UNIFORM FINITE GENERATION OF THE ORTHOGONAL GROUP

AND

APPLICATIONS TO CONTROL THEORY

by

MARIA DE FÁTIMA DA SILVA LEITE

A Thesis submitted in candidature for the degree of

DOCTOR OF PHILOSOPHY

at the

UNIVERSITY OF WARWICK

in the

CONTROL THEORY CENTRE

NOVEMBER 1982

TABLE OF CONTENTS.

ACKNOWLEDGEMENTS.

I wish to pay a special tribute to my supervisor, Dr. P. Crouch, for his guidance and encouragement.

I am also most grateful to the Calouste Gulbenkian Foundation for their financial support.

Many thanks are also due to Peta McAllister for her excellent typing.

SUMMARY.

A Lie group G is said to be uniformly finitely generated by one parameter subgroups $\exp(tX_i)$, $i = 1,\ldots,n$, if there exists a positive integer k such that every element of G may be expressed as a product of at most k elements chosen alternatively from these one-parameter subgroups.

In this text we construct sets of left invariant vector fields on $SO(n)$, in particular pairs $\{A,B\}$, whose one-parameter subgroups uniformly finitely generate $SO(n)$. As a consequence, we also partially solve the uniform controllability problem for a class of systems $\dot{x}(t) = (\sum_{i=1}^{m} u_i(t)X_i)x(t)$, $x \in SO(n)$, $\{X_i, i = 1,\ldots,m\}_{L.A} = so(n)$ by putting an upper bound on the number of switches in the trajectories, in positive time, of $X_1,\ldots,X_m$ that are required to join any two points of $SO(n)$.

This result is also extended to any connected and paracompact C^k-manifold of dimension n using a result of N. Levitt and H. Sussmann. An upper bound is put on the minimum number of switches of trajectories, in positive time, required to join any two states on M by two vector fields on M. This bound depends only on the dimension of M.

INTRODUCTION.

Most interest in controllability on connected Lie groups G, or homogeneous spaces of G has, so far, concentrated on finding conditions under which a system

$$\dot{x}(t) = X_0(x(t)) + \sum_{i=1}^{n} u_i(t)X_i(x(t)) \ , \quad x \in G \ , \quad |u_i(t)| \leq M \leq \infty$$

is controllable, where X_0, X_1, ..., X_n are left (or right) invariant vector fields on G. That is, characterizing elements $X_0, X_1, \ldots, X_n$ of the Lie algebra $L(G)$ of G, which generate $L(G)$, in such a way that the expression for $g \in G$, can be assumed to involve only elements of the form $\exp(t(X_0 + \sum_{i=1}^{n} u_i(t)X_i)$, $0 < t < \infty$, where exp is the exponential map on G. If X_0 generates a compact one-parameter subgroup or G is compact then the problem reduces to that of characterizing generators of the Lie algebra; see Jurdjevic and Sussmann [7] and Jurdjevic and Kupka [5].

Little attention has been devoted to the problem of expressing particular elements of the group (or related homogeneous space) as products of elements from the one-parameter subgroups generated by generators $X_1, \ldots, X_n$ of the Lie algebra.

It is well known that if the Lie algebra of a connected Lie group G is generated by the elements $X_1,\ldots,X_n$, then every element g belonging to G may be expressed as a finite product of elements from the one-parameter subgroups generated by $X_1,\ldots,X_n$; see Jurdjevic and Sussmann [7]. However the number of elements required in the expression for g may not be uniformly bounded as g ranges through G. It follows from an argument in Lowenthal [14] that if in addition G is compact and the one-parameter subgroups generated by $X_1,\ldots,X_n$ are also compact, then G is uniformly finitely generated by $\exp(tX_1),\ldots,\exp(tX_n)$. That is, there exists a positive integer k such that every element of G may be expressed as a product of at most k elements from the one-parameter subgroups generated by $X_1,\ldots,X_n$.

The compactness of $\exp(tX_1),\ldots,\exp(tX_n)$ is not a necessary condition for the uniform finite generation of G even when G is compact (an example of this will be given in Chapter I).

Of particular interest due to its immediate consequences for controllability on Lie groups is the problem of characterizing the Lie groups G which are uniformly finitely generated and the corresponding generators $X_1,\ldots,X_n$ of $L(G)$.

In [12], Levitt and Sussmann show that for any connected and paracompact C^k $(2 \leq k \leq \infty)$ manifold of dimension m, there exists

a pair $\{X,Y\}$ of vector fields on M, such that any two points of M can be joined by trajectories, in positive time, of the vector fields X and Y, which involve a number of switches that is uniformly bounded by an integer $N(m)$, depending only on m. However, if M is a Lie Group, or homogeneous space of G, X and Y are not elements of the Lie algebra $L(G)$, and this result cannot be applied to the uniform finite generation problem.

The complete solution of this problem has been found by Lowenthal and by Koch and Lowenthal but only for two and three-dimensional Lie groups; [8], [9], [10], [13], [14], [15], [16]. In particular, in [14] the complete answer is given for $SO(3)$, the real special orthogonal group of dimension three, with Lie algebra $so(3)$. Lowenthal calculates the integer k of uniform finite generation and shows that it is a function of the angle between the axes of two generators. (Note that any two linearly independent elements of $so(3)$ generate $so(3)$ as a Lie algebra and the corresponding one-parameter subgroups are compact.) In particular $k = 3$ if and only if the generators are orthogonal (identifying elements of $so(3)$ with vectors in $\mathbb{R}^3$ as usual). See also Davenport [1].

In this case the decomposition of $SO(3)$ by one-parameter

subgroups corresponds to the classical Euler decomposition.

The complete solution of the uniform finite generation problem in general, does not appear to be easily answered. One of the main difficulties being lack of a complete characterization of the generators of a Lie algebra, although significant results have already been obtained in this direction. For instance see Jurdjevic and Kupka [5] and Jurdjevic and Sussmann [6].

This thesis takes the initial steps in the uniform finite generation problem of $SO(n)$, the real, $n(n-1)/2$ - dimensional special orthogonal group, with Lie algebra $so(n)$. The results obtained here are original unless otherwise referred.

Chapter I is mainly introductory but includes an alternative proof to a result by Lowenthal [14] on the uniform generation of $SO(3)$ and also pairs of generators of $so(n)$ are constructed, some of which do not generate compact one-parameter subgroups.

Chapters II, III and IV are concerned with the main problem. Unlike the methods of [14], the basic idea is to use a generalization of the Euler decomposition as in Hermann [3], which is itself a result of a general decomposition theory for semisimple Lie groups G, based on the theory of symmetric spaces, and briefly discussed in §1, Chapter II. (Presumably other decompositions of Lie groups

could also be used successfully.) The resultant decomposition of the group into a finite number of one-parameter subgroups involves a certain set $\{A_1,\ldots A_m\}$ of elements of $L(G)$, the corresponding generating set of $L(G)$. In §2 and §3, Chapter II, some of the possible decompositions of $SO(n)$ are considered (using this theory). An upper bound is found for the uniform finite generation of $SO(n)$ by the one-parameter subgroups generated by those elements of $so(n)$ that belong to the corresponding generating set.

Special attention is however given to pairs $\{A,B\}$ of generators of $so(n)$ which are known to exist for every real semisimple Lie algebra [Theorem 3.1, Chapter I]. Since not all elements of $so(n)$, generate compact subgroups, for $n \geq 4$, (a fact seemingly overlooked in [12]), Chapters III and IV concentrate on the problem of finding pairs of generators of $so(n)$, whose corresponding one-parameter subgroups are compact and uniformly finitely generate $SO(n)$.

In Chapter III, a class of pairs of generators of $so(n)$, orthogonal with respect to the killing form, is constructed. Each of these pairs is such that every element belonging to $\exp(tA_i)$, $i = 1,\ldots,m$, $t \in \mathbb{R}$ (where $\{A_1,\ldots,A_m\}$ is the generating set obtained in Chapter II), may be expressed as a finite product

involving only elements from the one-parameter subgroups generated by A and B, uniformly in $t \in \mathbb{R}$. In particular, this result is combined with one obtained in Chapter II to find an upper bound for the uniform finite generation of $SO(n)$ by $\exp(tA)$ and $\exp(\tau B)$.

In general, this upper bound depends on the decomposition of the group used, the generators of the Lie algebra used and their relation to each other.

Chapter IV is concerned with the same problem for nonorthogonal pairs of generators. The methods used to construct such pairs are similar in both Chapters III and IV and permutation matrices play a very important role.

Applications to Control Theory appear in Chapter V. The uniform finite generation of $SO(n)$ by compact one-parameter subgroups generated by A and B is the same as uniform complete controllability of $\{A,B\}$ and consequent uniform controllability of symmetric systems $\dot{x}(t) = (u_1(t)A + u_2(t)B)x(t)$, $x \in SO(n)$, $|u_i(t)| \leq M \leq \infty$, $i = 1,2$. $\{A,B\}$ is said to be completely controllable on $SO(n)$ if any two points of $SO(n)$ can be joined by a trajectory, in positive time, of $\{A,B\}$. If there also exists

a positive integer $R(n)$ such that the number of switches that the trajectory of $\{A,B\}$ involves, is at most $R(n)$, $\{A,B\}$ is said to be uniformly completely controllable. Since the integer $N(n)$ appearing in [12] depends only on $R(n)$, for some pair $\{A,B\}$ it is possible to put an upper bound on the minimum number of switches required to join any two states on a connected and paracompact n-dimensional manifold, by trajectories, in positive time, of two vector fields on M. This bound depends only on the dimension of M. Finally, the controllability properties of pairs $\{A,B\}$ of vector fields on $SO(n)$ constructed in Chapters III and IV are used to obtain a set of left-invariant vector fields on $SO_0(n,1)$, which is uniformly completely controllable.

Chapter VI contains a few concluding remarks and also points to some directions for further research in the uniform finite generations of Lie groups.

CHAPTER I

UNIFORM FINITE GENERATION OF LIE GROUPS.

§1. UNIFORM FINITE GENERATION OF LIE GROUPS AND ITS ORDER OF GENERATION.

DEFINITION 1.1. - A connected Lie Group G is said to be uniformly finitely generated by one - parameter subgroups $\exp(tX_1),\ldots,\exp(tX_n)$ if there is a positive integer k such that every element of G can be written as a product of at most k elements chosen from these subgroups. The least such k is called the *order of generation* of G.

Although the order of generation of G depends on the one-parameter subgroups, it must be greater than or equal to the dimension of G. In fact, if $f:\mathbb{R}^k \to G$ is defined to be the map which to each element $(t_1,\ldots,t_k)$ of $\mathbb{R}^k$ assigns $\prod_{j=1}^{k} \exp(t_j X_{i_j})$, $i_j \in \{1,\ldots,n\}$ and if it is assumed that the order of generation of G is less than $\dim G$ i.e. $k < \dim G$, all points of $\mathbb{R}^k$ are critical. Since f is real analytic the set of its critical values has measure zero (Sard's theorem [18]) so $k \geq \dim G$.

The following theorem, proved by Lowenthal [14] for a pair of generators, is a sufficient condition for the uniform finite generation of a connected and compact Lie group.

THEOREM 1.1. - Let G be a connected and compact Lie Group, $X_1,\dots,X_n$ generators of the Lie algebra $L(G)$ and $\exp(tX_i)$, $i = 1,\dots,n$, compact. Then G is uniformly finitely generated by $\exp(tX_i)$, $i = 1,\dots,n$.

Proof - Let G_m be the set of all products of m elements $\exp(tX_i)$, $i = 1,\dots,n$. $\exp(tX_i)$ is compact for every i so G_m is also compact. Since G is connected and $\{X_1,\dots,X_n\}_{L.A} = L(G)$, for every $g \in G$ there is an integer ℓ s.t. g is a product of ℓ elements of the form $\exp(tX_i)$, $i = 1,\dots,n$, $t \in \mathbb{R}$ (Sussmann and Jurdjevic [7]). Then $\forall\, g \in G$, $g \in G_\ell$ and $G = \bigcup_{\ell=1}^{\infty} G_\ell$. G is complete since, being connected and compact, it is metrizable (Riemannian metric) so by the Baire category theorem, G is of second category and G_ℓ, for some ℓ, contains an open set U. Hence $G = \bigcup_{g\in G} gU$; since $\forall g \in G$, gU is open this is an open cover for G and clearly it contains a finite subcover i.e. there are $g_1,\dots,g_r$ s.t. $G = \bigcup_{i=1}^{r} g_i U$. But each g_i, $i = 1,\dots,r$ is a finite product of elements of $\exp(tX_i)$, $i = 1,\dots,n$ and $U \subset G_\ell$ so the proof is complete.

□

§2. UNIFORM FINITE GENERATION OF SO(3).

Corollary 2.1. - SO(3) is uniformly finitely generated by any two one-parameter subgroups $\exp(tA)$ and

$\exp(sB)$ unless $[A,B] = 0$.

Proof - Since $so(3)$ (the set of all 3×3 skew-symmetric real matrices) is isomorphic to $\mathbb{R}^3$ with the Lie bracket corresponding to the vector product, it is clear that if A and B are any two elements of $so(3)$ that do not commute, then $\{A,B,[A,B]\}$ is a basis for $so(3)$ and $\{A,B\}_{L.A.} = so(3)$. Every rotation of $SO(3)$ is a plane rotation and as a consequence $\exp(tA)$ and $\exp(sB)$ are compact. Now theorem 1.1 applies since $SO(3)$ is connected and compact and the result follows. □

The order of generation of $SO(3)$ by two one-parameter subgroups was found by Lowenthal [14] and it is a function of the angle between the axes of the two rotations as follows:

THEOREM 2.1. - Let ψ , $0 < \psi \leq \pi/2$, be the angle between the axes of two one-parameter rotation groups $\exp(tA)$ and $\exp(sB)$ of $SO(3)$. If $\psi = \pi/2$, the order of generation of $SO(3)$ by those one-parameter subgroups is 3 ; if $\pi/(k+1) \leq \psi < \pi/k$, then the order of generation is $k+2$ $(k\geq2)$.

The proof of this theorem is rather long. Instead of working with $SO(3)$ Lowenthal works with the induced subgroup of the Möbius

group and Tchebychev polynomials play an important role in the proof.

When $\psi \in [\pi/2k , \pi/(2k-1))$, $k \geq 2$, a much shorter proof was found to determine the order of generation of $SO(3)$. Although when $\psi \in [\pi/(2k-1) , \pi/(2k-2))$ the result is not as good as Lowenthal's, the complete proof, in both cases, is included here.

THEOREM 2.2. - The order of generation of $SO(3)$ by the two one-parameter subgroups $\exp(tA_1)$ and $\exp(sA_2)$ is 3 if $\psi = \pi/2$ and if $\psi \in [\pi/2(k-1) , \pi/2(k-2))$, $k \geq 3$, the order of generation is $2k-1$. (ψ is the angle between the axes of the two rotations).

The term "order of generation" is not correctly used here when $\psi \in [\pi/(2k-1), \pi/(2k-2))$; instead "an upper bound on the order of generation" should be used. However, for the sake of simplicity, the former is preferred to the latter.

This theorem was proved without any prior knowledge of the result that constitutes theorem 2.1. Several lemmas are needed to prove theorem 2.2.

For every vector $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ a skewsymmetric matrix $X = \begin{pmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{pmatrix}$, formed with the components of x is defined. It is easy to check that $\forall y \in \mathbb{R}^3$, $Xy = x \times y$.

Lemma 2.1.- $\forall R \in SO(3)$ and $\forall x, y \in \mathbb{R}^3$ with $||x|| = ||y||$, $Rx = y$ if and only if $RXR^{-1} = Y$.

Proof - Let x and y be nonzero vectors. If $RXR^{-1} = Y$ then $RXR^{-1}y = Yy = 0$ and $XR^{-1}y = 0$ since $R \in SO(3)$ preserves the norm. Let $R^{-1}y = z$; then $Xz = 0$. Since $||x|| = ||y|| = ||z||$, $R^{-1}y = x$ or $Rx = y$.

Now $Rx = y$ i.e. $R^{-1}y = x$. Then, $RXR^{-1}y = 0$ since $XR^{-1}y = Xx = 0$. Let $RXR^{-1} = Z$; then $Zy = 0$ i.e. $Z = Y$ and the lemma is proved.

□

Lemma 2.2. - Every rotation $R \in SO(3)$ is representable as a product $R = \exp(t_1X) \exp(t_2Y) \exp(t_3Z)$, $t_i \in \mathbb{R}$, $i = 1,2,3$, if and only if y is perpendicular to x and z.

The proof can be found in Davenport [1]. $\forall x \in \mathbb{R}^3$, $\exp(tX)$ is the one-parameter subgroup of $SO(3)$ that leaves x fixed. It is assumed that x and z may be equal. If that is the case then Lemma 2.2 states the same thing as the first part of theorem 2.1. If not just x and z are equal but also x and y are two orthogonal unit vectors in $\mathbb{R}^3$, the representation of R in Lemma 2.2 is the Euler representation of a rotation by three angular parameters, the Euler angles.

Now, let a_1 and a_2 be two linearly independent vectors of $\mathbb{R}^3$ and $\psi = \sphericalangle(a_1,a_2)$ the angle between them. a_1 and a_2 generate a plane Π. Without loss of generality, a_1 and a_2 can be assumed to be unit vectors. Let $\{a_1,a_2,a_3,\ldots\}$ be a sequence of vectors on Π where, $\forall\, i \geq 3$, $a_i = \exp(\pi A_{i-1}).a_{i-2}$. ($A_j$ is the skewsymmetric matrix corresponding to a_j, $\forall\, j$). $\sphericalangle(a_i,a_{i+1}) = \psi$, $\forall\, i \geq 1$ and $\sphericalangle(a_1,a_i) = (i-1)\psi$, $\forall\, i \geq 1$. Let a_k be the first element in the sequence satisfying $\sphericalangle(a_1,a_k) \geq \pi/2$ i.e. $(k-1)\,\psi \geq \pi/2$ or $\psi \geq \pi/2(k-1)$. (See fig. 1.) Clearly there exists a vector $x \in \Pi_1$ (Π_1 is the plane perpendicular to a_1) such that $x = \exp(tA_{k-1}).a_{k-2}$ for some $t \in (0,2\pi]$. Since a_1 and x are perpendicular, Lemma 2.2 can be applied and $\forall\, R \in SO(3)$,

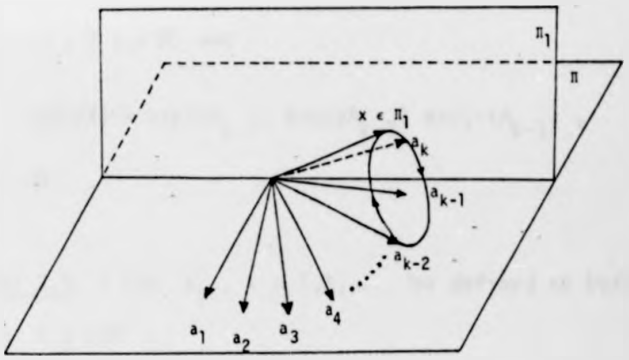


Figure 1.

$$R = \exp(t_1 A_1)\, \exp(t_2 X)\, \exp(t_3 A_1) \ , \ t_i \in \mathbb{R} \ . \qquad (2.1)$$

At this stage the aim is to write $\exp(t_2 X)$ as a product of elements from the one-parameter subgroups $\exp(tA_1)$ and $\exp(sA_2)$.

Since $a_i = \exp(\pi A_{i-1}).a_{i-2}$, $i \geq 3$ and $x = \exp(tA_{k-1}).a_{k-2}$, for some t , using lemma 2.1 it follows that

$\forall i \geq 3$, $A_i = \exp(\pi \text{ ad } A_{i-1}).A_{i-2}$ and $X = \exp(t \text{ ad } A_{k-1}).A_{k-2}$;

hence, by the Baker-Campbell-Hausdorff formula

$$\exp(\theta A_i) = \exp(\pi A_{i-1}) \exp(\theta A_{i-2}) \exp(-\pi A_{i-1}), \qquad (2.2)$$

$\forall\, i \geq 3$, $\forall\, \theta \in \mathbb{R}$ and

$$\exp(\theta X) = \exp(tA_{k-1}) \exp(\theta A_{k-2}) \exp(-tA_{k-1}) , \qquad (2.3)$$

$\forall\, \theta \in \mathbb{R}$.

Lemma 2.3. - Let A_i , $i = 1,2,\ldots$ be defined as before.

Then $\forall\, \theta \in \mathbb{R}$,

$$e^{\theta A_i} = \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2} e^{\pi A_1}}_{i-2} e^{\theta A_2} \underbrace{e^{-\pi A_1} e^{-\pi A_2} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{i-2}, \qquad (2.4)$$

$i = 2n$ and

$$e^{\theta A_i} = \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2} e^{\pi A_1} e^{\pi A_2}}_{i-2} e^{\theta A_1} \underbrace{e^{-\pi A_2} e^{-\pi A_1} \ldots e^{-\pi A_2}}_{i-2}, \qquad (2.5)$$

$i = 2n+1$.

Proof (by induction) - It will be proved first that the lemma is true for $i = 2$ and $i = 3$. Then, assuming that it is true for $i = 2m-2$ and $i = 2m-1$ it will be proved to be also true for $i = 2m$ and $i = 2m+1$, $m \in \mathbb{N}$.

The relation (2.4) is trivial when $i = 2$ and when $i = 3$ both, (2.5) and (2.2) are the same relation so (2.5) is true when $i = 3$.

Now, from (2.2) with $i = 2m$,

$$e^{\theta A_{2m}} = e^{\pi A_{2m-1}} e^{\theta A_{2m-2}} e^{-\pi A_{2m-1}} \quad \text{and}$$

since (2.4) and (2.5) are assumed to be satisfied when $i = 2m-2$ and $i = 2m-1$ respectively, it follows,

$$e^{\theta A_{2m}} = \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2}}_{2m-3} e^{\pi A_1} \underbrace{e^{-\pi A_2} \ldots e^{-\pi A_1}}_{2m-3} e^{-\pi A_2} \underbrace{e^{\pi A_2} \ldots e^{\pi A_1}}_{2m-4} e^{\theta A_2}$$

$$\underbrace{e^{-\pi A_1} e^{-\pi A_2} \ldots e^{-\pi A_2}}_{2m-4} \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2}}_{2m-3} e^{-\pi A_1} \underbrace{e^{-\pi A_2} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{2m-3} =$$

$$= \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2}}_{2m-3} e^{\pi A_1} e^{-\pi A_2} e^{\theta A_2} e^{\pi A_2} e^{-\pi A_1} \underbrace{e^{-\pi A_2} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{2m-3} =$$

$$= \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2} e^{\pi A_1}}_{2m-2} e^{\theta A_2} \underbrace{e^{-\pi A_1} e^{-\pi A_2} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{2m-2} .$$

Similarly, from (2.2) with $i = 2m+1$,

$$e^{\theta A_{2m+1}} = e^{\pi A_{2m}} e^{\theta A_{2m-1}} e^{-\pi A_{2m}}$$

and since (2.4) and (2.5) are assumed to be satisfied when $i = 2m$

and $i = 2m-1$ respectively it follows

$$e^{\theta A_{2m+i}} = \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2} e^{\pi A_1}}_{2m-2} e^{\pi A_2} \underbrace{e^{-\pi A_1} e^{-\pi A_2} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{2m-2}$$

$$\underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2}}_{2m-3} e^{\theta A_1} \underbrace{e^{-\pi A_2} \ldots e^{-\pi A_1}}_{2m-3} e^{-\pi A_2} \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2} e^{\pi A_1}}_{2m-2}$$

$$e^{-\pi A_2} \underbrace{e^{-\pi A_1} e^{-\pi A_2} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{2m-2} =$$

$$= \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2} e^{\pi A_1}}_{2m-2} e^{\pi A_2} e^{-\pi A_1} e^{\theta A_1} e^{\pi A_1} e \underbrace{e^{-\pi A_2} e^{-\pi A_1} \ldots . e^{-\pi A_1} e^{-\pi A_2}}_{2m-2} =$$

$$= \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2}}_{2m-1} e^{\theta A_1} \underbrace{e^{-\pi A_2} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{2m-1}$$

and the lemma is proved.

□

Lemma 2.4. - If the angle $\psi = \sphericalangle(a_1, a_2) \in [\pi/2(k-1), \pi/2(k-2))$, $k \geq 3$, then,

$$e^{\theta X} = \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_2}}_{k-3} e^{tA_1} e^{\theta A_2} e^{-tA_1} \underbrace{e^{-\pi A_2} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{k-3}, \text{ if } k \text{ even} \quad (2.6)$$

and

$$e^{\theta X} = \underbrace{e^{\pi A_2} e^{\pi A_1} \ldots e^{\pi A_1}}_{k-3} e^{tA_2} e^{\theta A_1} e^{-tA_2} \underbrace{e^{-\pi A_1} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{k-3}, \text{ if } k \text{ odd} \quad (2.7)$$

for some $t \in (0,2\pi]$, $\theta \in \mathbb{R}$.

Proof - $e^{tA_{k-1}}$ and $e^{\theta A_{k-2}}$ can be written as a product of elements from $e^{\tau A_1}$ and $e^{\tau A_2}$ ($\tau \in \mathbb{R}$) by using (2.4) and (2.5) respectively if k is even or (2.5) and (2.4) respectively if k is odd. Now, using (2.3) and taking into account the composition of terms with the same generator the relations (2.6) and (2.7) follow.

Proof of Theorem 2.2 - When $\psi = \pi/2$, the result is an immediate consequence of Lemma 2.2 with $x = z = a_1$ and $y = a_2$; the order of generation is then equal to 3 . When $\psi \in [\pi/2(k-1),\pi/2(k-2))$ it was seen that $\exists\, x \in \mathbb{R}^3$, x perpendicular to a_1 , such that $R = \exp(t_1 A_1) \exp(t_2 X) \exp(t_3 A_1)$, for every $R \in SO(3)$ and

$t_i \in \mathbb{R}$. But $\exp(t_2 X)$ can be written as a product of $2(k-3)+3$ elements from the one-parameter subgroups $\exp(\tau_1 A_1)$ and $\exp(\tau_2 A_2)$ (Lemma 2.4) and so, the order of generation of $SO(3)$ is in this case $2(k-3)+3+2 = 2k-1$, $\forall\, k \geq 3$ which completes the proof.

□

Remark - Since there exists an automorphism of $SO(3)$ that interchanges the two one-parameter subgroups $\exp(tA_1)$ and $\exp(\tau A_2)$, every element of $SO(3)$ can also be written as a product of $2k-1$ elements from those subgroups whose first and last elements belong to $\exp(tA_2)$.

§3. LIE ALGEBRAS GENERATED BY TWO ELEMENTS. so(n) AS A PARTICULAR CASE.

The following theorem, which gives a sufficient condition for Lie algebras to be generated by two elements, is due to Kuranishi [11].

THEOREM 3.1. - Every finite dimensional and semisimple Lie algebra over a field of characteristic zero has a pair of generators.

As an immediate consequence of this theorem, the semisimple

Lie algebra $so(n,\mathbb{R})$, $n \geq 3$, is generated by a pair of vector fields. It is not clear, however, as it is in the 3-dimensional case, whether or not the corresponding one-parameter subgroups are compact and so theorem 1.1 can not be applied. An interesting question to be answered then is: Do sets of generators of $so(n,\mathbb{R})$ (in particular a pair) generate compact one parameter subgroups? The answer will be given at the end of this paragraph.

