemma 3.6 that there is a non-empty Zariski open subset \( \mathcal{Z} \) of \( \Gamma^2 \) such that if \((g, h) \in \mathcal{Z} \), then the projection of \( \langle g, h \rangle \) into each simple factor of \( \Gamma \) is infinite. Let \( L(\mathfrak{g}) \) denote the space of \( \mathbb{R} \)-linear endomorphisms of \( \mathfrak{g} \) and \( L^r(\mathfrak{g}) \) denote the subspace of endomorphisms which commute with \( \Gamma \). Given \( g, h \in \Gamma \), let \( S(g, h) \subset L(\mathfrak{g}) \) denote the solution set of the linear system of equations \([g, T] = 0\) and \([h, T] = 0\). It follows from the density theorem of Auerbach and Kuranishi that there exists a pair \((\gamma, \eta)\) such that \( \langle \gamma, \eta \rangle = \Gamma \). Obviously, \( S(\gamma, \eta) = L^r(\mathfrak{g}) \) and \( S(g, h) \supset S(\gamma, \eta) \), all \( g, h \in \Gamma \). Let \( \mathcal{S}' \) be the set of pairs \((g, h)\) for which we have equality. Since the complement of \( \mathcal{S}' \) is defined by the vanishing of determinants, depending polynomially on \( g, h \), it follows that \( \mathcal{S}' \) is a non-empty Zariski open set of \( \Gamma^2 \). Set \( \mathcal{S} = \mathcal{S}' \cap \mathcal{Z} \).
Given \( g, h \in \Gamma \), suppose that \( \langle g, h \rangle_0 \) is a proper non-trivial subgroup of \( \Gamma \). It suffices to prove that \( \langle g, h \rangle \notin S \). Denote the Lie algebra of \( \langle g, h \rangle_0 \) by \( \mathfrak{n} \). Let \( \mathfrak{v} \) denote the minimal \( \Gamma \)-invariant subspace of \( \mathfrak{g} \) containing \( \mathfrak{n} \). If \( \mathfrak{v} = \mathfrak{n} \), \( \langle g, h \rangle_0 \) must be a proper normal subgroup of \( \Gamma \) and must therefore be a product of simple factors of \( \Gamma \). If \( \langle g, h \rangle \in Z \), then the projection of \( \langle g, h \rangle_0 \) on every simple factor of \( \Gamma \) is infinite and so \( \langle g, h \rangle \notin Z \supset S \). On the other hand, if \( \mathfrak{v} \neq \mathfrak{n} \), then the projection of \( \mathfrak{v} \) on \( \mathfrak{n} \) commutes with \( g \) and \( h \) but not \( \Gamma \).

5. Proof of the main theorem

**Lemma 5.1.** Let \( \Gamma \) be a connected compact and semisimple Lie group. There is a non-empty Zariski open subset \( Z \) of \( \Gamma^2 \) consisting of topological generators for \( \Gamma \).

**Proof.** It follows from Theorem 2.1 and Lemma 2.2 that we may assume that \( \Gamma \) is a finite product of compact connected simple Lie groups. The result follows from Lemmas 3.6, 4.1.

**Theorem 5.2.** If \( \Gamma \) is a compact connected semisimple Lie group, then the set of pairs of topological generators of \( \Gamma \) is a non-empty Zariski open subset of \( \Gamma^2 \).

**Proof.** Suppose that \( \langle g, h \rangle = \Gamma \). Then we may find a word \( W(g, h) = (w_1(g, h), w_2(g, h)) \) such that \( (w_1(g, h), w_2(g, h)) \in Z \). But \( W^{-1}(Z) \) is a Zariski open neighborhood of \( (g, h) \) consisting of topological generators of \( \Gamma \).

We conclude with a question suggested by Peter Rowley. If \( \Gamma \) is a finite simple group, it is known that for every non-identity element \( g \in \Gamma \), it is possible to choose \( h \in \Gamma \) such that \( \Gamma = \langle g, h \rangle \). Groups with this property are said to have ‘one and a half’ generators. We conjecture that if \( \Gamma \) is a compact simple group and \( g \) is a non-identity element of \( \Gamma \), then the subset of \( h \in \Gamma \) for which \( \langle g, h \rangle = \Gamma \) is non-empty and Zariski open.

Acknowledgements

It is a pleasure to acknowledge the assistance of Harold Rindler who alerted me to the references Kuranishi [8] and Hoffman & Morris [7]. Thanks to Bill Parry who discovered the reference to Kuranishi [9], and to Gerald Schwarz for showing me proofs of Kuranishi’s density theorem. Finally, thanks to the referee who suggested the elementary approach based on Lemma 4.1 and to Gopal Prasad who pointed out a gap in the proof of Lemma 4.1.

**References**


Department of Mathematics, University of Houston, Houston, Texas 77204-3476

E-mail address: mf@uh.edu