In the next theorem pairs of generators of $so(n,\mathbb{R})$ will be constructed. Before starting several definitions and concepts are recalled. For details concerning these ideas see Helgason [2] and Humphreys [4].

Let $g_{\mathbb{C}}$ be a finite-dimensional semisimple Lie algebra over $\mathbb{C}$, h a Cartan subalgebra of $g_{\mathbb{C}}$ and Φ the set of nonzero roots of $g_{\mathbb{C}}$ (with respect to h).

For each $\alpha \in \Phi$, there exists a unique $H_\alpha \in h$ such that $\langle H,H_\alpha \rangle = \alpha(H)$, $\forall H \in h$ ($\langle \cdot,\cdot \rangle$ is the bilinear form on $g_{\mathbb{C}} \times g_{\mathbb{C}}$ defined by $\langle X,Y \rangle = \text{trace}(\text{adX adY})$ and called the killing form of $g_{\mathbb{C}}$). Define $h_{\mathbb{R}} = \sum_{\alpha \in \Phi} \mathbb{R} H_\alpha$; the killing form is strictly positive definite on $h_{\mathbb{R}} \times h_{\mathbb{R}}$ and $h = h_{\mathbb{R}} \oplus i h_{\mathbb{R}}$ (Helgason [2, p.170]). It is convenient to identify Φ with $h_{\mathbb{R}}$ and then define an ordering of Φ induced by some vector space ordering of

$h_{\mathbb{R}}^*$ (the dual space of $h_{\mathbb{R}}$) . A positive root is called simple or fundamental if it cannot be written as a sum of two positive roots. Φ^+ and Δ will denote the set of positive roots and the set of simple roots respectively. The following properties of Δ will be used later.

1. If $\alpha,\beta \in \Delta$ then $\alpha-\beta \notin \Phi$.

2. Δ is a basis for Φ . In fact, $\forall\, \alpha \in \Phi, \alpha = \Sigma\, n_i\, \beta_i$ with $\beta_i \in \Delta$ and n_i integers that are either all positive or all negative.

For each $\alpha \in \Phi$ there also exists an element $X_\alpha \in g_{\mathbb{C}}$ such that $\langle X_\alpha, X_{-\alpha}\rangle = 1$, and $\forall\, \alpha,\beta \in \Phi$

$$[X_\alpha, X_{-\alpha}] = H_\alpha \quad ; \quad [H, X_\alpha] = \alpha(H) X_\alpha \ , \ \forall\, H \in h$$
$$[X_\alpha, X_\beta] = \begin{cases} 0 & \text{if } \alpha+\beta \notin \Phi \\ N_{\alpha,\beta} X_{\alpha+\beta} & \text{if } \alpha+\beta \in \Phi \end{cases} \tag{3.1}$$

where $N_{\alpha,\beta}$ are real constants satisfying $N_{\alpha,\beta} = -N_{-\alpha,-\beta}$. $\{X_\alpha, \alpha \in \Phi\}$ is called the Weyl basis of $g_{\mathbb{C}}$ (with respect to h).

Now let $g_{\mathbb{C}} = so(n,\mathbb{C})$. The compact real form $so(n,\mathbb{R})$ of $g_{\mathbb{C}}$ is spanned by the elements iH_α , $X_\alpha - X_{-\alpha}$ and $i(X_\alpha + X_{-\alpha})$;

(H_α, X_α and $X_{-\alpha}$ defined as above) and

$$so(n,\mathbb{R}) = \sum_{\alpha\in\Phi} \mathbb{R}(iH_\alpha) \oplus \sum_{\alpha\in\Phi} \mathbb{R}(X_\alpha - X_{-\alpha}) \oplus \sum_{\alpha\in\Phi} i\mathbb{R}(X_\alpha + X_{-\alpha})$$

$$= A \oplus \sum_{\alpha\in\Phi} \mathbb{R} E_\alpha \oplus \sum_{\alpha\in\Phi} \mathbb{R} F_\alpha$$

$A = ih$ is the Cartan subalgebra of $so(n,\mathbb{R})$.

Using (3.1) it follows that, $\forall\ \alpha \in \Phi$

$$\begin{aligned} [iH, E_\alpha] &= \alpha(H) F_\alpha \quad , \quad \forall\ H \in h \\ [iH, F_\alpha] &= -\alpha(H) E_\alpha \quad , \quad \forall\ H \in h \\ [E_\alpha, F_\alpha] &= 2iH_\alpha \quad . \end{aligned} \tag{3.2}$$

Hence, using (3.1) and property 1. of Δ it follows that $\forall\ \alpha,\beta \in \Delta$,

$$[E_\alpha, E_\beta] = -[F_\alpha, F_\beta] = \begin{cases} 0 & \text{if } \alpha+\beta \notin \Phi \\ N_{\alpha,\beta} E_{\alpha+\beta}, & \text{if } \alpha+\beta \in \Phi \end{cases}$$

$$[E_\alpha, F_\beta] = \begin{cases} 0 & \text{if } \alpha+\beta \notin \Phi \\ N_{\alpha,\beta} F_{\alpha+\beta}, & \text{if } \alpha+\beta \in \Phi \end{cases} .$$

THEOREM 3.2. - Let $g = so(n,\mathbb{R})$, $n > 3$ and $B = \sum_{\alpha\in\Delta} e_\alpha E_\alpha \in g$. There are real numbers e_α and $A \in g$ such that $\{A,B\}_{L.A} = g$.

Proof - Let $A \in \mathcal{A}$. Then $A = iH$ for some $H \in h$ (h - the Cartan subalgebra of $g_{\mathbb{C}}$). $B = \sum_{\alpha\in\Delta} e_\alpha E_\alpha$ and using (3.2) it follows

$$
\begin{aligned}
&\operatorname{ad} A(B) = \sum_{\alpha\in\Delta} e_\alpha\, \alpha(H) F_\alpha \\
&\operatorname{ad}^2 A\,(B) = -\sum_{\alpha\in\Delta} e_\alpha\, (\alpha(H))^2\, E_\alpha \qquad (3.3)\\
&\operatorname{ad}^3 A\,(B) = -\sum_{\alpha\in\Delta} e_\alpha\, (\alpha(H))^3\, F_\alpha \\
&\quad\vdots \\
&\operatorname{ad}^{2\ell-2} A(B) = (-1)^{\ell-1} \sum_{\alpha\in\Delta} e_\alpha\, (\alpha(H))^{2\ell-2} E_\alpha \\
&\operatorname{ad}^{2\ell-1} A(B) = (-1)^{\ell-1} \sum_{\alpha\in\Delta} e_\alpha\, (\alpha(H))^{2\ell-1} F_\alpha \\
&\quad\vdots
\end{aligned}
$$

Now, $\{\alpha(H)\ ,\ \alpha \in \Delta\} = \{\alpha_1,\alpha_2,\ldots,\alpha_{[n/2]}\}$, E_i and F_i denote E_{α_i} and F_{α_i} respectively, $i = 1,\ldots,[n/2]$ (similarly e_i and f_i stand for e_{α_i} and f_{α_i} respectively). From $B = \sum_{\alpha\in\Delta} e_\alpha E_\alpha$ and the first $2\ell-1$ equations in (3.3) with $\ell = [n/2]$ it follows

$$\begin{pmatrix} B \\ adA(B) \\ ad^2A(B) \\ ad^3A(B) \\ \vdots \\ ad^{2\ell-2}A(B) \\ ad^{2\ell-1}A(B) \end{pmatrix} = \underbrace{\begin{pmatrix} e_1 & e_2 & \cdots & e_\ell & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \alpha_1 e_1 & \alpha_2 e_2 & \cdots & \alpha_\ell e_\ell \\ -\alpha_1^2 e_1 & -\alpha_2^2 e_2 & \cdots & -\alpha_\ell^2 e_\ell & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & -\alpha_1^3 e_1 & -\alpha_2^3 e_2 & \cdots & -\alpha_\ell^3 e_\ell \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ (-1)^{\ell-1}\alpha_1^{2\ell-2}e_1 & (-1)^{\ell-1}\alpha_2^{2\ell-2}e_2 \cdots & & (-1)^{\ell-1}\alpha^{2\ell-2}e_\ell & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & (-1)^{\ell-1}\alpha_1^{2\ell-1}e_1 & (-1)^{\ell-1}\alpha_2^{2\ell-1}e_2 \cdots & & (-1)^{\ell-1}\alpha^{2\ell-1}e_\ell \end{pmatrix}}_{M} \begin{pmatrix} E_1 \\ E_2 \\ \vdots \\ E_\ell \\ F_1 \\ F_2 \\ \vdots \\ F_\ell \end{pmatrix}$$

If M is invertible, B, $adA(B),\ldots,ad^{2\ell-1}A(B)$ are linearly independent and the minimal subalgebra containing them also contains $\{E_i, F_i,\ i = 1,\ldots,\ell\}$. Since the absolute value of a determinant does not change when a permutation is applied to its rows, it is clear that M is invertible if and only if

$$\begin{vmatrix} e_1 & e_2 & \cdots & e_\ell \\ -\alpha_1^2 e_1 & -\alpha_2^2 e_2 & \cdots & -\alpha_\ell^2 e_\ell \\ \vdots & \vdots & & \vdots \\ (-1)^{\ell-1}\alpha_1^{2\ell-2} e_1 & (-1)^{\ell-1}\alpha_2^{2\ell-2} e_2 & \cdots & (-1)^{\ell-1}\alpha^{2\ell-2} e_\ell \end{vmatrix} \begin{vmatrix} \alpha_1 e_1 & \alpha_2 e_2 & \cdots & \alpha_\ell e_\ell \\ -\alpha_1^3 e_1 & -\alpha_2^3 e_2 & \cdots & -\alpha_\ell^3 e_\ell \\ \vdots & \vdots & & \vdots \\ (-1)^{\ell-1}\alpha_1^{2\ell-1} e_1 & (-1)^{\ell-1}\alpha_2^{2\ell-1} e_2 & \cdots & (-1)^{\ell-1}\alpha^{2\ell-1} e_\ell \end{vmatrix} \neq 0$$

or,
$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ -\alpha_1^2 & -\alpha_2^2 & \cdots & -\alpha_\ell^2 \\ \vdots & \vdots & & \vdots \\ (-1)^{\ell-1}\alpha_1^{2\ell-2} & (-1)^{\ell-1}\alpha_2^{2\ell-2} & \cdots & (-1)^{\ell-1}\alpha_\ell^{2\ell-2} \end{vmatrix}^2 \begin{vmatrix} \alpha_1 & & & 0 \\ & \alpha_2 & & \\ & & \ddots & \\ 0 & & & \alpha_\ell \end{vmatrix} \begin{vmatrix} e_1 & & & 0 \\ & e_2 & & \\ & & \ddots & \\ 0 & & & e_\ell \end{vmatrix}^2 \neq 0 .$$

Since the first determinant has the same absolute value as a Vandermonde determinant, M is invertible iff

$$\prod_{1\le i<j\le \ell} (\alpha_i^2-\alpha_j^2)^2 \prod_{i=1}^{\ell} \alpha_i \prod_{i=1}^{\ell} e_i^2 \neq 0 \ .$$

So, if $\forall\, \alpha \in \Delta$, $e_\alpha \neq 0$ and A is an element of the Cartan subalgebra of g satisfying $|\alpha(A)|$ are nonzero and distinct, $\forall\, \alpha \in \Delta$, then $\{B,A\}_{L.A}$ contains $\{E_\alpha, F_\alpha, \alpha \in \Delta\}_{L.A}$. It can easily be proved that $\{E_\alpha, F_\alpha, \alpha \in \Delta\}_{L.A} = so(n,\mathbb{R})$. In fact, let $g' = \{E_\alpha, F_\alpha, \alpha \in \Delta\}_{L.A}$. $\{H_\alpha, \alpha \in \Delta\} \subset g'_{\mathbb{C}}$ since $[E_\alpha, F_\alpha] = 2i\, H_\alpha$. $\{H_\alpha, \alpha \in \Delta\}$ is a basis of h (the Cartan subalgebra of $so(n,\mathbb{C})$) so h is a Cartan subalgebra of $g'_{\mathbb{C}}$. Hence, $\forall\, \beta \in \Phi$, $\beta = \sum_{\alpha_i \in \Delta} n_i \alpha_i$ (property 2. of Δ) so, Φ is the set of roots of $g'_{\mathbb{C}}$. Since a semisimple Lie algebra over $\mathbb{C}$ is determined (up to isomorphism) by means of a Cartan subalgebra and the corresponding set of roots (Helgason [2, p.173]), $g'_{\mathbb{C}} = so(n,\mathbb{C})$ and $\{E_\alpha, F_\alpha, \alpha \in \Delta\}_{L.A} = so(n,\mathbb{R})$.

To summarize, if $\forall\, \alpha \in \Delta$, $e_\alpha \neq 0$ and $A \in A$ satisfies $|\alpha(A)|$ are nonzero and distinct $\forall\, \alpha \in \Delta$, then $\{B = \sum_{\alpha \in \Delta} e_\alpha E_\alpha,\ A\}_{L.A} = so(n,\mathbb{R})$.

□

Remark - In a similar way it can be proved that if $B_1 = \sum_{\alpha\in\Delta} f_\alpha F_\alpha$, $f_\alpha \neq 0$ $(\forall\, \alpha \in \Delta)$ and A as above, then $\{B_1, A\}_{L.A} = so(n,\mathbb{R})$.

A canonical basis of $so(n,\mathbb{R})$ can be defined, namely the skewsymmetric matrices A_{ij} ; $1 \leq i < j \leq n$ where

$$[A_{ij}]_{k\ell} = \begin{cases} \delta_{ik}\ \delta_{j\ell} & \text{if} \quad 1 \leq k \leq \ell \leq n \\ -\delta_{i\ell}\ \delta_{jk} & \text{if} \quad 1 \leq \ell \leq k \leq n \end{cases}$$

($[A]_{k\ell}$ stands for the $k\ell$-th component of a matrix A.)

$\{A_{2i-1,2i}$, $i = 1,\ldots,[n/2]\}$ is a basis of a Cartan subalgebra A of $so(n,\mathbb{R})$.

Given $A = \sum_{i=1}^{[n/2]} \beta_i A_{2i-1,2i} \in A$, $A = iH$

$$\{\alpha(H), \alpha\in\Delta\} = \{\beta_i - \beta_{i+1}, i = 1,\ldots\tfrac{n}{2} - 1\} \cup \{\beta_{\frac{n}{2}-1} + \beta_{\frac{n}{2}}\} \text{ , if } n \text{ even}$$

and

$$\{\alpha(H), \alpha\in\Delta\} = \{\beta_i - \beta_{i+1},\ i = 1,\ldots,\tfrac{n-3}{2}\} \cup \{\beta_{\frac{n-1}{2}}\} \text{ , if } n \text{ is odd.}$$

Example 3.1. - $g = so(4,\mathbb{R})$. $A = A_{12} + \sqrt{2}\, A_{34} \in A$

and $\alpha(A) = \{i(1-\sqrt{2}), i(1+\sqrt{2})\}$. So, A satisfies the conditions $\alpha \in \Delta^+$ of theorem 3.2 and there exists $B \in g$ s.t. $\{A,B\}_{L.A} = so(4,\mathbb{R})$.

This example answers the question formulated earlier. In fact, although $\{A,B\}$ generates $so(4,\mathbb{R})$, $\exp(tA)$, $t \in \mathbb{R}$ is not compact since it is the noncompact line on the torus T generated by $\exp(A_{12}t)$ and $\exp(sA_{34})$. Theorem 1.1. cannot be applied here.

Although there are Lie Groups that can be uniformly finitely generated by one-parameter subgroups that are not compact (for instance $T = SO(2)\times SO(2)$ is generated by $\exp(tA_{12})$ and $\exp(s(A_{12} + \sqrt{2}\, A_{34})$ and the order of generation is 2), only compact one-parameter subgroups will be considered in order to be able to use Theorem 1.1.

CHAPTER II

DECOMPOSITION OF LIE GROUPS BASED ON SYMMETRIC SPACES AND CORRESPONDING GENERATING SETS OF SO(n).

§1. DECOMPOSITION OF LIE GROUPS BASED ON RIEMANNIAN SYMMETRIC SPACES.

This paragraph contains general ideas concerning Riemannian symmetric manifolds (R.S. Manifolds) and it is explained how Lie groups that can be regarded as Lie transformation groups on R.S. manifolds may be decomposed as a product of abelian subgroups. For full details see Helgason [2] and Wolf [20].

A Riemannian manifold M is called symmetric if each point $p \in M$ is an isolated fixed point of any involutive isometry s_p of M ($s_p \neq$ identity and $s_p^2 =$ identity). Connected R.S. manifolds are complete and any two points p and q in M can be joined by a geodesic γ of minimal length. If m is the midpoint of γ, s_m sends p to q therefore, the group $I(M)$ of isometries of M acts transitively on M. This action gives M the structure of a homogeneous space G/K where $G = I_0(M)$ is the identity component of $I(M)$ and K is the isotropy subgroup of G at a point x_0. The mapping $\sigma: G \to G$ defined by $\sigma(x) = s_{x_0} x s_{x_0}$ is an involutive automorphism of G and $K = \{x \in G: \sigma(x) = x\}$. The study of homogeneous spaces can then be reduced to the study of coset spaces G/K where G is a connected Lie group and K a compact subgroup of G. If g and $\mathcal{T}$ denote the Lie algebras of G and K respectively, $(d\sigma)_e$ is an involutive automorphism

of g and g admits a direct sum decomposition $g = T \oplus P$ with $T = \{X \in g : (d\sigma)_e X = X\}$ and $P = \{X \in g : (d\sigma)_e X = -X\}$. Since $(d\sigma)_e$ is an automorphism, it follows

$$[T,P] \subset P \ , \ [P,P] \subset T \ \text{ and } \ [T,T] \subset T \ . \tag{1.1}$$

T is a subalgebra of g and P is a vector space.

If Π denotes the natural mapping of G into M defined by $x \mapsto x.x_0$, $(d\Pi)_e$ is a linear mapping of g onto $T_{x_0}M$ (the tangent space of M at x_0) with kernel T that maps P isomorphically onto $T_{x_0}M$. Now, if $P = \exp P$, Π maps one-parameter subgroups contained in P into the geodesics emanating from x_0, $\exp(tX) \mapsto \exp tX.x_0$.

A Lie algebra g which admits a direct sum decomposition $g = T \oplus P$, into the ± 1 eigenspaces of an involutive automorphism s satisfying (1.1) and such that the group of inner automorphisms of g generated by T is compact, is said to be an orthogonal symmetric Lie algebra (g,s). A pair (G,K), where G is a connected Lie group with Lie algebra g and K is a Lie subgroup of G with Lie algebra T is said to be the

pair associated with the orthogonal symmetric Lie algebra (g,s) and K is called the symmetric subgroup.

A Cartan subalgebra of an orthogonal symmetric Lie algebra (g,s) is a maximal abelian subalgebra of P. All Cartan subalgebras of (g,s) are conjugate under $Ad_G K$, the adjoint representation of K, and for a Cartan subalgebra A, $P = \bigcup_{k\in K} Ad_G kA$.

Lemma 1.1. - If M is a R.S. manifold G/K then $G = KAK$ where $A = \exp A$ for any Cartan subalgebra A of the orthogonal symmetric Lie algebra associated with (G,K).

Proof - G acts transitively on M with action

$$\phi: G \times M \to M$$
$$(g,x) \mapsto g.x .$$

Any two points in M can be joined by a geodesic since M is complete. Therefore, $\forall\, g \in G$ and $\forall\, x \in M$ there exists a geodesic γ joining x and $g.x$. Identifying, as usual, the

tangent space T_xM with the subspace P , there exists $p \in P$ such that $g.x = p.x$. Since $(p^{-1}g).x = (p^{-1}p).x = x$, $p^{-1}g \in K$ and $g = pk$ for some $k \in K$ i.e. $G = PK$. But $P = \exp P =$

$= \exp \bigcup_{k\in K} Ad_G kA = \bigcup_{k\in K} k \exp A\, k^{-1} = \bigcup_{k\in K} kAk^{-1} \subset KAK$ and so

$G = KAKK$ or $G = KAK$.

□

Given a Lie group G , an involutive automorphism σ and corresponding symmetric subgroup K_1 define a decomposition $G = K_1A_1K_1$. If M is a R.S. manifold of the form G/K_1 each involutive isometry of M gives rise to an involutive automorphism of G . It is clear that R.S. manifolds play an important part in decompositions of Lie groups.

After having decomposed $G = K_1A_1K_1$, K_1 can be decomposed similarly, $K_1 = K_2A_2K_2$ to obtain $G = K_2A_2K_2A_1K_2A_2K_2$. If this procedure is continued until an abelian group K_i is encountered, G becomes a product of abelian subgroups $K_i, A_i, A_{i-1}, \ldots A_1$ namely

$$G = K_iA_iK_iA_{i-1}K_iA_iK_iA_{i-2}K_iA_iK_iA_{i-1}\ldots K_iA_iK_iA_1 \qquad (1.2)$$

$$K_iA_iK_i\ldots A_{i-1}K_iA_iK_iA_{i-2}K_iA_iK_iA_{i-1}K_iA_iK_i \ .$$

At each stage, different choices of involutive automorphisms may exist, each of which gives a different decomposition of the symmetric subgroup K_j and consequently of G.

After decomposing G as a product of abelian subgroups, the decomposition of G as a product of one-parameter subgroups is a trivial matter.

Involutive automorphisms σ for the classical matrix groups always exist. Full details can be found in Helgason [2].

§2. DECOMPOSITION OF SO(n)

Referring to Chapter I of Helgason [2], when $n \geq 3$, the only choices of R.S. manifolds $M = SO(n)/K$, and associated orthogonal symmetric Lie algebras $(so(n),\sigma)$ are given up to conjugacy by

$$I - g = so(p+q) = \left\{ \begin{pmatrix} X_1 & X_2 \\ -X_2^t & X_3 \end{pmatrix} ; X_1 \in so(p), X_3 \in so(q) \right\}$$
$$p \geq q \geq 1 \qquad\qquad X_2 \text{ arbitrary}$$

$$\sigma(X) = I_{p,q} X I_{p,q}, \quad I_{p,q} = \begin{pmatrix} -I_p & 0 \\ 0 & I_q \end{pmatrix}$$

$$T = \left\{ \begin{pmatrix} X_1 & 0 \\ 0 & X_3 \end{pmatrix} , \quad \begin{matrix} X_1 \in so(p) \\ X_3 \in so(q) \end{matrix} \right\} , \quad P = \left\{ \begin{pmatrix} 0 & X_2 \\ -X_2^t & 0 \end{pmatrix} , X_2 \text{ arbitrary} \right\}$$

$$K = SO(p) \times SO(q) \ .$$

A Cartan subalgebra of (g,σ) is $A = \sum_{i=1}^{q} \mathbb{R} A_{i,p+i}$ with dimension q .

II - $g = so(2n)$,

$n \geq 1$

$$\sigma(X) = J_n X J_n^{-1} \quad , \quad J_n = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

$$T = so(2n) \cap sp(n) \simeq u(n) = \left\{ \begin{pmatrix} X_3 & X_4 \\ -X_4 & X_3 \end{pmatrix} , \begin{matrix} X_3 \in so(n) \\ X_4 = X_4^t \end{matrix} \right\}$$

$$P = \left\{ \begin{pmatrix} X_1 & X_2 \\ X_2 & -X_1 \end{pmatrix} , \ X_1, X_2 \in so(n) \right\}$$

$K = U(n)$, where $U(n)$ is embedded into $SO(2n)$ via $A + iB \mapsto \begin{pmatrix} A & B \\ -B & A \end{pmatrix}$, $A + iB \in U(n)$.

A Cartan subalgebra of (g,σ) is $[\frac{n}{2}]$ - dimensional and generated by

$$\{A_{12} - A_{n+1,n+2}\ ,\ A_{34} - A_{n+2,n+3}, \cdots\}\ .$$

Since every Cartan subalgebra of $so(p+q)$ is $[\frac{p+q}{2}]$- dimensional, a Cartan subalgebra of the orthogonal symmetric Lie algebra $(so(p+q),\sigma)$ is a Cartan subalgebra of $so(p+q)$ iff in I, $p = q$ ($p+q$ even) or $p = q+1$ ($p+q$ odd).

For $SO(4)$, there are more choices for the orthogonal symmetric Lie algebras $(so(4),\sigma)$ since $so(4)$ is isomorphic to $so(3) \times so(3)$. However these do not yield any further R.S. manifolds $SO(4)/K$.

When $n = 3$, the decomposition $SO(3) = K_1A_1K_1$ based on I with $p = 2$, $q = 1$ is just the Euler decomposition. K_1 and A_1 are one-parameter subgroups generated by A_{12} and A_{13} respectively.

Different choices of involutive automorphisms σ give a different direct sum decomposition $so(p+q) = T \oplus P$ and hence different decomposition of $SO(p+q)$. The diagrams below illustrate a choice of canonical basis elements that generate T and A for each choice of σ in I when $g = so(5)$ and $g = so(6)$. The

diagrams for so(2n+1) and so(2n) are constructed similarly.

1. $g = so(5)$

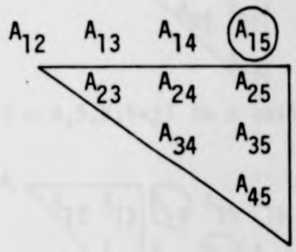
a) $p = 4$, $q = 1$

$\{A_{ij}; i,j = 2,\ldots,5; i < j\}$ is a basis of T .

$A = \mathbb{R}A_{15}$

$K_1 = SO(4)$ and

$A_1 = \exp(tA_{15})$, $t \in \mathbb{R}$



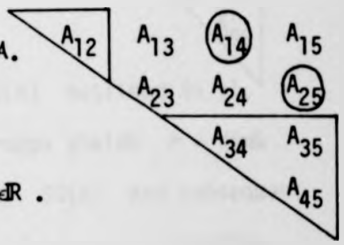
b) $p = 3$, $q = 2$

$\{A_{ij}; i,j = 3,4,5; i < j\} \cup \{A_{12}\}$ is a basis of T .

$\{A_{14}, A_{25}\}$ is a basis for A.

$K_1 = SO(3) \times SO(2)$

$A_1 = \exp(tA_{14})\exp(\theta A_{25}), t,\theta \in \mathbb{R}$.



2. $g = so(6)$

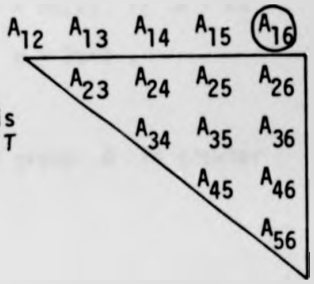
a) $p = 5$, $q = 1$

$\{A_{ij}, i,j=2,\ldots,6, i<j\}$ is a basis of T

$A = \mathbb{R}A_{16}$

$K_1 = SO(5)$

$A_1 = \exp(tA_{16}), t \in \mathbb{R}$



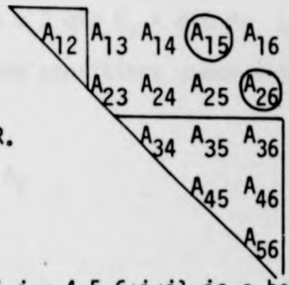
b) $p = 4$, $q = 2$

$\{A_{ij}; i,j = 3,\ldots,6; i < j\} \cup \{A_{12}\}$ is a basis of T .

$A = \mathbb{R} A_{15} + \mathbb{R} A_{26}$

$K_1 = SO(4)\times SO(2)$

$A_1 = \exp(tA_{15})\exp(\theta A_{26}), t,\theta \in \mathbb{R}$.



c) $p = 3 = q$

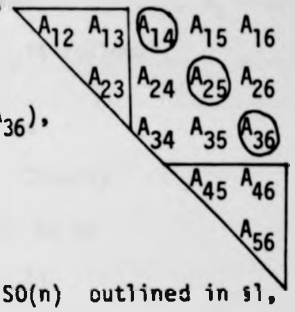
$\{A_{ij}; i,j=1,2,3; i<j\} \cup \{A_{ij}; i,j = 4,5,6; i<j\}$ is a basis of T .

$\{A_{14}, A_{25}, A_{36}\}$ is a basis of A

$K_1 = SO(3)\times SO(3)$

$A_1 = \exp(tA_{14})\exp(\theta A_{25})\exp(\tau A_{36})$,

$t,\theta,\tau \in \mathbb{R}$.



Lemma 2.1. - The decomposition of $G = SO(n)$ outlined in §1, into r one-parameter subgroups yields $r = \dim G$ if and only if one decomposes $SO(n)$ and subsequent symmetric subgroups $SO(m)$, $2 < m < n$ according to the symmetric space structure in I above, with symmetric subgroup $K_1 = SO(\ell) \times SO(\ell)$ if $m = 2\ell$ and $K_1 = SO(\ell+1) \times SO(\ell)$ if $m = 2\ell+1$.

Proof - Since the order of generation of a group G is greater

than or equal to the dimension of G, it follows that if $SO(n) = K_1 A_1 K_1$ as in lemma 1.1, with K_1 any symmetric subgroup as given in I or II, $\dim SO(n) \leq 2 \dim K_1 + \dim A_1$. Therefore, for such decompositions, the conditions under which

$$\dim SO(n) = 2 \dim K_1 + \dim A_1 \tag{2.1}$$

have to be found.

For the decomposition based on II where $m = 2\ell$, $K_1 = U(\ell)$ with dimension ℓ^2 and $\dim A_1 = [\ell/2]$ it follows

$2 \dim K_1 + \dim A_1 = 2\ell^2 + [\ell/2]$ and
$\dim SO(2\ell) = 2\ell\,(2\ell-1)/2 = 2\ell^2-\ell$. Clearly
$2\ell^2-\ell < 2\ell^2 + [\ell/2]$ for all $\ell > 0$ so no
decomposition based on II yields (2.1).

For decompositions based on I where $n = p+q$, $p \geq q$, $K_1 = SO(p) \times SO(q)$ with dimension

$p(p-1)/2 + q(q-1)/2 = (p^2-p)/2 + (q^2-q)/2$ and

A_1 is q-dimensional it follows

$2 \dim K_1 + \dim A_1 = p^2 + q^2 - p$ and
$\dim SO(p+q) = (p+q)(p+q-1)/2 = (p+q)^2/2 - (p+q)/2$.

Now,

$$2 \dim K_1 + \dim A_1 - \dim SO(p+q) = ((p-q)^2-(p-q))/2 =$$

$$= \tfrac{1}{2}(p-q)(p-q-1) \ . \ \text{Thus (2.1) holds if and only}$$

$$\text{if } p = q \text{ or } p = q+1 \ .$$

□

Here, only decompositions of $SO(n)$ based on I will be considered.

Lemma 2.2. - The number of one-parameter subgroups that decompositions of $SO(n)$ yield when one decomposes $SO(m)$, $2 < m \leq n$ according to the symmetric space structure in I increases with p, being maximal when $p = m-1$, $q = 1$ and minimal when $p = q$ (or $p = q+1$).

Proof - Since the number of one-parameter subgroups yielded by decompositions of $SO(n)$ is greater than or equal to $\dim SO(n)$, as a simple consequence of lemma 2.1 this number is minimal when $p = q$ or $p = q+1$. To prove that it increases with p it is enough to show that, if for some $m \in (2,n]$, $SO(m)$ is decomposed as $SO(m) = KAK$ with $K = SO(p) \times SO(m-p)$, $p \in [[m/2],m-1] \cap \mathbb{Z}$

and A (m-p)-dimensional, 2 dim K + dim A increases with p .

$$2 \dim K + \dim A = p^2 + (m-p)^2 - p = 2p^2 + p(-2m-1) + m^2 .$$

Now, $\forall$ m let $f:\mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x^2 + x(-2m-1)+m^2$. $f'(x) = 4x-2m-1 = 0$ iff $x = (2m+1)/4$ and $f(x)$ is an increasing function in the interval $[(2m+1)/4,\infty)$. Since $p \in [[m/2],m-1] \cap \mathbb{Z}$ and $m/2 < (2m+1)/4 < (m+1)/2$, it follows that 2 dim K + dim A increases when $p \in [(m+1)/2,m-1] \cap \mathbb{Z}$. Hence $f(m/2) = m(m-1)/2 < m(m+1)/2 = f((m+1)/2)$ so, dim K + dim A increases with p for $p \in [[m/2],m-1] \cap \mathbb{Z}$ and the proof is complete.

□

§3. GENERATING SETS AND THE NUMBER OF GENERATION OF SO(n).

Let $\mathcal{B}$ denote the canonical basis of so(n) defined in chapter I i.e. $\mathcal{B} = \{A_{ij} ; i,j = 1,\dots,n; i < j\}$, with commutation relations ([A,B] = AB-BA)

$$[A_{ij},A_{k\ell}] = \delta_{jk}A_{i\ell} + \delta_{i\ell} A_{jk} - \delta_{ik} A_{j\ell} - \delta_{j\ell} A_{ik}$$

and $\mathcal{B}_S \subset \mathcal{B}$ the canonical basis of any subspace S of so(n) that has a canonical basis.

DEFINITION 3.1. - A generating set $\{X_1,\dots,X_\ell\}$ of the Lie algebra so(n) is called a minimal generating set if no subset of $\{X_1,\dots,X_\ell\}$ generates so(n) .

Since $SO(n)$ is compact and connected, $\{X_i, i=1,\dots,\ell\}_{L.A} = so(n)$ iff $\{\exp(t_i X_i); i = 1,\dots,\ell \; ; \; t_i \in \mathbb{R}\}$ is a generating set of $SO(n)$. As a consequence, some of the results concerning the Lie algebra $so(n)$ in this paragraph, have a dual form for the Lie group $SO(n)$.

In this chapter only generating sets whose elements belong to B will be considered and from now onwards, whenever generating sets of $so(n)$ are mentioned, it will be understood that its elements have the form A_{ij}, $i < j$.

Remark - Every one-parameter subgroup $\exp(tA_{ij}), t \in \mathbb{R}$ of $SO(n)$ is compact since it can be viewed as rotations in the (e_i, e_j)-plane. So, any generating set $\{\exp(t_i A_{ij}), t_i \in \mathbb{R}\}$, uniformly finitely generates $SO(n)$. (Theorem 1.1. chapter I).

Lemma 3.1. - Any minimal generating set of $so(n)(SO(n))$ contains $n-1$ elements.

Proof (by induction) - If $n = 3$, any element belonging to the canonical basis of $so(3)$ generates a one-dimensional abelian subalgebra of $so(3)$ and on the other hand any two distinct elements generate $so(3)$ as was made clear in chapter I. So, the generating set of $so(3)$ contains 2 elements.

Now, assuming that any minimal generating set of $so(n-1)$ contains $n-2$ elements it will be shown that any minimal generating set of $so(n)$ contains $n-1$ elements. Assume the contrary i.e. there exists a minimal generating set of $so(n)$ with $m \leq n-2$ elements. Then, since $SO(n) = SO(n-1)A\,SO(n-1)$ with A one-dimensional there must exist a minimal generating set for $so(n-1)$ with at most $n-3$ elements which is false by assumption and the lemma is proved.

□

Now, let P denote the $(n-1)$-dimensional subspace of $so(n)$ defined as the (-1) eigenspace of the involutive automorphism σ_1 of $so(n)$ (as in I, §2) when $p = n-1$, $q = 1$. If B_p denotes the canonical basis of P (since $so(n) = T \oplus P$, P has a canonical basis) it follows

Lemma 3.2. - $B_p = \{A_{ij} \in B \text{ s.t. } j \text{ is fixed}, i = 1,\ldots,j-1\} \cup \{A_{ji} \in B \text{ s.t. } j \text{ is fixed}, i = j+1,\ldots,n\}$.

Proof - Since any Cartan subalgebra of $(so(n),\sigma_1)$ is 1-dimensional let $A_{k\ell}$ $(k < \ell)$ be its generator i.e. $A = \mathbb{R}\,A_{k\ell}$. A is the maximal abelian subalgebra contained in P so no other elements of B_p commute with $A_{k\ell}$. That is, all the elements of $B_p \setminus \{A_{k\ell}\}$ have either k or ℓ as an index. The proof will be

complete when it is shown that the elements of $B_p \setminus \{A_{k\ell}\}$ all have index k or index ℓ. Assume the contrary i.e. $\exists\ A_{rk} \in B_p$ for some $r \neq \ell$ and $\exists\ A_{s\ell} \in B_p$ for some $s \neq k$. Since $k \neq \ell$ it follows that

$$[A_{rk}, A_{s\ell}] = \begin{cases} -A_{k\ell} & \text{if } s = r \\ 0 & \text{otherwise.} \end{cases}$$

But the relation $[P,P] \subset T$ implies that A_{rk} and $A_{s\ell}$ commute and the maximal abelian subalgebra contained in P would not be 1-dimensional. So, the lemma is proved.

□

Lemma 3.3. - B_p is a minimal generating set of $so(n)$.

Proof - The proof is an immediate consequence of lemma 3.2 and the commutation relations. In fact $\forall\ A_{ik} \in B \setminus B_p$, $A_{ik} = -[A_{ij}, A_{kj}]$ if $k < j$ and $A_{ik} = [A_{ij}, A_{jk}]$ if $k > j$. Since $A_{ij}, A_{kj} \in P$ the lemma follows.

□

As a consequence of decompositions of $SO(n)$ outlined in §1 and in I, §2 into r one-parameter subgroups of the form $\exp(tA_{ij})$, one can associate with each such decomposition a

generating set of $SO(n)$, "the corresponding generating set", and a number, the number of one-parameter subgroups that such a decomposition yields. Although it is true in some cases that this number coincides with the order of generation of $SO(n)$ by the one-parameter subgroups of the corresponding generating set, in general this number is just an upper bound on the order of generation.

DEFINITION 3.2. - The number of generation of $SO(n)$ is the upper bound on its order of generation resulting from a decomposition of $SO(n)$ into r one-parameter subgroups when $SO(n)$ and subsequent symmetric subgroups are decomposed according to the symmetric space structure in §2.

Whereas the order of generation only depends on the generating set, the number of generation is also a function of the decomposition chosen.

Now, lemma 2.2, §2. can be restated as follows

Lemma 3.4. - The number of generation of $SO(n)$ corresponding to a decomposition of $SO(n)$ by one-parameter subgroups of the form $\exp(tA_{ij})$ increases with p

being minimal (equal to the dim of SO(n))
when SO(m) , $\forall$ m $\in$ {3,...,n} is decomposed
as in I, §2. with p = q or p = q+1 (p+q = m)
and being maximal when SO(m), $\forall$ m $\in$ {3,...,n} is
decomposed with p = m-1, q = 1 .

Lemma 3.5. - The cardinality of the generating set of so(n)
(or SO(n)) corresponding to a decomposition of
SO(n) decreases when p increases, being minimal
when SO(m) , $2 < m \leq n$ is decomposed according
to the symmetric space structure in I, with p = m-1 ,
q = 1 .

Proof - If $\forall$ i = 0,1,...,n-3 SO(n-i) is decomposed according to the symmetric space structure in I, §2. with p = n-i-1 , q = 1 , the result is the decomposition

$$SO(n) = K_{n-2}A_{n-2}K_{n-2}A_{n-1}K_{n-2}A_{n-2}K_{n-2} \cdots K_{n-2}A_{n-2}K_{n-2}A_1$$
$$K_{n-2}A_{n-2}K_{n-2} \cdots K_{n-2}A_{n-2}K_{n-2}A_{n-1}K_{n-2}A_{n-2}K_{n-2} ,$$

where $K_{n-2}, A_{n-2}, \ldots, A_2, A_1$ are distinct one-parameter subgroups of the form $\exp(tA_{ij})$. So, the generating set of so(n) contains n-1 elements and it is clearly a minimal generating set (lemma 3.1.).

To prove that # (generating set) increases when p decreases, it is sufficient to show that if for a certain i , SO(n-i) is decomposed as in I §2. with $p < n-i-1$ then # (generating set) is greater than n-1 . Without loss of generality i can be taken equal to zero. Now $SO(n) = KAK$ with $K = SO(p) \times SO(n-p)$, $p < n-1$ and A is n-p dimensional. Then, # (generating set) $\geq (p-1) + (n-p-1) + n-p = 2n - 2 - p > n-1$. (p-1 and n-p-1 being the cardinal number of minimal generating sets of SO(p) and SO(n-p-1) respectively.) Clearly 2n-2-p increases when p decreases and the result of the lemma follows.

□

It is clear from lemma 3.4 that, although the number of generation of SO(n) by one-parameter subgroups of the form $\exp(tA_{ij})$ is minimal when $\forall$ m s.t. $3 \leq m \leq n$, SO(m) is decomposed as in I, §2. with $p = q$ or $p = q+1$ $(p+q = m)$, the generating set of SO(n) corresponding to this decomposition contains more elements than the generating set corresponding to any other decomposition based in I, §2. (lemma 3.5).

In the next chapter only generating set of SO(n) with either n or n-1 elements will be considered. The reason for that choice will become clear later. Now, two decompositions of SO(n) are found to give generating sets of SO(n) with n-1 and n elements.

Lemma 3.6. - 1) The generating set corresponding to a decomposition of $SO(n)$ by one-parameter subgroups of the form $\exp(tA_{ij})$ resulting from decompositions of $SO(n)$ and subsequent symmetric subgroups as in I, §2. contains $n-1$ elements iff $p = m-1$, $q = 1$ for every m, $3 \leq m \leq n$.

2) The generating set corresponding to a decomposition of $SO(n)$ by one-parameter subgroups resulting from decompositions of $SO(n)$ and subsequent symmetric subgroups as in I, §2. contains n elements iff for some $m_1 \in [4,n] \cap \mathbb{Z}$ $SO(m_1)$ is decomposed with $p = m_1-2$, $q = 2$ and $SO(m)$, $m \in [3,n] \cap \mathbb{Z}$, $m \neq m_1$ is decomposed as in 1) above.

Proof - 1) is obvious from lemma 3.5. Without loss of generality, 2) can be proved when $m_1 = n$. Then $SO(n) = KAK$ with $K = SO(n-2) \times SO(2)$ and A 2-dimensional. Now $SO(n-2)$ and subsequent symmetric subgroups are decomposed as in 1) above, and the corresponding generating set contains $(n-3) + 1 + 2 = n$ elements. Now the lemma follows as a consequence of lemma 3.5.

□

The next lemma, included here just for the sake of completeness, is given without proof. However, it follows easily by using arguments similar to those used to prove the last 2 lemmas.

Lemma 3.7. - If $SO(m_1)$, for some $m_1 \in [3,n] \cap \mathbb{Z}$ is decomposed as in I, section 2, with $p = (m_1-1)-i$, $(i=0,1,\ldots, m_1-3)$ and $q = i+1$ and $SO(m)$ $\forall\, m \neq m_1$, $m \in [3,n] \cap \mathbb{Z}$ is decomposed with $p = m-1$, $q = 1$, then the corresponding generating set of $SO(n)$ contains $(m_1 - 1+i)$ elements.

Next theorem contains the main results, in this paragraph, which will be used later in chapters III and IV.

THEOREM 3.1. - 1) $SO(n)$ is uniformly finitely generated by $(n-1)$ one-parameter subgroups (picked as in lemma 3.6-1)) and the number of generation is $2^{n-1} - 1$.

2) $SO(n)$ is uniformly finitely generated by n one-parameter subgroups (picked as in lemma 3.6-2)) and the number of generation is $2^{n-2} + 2$.

Proof - The first part of 1) and 2) is a consequence of lemma 3.6-1) and lemma 3.6-2) respectively.

Now, if the decomposition mentioned in lemma 3.6-1) is applied to $SO(n)$ and subsequent symmetric subgroups, the result is the equation (1.2) with $G = SO(n)$, $i = n-2$. One has $K_{n-2} = SO(2)$ occurring 2^{n-2} times and A_i, $1 \leq i \leq n-2$, occurring 2^{i-1} times. Thus $SO(n)$ is a product of $2^{n-2} + \sum_{i=1}^{n-2} 2^{i-1} = \sum_{i=0}^{n-2} 2^i = 2^{n-1} - 1$ subgroups.

On the other hand, if the decomposition is as in lemma 3.6-2) (with $m_1 = n$), $SO(n) = SO(n-2)\,SO(2)\,A\,SO(2)\,SO(n-2)$, with A a 2-dimensional abelian subgroups and hence $SO(n-2) = K_i A_i K_i A_{i-1} \ldots A_1 \ldots A_{i-1} K_i A_i K_i$ with $i = n-4$. This decomposition of $SO(n-2)$ is as in 1) above and so $SO(n-2)$ is a product of $2^{n-3} - 1$ one-parameter subgroups. Then $SO(n)$ is a product of $2(2^{n-3} - 1 + 1) + 2 = 2^{n-2} + 2$ subgroups.

□

Remark - It is easy to conclude that in particular $\{\exp(t_i A_{in}),\ i = 1,\ldots,n-1; t_i \in \mathbb{R}\}$ is a generating set satisfying Theorem 3.1-1) and $\{\exp(t_i A_{i,i+1});\ i = 1,\ldots,n-1; t_i \in \mathbb{R}\} \cup \{\exp(tA_{1n})\}$ is a generating set satisfying theorem 3.1-2).

CHAPTER III

UNIFORM FINITE GENERATION OF SO(n) BY ONE-PARAMETER SUBGROUPS GENERATED BY ORTHOGONAL PAIRS OF LEFT-INVARIANT VECTOR FIELDS.

§1. PRELIMINARIES.

Let $x = (x_1, x_2, \ldots, x_m)$, $m = n(n+1)/2$ be a vector in the m-dimensional real space $\mathbb{R}^m$. With such a vector, an element X of $so(n+1,\mathbb{R})$ defined by

$$X = \left(\begin{array}{ccc|ccc} 0 & x_1 & x_2 & x_4 & \cdots & x_{m-n+1} \\ -x_1 & 0 & x_3 & x_5 & & \vdots \\ -x_2 & -x_3 & 0 & x_6 & & \\ \hline -x_4 & -x_5 & -x_6 & 0 & & \vdots \\ \vdots & & & & \ddots & x_m \\ -x_{m-n+1} & \cdots & & \cdots & -x_m & 0 \end{array}\right)$$

is associated. A simple calculation shows that $\forall\, X,Y \in so(n+1)$, trace $(XY) = -2(x,y)$. ((x,y) is the inner product of x and y.) Since $\forall\, X,Y \in so(n+1), n \geq 2, \langle X,Y\rangle = \text{trace}\,(\text{ad } X \text{ ad } Y) = (n-1)\,\text{trace}\,(XY)$ (Helgason [2, p.189]) it follows

$$\forall\ X,Y \in so(n+1), \langle X,Y\rangle = -2(n-1)(x,y)$$

i.e. X and Y are orthogonal with respect to the killing form iff the corresponding vectors x and y are orthogonal.

A canonical representation of $so(n+1)$ as $\mathbb{R}^{n(n+1)/2}$ is then

defined with canonical basis elements $e_1, e_2, \ldots, e_m$ representing $A_{12}, A_{13}, \ldots, A_{n,n+1}$ respectively.

$\forall A \in so(n+1)$, the induced representation of ad A is the $m \times m$ skewsymmetic matrix $\sum_{1 \le i < j \le m} a_{ij} A_{ij}$, where A_{ij} are the canonical basis elements of so(m) and exp(t ad A) acts on the (m-1)-dimensional unit sphere imbedded in $\mathbb{R}^m$.

Now, if SO(n+1) is decomposed as in I, chapter II with $p = n$, $q = 1$ and the corresponding direct sum decomposition of so(n+1) is considered i.e. $so(n+1) = T \oplus P$, $T = so(n)$, $P = \text{span}\{A_{i,n+1}, i=1,\ldots,n\}$ and if in particular $A = \sum_{1 \le i < j \le n} a_{ij} A_{ij} \in T$, since both T and P are invariant subspaces of ad A , the induced representation of ad A is the $m \times m$ matrix

$$\begin{pmatrix} \text{ad}_T A & \vdots & 0 \\ \cdots & \vdots & \cdots \\ 0 & \vdots & \text{ad}_P A \end{pmatrix}$$

where $\text{ad}_T A$ and $\text{ad}_P A$ are the induced representations of ad A restricted to T and P respectively. Hence, since P is a n-dimensional vectorspace with canonical basis elements

$A_{1,n+1},\ldots,A_{n,n+1}$ and

$$adA.A_{p,n+1} = \sum_{1\le i<j\le n} a_{ij}(\delta_{jp} A_{i,n+1} - \delta_{ip}A_{j,n+1})$$

$\forall\ p = 1,\ldots,n$ it follows that the induced representation of ad_pA is the $n\times n$ matrix $\sum_{1\le i<j\le n} a_{ij} A'_{ij}$ where A'_{ij} are the canonical basis elements of $so(n)$ and so $\exp(t\ ad_pA)$ acts on $S^{n-1} \subset \mathbb{R}^n$.

P is isomorphic to $\mathbb{R}^n$ (§1, chapter II); its canonical basis elements viewed as vectors in S^{n-1}.

§2. THE USE OF PERMUTATION MATRICES IN CONSTRUCTING ORTHOGONAL PAIRS {A,B} OF VECTOR FIELDS THAT GENERATE so(n) AND THE UNIFORM GENERATION OF SO(n) BY exp(tA) AND exp(τB).

Since $SO(n+1)$ is semisimple, there are pairs $\{A,B\}$ of vector fields that generate $so(n+1)$ (T.3.1, chapter I). If $\exp(tA)$ and $\exp(sB)$ are compact theorem 1.1. (chapter I) can be applied and $SO(n+1)$ is uniformly finitely generated by these one-parameter subgroups.

In this section, pairs $\{A,B\}$ of generators of $so(n+1)$, orthogonal with respect to $\langle\cdot,\cdot\rangle$, that generate compact one-

parameter subgroups are constructed and the number of generation of $SO(n+1)$ by $\exp(tA)$ and $\exp(sB)$ is found.

Permutation matrices play a very important role in this chapter.

A real matrix P_Π^α satisfying $P_\Pi^\alpha e_i = \alpha_i\, e_{\Pi(i)}$, $1 \le i \le n$, $\alpha_i^2 = 1$, Π a permutation on n letters, is a permutation matrix. The following results are standard. $P_\Pi^\alpha \in SO(n)$ iff $\prod_{i=1}^{n} \alpha_i = 1\ (-1)$, n is odd (even) and Π cannot be written as a product of disjoint cycles iff P_Π^α has no invariant subspaces.

Since $SO(n)$ is connected and compact, the exponential map $\exp: so(n) \to SO(n)$ is onto (Helgason [2, p.135]). So, if P_Π^α is a permutation matrix in $SO(n)$, viewed as an endomorphism of the canonical representation of P (P defined as in §1.), there exists $A_\Pi^\alpha \in so(n)$ such that the induced representation of $\exp(\mathrm{ad}_P A_\Pi^\alpha)$ coincides with P_Π^α. Assume that P_Π^α has no invariant subspaces. Hence, $(P_\Pi^\alpha)^n = \pm I_n$ and $O_n = \{\exp(t \operatorname{ad} A_\Pi^\alpha).\, A_{i,n+1} \;;\; t \in \mathbb{R},\ i \in \{1,\ldots,n\}\}$ is a compact subset of P which contains the elements $A_{1,n+1},\ldots,A_{n,n+1}$.

THEOREM 2.1. - For $n \geq 3$, let $A_{\Pi}^{\alpha} \in so(n+1)$ satisfy $\exp(\mathrm{ad}\, A_{\Pi}^{\alpha}) = P_{\Pi}^{\alpha}$, P_{Π}^{α} a permutation matrix of $P = \mathrm{span}\{A_{i,n+1}, i=1,\ldots,n\}$ viewed in its canonical representation, such that Π is not a product of disjoint cycles and $B \in O_n \subset so(n+1)$, then $SO(n+1)$ is uniformly generated by $\exp(tA_{\Pi}^{\alpha})$ and $\exp(sB)$ with number of generation $2^{n+1}-1$ and A_{Π}^{α} and B generate $so(n+1)$. If $B = A_{n,n+1}$ the number of generation may be reduced to $2^{n+1}-3$. The elements A_{Π}^{α} and B are orthogonal with respect to the killing form $\langle \cdot,\cdot \rangle$ on $so(n+1)$.

Proof - Clearly if $SO(n+1)$ is generated by $\exp(tA_{\Pi}^{\alpha})$ and $\exp(sB)$; $t,s \in \mathbb{R}$, then $\{A_{\Pi}^{\alpha}, B\}_{L.A} = so(n+1)$.

If $SO(n+1)$ is decomposed as in Lemma 3.6-1) (chapter II) and $so(n+1)$ decomposed according to the corresponding canonical decomposition i.e. $so(n+1) = T_1 \oplus P_1$ with $P_1 = \mathrm{span}\{A_{1j}, 2 \leq j \leq n+1\}$ and $T_i = so(n-i+1) = T_{i+1} \oplus P_{i+1}$, $P_{i+1} = \mathrm{span}\{A_{i+1,j}, i+2 \leq j \leq n+1\}$, $1 \leq i \leq n-2$, since $A_i = \exp(A_i)$ and A_i is a one-dimensional subalgebra contained in P_i it follows that the set $\{A_{i,n+1}, i=1,\ldots,n\}$ contains a generator for a candidate A_i for $1 \leq i \leq n-1$. Hence, the Lie algebra $T_{n-1} = so(2)$ in this decomposition is generated by

$A_{n,n+1}$. Then, $SO(n+1)$ is uniformly generated by the n one-parameter subgroups generated by $\{A_{i,n+1}, i=1,\ldots,n\}$, with number of generation 2^n-1 (Theorem 3.1-1), Chapter II). By construction of A_Π^α and B there exist reals $t_1,\ldots,t_n$ such that $\exp(t_i \text{ ad } A_\Pi^\alpha).B = A_{i,n+1}$, $1 \leq i \leq n$. Using the Baker-Campbell-Hausdorff formula it follows

$$\exp(s_i A_{i,n+1}) = \exp(t_i A_\Pi^\alpha)\exp(s_i B)\exp(-t_i A_\Pi^\alpha) \ , \ s_i \in \mathbb{R} \ .$$

Hence the 2^n-1 subgroups generated by $\{A_{i,n+1}, i=1,\ldots,n\}$ appearing in the expression for $SO(n+1)$ can each be expressed as a product of three one-parameter subgroups generated by A_Π^α and B . Taking into account the composition of terms with the same generator, a total number of subgroups $3(2^n-1)-(2^n-2) = 2^{n+1}-1$ is obtained.

If $B = A_{n,n+1}$, then each subgroup generated by $A_{1,n+1},\ldots,A_{n-1,n+1}$ is a product of three one-parameter subgroups generated by A_Π^α and B , whereas each subgroup K_{n-1} is generated by B already. However, in this case there are no composition of terms in the resulting expression and $SO(n+1)$ is written as a product of

$2^{n-1} + 3(2^{n-1}-1) = 2^{n+1} - 3$ one-parameter subgroups

generated by A_{Π}^{α} and B .

By construction $A_{\Pi}^{\alpha} = \sum_{1\le i<j\le n} \alpha_{ij} A_{ij}$; $B = \sum_{1\le i\le n} \beta_i A_{i,n+1}$

and clearly $\langle A_{\Pi}^{\alpha}, B\rangle = 0$.

□

The description that preceded Theorem 2.1 about permutation matrices and the way they act as elements of $SO(n+1)$ on canonical basis elements of $so(n+1)$ when $so(n+1)$ is viewed as the real vector space $\mathbb{R}^{n(n+1)/2}$, can be explained in a different and very simple way, using basically the following result.

Lemma 2.1. - If P_{Π}^{α} is a real permutation matrix defined by $P_{\Pi}^{\alpha} e_i = \alpha_i e_{\Pi(i)}$, $i = 1,\ldots,n$, $\alpha_i^2 = 1$, Π a permutation on n letters, then

$\forall\, i,j \in \{1,\ldots,n\}$

$$P_{\Pi}^{\alpha} A_{ij} (P_{\Pi}^{\alpha})^{-1} = \alpha_i \alpha_j A_{\Pi(i),\Pi(j)} \quad .$$

Proof - Let E_{ij} be the $n\times n$ matrix defined by $[E_{ij}]_{k\ell} = \delta_{ik}\delta_{j\ell}$ i.e. E_{ij} is the matrix whose r^{th}-column is the zero vector if $r \neq j$ and is the vector e_i if $r = j$. Clearly $E_{ij}-E_{ji} = A_{ij}$. Since $P^{\alpha}_{\pi} e_i = \alpha_i e_{\pi(i)}$ and $P^{\alpha}_{\pi} e_j = \alpha_j e_{\pi(j)}$ then

$$P^{\alpha}_{\pi} A_{ij} = P^{\alpha}_{\pi}(E_{ij}-E_{ji}) = \alpha_i E_{\pi(i),j} - \alpha_j E_{\pi(j),i} \qquad (2.1)$$

and

$$A_{\pi(i),\pi(j)}P^{\alpha}_{\pi} = ((P^{\alpha}_{\pi})^{-1}A^{t}_{\pi(i),\pi(j)})^{t} =$$

$$= -((P^{\alpha}_{\pi})^{-1}(E_{\pi(i),\pi(j)} - E_{\pi(j),\pi(i)}))^{t} =$$

$$= -(\frac{1}{\alpha_i} E_{i,\pi(j)} - \frac{1}{\alpha_j} E_{j,\pi(i)})^{t} =$$

$$= \frac{1}{\alpha_j} E_{\pi(i),j} - \frac{1}{\alpha_i} E_{\pi(j),i} \cdot$$

Hence, $$\alpha_i\alpha_j A_{\pi(i),\pi(j)}P^{\alpha}_{\pi} = \alpha_i E_{\pi(i),j} - \alpha_j E_{\pi(j),i} \qquad (2.2)$$

and (2.1) and (2.2) give

$$P^{\alpha}_{\Pi} A_{ij} = \alpha_i \alpha_j A_{\Pi(i),\Pi(j)} P^{\alpha}_{\Pi} \qquad \text{i.e.}$$

$$P^{\alpha}_{\Pi} A_{ij} (P^{\alpha}_{\Pi})^{-1} = \alpha_i \alpha_j A_{\Pi(i),\Pi(j)} \ .$$

□

Now, if P^{α}_{Π} is assumed to have no invariant subspaces and belong to $SO(n)$, $P_{\Pi} = \left(\begin{array}{c|c} P^{\alpha}_{\Pi} & 0 \\ \hline 0 & 1 \end{array}\right) \in SO((n+1)$

and $\exists\ A_{\Pi} \in so(n+1)$ s.t. $\exp(A_{\Pi}) = P_{\Pi}$. Since

$$\begin{cases} P_{\Pi} e_i = \alpha_i e_{\Pi(i)} \ , \ i = 1,\ldots,n \\ P_{\Pi} e_{n+1} = e_{n+1} \end{cases} \tag{2.3}$$

$A_{\Pi} e_{n+1} = 0$ and $A_{\Pi} = \left(\begin{array}{c|c} A^{\alpha}_{\Pi} & 0 \\ \hline 0 & 0 \end{array}\right) \in so(n)$

($\exp A^{\alpha}_{\Pi} = P^{\alpha}_{\Pi}$) . Lemma 2.1 applied to (2.3) gives

$$P_{\Pi} A_{i,n+1} P_{\Pi}^{-1} = \alpha_i A_{\Pi(i),n+1} \quad \text{and since}$$

$(P_\Pi)^n = \pm I$ it follows that $\forall\, i,j = 1,\ldots,n \;\exists\; t_{ij} \in \mathbb{R}$ such that $\exp(t_{ij} \mathrm{ad} A_\Pi).A_{i,n+1} = A_{j,n+1}$. Hence $O_n = \{\exp(t \mathrm{ad}\, A_\Pi).A_{i,n+1} \;,\; t \in \mathbb{R} \;,\; i \in \{1,\ldots,n\}\}$ is a compact subset of P (as previsouly defined) which contains the elements $A_{i,n+1}$, $\forall\, i = 1,\ldots,n$ and if $B \in O_n$ the pair $\{A_\Pi, B\}$ satisfy the conditions of theorem 2.1.

Given a permutation matrix $P \in SO(n)$, the existence of $A \in so(n)$ s.t. $\exp(A) = P$ is, as already pointed, a mere consequence of the exponential map being surjective. Conditions on the entries of A may be found using the fact that if P has eigenvector x corresponding to the eigenvalue λ then A has the same eigenvector corresponding to the eigenvalue $\xi_\lambda = \log_\theta \lambda$, for some θ .

The following results are standard. If Π_1 and Π_2 are any two permutations on n letters that cannot be written as a product of disjoint cycles, the corresponding permutation matrices P_{Π_1} and P_{Π_2} are conjugate i.e. there exists a permutation matrix U s.t. $U P_{\Pi_1} U^{-1} = P_{\Pi_2}$. If x is an eigenvector of P_{Π_1} corresponding to an eigenvalue λ then Ux is an eigenvector

of P_{Π_2} corresponding to λ. Hence, if $P_{\Pi_1} \in SO(n)$ and $\exp(A_{\Pi_1}) = P_{\Pi_1}$ for some $A_{\Pi_1} \in so(n)$, it follows that

$$U \exp(A_{\Pi_1}) U^{-1} = UP_{\Pi_1} U^{-1} = P_{\Pi_2}$$

or $$\exp(UA_{\Pi_1} U^{-1}) = P_{\Pi_2} .$$

Since U is a permutation matrix (the matrix of a permutation Π) and $A_{\Pi_1} = \sum_{1 \le i < j \le n} a_{ij} A_{ij}$ it follows from lemma 2.1. that

$$A_{\Pi_2} = U A_{\Pi_1} U^{-1} = \sum_{1 \le i < j \le n} a_{ij} A_{\Pi(i),\Pi(j)} .$$

Clearly, conditions on the entries of a skew-symmetric matrix A s.t. $\exp(A) = P$ for some permutation matrix P without invariant subspaces are sufficient to derive conditions on the entries of any other matrix A_Π satisfying $\exp(A_\Pi) = P_\Pi$ (P_Π and P conjugate).

Next, P is the permutation matrix defined by $Pe_i = e_{i+1}$, $i = 1,\ldots,n-1$, $Pe_n = (-1)^{n+1} e_1$ and conditions on the entries of

A s.t. $\exp(A) = P$ are found. Both cases, n odd (even) will be considered independently although in a similar way.

I - n odd

P has eigenvalues $\{\lambda : \lambda = \sqrt[n]{1} = e^{(2k\pi i)/n}; k=0,1,\ldots,n-1\}$

with corresponding eigenvectors $\{x = (\lambda^{n-1},\ldots,\lambda^2,\lambda,1)^t\}$

$A = \sum_{1\le i<j\le n} a_{ij} A_{ij}$ satisfies $Ax = \xi_\lambda x$ where $\xi_\lambda = \log_\theta \lambda$, for some θ . In matrix form the equation $Ax = \xi_\lambda x$ can be written as,

$$\begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} \\ -a_{12} & 0 & a_{23} & \cdots & a_{2n} \\ -a_{13} & -a_{23} & 0 & & \vdots \\ \vdots & \vdots & & \ddots & a_{n-1,n} \\ -a_{1n} & -a_{2n} & \cdots & -a_{n-1,n} & 0 \end{pmatrix} \begin{pmatrix} \lambda^{n-1} \\ \lambda^{n-2} \\ \vdots \\ \lambda \\ 1 \end{pmatrix} = \xi_\lambda \begin{pmatrix} \lambda^{n-1} \\ \lambda^{n-2} \\ \vdots \\ \lambda \\ 1 \end{pmatrix} .$$ So,

$$\begin{cases} \lambda^{n-2}a_{12} + \lambda^{n-3}a_{13} + \ldots + \lambda a_{1,n-1} + a_{1,n} = \xi_\lambda \lambda^{n-1} & 1) \\ -\lambda^{n-1}a_{12} + \lambda^{n-3}a_{23} + \ldots + \lambda a_{2,n-1} + a_{2n} = \xi_\lambda \lambda^{n-2} & 2) \\ \vdots & \vdots \\ -\lambda^{n-1}a_{1n} - \lambda^{n-2}a_{2n} - \ldots - \lambda a_{n-1,n} = \xi_\lambda & n) \end{cases} \qquad (2.4)$$

Multiplying the equations 1), 2),..., n) in (2.4) by $1/\lambda^{n-1}$, $1/\lambda^{n-2}$,...,$1/\lambda$, 1 respectively and since $\lambda^n = 1$ implies $\lambda^{n-p} = 1/\lambda^p$, $\forall$ p , it follows

$$\begin{cases} \lambda^{n-1}a_{12} + \lambda^{n-2}a_{13} + \lambda^{n-3}a_{14} + \ldots + \lambda^2 a_{1,n-1} + \lambda a_{1n} = \xi_\lambda \\ -\lambda\ a_{12} + \lambda^{n-1}a_{23} + \lambda^{n-2}a_{24} + \ldots + \lambda^3 a_{2,n-1} + \lambda^2 a_{2,n} = \xi_\lambda \\ \vdots \\ -\lambda^{n-1}a_{1n} - \lambda^{n-2}a_{2n} - \ldots - \lambda a_{n-1,n} = \xi_\lambda \end{cases}$$

i.e.

$$\begin{pmatrix} \xi_\lambda \\ \xi_\lambda \\ \vdots \\ \xi_\lambda \end{pmatrix}^t = \begin{pmatrix} \lambda^{n-1} \\ \lambda^{n-2} \\ \vdots \\ \lambda \\ 1 \end{pmatrix}^t \begin{pmatrix} a_{12} & a_{23} & a_{34} & \cdots & -a_{1n} \\ a_{13} & a_{24} & a_{35} & \cdots & -a_{2n} \\ a_{14} & a_{25} & a_{36} & \cdots & -a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{1,n-1} & a_{2,n-2} & -a_{13} & \cdots & -a_{n-2,n} \\ a_{1n} & -a_{12} & -a_{23} & \cdots & -a_{n-1,n} \end{pmatrix}$$

This implies that the entries of A satisfy the following set of linearly independent equations.

$$\begin{cases} a_{12} = a_{23} = a_{34} = \dots = a_{n-1,n} = -a_{1n} = \alpha_1 \\ a_{13} = a_{24} = a_{35} = \dots = a_{n-2,n} = -a_{1,n-1} = -a_{2n} = \alpha_2 \\ a_{14} = a_{25} = a_{36} = \dots = a_{n-3,n} = -a_{1,n-2} = -a_{2,n-1} = -a_{3n} = \alpha_3 \\ \vdots \end{cases}$$

where α_1 , α_2 ,..., $\alpha_{(n-1)/2}$ are real numbers satisfying the equation

$$\lambda^{n-1}\alpha_1+\lambda^{n-2}\alpha_2+\dots+\lambda^{(n-1)/2}\alpha_{(n-1)/2}-\lambda^{-(n-1)/2}\alpha_{(n-1)/2}-\dots$$

$$\dots-\lambda^{-(n-2)}\alpha_2-\lambda^{-(n-1)}\alpha_1 = \xi_\lambda$$

i.e.

$$-\alpha_1(\lambda-\lambda^{-1})-\alpha_2(\lambda^2-\lambda^{-2})- \dots -\alpha_{(n-1)/2}(\lambda^{(n-1)/2}-\lambda^{-(n-1)/2}) =$$

$$= i\,(\arg\lambda + 2k_\lambda\pi) \ , \ \forall\,\lambda = \sqrt[n]{1} \text{ and some } k_\lambda \in \mathbb{Z} \ .$$

Then, the matrix A has the following form

$$
\begin{pmatrix}
0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{\frac{n-1}{2}} & -\alpha_{\frac{n-1}{2}} & \cdots & -\alpha_2 & -\alpha_1 \\
-\alpha_1 & 0 & \alpha_1 & \ddots & \vdots & \alpha_{\frac{n-1}{2}} & \ddots & & -\alpha_2 \\
-\alpha_2 & -\alpha_1 & 0 & \ddots & \alpha_2 & \vdots & \ddots & & \vdots \\
\vdots & \ddots & \ddots & \ddots & \alpha_1 & \alpha_2 & & & -\alpha_{\frac{n-1}{2}} \\
-\alpha_{\frac{n-1}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0 & \alpha_1 & & & \alpha_{\frac{n-1}{2}} \\
\alpha_{\frac{n-1}{2}} & -\alpha_{\frac{n-1}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0 & \alpha_1 & \alpha_2 & \vdots \\
\vdots & \ddots & & & & -\alpha_1 & 0 & & \alpha_2 \\
\alpha_2 & & \ddots & & & -\alpha_2 & & 0 & \alpha_1 \\
\alpha_1 & \alpha_2 & \cdots & \alpha_{\frac{n-1}{2}} & -\alpha_{\frac{n-1}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0
\end{pmatrix}
\tag{2.5}
$$

with $-\sum_{\ell=1}^{(n-1)/2} \alpha_\ell(\lambda^\ell - \lambda^{-\ell}) = i(\theta+2k_\lambda\pi)$, $\forall\ \lambda = \sqrt[n]{1}$, $k_\lambda \in \mathbb{Z}$. (2.6)

($\theta = \arg \lambda$) .

Now, let $\lambda_k = e^{2\pi ik/n}$, $k = 0,\ldots,n-1$ denote the n eigenvalues of P . If, in equation (2.6), λ is replaced by λ_k , $k = 0,\ldots,n-1$ one obtains a system of n equations the

first of which is verified $\forall\, \alpha_1,\ldots,\alpha_{(n-1)/2}$, $k_{\lambda_0} = 0$ since $\lambda_0 = 1$. The remaining $(n-1)$ equations can still be reduced to a system of $(n-1)/2$ equations. In fact, $\forall\, j = 1,\ldots,(n-1)/2$, $\lambda_{n-j} = \lambda_j^{-1}$, $\theta_{n-j} = 2\pi - \theta_j$ and if one chooses $k_{\lambda_{n-j}} = -1 - k_{\lambda_j}$, the first $(n-1)/2$ equations are nothing else but the last $(n-1)/2$. Hence $\forall\, j = 1,\ldots,(n-1)/2$, $\theta_j = j\theta_1$, $\lambda_j - \lambda_j^{-1} = 2i\ \mathrm{Im}(\lambda_j) = 2i \sin\theta_j$ thus the equation (2.6) gives rise to the following system of $(n-1)/2$ equations in the $(n-1)/2$ unknowns $\alpha_1,\ldots,\alpha_{(n-1)/2}$ when λ runs over $\{\lambda_k\ ,\ k = 1,\ldots,(n-1)/2\}$

$$\begin{cases} \sum_{\ell=1}^{(n-1)/2} -2\,\alpha_\ell \sin(\ell\theta_1) = \theta_1 + 2\pi k_1 \\ \sum_{\ell=1}^{(n-1)/2} -2\,\alpha_\ell \sin(2\ell\theta_1) = 2\theta_1 + 2\pi k_2 \\ \vdots \\ \sum_{\ell=1}^{(n-1)/2} -2\,\alpha_\ell \sin(\frac{(n-1)}{2}\ell\theta_1) = (n-1)\theta_1/2 + 2\pi k_{(n-1)/2} \end{cases} \tag{2.7}$$

for some $k_1,\ldots,k_{(n-1)/2} \in \mathbb{Z}$, $\theta_1 = 2\pi/n$.

To summarize, if n is odd and P is the matrix of the cyclic permutation on n letters, the matrix $A \in so(n)$ satisfying $\exp(A) = P$ has the form (2.5) and its entries satisfy the system (2.7).

Remark - Since the elements belonging to each row of A are permutations of $(0,\alpha_1,\alpha_2,\ldots\alpha_{(n-1)/2},-\alpha_{(n-1)/2},\ldots,-\alpha_2,-\alpha_1)$ its sum is zero. Thus, as expected, A annihilates the vector $(1,1,\ldots,1)^t$ that is fixed by P.

II - n even

In this case, P is the $n\times n$ matrix

$$P = \begin{pmatrix} 0 & 0 & \ldots & 0 & -1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} .$$

Its eigenvalues $\{\lambda : \lambda = \sqrt[n]{-1} = e^{(\pi+2\pi k)i/n}\ ,\ k = 0,\ldots,n-1\}$ have corresponding eigenvectors $\{x = (\lambda^{n-1},\lambda^{n-2},\ldots,\lambda,1)^t\}$.

From the equation $Ax = \xi_\lambda x$ with $A = \sum_{1\le i<j\le n} a_{ij}A_{ij}$,

$\xi_\lambda = \log_\theta \lambda$, for some θ one obtains, as in I, the system (2.4). Multiplying the equations $1),\dots,n)$ in (2.4) by $1/\lambda^{n-1}$, $1/\lambda^{n-2},\dots,1$ respectively and since $\lambda^n = -1$ implies $\lambda^{n-p} = -\lambda^{-p}$, $\forall\, p$ it follows

$$\begin{cases} -\lambda^{n-1} a_{12} - \lambda^{n-2} a_{13} - \dots - \lambda^2 a_{1,n-1} - \lambda a_{1n} = \xi_\lambda \\ \\ -\lambda a_{12} - \lambda^{n-1} a_{23} - \dots - \lambda^3 a_{2,n-1} - \lambda^2 a_{2n} = \xi_\lambda \\ \vdots \\ -\lambda^{n-1} a_{1n} - \lambda^{n-2} a_{2n} - \dots - \lambda a_{n-1,n} = \xi_\lambda \ . \end{cases}$$

Therefore, the entries of A satisfy in this case the following set of equations

$$a_{12} = a_{23} = \dots = a_{n-1,n} = a_{1n} = \alpha_1$$

$$a_{13} = a_{24} = \dots = a_{n-2,n} = a_{1,n-1} = a_{2,n} = \alpha_2$$

$$a_{14} = a_{25} = \dots = a_{n-3,n} = a_{1,n-2} = a_{2,n-1} = a_{3n} = \alpha_3$$

$$\vdots$$

with $\alpha_1, \alpha_2, \ldots \alpha_{n/2}$ satisfying the equation

$$\xi_\lambda = -\alpha_1(\lambda-\lambda^{-1}) - \alpha_2(\lambda^2-\lambda^{-2}) - \ldots -\alpha_{(n-2)/2}(\lambda^{(n-2)/2}-\lambda^{-(n-2)/2}) - \\ -\alpha_{n/2}\lambda^{n/2}$$

i.e.

$$-2i\alpha_1 \mathrm{Im}(\lambda) - 2i\alpha_2 \mathrm{Im}(\lambda^2) - \ldots -2i\alpha_{(n-2)/2}\mathrm{Im}(\lambda^{(n-2)/2}) - \\ -i\,\alpha_{n/2}\mathrm{Im}(\lambda^{n/2}) = i(\arg\lambda + 2\pi k_\lambda)\ ,\ \forall\ \lambda = \sqrt[n]{-1}\ ,\ k_\lambda \in \mathbb{Z}\ .$$

Then the matrix A has, in this case, the form

$$\begin{pmatrix}
0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{\frac{n-2}{2}} & \alpha_{\frac{n}{2}} & \alpha_{\frac{n-2}{2}} & \cdots & \alpha_2 & \alpha_1 \\
-\alpha_1 & 0 & \alpha_1 & \ddots & & \alpha_{\frac{n-2}{2}} & \ddots & \ddots & & \alpha_2 \\
-\alpha_2 & -\alpha_1 & 0 & \ddots & \alpha_2 & \vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \alpha_1 & \alpha_2 & \ddots & \ddots & \ddots & \alpha_{\frac{n-2}{2}} \\
\alpha_{\frac{n-2}{2}} & & -\alpha_2 & -\alpha_1 & 0 & \alpha_1 & \ddots & \ddots & \ddots & \alpha_{\frac{n}{2}} \\
-\alpha_{\frac{n}{2}} & -\alpha_{\frac{n-2}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{\frac{n-2}{2}} \\
-\alpha_{\frac{n-2}{2}} & \ddots & & \ddots & \ddots & -\alpha_1 & 0 & \alpha_1 & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & -\alpha_2 & -\alpha_1 & 0 & \ddots & \alpha_2 \\
\alpha_2 & & \ddots & \ddots & \ddots & \vdots & \ddots & \ddots & \ddots & \alpha_1 \\
\alpha_1 & \alpha_2 & \cdots & -\alpha_{\frac{n-2}{2}} & -\alpha_{\frac{n}{2}} & -\alpha_{\frac{n-2}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0
\end{pmatrix} \tag{2.8}$$

$$\text{with } -2\sum_{\ell=1}^{(n-2)/2} \alpha_\ell \, I_m(\lambda^\ell) - \alpha_{n/2} \mathrm{Im}(\lambda^{n/2}) = \arg\lambda + 2\pi k_\lambda \,, \qquad (2.9)$$

$\forall\, \lambda = \sqrt[n]{-1}$, $k_\lambda \in \mathbb{Z}$.

Let $\lambda_k = e^{(2k-1)\pi/n}$, $k = 1,\ldots,n$ denote the n eigenvalues of P . Since $\forall\, j = 1,\ldots,n/2$, $\lambda_{n-(j-1)} = \lambda_j^{-1}$, $\theta_{n-(j-1)} = 2\pi - \theta_j$ if one chooses $k_{n-(j-1)} = -1-k_{j-1}$ $\forall\, j = 1,\ldots,n/2$, the system of n equations obtained from (2.9) by replacing λ by λ_k , $k = 1,\ldots,n$ becomes reduced to a system of $n/2$ equations on $n/2$ unknowns $\alpha_1,\ldots,\alpha_{n/2}$.

Hence, $\forall\, j = 1,\ldots,n/2$, $\theta_j = (2j-1)\theta_1$, $(\lambda_j)^{n/2} = i\ (-i)$ if j is odd (even) and the system has the form

$$\begin{cases} \sum_{\ell=1}^{(n-2)/2} -2\alpha_\ell \sin(\ell\theta_1) - \alpha_{n/2} = \theta_1 + 2\pi k_1 \\ \sum_{\ell=1}^{(n-2)/2} -2\alpha_\ell \sin(3\ell\theta_1) + \alpha_{n/2} = 3\theta_1 + 2\pi k_2 \\ \quad\vdots \\ \sum_{\ell=1}^{(n-2)/2} -2\alpha_\ell \sin((n-1)\ell\theta_1) + (-1)^{1+n/2}\alpha_{n/2} = (n-1)\theta_1 + 2\pi k_{n/2} \end{cases} \qquad (2.10)$$

for some $k_1, k_2, \ldots, k_{n/2} \in \mathbb{Z}$, $\theta_1 = \pi/n$.

It is clear from (2.10) and also from the condition $\{A,B\}_{L.A} = so(n+1)$ when $B = A_{n,n+1}$ (for instance) that $\alpha_{n/2} \neq 0$ and $\alpha_i = 0$, $i = 1,\ldots,(n-2)/2$ cannot happen. In fact, if that was the case, equations 1) and 2) in (2.10) would imply $k_1 + k_2 = -2/n$ which is impossible.

The next lemma gives conditions on the entries of A which, although implicit in (2.10) are not immediately detectable.

Lemma 2.2. - If the entries of A given by (2.8) satisfy $\alpha_k = 0$, $\forall$ k even ($\alpha_k = 0$, $\forall$ k odd) then $\exp(A) \neq P$. (P as defined earlier.)

To prove the lemma certain properties of the n-th roots of (-1) are used. Although standard, they are recalled before the proof is given.

Let $R_1^n = \{\lambda \in \mathbb{C} : \lambda^n = 1\}$, $R_{-1}^n = \{\lambda \in \mathbb{C} : \lambda^n = -1\}$

1 - $\forall\, n,k \in \mathbb{Z}$, $e^{(2k-1)\pi i/n} \in R_{-1}^n$

2 - $\lambda \in R_{-1}^n$ and n even $\Rightarrow \lambda^k \in R_{-1}^n$ ($\lambda^k \in R_1^n$)

if k is odd (if k is even).

3 - $\lambda \in R_{-1}^n$ and n even $\Rightarrow -\lambda \in R_{-1}^n$, $\lambda^{-1} \in R_{-1}^n$.

4 - $\lambda \in R_{-1}^n$ and n even => a) $\operatorname{Im} \lambda^k = \begin{cases} \operatorname{Im}(-\lambda)^k , & k \text{ even} \\ -\operatorname{Im}(-\lambda)^k , & k \text{ odd} \end{cases}$

b) $\operatorname{Im} \lambda^k = \begin{cases} \operatorname{Im}(-\lambda^{-1})^k , & k \text{ odd} \\ -\operatorname{Im}(-\lambda^{-1})^k , & k \text{ even.} \end{cases}$

Proof of lemma 2.2 - $\forall \lambda \in R_{-1}^n$, n even

$$\xi_\lambda = -2i \sum_{\ell=1}^{(n-2)/2} \alpha_\ell \operatorname{Im}(\lambda^\ell) - i \alpha_{n/2} \operatorname{Im}(\lambda^{n/2}) .$$

Assume that $\forall \ell$ odd , $\alpha_\ell = 0$. Then,

$$\xi_\lambda = -2i \sum_{k=1}^{k_1} \alpha_{2k} \operatorname{Im}(\lambda^{2k}) - i \alpha_{n/2} \operatorname{Im}(\lambda^{n/2})$$

for some integer k_1 , (the last term only if $n/2$ is even). A mere consequence of property 4-a) above is that, in this case, $\xi_\lambda = \xi_{-\lambda}$ which is impossible since the condition $\exp(A) = P$ implies that the eigenvalues of A are distinct.

On the other hand, if $\forall \ell$ even, $\alpha_\ell = 0$,

$$\xi_\lambda = -2i \sum_{k=1}^{k_1} \alpha_{2k-1} \operatorname{Im}(\lambda^{2k-1}) - i \alpha_{n/2} \operatorname{Im}(\lambda^{n/2})$$

for some integer k_1 (the last term only if $n/2$ is odd). Now property 4-b) above, implies $\xi_\lambda = \xi_{(-\lambda)^{-1}}$ which is impossible. The proof is complete.

□

Example 2.1. - $G = SO(4)$.

$$A = \sum_{1 \le i < j \le 3} a_{ij} A_{ij} \quad , \quad P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} .$$

Eigenvalues of $P = \{1, e^{2\pi i/3}, e^{4\pi i/3}\}$

Eigenvectors of $P = \{x = (\lambda^{-2}, \lambda^{-1}, 1)^t : \lambda^3 = 1\}$.

$Ax = \xi_\lambda x$ can be written in matricial form

$$\begin{pmatrix} 0 & a_{12} & a_{13} \\ -a_{12} & 0 & a_{23} \\ -a_{13} & -a_{23} & 0 \end{pmatrix} \begin{pmatrix} \lambda^{-2} \\ \lambda^{-1} \\ 1 \end{pmatrix} = \xi_\lambda \begin{pmatrix} \lambda^{-2} \\ \lambda^{-1} \\ 1 \end{pmatrix} .$$

Hence $\begin{cases} \lambda^{-1} a_{12} + a_{13} = \lambda^{-2} \xi_\lambda \\ -\lambda^{-2} a_{12} + a_{23} = \lambda^{-1} \xi_\lambda \\ -\lambda^{-2} a_{13} - \lambda^{-1} a_{23} = \xi_\lambda \end{cases}$ or $\begin{cases} \lambda a_{12} + \lambda^2 a_{13} = \xi_\lambda \\ -\lambda^2 a_{12} + \lambda a_{23} = \xi_\lambda \\ -\lambda a_{13} - \lambda^2 a_{23} = \xi_\lambda \end{cases}$

Thus, $a_{12} = a_{23} = -a_{13} = \alpha_1$

with α_1 satisfying the equation

$$(\lambda-\lambda^2)\alpha_1 = i\,(\arg\lambda+2\pi k_\lambda)\ ,\ k_\lambda \in \mathbb{Z} \quad \text{and} \quad \lambda = e^{2\pi i/3}$$

i.e. $2i\sin(2\pi/3)\alpha_1 = i\,(2\pi/3+2\pi k_1)\ ,\ k_1 \in \mathbb{Z}$. So,

$$A = \alpha_1(A_{12}+A_{23}-A_{13}) \quad \text{with} \quad \alpha_1 = \frac{2\pi(k_1+1/3)}{\sqrt{3}}\ ,\ k_1 \in \mathbb{Z}\ .$$

If in particular $B = A_{34}$ since $P\,e_3 = e_1$, $P^2 e_3 = e_2$ it follows from lemma 2.1 that $PA_{34}P^{-1} = A_{14}$, $P^2A_{34}P^{-2} = A_{24}$. Hence $e^A\,e^{t_1A_{34}}\,e^{-A} = e^{t_1A_{14}}$, $e^{2A}\,e^{t_2A_{34}}\,e^{-2A} = e^{t_2A_{24}}$, $\forall\ t_1,t_2 \in \mathbb{R}$.

Now, if $SO(m)$, $m = 3,4$ are decomposed as in I, Chapter II with $p = m-1$, $q = 1$ one obtains

$$SO(4) = K_2A_2K_2A_1K_2A_2K_2 \quad \text{where the}$$

one-parameter subgroups K_2, A_2 and A_1 can be chosen to be generated by A_{34} , A_{24} and A_{14} respectively. Clearly, the final result is

$$SO(4) = e^{\theta_1 B}\, e^{2A}\, e^{\theta_2 B}\, e^{-2A}\, e^{\theta_3 B}\, e^{A}\, e^{\theta_4 B}\, e^{-A}\, e^{\theta_5 B}$$

$$e^{2A}\, e^{\theta_6 B}\, e^{-2A}\, e^{\theta_7 B}\ ;\ \theta_1,\ldots,\theta_7 \in \mathbb{R}\ .$$

Thus, $SO(4)$ is uniformly generated by $\exp(tA)$ and $\exp(sB)$ and the number of generation is 13.

Remark - As a consequence of the definition of P it is clear that $\{\exp(tA).A_{12}, t \in \mathbb{R}\}$ is also compact and contains the elements A_{12}, A_{13} and A_{23}. However, none of these vector fields is a candidate for an element B that satisfies $\{A,B\}_{L.A} = so(4)$ since $A \in T = \text{span}\{A_{12},A_{13},A_{23}\}$. This argument is also valid in general.

Theorem 2.1. establishes an upper bound for the uniform finite generation of $SO(n+1)$ by one-parameter subgroups generated by A^{α}_{Π} and B. In particular, for $n = 3$ the number of generation is 13. However, even for $SO(4)$ a pair of generators $\{A,B\}$ of $so(4)$ can be found such that every element of $SO(4)$ may be written as a product of 11 elements from $\exp(tA)$ and $\exp(sB)$. Let $A = A_{12} + A_{23}$, $B = A_{34}$. Then $\exp(t\ \text{ad}\ A).B = A_{14}(\frac{1}{2}-\frac{1}{2}\cos\sqrt{2}t) + A_{34}(\frac{1}{2}+\frac{1}{2}\cos\sqrt{2}t) + A_{24}(\sin\sqrt{2}t)/\sqrt{2}$. Now set $SO(4) = K_1 A_1 K_1$ with $T_1 = L(K_1) = \text{span}\{A_{13},A_{14},A_{34}\}$,

$A_1 = L(A_1) = \text{span}\{A_{12}+A_{23}\} \subset P_1 = \text{span}\{A_{12},A_{23},A_{24}\}$.

$K_1 = K_2A_2K_2$ with $T_2 = L(K_2) = \text{span}\{A_{34}\}$,

$A_2 = L(A_2) = \text{span}\{A_{14}\} \subset P_2 = \text{span}\{A_{13},A_{14}\}$.

Thus $SO(4) = K_2A_2K_2A_1K_2A_2K_2$ with

$$K_2 = \{\exp(tA_{34}), t \in \mathbb{R}\} \ , \ A_2 = \{\exp(tA_{14}), t \in \mathbb{R}\} \ ,$$

$$A_1 = \{\exp(tA_{34}), t \in \mathbb{R}\} \ .$$

Now if $\cos \sqrt{2}\, t_0 = -1$, $\exp(t_0 \text{ ad } A).B = A_{14}$ so that $\exp(tA_{14}) = \exp(t_0A)\exp(tB)\exp(-t_0A)$. Hence for each $g \in SO(4)$ there exist reals $t_1,\ldots,t_7 \in \mathbb{R}$ s.t.

$$g = \exp(t_1B)\exp(t_0A)\exp(t_2B)\exp(-t_0A)\exp(t_3B)\exp(t_4A)$$

$$\exp(t_5B)\exp(t_0A)\exp(t_6B)\exp(-t_0A)\exp(t_7B) \ .$$

Theorem 2.1 gives a criterion for constructing pairs of generators of $so(n+1)$ that satisfy some requirements. The following statement is a consequence of Theorem 2.1.

"Given $B = A_{i,n+1}$, $i \in \{1,\ldots,n\}$, there exists a class $\mathcal{A}_1$ of vector fields of $so(n+1)$ orthogonal (with respect to the killing form) to B , such that $\forall\, A \in \mathcal{A}_1$, $\{A,B\}_{L.A} = so(n+1)$, (2.11)

$\exp(tA)$ and $\exp(sB)$, $t,s \in \mathbb{R}$ are compact and uniformly generate $SO(n+1)$ with number of generation $2^{n+1}-3$".

This statement deserves some comments. At first glance, when $i \neq n$ the result concerning the number of generation seems to be more general here than in Theorem 2.1. However, given $i \in \{1,\ldots,n-1\}$, $SO(n+1)$ and subsequent symmetric subgroups $SO(m)$, $2<m\leq n+1$ can be decomposed as in I, Chapter II with $p = m-1$, $q = 1$ in such a way that $K_{n-1} \simeq SO(2) = \exp(tA_{i,n+1})$ and $\{A_{j,n+1};j = 1,\ldots,n;j \neq i\}$ contains the generators of $A_{n-1},A_{n-2},\ldots,A_1$. Such a decomposition only differs from the one made to prove Theorem 2.1 by conjugacy. For example, take $B = A_{n-1,n+1}$. There exists an automorphism of $so(n+1)$ defined by $X \mapsto e^{-A} X e^{A}$, where A has the form (2.5) ((2.8)) if n is odd (even) that maps $A_{n,n+1}$ into $A_{n-1,n+1}$. Under this automorphism, the direct sum decomposition $so(n+1) = T_{n-1} \oplus (\bigoplus_{i=n-1}^{1} P_i)$ where $P_i = \text{span}\{A_{ij} ; j = i+1,\ldots,n+1\}$, $i = 1,\ldots,n-1$ and $T_{n-1} = \mathbb{R} A_{n,n+1}$, resulting of decompositions of the orthogonal symmetric Lie algebra $(so(m),\sigma_m)$ corresponding to the decompositions of the symmetric subgroups $SO(m)$, $2 < m \leq n-1$ (as in I, Chapter II) gives rise to a direct sum decomposition

$so(n+1) = T^1_{n-1} \oplus \left(\bigoplus_{i=n-1}^{1} P^1_i\right)$ where

$$P^1_i = \text{span}\{e^{-A} A_{ij} e^{A} \ , \ j = i+1,\ldots,n+1\} \ , \ i = 1,\ldots,n-1$$

and

$t^1_{n-1} = \mathbb{R}(e^{-A} A_{n,n+1} e^{A}) = \mathbb{R}\, A_{n-1,n+1}$. Obviously

$A_{i-1,n+1} \in P^1_i \ , \ \forall\, i = 2,\ldots,n-1 \ , \ A_{n,n+1} \in P^1_1$.

Thus, taking $A_1 = \exp(tA_{n,n+1})$, $A_i = \exp(tA_{i-1,n+1})$, $i = 2,\ldots,n-1$ and $K_{n-1} = \exp(tA_{n-1,n+1})$ it follows that the number of generation $2^{n+1}-3$ does not depend on $B = A_{i,n+1}$ when $i \in \{1,\ldots,n\}$.

The statement (2.11) is a weaker form of Theorem 2.1 since many candidates for B are ignored due to difficulties in characterizing elements that belong to the orbit O_n (defined in Theorem 2.1) and are not canonical basis elements.

The class $\mathcal{A}_1$ of vector fields is clearly defined by

$$\mathcal{A}_1 = \{A_1 \in \text{span}\{A_{ij}; i,j=1,\ldots,n; i<j\} : \exp A_1 = U P_{\Pi_1} U^{-1} \quad \text{for}$$

some permutation matrix $U\}$, $P_{\Pi_1} e_i = e_{\Pi_1(i)}, \forall\, i.\{1,\ldots,n-1\}\cup\{n+1\}$,

$P_{\Pi_1} e_n = (-1)^{n+1} e_{\Pi_1(n)}$ and $\Pi_1 = \begin{pmatrix} 1 & 2 & 3 & \ldots & n & n+1 \\ 2 & 3 & 4 & \ldots & 1 & n+1 \end{pmatrix}$.

The following lemma is given without proof. It states an even more general result than (2.11).

Lemma 2.3. - Give $B = A_{i,n+1}$, $i \in \{1,\ldots,n\}$ there exist two classes $\mathcal{A}_1$ and $\mathcal{A}_2$ of vector fields orthogonal (with respect to $\langle\cdot,\cdot\rangle$) to B such that $\forall\, A_k \in \mathcal{A}_k$ $(k = 1,2)$, $\{A_k,B\}_{L.A} = so(n+1)$, $\exp(tA_k)$ and $\exp(sB)$ are compact and uniformly generate $SO(n+1)$ with number of generation $2^{n+1} - 3$.

$\mathcal{A}_1$ is defined as in (2.11) and

$\mathcal{A}_2 = \{A_2 \in \operatorname{span}\{A_{s,r} : s,r \in \{1,\ldots,n+1\}\setminus\{i\}; s < r\}$ s.t.

$\exp(A_2) = U P_{\Pi_2} U^{-1}$ for some permutation matrix $U\}$,

$P_{\Pi_2} e_j = e_{\Pi_2(j)}, \forall\, j = 1,\ldots,n$, $P_{\Pi_2} e_{n+1} = (-1)^{n+1} e_{\Pi_2(n+1)}$,

$$\Pi_2 = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & n & n+1 \\ 2 & 3 & \dots & i+1 & i & i+2 & \dots & n+1 & 1 \end{pmatrix} .$$

Note that $B = A_{i,n+1}$ also belongs to the minimal generating set $\{A_{ji}, j = 1,\dots,i-1\} \cup \{A_{ij}, j = i+1,\dots,n+1\}$ and when the pair $\{B,A_2\}$, $A_2 \in \mathcal{A}_2$ is considered, this minimal generating set plays the role in the proof of Lemma 2.3.

After all the comments made throughout this section, the next theorem is clearly a summary of previous results.

THEOREM 2.2. - Given $B = A_{ij} \in so(n+1)$ there exist two classes $\mathcal{A}_1$ and $\mathcal{A}_2$ of vector fields orthogonal (with respect to $\langle\cdot,\cdot\rangle$ to B such that $\forall A_k \in \mathcal{A}_k$ $(k = 1,2)$ $\{B,A_k\}_{L.A} = so(n+1)$, $\exp(tB)$ and $\exp(sA_k)$ are compact and uniformly generate $SO(n+1)$ with number of generation $2^{n+1} - 3$.

$\mathcal{A}_1 = \{A_1 \in \text{span}\{A_{r,s}, r,s \in \{1,\dots,n+1\}\backslash\{i\}, r < s\}$ s.t.

$\exp(A_1) = U P_{\Pi_1} U^{-1}$ for some permutation matrix $U\}$

where $P_{\Pi_1} e_r = e_{\Pi_1(r)}$, $r = 1,\ldots,n$, $P_{\Pi_1} e_{n+1} = (-1)^{n+1} e_{\Pi_1(n+1)}$

and $$\Pi_1 = \begin{pmatrix} 1 & 2 & \ldots & i-1 & i & i+1 & \ldots & n & n+1 \\ 2 & 3 & \ldots & i+1 & i & i+2 & \ldots & n+1 & 1 \end{pmatrix} .$$

$$\mathcal{A}_2 = \{A_2 \in \operatorname{span}\{A_{r,s}, r,s \in \{1,\ldots,n+1\}\backslash\{j\},\ r < s\} \text{ s.t.}$$

$$\exp(A_2) = U P_{\Pi_2} U^{-1} \quad \text{for some permutation matrix } U\}$$

where $P_{\Pi_2} e_r = e_{\Pi_2(r)}$, $r = 1,\ldots,n$, $P_{\Pi_2} e_{n+1} = (-1)^{n+1} e_{\Pi_2(n+1)}$

and

$$\Pi_2 = \begin{pmatrix} 1 & 2 & \ldots & j-1 & j & j+1 & \ldots & n & n+1 \\ 2 & 3 & \ldots & j+1 & j & j+2 & \ldots & n+1 & 1 \end{pmatrix} .$$

CHAPTER IV

UNIFORM FINITE GENERATION OF SO(n) BY ONE-PARAMETER SUBGROUPS GENERATED BY NON-ORTHOGONAL PAIRS OF LEFT-INVARIANT VECTOR FIELDS.

§1. THE USE OF PERMUTATION MATRICES IN CONSTRUCTING NONORTHOGONAL PAIRS {A,B} OF VECTOR FIELDS THAT GENERATE so(n) AND THE UNIFORM GENERATION OF SO(n) BY exp(tA) AND exp(τB).

The order of generation of SO(3) by two one-parameter subgroups exp(tA) and exp(sB) is a function of the angle between the axes of rotation of both rotation subgroups being minimal when this angle is $\pi/2$, that is when $\langle A,B\rangle = 0$. (Chapter I, theorem 2.1 and theorem 2.2).

The order of generation problem for SO(n) is certainly more complicated when $n > 3$, the main difficulty being a consequence of lack of a complete characterization of pairs of generators of so(n) . Even when a pair {A,B} is known to generate so(n) , the number of generation depends on the decomposition of SO(n) used and also on the relation between the pair {A,B} and the generating set of so(n) corresponding to that decomposition.

In Chapter III, pairs {A,B} of generators of so(n) , orthogonal with respect to the killing form, were constructed and an upper bound on the order of generation of SO(n) by the subgroups generated by A and B was determined.

In this chapter, pairs of generators of so(n), nonorthogonal with respect to the killing form, will be constructed and the uniform generation problem of SO(n) partially solved for these pairs. Again, permutation matrices play an important role in here.

The diagram below, already used in Chapter II, showing the canonical basis elements of so(n) will be often referred to throughout this paragraph. Its use comes from the fact that it provides a good visualization of some of the results obtained here.

$$
\begin{array}{ccccccc}
A_{12} & A_{13} & A_{14} & A_{15} & \cdots & A_{1,n-1} & A_{1n} \\
 & A_{23} & A_{24} & A_{25} & \cdots & A_{2,n-1} & A_{2n} \\
 & & A_{34} & A_{35} & \cdots & A_{3,n-1} & A_{3n} \\
 & & & A_{45} & \cdots & A_{4,n-1} & A_{4n} \\
 & & & & \ddots & \vdots & \vdots \\
 & & & & & A_{n-2,n-1} & A_{n-2,n} \\
 & & & & & & A_{n-1,n}
\end{array}
$$

Diagram 1.1.

Let $A \in so(n)$ be defined as in (2.5) ((2.8)), Chapter III if n is odd (even) its entries satisfying (2.7) ((2.10)), Chapter III.

As a consequence of the condition $\exp(A) = P_\pi$, where $P_\pi e_i = e_{\pi(i)}$, $i = 1,\ldots,n-1$, $P_\pi e_n = (-1)^{n+1} e_{\pi(n)}$, $\pi = \begin{pmatrix} 1 & 2\ldots n \\ 2 & 3\ldots 1 \end{pmatrix}$, together with lemma 2.1 (Chapter III), the canonical basis B of $so(n)$ can be divided into $[n/2]$ equivalence classes. The equivalence class of a certain element A_{ij} being the set of canonical basis elements that belong to the orbit of $\exp(t \text{ ad } A)$, $t \in \mathbb{R}$ that passes through A_{ij} .

Let $[\alpha_i]$, $i = 1,\ldots,[n/2]$ denote the equivalence classes. (The choice of this notation to agree with the structure of A.) Note that for a certain i , $[\alpha_i]$ is the set of canonical basis elements with coefficients $\pm \alpha_i$ in the expression of A . Clearly,

$$[\alpha_i] = \{A_{k\ell} \in B : \ell-k = i\} \cup \{A_{k\ell} \in B : \ell-k = n-i\}$$

$\forall$ $i = 1,\ldots,[n/2]$. If β_i and β_{n-i} denote $\{A_{k\ell} \in B : \ell-k = i\}$ and $\{A_{k\ell} \in B : \ell-k = n-i\}$ respectively, $[\alpha_i] = \beta_i \cup \beta_{n-i}$, $i = 1,\ldots,[n/2]$. Hence $\forall$ $j = 1,\ldots,n-1$ $\#\beta_j = n-j$ and β_j can be seen as the set of elements along the j-th diagonal (counted from left to right) in diagram 1.1.

If $SO(n)$ is decomposed as in lemma 3.6-1) (Chapter II) and $so(n)$ decomposed according to the corresponding canonical decomposition i.e.

$$so(n) = T_{n-2} \oplus \left(\bigoplus_{i=1}^{n-2} P_i\right) , \quad P_i = \text{span}\{A_{ij},\ j = i+1,\ldots,n\} ,$$

$$T_{n-2} = \mathbb{R}\, A_{n-1,n} \quad \text{since} \quad A_{i,i+1} \in P_i , \ \forall\ i = 1,\ldots,n-2$$

$A_{i,i+1}$ can be chosen to generate $A_i = \exp(A_i)$ and it follows that $\{A_{i,i+1} ,\ i = 1,\ldots,n-2\} \cup \{A_{n-1,n}\} = \beta_1$ is a generating set of $so(n)$ and it is minimal (see lemma 3.1.-Chapter II). Clearly $[\alpha_1]$ is a generating set since it contains β_1 and β_i , $i \neq 1$ is not a generating set.

THEOREM 1.1. - For $n > 3$, let $A \in so(n)$ satisfy $\exp(A) = P_\Pi$, P_Π the permutation matrix defined by $P_\Pi e_i = e_{\Pi(i)}$, $i = 1,\ldots,n-1$ $P_\Pi e_n = (-1)^{n+1} e_{\Pi(n)}$, Π the cyclic permutation on n letters and $B \in \{\exp(t \text{ ad } A).A_{n-1,n}, t \in \mathbb{R}\} \subset so(n)$. Then $SO(n)$ is uniformly generated by $\exp(tA)$ and $\exp(sB)$ with number of generation $2^{n-1} + 5$ and $\{A,B\}_{L.A} = so(n)$.

If B also belongs to $\mathcal{B}$ then the number of generation is $2^{n-1} + 3$ and $\langle A,B \rangle$ is not zero in general.

Proof - If $SO(n)$ is decomposed as in lemma 3.6-2) (Chapter II) with $m_1 = n$ and $so(n)$ decomposed according to the corresponding canonical decomposition i.e. $so(n) = T_1 \oplus P_1$, $T_1 = so(n-2) \oplus so(2) =$ $= so(n-2) \oplus \mathbb{R} A_{12}$, $P_1 = \text{span}(\{A_{1j}, j = 3,\ldots,n\} \cup \{A_{2j}, j = 3,\ldots,n\})$ and $T_2 = so(n-2) = T_{n-2} \oplus (\bigoplus_{i=3}^{n-2} P_i)$, $P_i = \text{span}\{A_{ij}, j = i+1,\ldots,n\}$ since A_1 is a 2-dimensional abelian subalgebra contained in P_1 and A_i is a one-dimensional abelian subalgebra of P_i $\forall$ $i = 3,\ldots,n-2$, take $A_1 = \mathbb{R}A_{1n} + \mathbb{R}A_{23}$, $A_i = \mathbb{R}A_{i,i+1}$, $i = 3,\ldots,n$ and $T_{n-2} = \mathbb{R}A_{n-1,n}$ then $SO(n)$ is uniformly generated by the n one-parameter subgroups generated by $[\alpha_1]$ with number of generation $2^{n-2} + 2$ (Theorem 3.1-2), Chapter II). That is

$$SO(n) = \underbrace{K_{n-2}A_{n-2}K_{n-2}A_{n-3}\cdots K_{n-2}A_{n-2}K_{n-2}A_{n-3}K_{n-2}A_{n-2}K_{n-2}\cdots}_{*}$$

$$\cdots \underbrace{A_{n-3}K_{n-2}A_{n-2}K_{n-2}}\exp(tA_{12})\, A_1 \exp(sA_{12})\, \underbrace{K_{n-2}A_{n-2}K_{n-2}}$$

$$\underbrace{A_{n-3}\cdots K_{n-2}A_{n-2}K_{n-2}A_3K_{n-2}A_{n-2}K_{n-2}\cdots A_{n-3}K_{n-2}A_{n-2}K_{n-3}}_{*} \quad , \qquad (1.1)$$

$t,s \in \mathbb{R}$, $K_{n-2} = \exp tA_{n-1,n}$, $A_i = L(A_i)$, $i = 3,\ldots,n-2$.

By construction of A and B there exist reals $t_1,\ldots,t_n$ s.t. $\exp(t_i \text{ ad } A).B = A_{i,i+1}$, $i = 1,\ldots,n-1$, $\exp(t_n \text{ad} A).B = A_{1n}$. The use of the Baker-Campbell-Hausdorff formula allows every one of the $2^{n-2} + 2$ one-parameter subgroups that appear in (1.1) to be expressed as a product of 3 one-parameter subgroups generated by A and B . Hence taking in account the composition of terms with the same generator a total number of $3(2^{n-2}+2)-(2^{n-2}+1) = 2^{n-1}+5$ subgroups generated by A and B is obtained.

If $B = A_{n-1,n}$, then the product $*$ in (1.1) contains $2^{n-2}-3$ elements, the first and the last of which is $\exp(tB)$ and after reducing the terms with the same generator in $\exp(tA_{12})A_1 \exp(sA_{12})$ a total number of $2(2^{n-2}-3) + 9 = 2^{n-1}+3$ one-parameter subgroups is obtained. The result when B is any element in $[\alpha_1] \cap B$ is a consequence of taking any decomposition of $SO(n)$ that is conjugate to the one considered above. Hence if $B \in [\alpha_1] \cap B$, $\langle A,B \rangle = -2(n-2)\ (a,b)$, $(a,b) = \alpha_1$ where a and b are defined as in §1 (Chapter III). Apart from the case $n = 4$, where α_1 cannot be zero (see Lemma 2.2, Chapter III)

it is not easy to see from conditions (2.7) and (2.10), (Chapter III) on the entries of A, whether or not α_1 can be zero. If however α_1 can be zero, $\langle A,B\rangle = 0$. Otherwise $\langle A,B\rangle \neq 0$. Hence, if $\phi = \sphericalangle(a;b)$

$$\cos\phi = \frac{\alpha_1}{||a||\,||b||} = \frac{\alpha_1}{||a||} < \frac{1}{\sqrt{n}} .$$

□

Clearly, A and B can be replaced by UAU^{-1} and UBU^{-1} for some permutation matrix U without changing the result.

If lemma 3.6-1) (Chapter II) is used instead of lemma 3.6-2) in the proof above to decompose $SO(n)$ as a product of one-parameter subgroups, only $(n-1)$ generators contained in $[\alpha_1]$ need to be considered. The result after applying Theorem 3.1-1) (Chapter II) is an upper bound on the order of generation of $SO(n)$ equal to 2^n-1 (2^n-3) instead of $2^{n-1}+5$ $(2^{n-1}+3)$. Hence, this decomposition gives the same number of generation when pairs $\{A,B\}$, orthogonal with respect to $\langle\cdot,\cdot\rangle$, are considered as in Theorem 2.1 (Chapter III). These facts emphasize what has already been pointed out about the dependence of the number of generation not just on the pair of generators but also on the decomposition chosen and on the relation to each other.

In the orthogonal case (Chapter III), $A \in \text{span}\{A_{ij}; i,j = 1,\ldots,n-1; i < j\}$ and the candidates for an element B cannot belong to $\text{span}\{A_{ij}; i,j = 1,\ldots,n-1, i<j\}$ since B has to satisfy $\{A,B\}_{L.A} = so(n)$. However, in this case, other canonical basis elements than those already considered (which belong to $[\alpha_1]$) may satisfy our requirements. It is not obvious which elements to exclude and which to consider as possible candidates. The following lemmas clarify the situation and a complete classification of canonical basis elements whose one-parameter subgroups generated by them together with $\exp(tA)$, $t \in \mathbb{R}$ uniformly generate $SO(n)$, is made. From earlier results it is known that if B belongs to the orbit of $\exp(t \text{ ad } A)$ that passes through $[\alpha_k]$ for some k then $\forall A_{ij} \in [\alpha_k]$, $\exists t_{ij} \in \mathbb{R}$ s.t.

$\exp(t_{ij} \text{ ad } A).B = A_{ij}$. Thus, if $[\alpha_k]$ is a generating set of $so(n)$, $\exp(tA)$ and $\exp(sB)$ uniformly generate $SO(n)$. It will be proved that $[\alpha_k]$ generates $so(n)$ if and only if n and k are coprime numbers.

Let β_j, $j = 1,\ldots,n-1$ be defined as before. The following notations will be used.

$$-\beta_j = \{A_{\ell k} \in B : A_{k\ell} \in \beta_j\};\ -[\beta_i,\beta_j] = \{A_{sr} \in B : A_{rs} \in [\beta_i,\beta_j]\}$$

Lemma 1.1. — $[\beta_i,\beta_i] = -\beta_{2i} \cup \beta_{2i} \cup \{0\}$, $\forall\, i \leq (n-1)/2$.

Proof — $\beta_i = \{A_{k\ell} \in B : \ell - k = i\}$. $\forall\, A_{k\ell}$, $A_{mn} \in \beta_i$

$$[A_{k\ell},A_{mn}] = \begin{cases} A_{\ell m} & \text{if } k = n \qquad 1) \\ A_{kn} & \text{if } \ell = m \qquad 2) \\ 0 & \text{otherwise.} \end{cases}$$

Since $n-m = \ell-k = i$ it follows that in 1)

$m-\ell = n-i-k-i = -2i + n-k = -2i$ and in 2)

$n-k = m+i+i-\ell = 2i$ that is $A_{\ell m} \in (-\beta_{2i})$

and $A_{kn} \in \beta_{2i}$. Thus $[\beta_i,\beta_i] \subset -\beta_{2i} \cup \beta_{2i} \cup \{0\}$. On the other hand $\forall\, A_{k\ell} \in \beta_{2i}$ there exist two elements A_{mn} and A_{rs} in β_i s.t. $[A_{mn},A_{rs}] = A_{k\ell}$. In fact taking $m = k$, $s = \ell$, $n = r = k+i$, since $\ell-k = 2i$ if follows $n-m = i$ and $s-r = \ell-k-i = i$ i.e. $A_{mn},A_{rs} \in \beta_i$. Clearly $\forall\, A_{\ell k} \in (-\beta_{2i})$, $A_{k\ell} \in \beta_{2i}$ and $A_{\ell k} = [A_{n\ell},A_{kn}]$ with $A_{n\ell},A_{kn} \in \beta_i$ (as above). So the result follows.

□

Lemma 1.2. - $\forall\, i \neq 1$, $\bigcup_{m\in\mathbb{N}} \beta_{mi}$ belongs to a proper subalgebra of $so(n)$.

Proof - Let $S = \bigcup_{m\in\mathbb{N}}(-\beta_{mi}\cup\beta_{mi})\cup\{0\}$. $\beta_{mi} = \{A_{rs} \in B; s-r = mi\}$

$[\beta_{m_1 i},\beta_{m_2 i}] = \{[A_{r_1 s_1},A_{r_2 s_2}] : s_1-r_1 = m_1 i \wedge s_2-r_2 = m_2 i\}$, $m_1,m_2 \in \mathbb{N}$.

Since

$$[A_{r_1 s_1},A_{r_2 s_2}] = \begin{cases} -A_{s_1 s_2} & \text{if } r_1 = r_2 \quad 1) \\ A_{s_1 r_2} & \text{if } r_1 = s_2 \quad 2) \\ -A_{r_1 r_2} & \text{if } s_1 = s_2 \quad 3) \\ A_{r_1 s_2} & \text{if } s_1 = r_2 \quad 4) \\ 0 & \text{otherwise} \end{cases}$$

it follows that in 1) $s_2-s_1 = s_2-s_1-r_2+r_1 = (s_2-r_2)-(s_1-r_1) =$

$= (m_2-m_1)i$, in 2) $r_2-s_1 = r_2-s_1+r_1-s_2 = -(s_2-r_2)-(s_1-r_1) =$

$= -(m_1+m_2)i$, and similarly in 3) $r_2-r_1 = -(-r_2+s_2)+(s_1-r_1) =$

$= (m_1-m_2)i$ and in 4) $s_2-r_1 = s_2-r_2+s_1-r_1 = (m_2+m_1)i$. Thus

$[A_{r_1s_1},A_{r_2s_2}] \in S$, $\forall\, A_{r_1s_1} \in \beta_{m_1 i}$, $A_{r_2s_2} \in \beta_{m_2 i}$.

□

The previous lemma applies whether or not n is even. However when n is even and $i = 2$ a more elegant proof can be given using the Weyl basis of $so(n,\mathbb{C})$. This proof will be given later.

Lemma 1.3. - 1) $\forall\, i < j$, $i+j \leq n$, $\beta_{j-i} \subset -[\beta_i,\beta_j]$

2) $\forall\, i,j$, $\beta_{j+i} \subset [\beta_i,\beta_j]$.

Proof - 1) $\forall\, A_{rs} \in \beta_{j-i}$, $s-r = j-i$. Since $\forall\, \ell \in \mathbb{N}$, $s-r = (s-\ell) - (r-\ell)$ take ℓ to satisfy $s-\ell = j$, $r-\ell = i$. (Such an ℓ always exists since $s-j = r-i$.) Clearly $A_{\ell r} \in \beta_i$ and $A_{\ell s} \in \beta_j$ unless $r = i$ and $s = j$ respectively. Hence $A_{rs} = -[A_{\ell r},A_{\ell s}]$, $\forall\, A_{rs} \in \beta_{j-i} \setminus \{A_{ij}\}$. For A_{ij} , $A_{ij} = -[A_{j,i+j} , A_{i,i+j}]$. With $i+j \leq n$, $A_{j,i+j} \in \beta_i$ and $A_{i,i+j} \in \beta_j$. If however $i+j > n$, the element $A_{ij} \in \beta_{j-i}$ cannot be obtained from brackets of two elements one of β_i and another of β_j .

2) Similarly if $A_{rs} \in \beta_{j+i}$, $s-r = j+i$.

Since $\forall\, \ell \in \mathbb{N}$, $s-r = (s-\ell) + (\ell-r)$ take $\ell = i+r = s-j$.

It follows that $A_{r\ell} \in \beta_i$, $A_{\ell s} \in \beta_j$ and $A_{rs} = [A_{r\ell}, A_{\ell s}]$.

The proof is complete. □

Lemma 1.4 - If both n and k have a common divisor $m \neq 1$, $[\alpha_k]$ is not a generating set of $so(n)$.

Proof - This is an immediate consequence of lemma 1.2 since, if both n and k have a common divisor m , also both n and $n-k$ have the same divisor m and β_k and β_{n-k} both belong to a proper subalgebra of $so(n)$. β_m is a generating set of this subalgebra (clearly a consequence of lemmas 1.1 and 1.3). □

In particular, when n is even and $k = n/2$, $[\alpha_k] = \beta_k = \beta_{n/2}$ and since $\beta_{n/2}$ is the canonical basis of a Cartan subalgebra of $so(n)$, $[\alpha_k]$ is not a generating set of $so(n)$.

The following lemma whose result is included in lemmas 1.2 and 1.4 is presented here for its proof. As already mentioned before, an alternative proof using the Weyl basis is given.

Lemma 1.5 - If $g = so(2n, \mathbb{R})$, $n > 1$, $[\alpha_{2k}]$, $k \in [1, n/2] \cap \mathbb{Z}$ is not a generating set of g .

Proof - $h = \begin{pmatrix} \lambda_1 & & 0 & & \\ & \ddots & & & 0 \\ 0 & & \lambda_n & & \\ & & & -\lambda_1 & \\ & 0 & & & \ddots \\ & & & 0 & & -\lambda_n \end{pmatrix}$ is a Cartan subalgebra of

$g_{\mathbb{C}} = so(2n,\mathbb{C}).\Phi = \{\varepsilon_1\lambda_i + \varepsilon_2\lambda_j \; ; \; i<j; \; i,j = 1,\ldots,n \; ; \; \varepsilon_1,\varepsilon_2 \in \{-1,1\}\}$

is the set of roots of $g_{\mathbb{C}}$. $\forall \lambda \in \Phi$, $E_\lambda = X_\lambda - X_{-\lambda}$ ($\{X_\lambda, \lambda \in \Phi\}$ is the Weyl basis) is defined by

$E_\lambda = \varepsilon_1 A_{2i-1,2j-1} + \varepsilon_2 A_{2i,2j}$. Consider the following set

$$\{\tfrac{1}{2}(E_{\lambda_i+\lambda_j} + E_{\lambda_i-\lambda_j})\} \cup \{-\tfrac{1}{2}(E_{\lambda_i+\lambda_j} + E_{-\lambda_i+\lambda_j})\} =$$

$$= \{\tfrac{1}{2}(A_{2i-1,2j-1} - A_{2i,2j} + A_{2i-1,2j-1} + A_{2i,2j})\} \cup$$

$$\cup \{-\tfrac{1}{2}(A_{2i-1,2j-1} - A_{2i,2j} - A_{2i-1,2j-1} - A_{2i,2j})\} =$$

$= \{A_{2i-1,2j-1}\ ,\ A_{2i,2j}\ ;\ i < j\ ;\ i,j = 1,\ldots,n\}\ =$

$= \{A_{2i-1,2j-1}\ ,\ A_{2i,2j}\ ;\ i = 1,\ldots,n-1\ ,\ j = i+1\}\ \cup$

$\cup\ \{A_{2i-1,2j-1}\ ,\ A_{2i,2j}\ ;\ i = 1,\ldots,n-2\ ;\ j = i+2\}\ \cup\ \ldots\ \cup$

$\cup\{A_{2i-1,2j-1}\ ,\ A_{2i,2j}\ ;\ i = 1\ ;\ j = n\}$. A simple calculation shows that this set is equal to

$\beta_2 \cup \beta_4 \cup \ldots \cup \beta_{2n-4} \cup \beta_{2n-2}$, that is $[\alpha_2] \cup [\alpha_4] \cup \ldots \cup [\alpha_{2n-2}]$.

Now using the fact that $\forall\ \alpha,\beta \in \Phi$,

$$[E_\alpha, E_\beta] = \begin{cases} 0 & , \{\alpha+\beta, \alpha-\beta\} \notin \Phi \\ N_{\alpha,\beta}\ E_{\alpha+\beta} & \alpha+\beta \in \Phi\ ,\ \alpha-\beta \notin \Phi \\ -N_{\alpha,-\beta}\ E_{\alpha-\beta} & \alpha-\beta \in \Phi\ ,\ \alpha+\beta \notin \Phi \\ N_{\alpha\beta}\ E_{\alpha+\beta} - N_{\alpha,-\beta}\ E_{\alpha-\beta} & , \{\alpha+\beta, \alpha-\beta\} \subset \Phi \end{cases}$$

the result follows.

□

The next lemma contains a result that will be used later.

Lemma 1.6. - If A and B are any two noncommutative canonical basis elements of $so(n)$ then $\{A,B,[A,B]\}$ is the canonical basis of a subalgebra g_1 of $so(n)$ isomorphic to $so(3)$.

Proof - Since A and B belong to $\mathcal{B}$ and do not commute they must be of the form $A = A_{ij}$, $B = A_{k\ell}$ with $\{i,j\} \cap \{k,\ell\} \neq \phi$. Without loss of generality assume $j = k$. That is $A = A_{ij}$, $B = A_{j\ell}$, $[A,B] = A_{i\ell}$. Clearly the Lie algebra g generated (as a vector space) by $\{A,B,[A,B]\}$ is isomorphic to $so(3)$, the isomorphism defined by

$$\begin{array}{ccc} g_1 \subset so(n) & \to & so(3) \subset so(n) \\ X & \mapsto & \theta X \theta^{-1} \end{array}$$

where θ is the matrix of the permutation

$$\begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & \ell-1 & \ell & \ell+1 & \dots & n \\ 4 & 5 & \dots & i+2 & 1 & i+3 & \dots & j+1 & 2 & j+2 & \dots & \ell & 3 & \ell+1 & \dots & n \end{pmatrix}$$

□

The next step is to prove that if n and k are coprime numbers, then $[\alpha_k]$ is a generating set of $so(n)$.

If every element of β_1 can be obtained by Lie brackets of elements of β_k and β_{n-k}, obviously $[\alpha_k]_{L.A} = so(n)$.

Assume that n and k are coprime numbers. Then $n \equiv k_1 \bmod k$ i.e. $n = j_0 k + k_1$ for some $k_1 \in \{1,\ldots,k-1\}$, $j_0 \in \mathbb{N}$. Consider the class $C_{j_0} = \{\beta_{n-k}, \beta_{n-2k}, \ldots, \beta_{n-j_0 k} = \beta_{k_1}\}$ whose elements satisfy the following j_0-1 relations.

$$\begin{aligned} &\beta_{n-2k} \subset -[\beta_k, \beta_{n-k}] && 1) \\ &\beta_{n-3k} \subset -[\beta_k, \beta_{n-2k}] && 2) \\ &\quad\vdots \\ &\beta_{k_1} = \beta_{n-j_0 k} \subset -[\beta_k, \beta_{n-(j_0-1)k}] && j_0-1) \end{aligned} \qquad (1.2)$$

(See lemma 1.3-1).) From 1) $\forall Z_2 \in \beta_{n-2k}$ there exist $X_2 \in \beta_k$ and $X_1 \in \beta_{n-k}$ such that $Z_2 = -[X_2, X_1]$. From 2), $\forall Z_3 \in \beta_{n-3k}$ there exist $X_3 \in \beta_k$ and $Y_1 \in \beta_{n-2k}$ s.t.

$Z_3 = -[X_3,Y_1]$. But $Y_1 \in \beta_{n-2k}$ thus $Y_1 = -[X_2,X_1]$ for some $X_2 \in \beta_k$, $X_1 \in \beta_{n-k}$. So $Z_3 = [X_3,[X_2,X_1]]$, for some X_1,X_2 and X_3 belonging to $[\alpha_k]$. The same argument used throughout the relations 3),....,j_0-1) clearly leads to the following. $\forall\, Z_{j_0} \in \beta_{n-j_0k} = \beta_{k_1}$, there exists $X_1,X_2,\ldots,X_{j_0} \in [\alpha_k]$ such that

$$Z_{j_0} = (-1)^{j_0+1}[X_{j_0},[X_{j_0-1},[\ldots[X_3,[X_2,X_1]]\ldots] \quad . \qquad (1.3)$$

Note that $n-j_0k = k_1 < k$ and $n-(j_0-i)k = k_1 + ik > k$, $\forall\, i \geq 1$. Therefore, if β_j is viewed as the j-th diagonal in diagram 1.1 (rigorously the set of elements along the j-th diagonal), C_{j_0} is a set of diagonals, β_{k_1} being the only diagonal in this set situated below β_k .

If $k_1 = 1$, then every element of β_1 can be obtained by Lie brackets of elements of $[\alpha_k]$ and $[\alpha_k]$ is a generating set of so(n) . If $k_1 \neq 1$, then $k \equiv k_2 \bmod k_1$ i.e. $k = j_1k_1+k_2$ for some $k_2 \in \{1,\ldots,k_1-1\}$, $j_1 \in \mathbb{N}$. $C_{j_1} = \{\beta_k,\beta_{k-k_1},\ldots,\beta_{k-j_1k_1} = \beta_{k_2}\}$ and its elements satisfy the following j_1 relations.

$$\beta_{k-k_1} \subset - [\beta_{k_1}, \beta_k] \qquad 1')$$

$$\beta_{k-2k_1} \subset - [\beta_{k_1}, \beta_{k-k_1}] \qquad 2') \qquad (1.4)$$

$$\vdots$$

$$\beta_{k_2} = \beta_{k-j_1k_1} \subset - [\beta_{k_1}, \beta_{k-(j_1-1)k_1}] \quad j_1')$$

It is easy to conclude, just using the same arguments as above, that $\forall\, Z'_{j_1} \in \beta_{k-j_1k_1} = \beta_{k_2}$ there exist $X'_1 \in \beta_k$ and $X'_2, X'_3, \ldots, X'_{j_1+1} \in \beta_{k_1}$ such that $Z'_{j_1} = (-1)^{j_1}[X'_{j_1+1}, [X'_{j_1}, [\ldots [X'_3, [X'_2, X'_1]\ldots]]$. Hence, (1.3) can be applied to every element of β_{k_1} and the result is that every element of β_{k_2} can be obtained by Lie brackets of elements of $[\alpha_k]$.

$k - j_1k_1 = k_2 < k_1$, $k - (j_1-i)k_1 = k_2+ik_1 > k_1$, $\forall\, i \geq 1$ so, β_{k_2} is the only diagonal of C_{j_1} situated below β_{k_1} (in diagram 1.1) and also no elements of C_{j_1} are situated above β_k .

If $k_1 = 1$, the process ends here and $[\alpha_k]$ is a generating set of $so(n)$. If $k_1 \neq 1$ then $k_1 \equiv k_3 \bmod k_2$ i.e. $k_1 = j_2k_2+k_3$

for some $k_3 \in \{1,\ldots,k_2-1\}$, $j_3 \in \mathbb{N}$. Once again one proceeds as previously. The system of equations

$$
\begin{aligned}
n &= j_0\, k + k_1 && (0 < k_1 < k)\\
k &= j_1\, k_1 + k_2 && (0 < k_2 < k_1)\\
k_1 &= j_2 k_2 + k_3 && (0 < k_3 < k_2)\\
&\vdots\\
k_{N-2} &= j_{N-1} k_{N-1} + k_N && (0 < k_N < k_{N-1})\\
k_{N-1} &= j_N k_N
\end{aligned}
$$

known as Euclid's algorithm is used in elementary arithmetic to determine the greatest common divisor k_N of n and k . Since it has been assumed that n and k are coprime, this process will end up with the equation $k_{N-2} = j_{N-1}k_{N-1} + k_N$, with $k_N = 1$, and some integer N . $C_{j_{N-1}} = \{\beta_{k_{N-2}}, \beta_{k_{N-2}-k_{N-1}}, \ldots, \beta_{k_{N-2}-j_{N-1}k_{N-1}} = \beta_1\}$ with elements satisfying the following j_{N-1} relations.

$$
\begin{aligned}
&\beta_{k_{N-2}-k_{N-1}} \quad c - [\beta_{k_{N-1}}, \beta_{k_{N-2}}] \\
&\beta_{k_{N-2}-2k_{N-1}} \quad c - [\beta_{k_{N-1}}, \beta_{k_{N-2}-k_{N-1}}] \\
&\quad \vdots \\
&\beta_1 = \beta_{k_N} \qquad c - [\beta_{k_{N-1}}, \beta_{k_{N-2}-(j_{N-1}-1)k_{N-1}}]
\end{aligned}
\tag{1.5}
$$

Clearly every element of β_1 may be written as brackets of elements from $[\alpha_k]$.

Therefore, one can formulate the lemma that has just been proved.

Lemma 1.7. - If n and k are coprime numbers,

$$[\alpha_k]_{L.A} = so(n) .$$

Lemmas 1.4 and 1.7 can be put together in the following

THEOREM 1.2. - Let $g = so(n,\mathbb{R})$, $[\alpha_k]$ as defined in the beginning of this paragraph. Then, $[\alpha_k]_{L.A} = g$ if and only if n and k are coprime numbers.

The procedure used above to show that $[\alpha_k]_{L.A} = so(n)$ when n and k are coprime numbers also shows that $\forall\, X$ belonging to any of the following sets: β_{n-ik}, $i = 2,\ldots,j_0$, β_{k-ik_1} , $i = 1,\ldots,j_1$, $\ldots$, $\beta_{k_{N-2}-ik_{N-1}}$, $i = 1,\ldots,j_{N-1}$ satisfying the relations (1.2), (1.4) ... and (1.5) respectively, $\exp(tX)$, $t \in \mathbb{R}$ may be written as a product of one parameter subgroups $\exp(\theta A)$ and $\exp(\tau B)$ where A is defined as in the beginning of the paragraph and B belongs to the orbit of $\exp(t \text{ ad } A)$ that passes through $[\alpha_k]$. In fact, from (1.2)-1), $\forall\, Z_2 \in \beta_{n-2k}$ there exist $X_2 \in \beta_k$ and $X_1 \in \beta_{n-k}$ such that $Z_2 = -[X_2,X_1]$. Lemma 1.6 plus the fact that Z_2,X_2 and X_1 are orthogonal with respect to the killing form imply $[X_2,Z_2] = X_1$, $[X_1,Z_2] = -X_2$. Thus, $\forall\, t \in \mathbb{R}$

$$\exp(tZ_2) = \exp((-\pi/2)X_2)\, \exp(t\, X_1)\, \exp((\pi/2)X_2) \,, \tag{1.6}$$

with X_1 and $X_2 \in [\alpha_k]$. By construction of A and B , $\forall\, X_i \in [\alpha_k]$, $\exists\ t_i \in \mathbb{R}$ such that $X_i = \exp(t_iA)B \exp(-t_iA)$. Hence $\exp(tX_i) = \exp(t_iA) \exp(tB) \exp(-t_iA)$, $\forall\ t \in \mathbb{R}$. Thus $\forall\, Z_2 \in \beta_{n-2k}$, $\exp(tZ_2)$ may be written as a product of at most 7 one-parameter subgroups generated by A and B . Similarly, from

(1.2)-2), $\forall\, Z_3 \in \beta_{n-3k}$ there exist $X_3 \in \beta_k$ and $Y_1 \in \beta_{n-2k}$ s.t. $\exp(tZ_3) = \exp(-\pi/2X_3)\exp(tY_1)\exp(\pi/2X_3)$ $\forall\, t \in \mathbb{R}$. Hence, using (1.6) with $Z_2 = Y_1$ it follows that, $\forall\, Z_3 \in \beta_{n-3k}$,

$$\exp(tZ_3) = \exp(-(\pi/2)X_3)\exp(-(\pi/2)X_2)\exp(tX_1)\exp(\tfrac{\pi}{2}X_2)\exp((\pi/2)X_3), \quad (1.7)$$

$\forall\, t \in \mathbb{R}$ and some X_1, X_2 and X_3 in $[\alpha_k]$.

It is clear by construction of A and B that again $\exp(tZ_3)$, $Z_3 \in \beta_{n-3k}$ may be written as a product of one-parameter subgroups generated by A and B and also that this procedure applied to every relation in (1.2), (1.4),...,(1.5) leads to the following. Every one-parameter subgroup generated by any element belonging to the sets in the left-hand side of relations (1.2), (1.4),...,(1.5) may be written as a product of one-parameter subgroups generated by A and B .

As it will become clear later, of special interest are the one-parameter subgroups generated by elements of $\beta_{k_1}, \beta_{k_2}, \ldots, \beta_1$.

Lemma 1.8. - For $n > 3$, let $A \in so(n)$ satisfy $\exp(A) = P_\Pi$, P_Π the permutation matrix

defined by $P_\pi e_i = e_{\pi(i)}$, $i = 1,\ldots,n-1$, $P_\pi e_n = (-1)^{n+1} e_{\pi(n)}$, π the cyclic permutation on n letters and $B \in \{\exp(t \operatorname{ad} A).X , t \in \mathbb{R} , X \in [\alpha_k]\} \subset so(n)$, (n and k are coprime). Then $\forall Z_{j_{i-1}} \in \beta_{k_i}$, $i = 0,1,\ldots,N$ ($k_N = 1$ and $\beta_{k_0} = \beta_k$) , $\exp(tZ_{j_{i-1}})$, $t \in \mathbb{R}$ may be written as a product of R_i one-parameter subgroups generated by A and B . $R_0 = 3$, $R_1 = 4j_0 - 1$, $R_s = 2R_{s-2} + (2j_{s-1} - 1)R_{s-1} - 2j_{s-1}$, $s = 2,\ldots,N$.

Proof - By construction of A and B , $\forall X \in [\alpha_k]$, $\exists \theta \in \mathbb{R}$ such that

$$\exp(tX) = \exp(\theta A)\exp(tB)\exp(-\theta A) , t \in \mathbb{R} . \qquad (1.8)$$

In particular for $X \in \beta_k \subset [\alpha_k]$, $R_0 = 3$.

If the process previously started for the relations 1) and 2) in (1.2), leading to the equations (1.6) and (1.7) respectively, is continued throughout the relations $3),\ldots,j_0)$, clearly the result is that every one-parameter subgroup generated by elements

of β_{k_1} can be written as a product of $2j_0-1$ one-parameter subgroups generated by elements in $[\alpha_k]$. Hence, since every $X \in [\alpha_k]$ satisfies (1.8) it follows after taking into account the composition of terms with the same generator that $\forall\, Z_{j_0} \in \beta_{k_1}$, $t \in \mathbb{R}$, $\exp(tZ_{j_0})$ may be written as a product of $R_1 = 3(2j_0-1) - (2j_0-2) = 4j_0-1$ subgroups generated by A and B.

From 1') in (1.4) it follows that $\forall\, Z_1' \in \beta_{k-k_1}$ there exist $X_1' \in \beta_{k_1}$ and $X_2' \in \beta_k$ s.t. $\exp(tZ_1') = \exp((-\pi/2)X_1')\exp(tX_2')\exp((\pi/2)X_1')$, $\forall\, t \in \mathbb{R}$. It is also true that

$$\exp(tZ_1') = \exp((\pi/2)X_2')\exp(tX_1')\exp((-\pi/2)X_2'),\ t \in \mathbb{R}$$

and since subgroups generated by elements in β_k involve less products (of subgroups generated by A and B) than subgroups generated by elements in β_k do, the latter equation is preferred to the former. Hence, using a previous result for $\exp(tX_1')$, $X_1' \in \beta_{k_1}$ one obtains $\exp(tZ_1')$, $\forall\, Z_1' \in \beta_{k-k_1}$, $t \in \mathbb{R}$ written as a product of $2j_0+1$ subgroups generated by elements of $[\alpha_k]$. The same argument used throughout the relations i'),

$i = 2,\ldots,j_1$ give for every $Z'_i \in \beta_{k-ik_1}$, $(i-1)R_1 + 2$ $j_0-(i-2)$ products. Therefore, $\forall\, Z'_{j_1} \in \beta_{k_2}$, $t \in \mathbb{R}$, $\exp(tZ'_{j_1})$ may be written as a product of

$R_2 = 3((j_1-1)R_1 + 2j_0-(j_1-2)) - ((j_1-1)R_1 + 2j_0-(j_1-2)-1) =$

$= 6 + (2j_1-1)R_1-2j_1 = 2R_0 + (2j_1-1)R_1-2j_1$ one-parameter subgroups generated by A and B.

The result for $s = 3,\ldots,N$ is clearly a consequence of the form how every set of relations can be obtained from the previous one. For instance, to obtain R_3 one simply replaces k, k_1 and j_1 in (1.4) by k_1, k_2 and j_2 respectively and then proceeds as for relations (1.4) making use of previous results for $s = 1,2$.

At this stage it is important to recall what the main problem is. Given an $A \in so(n)$ satisfying $\exp(A) = P_\Pi$, P_Π the permutation matrix defined by $P_\Pi e_i = e_{\Pi(i)}$, $i = 1,\ldots,n-1$, $P_\Pi e_n = (-1)^{n+1} e_{\Pi(n)}$, Π the cyclic permutation on n letters, find $B \in so(n)$ such that $\exp(tA)$ and $\exp(\theta B)$ uniformly generate $SO(n)$ and determine the corresponding number of generation.

The previous lemma answers the first part of the problem but the number of generation has still to be found. This will be the next task.

Of great help for a better understanding of the next procedure is the use of the diagram 1.1, each of its i-th diagonals, $i = 1,\ldots,n-1$ is viewed as β_i. The following set

$$\beta_k \cup \{\beta_{n-ik},\ i=1,\ldots,j_0\} \cup \{\beta_{k-ik}, i=1,\ldots,j_1\} \cup \tag{1.9}$$

$\{\beta_{k_1-ik_2},\ i = 1,\ldots,j_2\} \cup \ldots \cup \beta_1$, whose elements are clearly identified with those diagonals obtained by successive use of Lie brackets of the elements in $[\alpha_k]$, is totally ordered by means of a relation $\lessdot$ defined as follows: $\beta_i \lessdot \beta_j$ iff $\beta_i = \beta_j$ or if β_i is situated below β_j in the diagram 1.1. From comments made during the proof of Lemma 1.7 it is easily seen that

$$\begin{aligned}
&\beta_k \prec \beta_{n-ik} \prec \beta_{n-k}\ , && \forall\ i = 2,\ldots,j_0-1\\
&\beta_{k_1} \prec \beta_{k-ik_1} \prec \beta_k\ , && \forall\ i = 1,\ldots,j_1-1\\
&\beta_{k_2} \prec \beta_{k_1-ik_2} \prec \beta_{k_1}, && \forall\ i = 1,\ldots,j_2-1\\
&\ \ \vdots
\end{aligned} \tag{1.10}$$

Hence, to each element in (1.9) a number N_i (the number of generation of $\exp(t\beta_i)$ by $\exp(\theta A)$ and $\exp(\tau B)$) is associated, $N_k, N_{k_1}, N_{k_2}, \ldots$ being $R_0, R_1, R_2, \ldots$ associated with $\beta_k, \beta_{k_1}, \beta_{k_2}, \ldots$ respectively. (Lemma 1.8.) Clearly,

$$N_k \leq N_{n-ik} < N_{k_1} < N_{k-jk_1} < N_{k_2} < N_{k_1-sk_2} < N_{k_3} < \ldots, \qquad (1.11)$$

$$\forall\ i = 1,2,\ldots j_0-1\ ,\ j = 1,\ldots,j_1-1\ ,\ s = 1,\ldots,j_2-1\ ,\ \ldots\ .$$

Any row in the diagram 1.1 intersects at least a member of the set of diagonals (1.9). Consider the set I_i of elements of B (canonical basis of $so(n)$) resulting of the intersection of (1.9) with the i-th row. ($i = 1,\ldots,n-1$.) Each of the elements of I_i belongs to a certain β_j associated with a number N_j. An element $A_{i,i+j} \in I_i$ is said to be "the best" among all the elements of I_i if the number N_j associated with $\beta_j (A_{i,i+j} \in \beta_j)$ is the least of the numbers N_ℓ associated with the diagonals β_ℓ that intersect the i-th row.

If $SO(n)$ and subsequent symmetric subgroups $SO(m)$ are decomposed as in I, Chapter II with $p = m-1$, $q = 1$, $3 \leq m \leq n$, the result is a decomposition of $SO(n)$ by one-parameter subgroups as in (1.2), Chapter II where the subgroups A_i, $i=1,2,\ldots,n-2$ and K_{n-2} can be chosen to be generated by $(n-1)$ canonical basis

elements A_{ij_i} , $i = 1,2,\ldots,n-1$ respectively. Clearly, if $\forall\, i = 1,\ldots,n-1$, A_{ij_i} is chosen to be "the best" element of the i-th row, one obtains far better results than if it belongs to any other diagonal of the set (1.9). It is also easy to see, as a consequence of (1.10) and (1.11) that these elements are the following.

$$\{A_{i,i+k}, i=1,\ldots,n-k\} \subset \beta_k \ , \ \{A_{i,i+k_1}, i = n-k+1,\ldots,n-k_1\} \subset \beta_{k_1} \ ,$$

$$\{A_{i,i+k_2} \ , \ i = n-k_1+1,\ldots,n-k_2\} \subset \beta_{k_2} \ , \ \ldots \ ,$$

$$\{A_{i,i+1} \ , \ i = n-k_{N-1}+1,\ldots,n-2\} \subset \beta_{k_N} = \beta_1 \ , \ \{A_{n-1,n}\} \subset \beta_1 \ .$$

Figure 1.1 shows their positions in diagram 1.1.

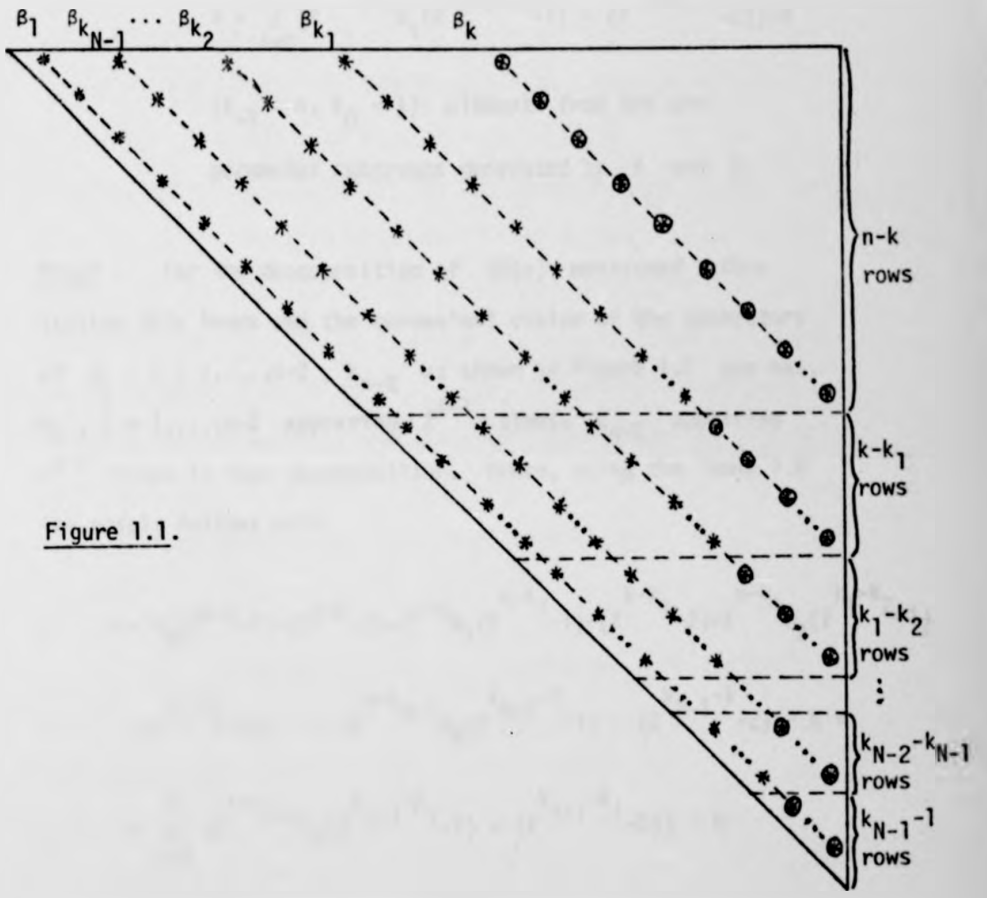


Figure 1.1.

Lemma 1.9. - Let A and B be defined as in the previous lemma. Then exp(tA) and exp(θB) uniformly generate SO(n) and every element of SO(n) may be

written as a product of at most

$$R = \sum_{i=0}^{N} (2^{n-k_{i-1}} R_i (2^{k_{i-1}-k_i}-1) - (2^{k_{i-1}-k_i}-2)) - N$$

$(k_{-1} = n,\ k_0 = k)$ elements from the one parameter subgroups generated by A and B.

Proof - For the decomposition of SO(n) mentioned before stating this lemma and the convenient choice of the generators of A_i , $i = 1,\ldots,n-2$, k_{n-2} as shown in figure 1.1 one has, A_i , $i = 1,\ldots,n-2$ appearing 2^{i-1} times, k_{n-2} appearing 2^{n-2} times in that decomposition. Hence, using the lemma 1.8 the result follows with

$$R = R_0(2^{n-k}-1)-(2^{n-k}-2)+2^{n-k}R_1(2^{k-k_1}-1)-(2^{k-k_1}-2)+2^{n-k_1}R_2(2^{k_1-k_2}-1) -$$

$$-(2^{k_1-k_2}-2)+ \ldots +2^{n-k_{N-1}}R_N(2^{k_{N-1}-1}-1) - (2^{k_{N-1}-1}-2) - N =$$

$$= \sum_{i=0}^{N} (2^{n-k_{i-1}} R_i (2^{k_{i-1}-k_i}-1) - (2^{k_{i-1}-k_i}-2)) - N$$

after composition of terms with same generator.

□

Similar problems treated before give, for different pairs $\{A,B\}$ of generators, better results when B is a canonical basis element that belongs to the orbit of $\exp(t \text{ ad } A)$; (see Theorem 2.1 (Chapter III) and Theorem 1.1). However in this case every $B \in \{\exp(t \text{ ad } A).X,\ X \in [\alpha_k],\ t \in \mathbb{R}$, n and k coprime, give the same result for the decomposition chosen. But a better result would be obtained if $SO(n)$ was decomposed in such a way that the greater the wordlength in terms of A and B a subgroup of $\{A_i,\ i = 1,\ldots,n-2,k_{n-2}\}$ is, fewer times it appears in the decomposition of $SO(n)$. Many things would then have to be taken in consideration and the final result does not appear to be very easy to obtain. However all the difficulties in trying to solve this problem are overcome as a consequence of the next result.

It will be proved that if $[\alpha_k]$ generates $so(n)$ there exist two decompositions of $SO(n)$ such that the corresponding generating sets of $so(n)$ only contain elements of $[\alpha_k]$. This has been seen to be true when $k = 1$; the generating sets corresponding to the decompositions of $SO(n)$ were in this case either $[\alpha_1]$ or just $\beta_1 \subset [\alpha_1]$ (the first giving a lower number of generation).

THEOREM 1.3. - For $n > 3$, let $A \in so(n)$ satisfy $\exp(A) = P_\Pi$, P_Π the permutation matrix defined by $P_\Pi e_i = e_{\Pi(i)}$ $i = 1,\ldots,n-1$, $P_\Pi e_n = (-1)^{n+1} e_{\Pi(n)}$, Π the cyclic permutation on n letters and $B \in \{\exp(t \text{ ad } A).X,\ X \in [\alpha_k],\ t \in \mathbb{R}\} \subset so(n)$, n and k coprime numbers. Then $SO(n)$ is uniformly generated by $\exp(tA)$ and $\exp(sB)$ with number of generation $2^{n-1}+5$ and $\{A,B\}_{L.A} = so(n)$. If B also belongs to $[\alpha_k]$ then the number of generation is $2^{n-1}+3$.

Proof - Let $\Pi_1 = \begin{pmatrix} 1 & 2 & \ldots & n-k & n-k+1 & \ldots & n \\ k+1 & k+2 & \ldots & n & 1 & \ldots & k \end{pmatrix}$ be a permutation on n letters. $\Pi_1 = \Pi^k$ where Π is defined above. A standard result is that since n and k are coprime, Π^k is conjugate to Π that is, there exists a permutation Π_C s.t. $\Pi_C \Pi \Pi_C^{-1} = \Pi^k$. Π_C is defined by $\Pi_C(i) = (i-1)k + 1$ if $(i-1)k+1 \leq n$, $\Pi_C(i) = j$ if $(i-1)k+1 \equiv j \mod n$. Clearly if P_{Π_C} is a permutation matrix satisfying $P_{\Pi_C} e_i = \alpha_i e_{\Pi_C(i)}$, $\prod_{i=1}^{n} \alpha_i = 1 (-1)$, n is odd (even), the automorphism of $so(n)$ defined by $X \mapsto P_{\Pi_C} X P_{\Pi_C}^{-1}$ also defines a one-to-one map from

$[\alpha_1]$ into a subset S of $\pm[\alpha_k]$ where S is such that, if $A_{ij} \in S$ then $A_{ji} \notin S$. Now instead of the decomposition of $SO(n)$ as in the proof of Theorem 1.1, one takes

$$A_1 = \mathbb{R}(P_{\pi_C} A_{1n} P_{\pi_C}^{-1}) + \mathbb{R}(P_{\pi_C} A_{23} P_{\pi_C}^{-1})$$

$$A_i = \mathbb{R}(P_{\pi_C} A_{i,i+1} P_{\pi_C}^{-1}) \quad , \quad i = 3,\ldots,n$$

$$T_{n-2} = \mathbb{R}(P_{\pi_C} A_{n-1,n} P_{\pi_C}^{-1}$$

$$T_2 = so(2) = \mathbb{R}(P_{\pi_C} A_{12} P_{\pi_C}^{-1})$$

and so $SO(n)$ becomes written as a product of $2^{n-2}+2$ one parameter subgroups generated by the elements of $[\alpha_k]$. The result follows in a similar way to the proof of Theorem 1.1.

□

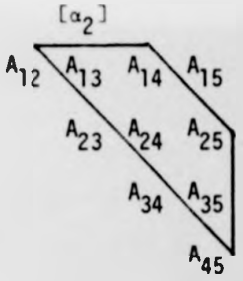
EXAMPLE 1.3. - $g = so(5)$, $k = 2$.

$[\alpha_2] = \{A_{13}, A_{24}, A_{35}\} \cup \{A_{14}, A_{25}\}$ generates $so(5)$.

$$\pi_C = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}$$

$$so(5) = so(3) \oplus so(2) \oplus P_1$$

$$T_1$$



$$P_1 = \text{span}\{A_{12}, A_{14}, A_{15}, A_{23}, A_{34}, A_{35}\}$$

$$A_1 = \mathbb{R}\, A_{14} + \mathbb{R}\, A_{35}$$

$$T_1 = \text{span}\{A_{13}, A_{24}, A_{25}, A_{45}\}\ ,\quad so(2) = \mathbb{R}\, A_{13}\ ,$$

$$so(3) = \text{span}\{A_{24}, A_{25}, A_{45}\} = T_3 \oplus P_3\ ,\quad P_3 = \text{span}\{A_{24}, A_{45}\}\ ,$$

$$T_3 = \mathbb{R}\, A_{25}\ ,\quad A_3 = \mathbb{R}\, A_{24}$$

$$SO(5) = K_3 A_3 K_3 SO(2) A_1 SO(2) K_3 A_3 K_3\ ,\quad K_3 = \exp(T_3)\ ,$$

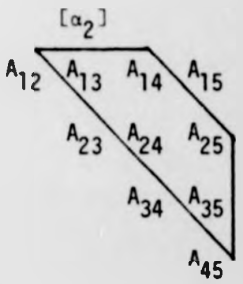
$$A_3 = \exp(A_3)\ ,\ A_1 = \exp(A_1)\ ,\ SO(2) = \exp(tA_{13})\quad \text{i.e.}$$

$$SO(5) = \exp(t_1 A_{25})\exp(t_2 A_{24})\exp(t_3 A_{25})\exp(t_4 A_{13})\exp(t_5 A_{14})$$

$$\exp(t_6 A_{35})\exp(t_7 A_{13})\exp(t_8 A_{25})\exp(t_9 A_{24})\exp(t_{10} A_{25})\ .$$

If A,B is defined as in the theorem 3.3, $SO(5)$ becomes generated by $\exp(tA)$ and $\exp(sB)$ with order of generation 21 (19 if $B \in [\alpha_k]$) .

$$so(5) = so(3) \oplus so(2) \oplus P_1$$
$$T_1$$



$$P_1 = \mathrm{span}\{A_{12}, A_{14}, A_{15}, A_{23}, A_{34}, A_{35}\}$$

$$A_1 = \mathbb{R}\, A_{14} + \mathbb{R}\, A_{35}$$

$T_1 = \mathrm{span}\{A_{13}, A_{24}, A_{25}, A_{45}\}$, $so(2) = \mathbb{R}\, A_{13}$,

$so(3) = \mathrm{span}\{A_{24}, A_{25}, A_{45}\} = T_3 \oplus P_3$, $P_3 = \mathrm{span}\{A_{24}, A_{45}\}$,

$T_3 = \mathbb{R}\, A_{25}$, $A_3 = \mathbb{R}\, A_{24}$

$SO(5) = K_3 A_3 K_3 SO(2) A_1 SO(2) K_3 A_3 K_3$, $K_3 = \exp(T_3)$,

$A_3 = \exp(A_3)$, $A_1 = \exp(A_1)$, $SO(2) = \exp(tA_{13})$ i.e.

$$SO(5) = \exp(t_1 A_{25})\exp(t_2 A_{24})\exp(t_3 A_{25})\exp(t_4 A_{13})\exp(t_5 A_{14})$$
$$\exp(t_6 A_{35})\exp(t_7 A_{13})\exp(t_8 A_{25})\exp(t_9 A_{24})\exp(t_{10} A_{25}) .$$

If A,B is defined as in the theorem 3.3, $SO(5)$ becomes generated by $\exp(tA)$ and $\exp(sB)$ with order of generation 21 (19 if $B \in [\alpha_k]$) .

CHAPTER V.

APPLICATIONS TO CONTROL THEORY.

§1. PRELIMINARIES.

This chapter is concerned with the application of the previous results to the study of the controllability properties of systems which are described by an equation in a n-dimensional connected manifold M, of the form

$$\dot{x}(t) = \sum_{i=1}^{k} u_i(t)\, X_i(x(t)) \qquad (1.1)$$

where $u_1(t),\ldots,u_k(t)$ are admissible (say, piecewise continuous) real-valued control functions and $X_1,\ldots,X_k$ are vector fields on M.

DEFINITION 1.1. - For every $x \in M$, the Reachable set at time τ from x is given by

$$R(x,\tau) = \{y \in M : y \in \gamma_{Y_1}(t_1) \circ \ldots \circ \gamma_{Y_r}(t_r)\cdot x,\ r \in \mathbb{Z}^+,\ t_i \in \mathbb{R}^+,\ \sum_{i=1}^{r} t_i = \tau\}$$

and the *Reachable set* from x is given by

$$R(x) = \bigcup_{\tau \geq 0} R(x,\tau)\ ,$$

where Y_i, $i = 1,\ldots,r$ are associated vector fields for system (1.1) and $(x,t) \to \gamma_{Y_i}(t)\cdot x$ is the flow of the vector field Y_i on M, $\gamma_{Y_i}(0)\cdot x = x$.

- the system (1.1) is said to be *controllable* if $R(x) = M$, for every $x \in M$.

Especial interest is given to systems of the form (1.1) that are evolved on a Lie Group G and where $X_1,\ldots,X_k$ are left or right invariant vector fields on G satisfying $\{X_1,\ldots,X_k\}_{L.A} = L(G)$. This condition is equivalent to controllability [6] and [7]. If in addition G is a semisimple group of matrices ($SO(n)$ for instance), the corresponding Lie algebra is generated by two elements A and B (Theorem 3.1, Chapter I). For this reason, our study is restricted to a class of systems evolved on G, of the form

$$\dot{x}(t) = (u(t)A + v(t)B)x(t) \qquad (1.2)$$

where $u(t)$ and $v(t)$ are piecewise continuous control functions.

Although it is known that (1.2) is controllable and even controllable in an arbitrarily short time [7] (this would not be the case if (1.2) was not homogeneous), more can be said about its controllability properties namely, the number of switches involved when any two points of G are joined by trajectories of the form $u(t)A + v(t)B$.

§2. UNIFORMLY COMPLETELY CONTROLLABLE SETS OF VECTOR FIELDS.

An autonomous control system such as (1.1) on a manifold M is defined by a set of vector fields on M. A set F of vector fields on M is said to be *completely controllable* if for every pair (x,y) of points in M, there exists a trajectory of F from x to y. By a trajectory or positive orbit it is meant a continuous curve which is a concatenation of integral curves of elements of F. Stronger than controllability, is the concept of uniform controllability. A set F of vector fields on M is said to be *uniformly completely controllable* if there exists a positive integer N such that every two points in M can be joined by a trajectory of F which involves at most N switches.

The next lemma may be seen as a generalization of a lemma by N. Levitt and H. Sussmann [lemma 3, 12] although extra conditions that seem to have been overlooked by the authors, have been included. Its proof is rather similar to the one presented in [12].

Lemma 2.1. - Let G be a n-dimensional, compact and connected Lie group whose Lie algebra is generated by a pair {A,B} of vector fields

and $\exp(tA)$, $\exp(\tau B)$, $t,\tau \in \mathbb{R}$ are compact. Then, $\forall\, T' > 0$, there exist a positive integer ℓ' and two vector fields A' and B' such that every element of G can be expressed as a finite product

$$\prod_{i=1}^{\ell'} \exp(t_i A')\exp(\tau_i B') \quad \text{with} \quad t_i,\tau_i \geq 0 \text{ and}$$

$$\sum_{i=1}^{\ell'} (t_i+\tau_i) < T' .$$

Proof - Let $f:\mathbb{R}^{2\ell} \to G$ denote the map defined by $(t_1,\ldots,t_\ell,\tau_1,\ldots,\tau_\ell) \mapsto \prod_{i=1}^{\ell} \exp(t_i A)\exp(\tau_i B)$. If $G_{2\ell}$ is the set of all products of 2ℓ elements of $\exp(tA)$ and $\exp(\tau B)$, $G_{2\ell}$ is compact and it was proved in Theorem 1.1. (Chapter I) that $G = \bigcup_{\ell=1}^{\infty} G_{2\ell}$ and for some ℓ fixed, $G_{2\ell}$ contains an open set U. By Sard's theorem [18] the set of points where the differential of f has rank $< n$ must be of measure zero. Therefore for some $t \in \mathbb{R}^{2\ell}$ the differential $df(t)$ is of rank n. By analiticity of f, rank $df(t) = n$ for every t in an open and dense subset of $\mathbb{R}^{2\ell}$. This shows that in particular

for all $t \in S = \{(t_1,\ldots,t_\ell,\tau_1,\ldots\tau_\ell) \in \mathbb{R}^{2\ell}: t_i,\tau_i \geq 0 , \sum_{i=1}^{\ell}(t_i+\tau_i) < \tau$ for some $\tau > 0\}$, rank $df(t) = n$, which implies, by the implicit function theorem that $f(t)$, $t \in S$ contains a non-empty open subset V of G . Since G is connected and compact it follows that G is a finite product of r elements of V . Taking $\ell' = r\ell$ and $T = r\tau$ the conclusion holds for some $T' = T$ and $A' = A$, $B' = B$. To complete the proof when T' is an arbitrary positive number just replace A,B,T by $\lambda A,\lambda B,\lambda^{-1}T$ for an arbitrary $\lambda > 0$.

□

THEOREM 2.1. - The pair $\{A',B'\}$ in lemma 2.1 is uniformly completely controllable. Any pair (m_1,m_2) of points of G can be joined by a trajectory of $\{A',B'\}$ which involves at most $N = 2\ell'-1$ switches.

Proof - The proof is an immediate consequence of lemma 2.1 and the fact that G is a group. In fact, for every pair (m_1,m_2) of points of G there exists $m \in G$ such that $mm_1 = m_2$ $(m=m_2m_1^{-1})$. But lemma 2.1 guarantees that $\exists\ \ell' \in \mathbb{Z}^+$, $t_i,\tau_i \geq 0$ such that $m = \prod_{i=1}^{\ell'} \exp(t_iA') \exp(\tau_iB')$ and the conclusion holds.

□

Remark - Lemma 2.1 can be reformulated as follows. The reachable set from e (the identity of G) by trajectories of $\{A',B'\}$ involving at most N switches is G. Then, since A' and B' are left invariant vector fields on G, $R(m) = R(e)m$, $\forall\, m \in G$ and theorem 2.1 follows.

Pairs $\{A,B\}$ of vector fields on $SO(n)$, which satisfy $\{A,B\}_{L.A} = so(n)$, $\exp(tA)$ and $\exp(\tau B)$, $t,\tau \in \mathbb{R}$ are compact, were constructed in chapters III and IV. Since $SO(n)$ is connected and compact, lemma 2.1 implies that these pairs are uniformly completely controllable. Since $SO(n)$ acts transitively on S^{n-1} (the unit sphere imbedded in $\mathbb{R}^n$) and the vector fields defined by $X(x) = Ax$, $Y(x) = Bx$ are obviously vector fields on S^{n-1}, (note that $A^t = -A$, $B^t = -B$ imply $\langle Ax,x\rangle = \langle Bx,x\rangle = 0$; $\langle\cdot,\cdot\rangle$ is the inner product in $\mathbb{R}^n$) which are uniformly completely controllable. Hence, an upper bound N on the number of switches in trajectories of $\{A,B\}$ is also an upper bound on the number of switches in trajectories of $\{X,Y\}$. Now, the stereographic projection of $S^{n-1}\backslash\{p\}$ onto $\mathbb{R}^{n-1}$ defined by

$$\psi(x) = \frac{1}{1 - \langle p,x\rangle}\,.x - \frac{\langle p,x\rangle}{1 - \langle p,x\rangle}\,.\,p$$

is a diffeomorphism and the restrictions X' and Y' of X and Y respectively to $S^{n-1}\setminus\{p\}$, are vector fields on $\mathbb{R}^{n-1}$. Hence $\{X',Y'\}$ is completely controllable [19]. We conjecture that $\{X',Y'\}$ is uniformly completely controllable and the number of switches that a trajectory of $\{X',Y'\}$ involves to join any two points in $\mathbb{R}^{n-1}$ is at most N. This case and more, will be considered later although for different pairs of vector fields.

To finalize this paragraph an important result is stated. It is the bridge between the uniform finite generation of a Lie group G and the uniform controllability of left-invariant control systems evolving on G.

THEOREM 2.2. - Let X_i, $i = 1,\ldots,k$ be left-invariant vector fields on a connected Lie group G satisfying $\{X_i,\ i = 1,\ldots,k\}_{L.A} = L(G)$, $\exp(tX_i)$, $t \in \mathbb{R}$ is compact, $\forall\ i = 1,\ldots,k$. Then, $\{X_i,\ i=1,\ldots,k\}$ is uniformly completely controllable if and only if G is uniformly finitely generated by $\{\exp(tX_i)\ ;\ i = 1,\ldots,k\ ;\ t \in \mathbb{R}\}$. Hence, if the order of generation of G by these one-parameter subgroups is N_1, any two points

of G can be joined by a trajectory of $\{X_i , i = 1,\ldots,k\}$ which involves not more than $N = N_1 - 1$ switches.

The proof follows directly from the definition of a uniformly completely controllable set of vector fields, the concept of uniform finite generation of a group and the assumption made that the one-parameter subgroups generated by $X_i , i = 1,\ldots,k$ are compact.

§3. UNIFORM CONTROLLABILITY ON SO(n)

As already pointed out in Chapter I, the compactness of the one-parameter subgroups that generate a Lie group is not a necessary condition for uniform finite generation. However, if $\exp(tA)$ and $\exp(\tau B)$ are compact, where $\{A,B\}$ is any pair of generators of $so(n)$ constructed in previous chapters, the last theorem can be applied and $\{A,B\}$ is uniformly completely controllable.

THEOREM 3.1. - Let $\psi , 0 < \psi \leq \pi/2$ be the angle between the axes of any two one-parameter subgroups $\exp(tA)$ and $\exp(\tau B)$ of $SO(3)$. $\{A,B\}$ is uniformly completely controllable and any two points of $SO(3)$ can be joined by a trajectory of $\{A,B\}$ which involves

at most 2 switches if $\psi = \pi/2$ or

$k + 1$ $(k \geq 2)$ switches if $\pi/(k+1) \leq \psi < \pi/k$.

Proof - This result is an immediate consequence of the Theorem 2.1 (Chapter I), the fact that every element of $so(3)$ generates compact one-parameter subgroups and Theorem 2.2 (§2).

□

The easy way of calculating the order of generation of $SO(3)$ by any two one-parameter subgroups and the complete characterization of generators $\{A,B\}$ of $so(3)$ have as a consequence that not just symmetric systems on $SO(3)$ (as (1.2)) but also systems of the form

$$\dot{x}(t) = (A + v(t)B)x(t) , \quad x \in SO(3) \tag{3.1}$$

($v(t)$ a piecewise continuous control function) are uniformly controllable.

Lemma 3.1. - If $[A,B] \neq 0$, the systems (1.2) and (3.1) are uniformly controllable and there exist controls such that every pair of points in

$SO(3)$ can be joined by a trajectory of the system only with two switches.

Proof - a and b denote the axes of the rotations $\exp(tA)$ and $\exp(\tau B)$ respectively. Let $\psi = \{(a,b) \in [\pi/(k+1),\pi/k)$, $k \geq 2$. For every pair of vectors (a,b) in $\mathbb{R}^3$ there exist constants u_1 and v_1 such that $u_1 a + v_1 b \perp a$. So $\forall g \in SO(3)$, $\exists\ t_1,t_2,t_3 \in \mathbb{R}$ such that $g = \exp(t_1 A)\exp((u_1 A+v_1 B)t_2)\exp(At_3)$ (lemma 2.2, Chapter I). Clearly the t's can be taken nonnegative. Now choose

$$u(t) = \begin{cases} u_1 & , t \in (t_3,t_2+t_3] \\ 1 & , t \in [0,t_3] \cup (t_2+t_3,t_2+t_3+t_1] \end{cases}$$

$$v(t) = \begin{cases} v_1 & , t \in (t_3,t_2+t_3] \\ 0 & \text{otherwise} \end{cases}$$

so every pair of points of $SO(3)$ can be joined by a trajectory of the system (1.2) (trajectory of A and $u_1 A + v_1 B$) involving two switches. For the system (3.1) just make $u_1 = 1$ and the result follows.

□

For $n > 3$, let $\{A,B\}$ be any pair of generators of $so(n)$ constructed in Chapters III and IV. When, in particular, $B \in \{\exp(t \text{ ad } A).X , X \in [\alpha_k] , t \in \mathbb{R}\}$ ($[\alpha_k]$ as in Chapter IV with n and k coprime) and it is not a canonical basis element it is difficult to characterize these vector fields. However, it can be proved that they all generate compact one-parameter subgroups. For the sake of completeness it is also proved here, although assumed to be true before, that $\exp(tA)$ and $\exp(\tau B)$ are compact for every pair $\{A,B\}$ constructed in the previous two chapters.

Lemma 3.2. - 1) Every canonical basis element of $so(n)$ generates a periodic one-parameter subgroup of $SO(n)$ with period 2π.

2) Every $A \in SO(n)$ that satisfies, $\exp(A) = P$, P a permutation matrix and $P^n = I_n(-I_n)$, generates a periodic one-parameter subgroup of $SO(n)$ with period n $(2n)$ if $P_n = I_n\ (-I_n)$.

3) If $\overline{B} \in \{\exp(t \text{ ad } A).B , B \in \mathcal{B}, t \in \mathbb{R}\}$ where A is defined as in 2), then $\exp(t\overline{B})$ is periodic with period 2π.

Proof - $\forall B = A_{ij} \in \mathcal{B}$, $\exp(tB)$, $t \in \mathbb{R}$ is the subgroup of rotations in the (e_i,e_j)-plane so it is periodic with period 2π .

Clearly, $\forall t \in \mathbb{R}$

$$\exp(tA) = \begin{cases} \exp\,(t+n)A & , \ P^n = I_n \\ \exp\,(t+2n)A & , \ P^n = -I_n \ . \end{cases}$$

Hence, $\forall \overline{B} \in \{\exp(t \operatorname{ad} A).B \ , \ B \in \mathcal{B} \ , \ t \in \mathbb{R}\}$, $\exists\, \theta \in \mathbb{R}^{+-}$ such that $\overline{B} = \exp(\theta A)\, B \exp(-\theta A)$. That is $\exp(\tau\overline{B}) = \exp(\theta A) \exp(\tau B) \exp(-\theta A)$, $\forall \tau \in \mathbb{R}$. But 1) implies that $\exp((\tau+2\pi k)\overline{B}) = \exp(\tau\overline{B})$, $\forall k \in \mathbb{Z}$.

□

Hence, $\forall t_1 \in \mathbb{R}^+$, $\exists$ positive integers k_1 and k_2 such that $\exp(-t_1 B) = \exp((2k_1\pi - t_1)B)$, $\exp(-t_1\overline{B}) = \exp((2k_1\pi - t_1)\overline{B})$ and $\exp(-t_1 A) = \exp((-t_1+k_2 n)A)$ with $2k_1\pi - t_1\pi \in \mathbb{R}^+$, $k_2 n - t_1 \in \mathbb{R}^+$ and A,B and $\overline{B}$ as in the lemma above.

THEOREM 3.2. - 1) For $n > 3$, let $\{A,B\}$ be any pair of left-invariant vector fields on $SO(n)$ that satisfy the conditions of the Theorem 2.2, Chapter III and $\overline{B} \in \{\exp(\operatorname{tad} A).B,\ t \in \mathbb{R}\} \subset so(n)$.

Then, $\{A,\bar{B}\}$ is uniformly completely controllable and for every pair (p,q) of points of $SO(n)$, there exists a trajectory of $\{A,\bar{B}\}$ from p to q, which involves not more than $N = 2^n-2$ ($N = 2^n-4$, if $\bar{B} \in B$) switches.

2) For $n > 3$, let $\{A,B\}$ be any pair of left-invariant vector fields on $SO(n)$ that satisfy the conditions of the theorem 1.3, Chapter IV. Then, $\{A,B\}$ is uniformly completely controllable and any pair (p,q) of points of $SO(n)$ can be joined by a trajectory of $\{A,B\}$ which involves not more than $N = 2^{n-1}+4$ ($N = 2^{n-1}+2$ if $B \in B$) switches.

Proof - The result follows directly from the theorems 2.1 and 2.2, Chapter III (if 1)) or from the theorem 1.3, Chapter IV (if 2)) plus the result of lemma 3.2 and theorem 2.2 in this chapter.

□

§4. SOME CONSEQUENCES OF THE UNIFORM CONTROLLABILITY ON SO(n) .

In [12, Theorem 2], N. Levitt and H. Sussmann constructed a completely controllable pair $\{X,Y\}$ of vector fields on M, M is any connected and paracompact C^k $(2 \le k \le \infty)$ manifold of dimension n, so that any two points of M can be joined by a trajectory of $\{X,Y\}$ involving not more than $N + 6$ switches, where N is the corresponding number of switches required for some pair $\{A,B\}$ of left-invariant vector fields on $SO(n)$. By Theorem 3.2 we may choose $\{A,B\}$ with $N = 2^{n-1}+2$ to give

THEOREM 4.1. - On any connected, paracompact n-dimensional C^k $(2 \le k \le \infty)$ manifold, there exist two vector fields X and Y, so that any two points of M may be joined by a trajectory of $\{X,Y\}$ involving not more than $2^{n-1}+8$ switches if $n \ge 4$, and 8 or 6 switches if $n = 3$ or $n = 2$ respectively.

When $n = 3$, $\{A,B\}$ may be chosen to be orthogonal, giving $N = 2$. For $n = 2$, $SO(2)$ is one-dimensional and there are no switches i.e. $N = 0$. So 2+6 (0+6) is the number of switches required by the pair $\{X,Y\}$ on a 3-dimensional (2-dimensional) manifold.

Note that the conjecture formulated earlier may bring the number of switches down to 2 when $M = \mathbb{R}^2$.

Theorem 4.1 applies to every connected Lie group since a Lie group is a paracompact C^∞- manifold. However, if $\{X,Y\}$ are restricted to belong to the set of left-invariant vector fields of G they may not necessarily satisfy the theorem above.

If $\{X,Y\}_{L.A} = L(G)$, then $\{X,Y,-X,-Y\}$ are completely controllable [7]. Hence if X and Y generate compact one-parameter subgroups, $\{X,Y\}$ is completely controllable. However, if G is non-compact $\{X,Y\}$ will not be uniformly completely controllable. The following example illustrates this fact.

EXAMPLE 4.1. - $G = SO_0(2.1)$ is the Lie group of real quadratic matrices of determinant 1 , leaving invariant the quadratic form $x_1^2 - x_2^2 - x_3^2$ with $(x_1,x_2,x_3) \in \mathbb{R}^3$. Its Lie algebra

$$so(2,1) = \left\{ \begin{pmatrix} X_1 & X_2 \\ X_2^t & 0 \end{pmatrix} : X_1 \in so(2),\ X_2 \text{ is arbitrary} \right\}$$ is of non-compact type and admits a direct sum decomposition, the Cartan decomposition, $so(2,1) = T_1 \oplus P_1$ where T_1 is the maximal compact subalgebra of $so(2,1)$ and P_1 a vector subspace.

The corresponding symmetric space decomposition of $SO_o(2,1)$ [2, p.453] as $SO_o(2,1) = K_1 A_1 K_1$, K_1 the maximal compact subgroup of $SO_o(2,1)$ whose Lie algebra is T_1 and $A_1 = \exp(A_1)$, A_1 a maximal abelian subalgebra of $so(2,1)$ contained in P_1 , give a decomposition of $SO_o(2,1)$ as a product of 3 one-parameter subgroups. If T_1 and A_1 are chosen to be generated by the elements A_{12} and $B_{13} = E_{13} + E_{31}$ respectively, it follows

$$SO_o(2,1) = \exp(tA_{12}) \exp(\tau B_{13}) \exp(\theta A_{12}) \; ; \quad t,\tau,\theta \in \mathbb{R} \; .$$

Since $[A_{12},B_{13}] = -B_{23}$, $[A_{12},B_{23}] = B_{13}$, $[B_{13},B_{23}] = A_{12}$ and $\{A_{12},B_{13},B_{23}\}$ is a basis of $so(2,1)$, $\{A_{12},B_{13}\}_{L.A} = so(2,1)$.

Take $A = A_{12}$, $B = B_{13}$. $\exp(\tau B_{13}) = \begin{pmatrix} \cosh \tau & 0 & \sinh \tau \\ 0 & 1 & 0 \\ \sinh \tau & 0 & \cosh \tau \end{pmatrix}$ is clearly noncompact and if $\tau_1 < 0$, there is no $\tau_2 > 0$ s.t. $\exp(\tau_1 B_{13}) = \exp(\tau_2 B_{13})$. Although $SO_o(2,1)$ is uniformly finitely generated by $\exp(tA)$ and $\exp(\tau B)$, controllability in a finite number of switches cannot be achieved with just these two vector fields. However, every pair of points in $SO_o(2.1)$ can be joined

by a trajectory of $\{A,B,-B\}$ involving at most 2 switches.

Next, a set of four left-invariant vector fields on $SO_o(n,1)$, $n \geq 3$ is constructed, which is uniformly completely controllable.

$SO_o(n,1)$ is the connected Lie group of quadratic matrices with determinant 1, which leave invariant the quadratic form $x_1^2 - x_2^2 - \ldots - x_{n+1}^2$, $(x_1,x_2,\ldots,x_{n+1}) \in \mathbb{R}^{n+1}$. Let B_{ij} be the symmetric matrix defined by $B_{ij} = E_{ij} + E_{ji}$.

$\{A_{ij};i,j=1,\ldots,n,i<j\} \cup \{B_{i,n+1};i=1,\ldots,n\}$ is a basis of $so(n,1)$, the canonical basis. The structure formulas of $so(n,1)$ with respect to this basis are as follows,

$$[B_{ij},B_{k\ell}] = \delta_{jk}A_{i\ell} + \delta_{i\ell}A_{jk} + \delta_{ik}A_{j\ell} + \delta_{j\ell}A_{ik} ,$$

$$[A_{ij},B_{k\ell}] = \delta_{jk}B_{i\ell} + \delta_{j\ell}B_{ik} - \delta_{\ell i}B_{kj} - \delta_{ki}B_{\ell j} ,$$

$$[A_{ij},A_{k\ell}] = \delta_{jk}A_{i\ell} + \delta_{ki}A_{jk} - \delta_{ik}A_{j\ell} - \delta_{j\ell}A_{ik} .$$

THEOREM 4.2. - There exists a completely controllable set D of four left-invariant vector fields on $SO_o(n,1)$ such that every pair (m_1,m_2) of points of $SO_o(n,1)$ can be linked by a trajectory of D involving at most $2N+2$ switches (N as in Theorem 3.2).

Proof - $so(n,1)$ admits a Cartan decomposition,

$so(n,1) = T_1 \oplus P_1$, $T_1 = so(n)$, $P_1 = \text{span}\{B_{i,n+1}; i = 1,\ldots,n\}$.

Let $C = \sum_{i=1}^{n} \alpha_i B_{i,n+1}$, $\alpha_i \in \mathbb{R}$ be any element of P_1 . C generates a maximal abelian subalgebra of $so(n,1)$ contained in P_1 . The symmetric space decomposition of $SO_0(n,1)$ corresponding to the Cartan decomposition of $so(n,1)$ is $SO_0(n,1) = K_1 A_1 K_1$, $K_1 = SO(n)$, $A_1 = \exp(\mathbb{R}C)$. If $\{A,B\}$ is any pair of left-invariant vector fields on K_1 , that satisfy the conditions of the theorem 1.3, Chapter IV and $B \in \mathcal{B}$, by applying Theorem 3.2-2) in this chapter it follows that $D = \{A,B,C,-C\}$ is uniformly completely controllable and any pair (m_1,m_2) of points of $SO_0(n,1)$ may be joined by a trajectory of D involving at most $2N+2$ switches, where $N = 2^{n-1}+2$ is the corresponding number of switches for the pair $\{A,B\}$ in $SO(n)$.

□

Although $SO_0(n,1)$ is uniformly finitely generated by $\exp(tA)$, $\exp(\tau B)$ and $\exp(\theta C)$, this last one-parameter subgroup is not compact and the results of the theorem can not be achieved with just 3 vector fields.

Clearly, any other pair $\{A,B\}$ as constructed in Chapters III and IV may be considered but the final number of switches will be bigger than when $\{A,B\}$ is chosen as above.

Remark - For $n = 2$, three vector fields $\{A,C,-C\}$ are enough to satisfy the requirements of the last theorem since, in this case, K_1 is a one-dimensional subgroup.

CHAPTER VI.

CONCLUSION AND OPEN PROBLEMS.

In this chapter, a few concluding remarks are made together with suggestion for further research.

The framework considered here seems to be the natural departure point for constructing a theory on the uniform controllability for a class of bilinear systems defined on connected Lie groups G. In fact, if G is uniformly finitely generated by R subgroups of the form $\exp(t(\Sigma\, u_i X_i))$, the system $\dot{x}(t) = (\Sigma\, u_i X_i)x(t)$, $x \in G$ is uniformly controllable. When all the generators of G are compact, the number of switches in trajectories of the system required to join any two state points can be reduced to $N-1$, where N is the order of generation of G corresponding to those generators (Theorem 2.2, Chapter V) and R (the number of vector fields needed) must be greater than or equal to two [12]. Clearly, only if G is compact may all its generators be compact. In the noncompact case, at least one of the R generators of G must be noncompact. However, uniform controllability can still be achieved in $N-1$ switches although the number of directions needed has to increase from R to $R+R_C$ where R_C is equal to the number of noncompact vector fields. R_C comes from considering $\pm X$ whenever X generates a noncompact subgroup.

In a series of papers [8], [9], [10], [13], [14], [15], [16], F. Lowenthal and R. Koch found the orders of generation for all real and complex Lie groups of dimension two and three. Therefore the uniform controllability problem is completely solved in these cases.

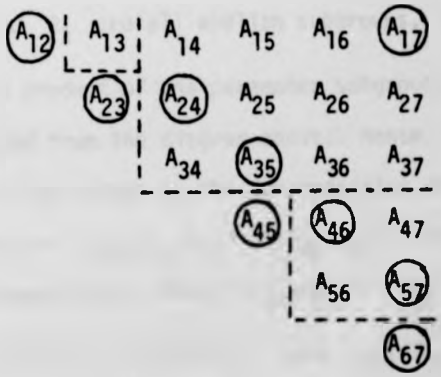
The present work also gives a complete solution for a particular set of vector fields on $SO(n)$ namely, the generating set of $so(n)$ corresponding to a particular decomposition of $SO(n)$ based on symmetric spaces. In fact, the number of one-parameter subgroups that decompositions of $SO(n)$ yield when one decomposes $SO(m)$, $2 < m \leq n$ according to the symmetric structure in I (Chapter II), increases with p, being minimal, equal to the dimension of $SO(n)$, when $p = q$ $(p = q+1)$ if $p+q = m$ is even (if $p+q = m$ is odd) (lemmas 2.1 and 2.2, Chapter II). Since the order of generation must be greater than or equal to the dimension of G, the generating set corresponding to this decomposition is uniformly completely controllable and hence, controllability cannot be achieved in less than $m-1$ switches $(m = \dim SO(n))$ that is, there exists at least a pair of points in $SO(n)$ that cannot be joined by a trajectory of this generating set, which involves less than $m-1$ switches. Note that, the generating set corresponding to a given decomposition is a subset of the canonical basis and consequently generates a set of compact one-parameter subgroups.

Any other decomposition of SO(n) (as considered in Chapter II) has a corresponding generating set (not unique) which is uniformly completely controllable. However only an upper bound (L-1) can be put on the number of switches. (L is the corresponding number of generation.) The same applies for the pairs {A,B} of generators of so(n) constructed in Chapters III and IV.

The present work has been devoted to reducing this upper bound to its minimum. The following example shows that for $G = SO(n)$, the upper bound given in this work is not the minimum achievable.

EXAMPLE - Let $G = SO(7)$, {A,B} a pair of generators of so(7) defined by, $\exp(A) = P$, P a permutation matrix satisfying $Pe_i = e_{i+1}$, $i = 1,\ldots,6$; $Pe_7 = e_1$ and $B = A_{34}$. Since $B \in \alpha_1$, $X \in \{\exp(tA).B , t \in \mathbb{R}\}$, $\forall X \in [\alpha_1]$. It has been proved that only two decompositions of SO(7) as in I, Chapter II, having corresponding generating sets contained in $[\alpha_1]$ and giving different numbers of generation exist (lemma 3.6 and theorem 3.1, Chapter II). By choosing the decomposition that gives the least number of generation and taking into account that $\forall X \in [\alpha_1]$ and $\forall t \in \mathbb{R}$, $\exp(tX) = \exp(\theta A) \exp(tB) \exp(-\theta A)$, for some θ

depending on X , it follows from Theorem 1.1 (Chapter IV) and Theorem 2.2 (Chapter V) that $\{A,B\}$ is uniformly completely controllable in at most $2^6+2 = 66$ switches. However if $SO(7)$ is decomposed as a product of one-parameter subgroups as in lemma 2.1, Chapter II, although the corresponding generating set is not contained in $[\alpha_1]$, its elements can be obtained by brackets of elements in $[\alpha_1]$. Using lemmas 1.1, 1.3 and 1.6 in Chapter IV one can reduce the number of switches found previously. The diagram below illustrates the decomposition of $so(7)$ corresponding to the chosen symmetric space decomposition of $SO(7)$ and also shows which canonical basis elements have been selected as a generating set.



For the Lie group, one has $SO(7) = K_1 A_1 K_1$,

$K_1 = \underset{\text{''}}{SO(4)}_{K_1^1} \times \underset{\text{''}}{SO(3)}_{K_1^2}$ is the Lie group of

$T_1 = \text{span}\{A_{12},A_{13},A_{23}\} \cup \text{span}\{A_{ij};i<j;i,j = 4,5,6,7)$,

$A_1 = \exp(A_1)$, $A_1 = \text{span}\{A_{24},A_{35},A_{17}\}$.

$K_1^1 = SO(4) = K_2A_2K_2$, $K_2 = SO(2) \times SO(2)$ is the Lie group of $T_2 = \text{span}\{A_{45},A_{67}\}$, $A_2 = \exp(A_2)$, $A_2 = \text{span}\{A_{46},A_{57}\}$. $K_1^2 = SO(3) = K_3A_3K_3$, $K_3 = SO(2) = \exp(\tau A_{12})$, $A_3 = \exp(tA_{23})$. So in the decomposition

$$SO(7) = K_2A_2K_2K_3A_3K_3A_1K_3A_3K_3K_2A_2K_2$$

since K_2,K_3,A_1,A_2 and A_3 are all abelian subgroups, $SO(7)$ may be decomposed as a product of one-parameter subgroups generated by the elements selected from the diagram above. Hence, $\exp(tX)$ appears once, twice or four times in the decomposition depending on whether X belongs to $\{A_{24},A_{35},A_{17}\}$, $\{A_{46},A_{57}\}$ or $\{A_{12},A_{23},A_{45},A_{67}\}$ respectively. Now, $[A_{34},A_{23}] = -A_{24}$, $[A_{34},A_{45}] = A_{35}$ so $\forall\ t \in \mathbb{R}$, $\exp(tA_{24})$ and $\exp(tA_{35})$ may be written as a product of 5 elements from $\exp(\tau A)$ and $\exp(\theta B)$ ($\{A,B\}$ as above) and $[A_{45},A_{56}] = A_{46}$, $[A_{56},A_{67}] = A_{57}$ so, seven

elements from $\exp(\tau A)$ and $\exp(\theta B)$ are required for $\exp(tA_{46})$ and $\exp(tA_{57})$. All the other one-parameter subgroups in the decomposition may be written as $\exp(tA)\exp(\theta B)\exp(-tA)$ and the final result after composition of terms with the same generator is that $SO(7)$ is uniformly finitely generated by $\exp(tA)$ and $\exp(\tau B)$ with number of generations 65. So $\{A,B\}$ is uniformly controllable with at most 64 switches.

To determine the order of generation of $SO(n)$ with respect to a set of one-parameter subgroups that generate $SO(n)$, one has to find out how generators and decompositions relate to each other.

This work is not by any means a fait accompli and opens up various directions for further research.

The first task is to characterize all the generators of the Lie algebra $L(G)$ a given Lie Group G . Although several important results have already been obtained (see Jurdjevic and Kupka [5], Jurdjevic and Sussmann [6], Kuranishi [11] and also Theorem 3.2, Chapter I in the present work) a complete characterization is far from being accomplished even when G is a semisimple Lie group of matrices and the generators are restricted to pairs $\{A,B\}$, which are known to exist. When G is noncompact and its Lie algebra

is generated by a set of compact elements ($X \in L(G)$ is said compact if the one-parameter subgroup it generates, $\exp(tX), t \in \mathbb{R}$, is compact), the order of generation of G corresponding to these generators is infinite. Therefore, such cases are without interest in studying the uniform controllability problem.

Decompositions of G based on symmetric spaces may be used to determine the order of generation of G by one-parameter subgroups generated by elements of $L(G)$. For the classical matrix Lie groups, involutive automorphisms always exist and such decompositions are always possible [2]. When G is connected and compact, the exponential map is onto and a prior knowledge of a set of generators of the Lie algebra $L(G)$ is not necessary since the decomposition itself provides a corresponding generating set $\{\exp(tX_i)$, $i = 1,\ldots,k$, $t \in \mathbb{R}\}$ of G and consequently a set $\{X_i, i = 1,\ldots,k\}$ of generators of $L(G)$. For the noncompact case, there may exist $X \in G$ which does not lie on a one-parameter subgroup of G. A result by L. Markus [17] says that $\forall X \in G$, G any classical Lie group of matrices $\exists$ a positive integer $p = p(X)$ such that X^p lies on a one-parameter subgroup of G. This result can presumably be used in finding a set of generators of $L(G)$ whose one-parameter subgroups uniformly finitely generate G. When G is noncompact, other decompositions than the Cartan

decomposition may be used with success. For instance, the Iwasawa and the Bruhat decompositions can both be considered in the noncompact case.

The $SO(n)$ case, appears to be the easiest one among all the classical groups of matrices due to the compactness of $SO(n)$, the very simple structure of the canonical basis of $so(n)$ and the existence of permutation matrices in $SO(n)$, which have been an important tool in the present work. As a consequence, a complete solution for $SO(n)$ may yield solutions to the same problem for other groups such as $SO_0(p,q)$ or $SL(n,\mathbb{R})$ (note that $SO(p) \times SO(q)$ and $SO(n)$ are the maximal compact subgroups of $SO_0(p,q)$ and $SL(n,\mathbb{R})$ respectively). This and the important role that generators of $so(n)$ play in constructing uniformly completely controllable vector fields on any paracompact and connected C^k-manifold, are, in the author's opinion, good reasons for having started with $SO(n)$ and to direct future research, primarily to the order of generation problem of the special orthogonal group.

However, since Lowenthal's methods are completely different, the solution may lie in a deep understanding of the representation theory for these groups.

REFERENCES.

[1] - P. DAVENPORT - Rotations about nonorthogonal axes; AIAA Journal, Vol. 11, No.6, 1973.

[2] - S. HELGASON - Diff. Geometry, Lie groups and symmetric spaces; Academic press, New York, 1978.

[3] - R. HERMANN - Lie groups for physicists; Benjamin, 1966.

[4] - J. HUMPHREYS - Introduction to Lie algebras and representation theory; Springer-Verlag, New York 1972.

[5] - V. JURDJEVIC and I. KUPKA - Control Systems on semi-simple Lie groups and their homogeneous spaces; Ann. Int. Fourier, Grenoble, Vol. 31, 4, 1981.

[6] - V. JURDJEVIC and H. SUSSMANN - Controllability of nonlinear systems; J. Diff. Equations 12, 1972.

[7] - V. JURDJEVIC and H. SUSSMANN - Control Systems on Lie groups; J. Diff. Equations 12, 1972.

[8] - R. KOCH and F. LOWENTHAL - Uniform finite generation of three-dimensional Linear Lie groups, Can. J. Math. 27, 1975.

[9] - R. KOCH and F. LOWENTHAL - Uniform finite generation of Lie groups locally isomorphic to $SL(2,\mathbb{R})$; Rocky Mountain Journal of Mathematics, Vol. 7, No.4, 1977.

[10] - R. KOCH and F. LOWENTHAL - Uniform finite generation of complex Lie groups of dimension two and three; Rocky Mountain Journal of Mathematics, Vol. 10, No.2, 1980.

[11] - M. KURANISHI - On everywhere dense imbedding of free groups in Lie groups; Nagoya Math. Journal 2, 1951.

[12] - N. LEVITT and H. SUSSMANN - On controllability by means of two vector fields; Siam J. Control, Vol. 13, No.6, 1975.

[13] - F. LOWENTHAL - Uniform finite generation of the isometry groups of Euclidean and non-Euclidean geometry; Can. J. Math. 23, 1971.

[14] - F. LOWENTHAL - Uniform finite generation of the rotation group; Rocky Mountain J. Math. 1, 1971.

[15] - F. LOWENTHAL - Uniform finite generation of the affine group; Pacific J. Math. 40, 1972.

[16] - F. LOWENTHAL - Uniform finite generation of SU(2) and $SL(2,\mathbb{R})$; Can. J. Math. 24, 1972.

[17] - L. MARKUS - Exponentials in algebraic matrix groups; Advances in Mathematics, 11, 1973.

[18] - J. MARSDEN and R. ABRAHAM - Foundations of Mechanics; Benjamin, 1978.

[19] - H. SUSSMANN - On the number of directions needed to achieve controllability; Siam J. Control, Vol. 13, No.2, 1975.

[20] - J. WOLF - Spaces of constant curvature; Publish or Perish, 1977.

9788/83

VA LEITE Mdef

160