ANNALES DE L'I. H. P., SECTION C

R. EL ASSOUDI
J. P. GAUTHIER
I. A. K. KUPKA

On subsemigroups of semisimple Lie groups

Annales de l'I. H. P., section C, tome 13, nº 1 (1996), p. 117-133
<http://www.numdam.org/item?id=AIHPC_1996__13_1_117_0>

© Gauthier-Villars, 1996, tous droits réservés.

L'accès aux archives de la revue « Annales de l'I. H. P., section C » (http://www.elsevier.com/locate/anihpc) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Inst. Henri Poincaré,

Vol. 13, n° 1, 1996, p. 117-133 *Analyse non linéaire*

On subsemigroups of semisimple Lie groups

by

R. El ASSOUDI

INSA de Rouen, LMI, AMS, URA CNRS 1378, BP n° 08,
place Émile Blondel, 76131, Mont-St-Aignan, France.

J. P. GAUTHIER*

INSA de Rouen, LMI, AMS, URA CNRS 1378, BP n° 08,
place Émile Blondel, 76131, Mont-St-Aignan, France.
Institut Universitaire de France.

and

I. A. K. KUPKA*

University of Toronto, Dpt. of Maths,
100 St Georges street, Toronto, Ontario, M5S-1A1, Canada.

ABSTRACT. – In this paper, we consider a real connected semisimple Lie group G and ask whether or not a subset S of G generates G as a semigroup. We deal with the special case where S is infinitesimally generated, *i.e.* $S = \{\exp t X | X \in \Sigma, t \in \mathbb{R}_+\}$ for some subset Σ of L, the Lie algebra of G. In the case where Σ is a symmetric subset of L (*i.e.* $\Sigma = -\Sigma$), this is equivalent to the fact that S generates G as a group. It is also known, by an old result of Kuranishi, that S generates G as soon as Σ is a symmetric subset of L of the form $\{\pm X, \pm Y\}$ for generic pairs (X, Y) in $L \times L$. In the case where $\Sigma = \{X, Y\}$, almost nothing is known, except in the compact case where Kuranishi's result still holds. We deal with the intermediate case where $\Sigma = \{X, \pm Y\}$. This case is specially important in control theory, where such sets Σ apear naturally through control systems of the "classical control-affine form $\dot{x} = X(x) + u Y(x)$".

A theorem is proven, which is the final form of several results in a series of papers of all of the authors. This theorem improves on all these results.

AMS Subject classification: Primary: 93 B 05, 17 B 20; secondary: 93 C 10, 22 E 46.

* Authors are partly supported by NSERC GRANT OGP 0036498.

Key words: Semi-simple Lie algebras, controllability, invariant vector fields, root systems.

RÉSUMÉ. – Dans cet article, on considère un groupe de Lie réel connexe semi-simple G et on se demande quand est-ce qu'une partie S de G engendre G en tant que semigroupe. On s'intéresse au cas particulier où S est infinitésimalement engendré, *i.e.* $S = \{\exp t X | X \in \Sigma, t \in \mathbb{R}_+\}$, par une partie Σ de L, l'algèbre de Lie de G. Dans le cas où Σ est une partie symétrique de L (*i.e.* $\Sigma = -\Sigma$) ceci est équivalent au fait que S engendre G comme un groupe. On sait, par un résultat de Kuranishi, que S engendre G dès que Σ est une partie symétrique de la forme $\{\pm X, \pm Y\}$ pour une paire générique dans $L \times L$. Dans le cas où $\Sigma = \{X, Y\}$, on ne sait presque rien sauf dans le cas compact où le résultat de Kuranishi est toujours vrai. On s'intéresse au cas intermédiaire où $\Sigma = \{X, \pm Y\}$. Ce cas est particulièrement important dans la théorie du contrôle (systèmes affines classiques du type : $\dot{x} = X(x) + uY(x)$).

Un théorème est démontré. Il est la forme finale de certains résultats d'une série d'articles des auteurs. Ce théorème implique tous les résultats précédents.

0. INTRODUCTION

$\mathbb{R}$ and $\mathbb{C}$ denote respectively the fields of real and complex numbers. For $a \in \mathbb{C}$, Re a and Im a are the real and imaginary part of a.

In this paper we study the following question: find conditions for a subset S of a group G to generate the group in the following sense: for any $g \in G$ there exist an integer N and a mapping $s : \{1, ..., N\} \to S$ such that $g = s(1)\, s(2) ... s(N)$. One may rephrase that as follows: the semigroup generated by S is G.

Special cases of this problem are known: if G is a topological connected group, any neighborhood V of the unit of G, generates G.

A more sophisiticated result due to Kuranishi is the following: let G be a semi-simple real connected Lie group. Then for any generic pair of elements X, Y in the Lie algebra of G, the set S union of the one-parameter groups $\{\exp t X | t \in \mathbb{R}\}$, $\{\exp s Y | s \in \mathbb{R}\}$ generated by X and Y respectively, generates G in the above sense ([13]). Let us remark here that this is in fact a Lie algebra result: all one has to show is that a generic pair of elements X, Y in the Lie algebra of G, generates this algebra. Let us remark that this condition is also necessary.

Now, may be more in accordance with the semigroup aspect of the definition of the generation of G by a subset S, one can ask: given two elements X, Y in the Lie algebra of G when does the union of the one-parameter **semigroups** $\{\exp tX | t \in \mathbb{R}_+\}$ and $\{\exp sY | s \in \mathbb{R}_+\}$, ($\mathbb{R}_+$ = non negative numbers) generate G. This seems to be a hard question and very little is known about it, however, in the case where G is semi-simple connected **compact**, the result of Kuranishi is still valid.

In this paper we consider the following intermediate case: given two elements A and B of the Lie algebra of G, when does the union of the one-parameter **semigroup** $\{\exp tA | t \in \mathbb{R}_+\}$ with generator A and the one-parameter group $\{\exp tB | t \in \mathbb{R}\}$ with generator B, generate G?

Let us mention that this question is of great interest in the branch of control theory dealing with accessibility properties of systems. For instance, our result implies other controllability results for homogeneous bilinear systems on $\mathbb{R}^n - \{0\}$ and, using the result of [1], other controllability results for non homogeneous bilinear systems on $\mathbb{R}^n$.

Here we are going to assume that G is a real connected semi-simple Lie group with finite center. Its Lie algebra will be denoted by L.

To state our results, we need a couple of simple concepts.

For $X \in L$, $\operatorname{ad} X : L \to L$ will denote the derivation $Y \to [X, Y]$ of L.

DEFINITION 0. – An element $B \in L$ will be called strongly regular if:

(i) zero is an eigenvalue of ad B of multiplicity equal to the rank of L.

(ii) every other eigenvalue (possibly complex) of ad B is simple.

Note that any strongly regular element is obviously regular in the usual sense.

Notation. – We shall denote by $\operatorname{Sp}(B)$ the subset of $\mathbb{C}$ of all **nonzero** eigenvalues of ad B. For $a \in \operatorname{Sp}(B)$ we denote by L_a the one dimensional eigenspace of a and by $L(a)$ the real space $(L_a + L_{a^*}) \cap L$, a^* =complex-conjugate of L.

$$(0) \qquad \begin{cases} L_{\mathbb{C}} = \operatorname{Ker} \operatorname{ad}_{\mathbb{C}} B \oplus \{L_a | a \in \operatorname{Sp}(B)\}, \\ L = \operatorname{Ker} \operatorname{ad} B \oplus \{L(a) | a \in \operatorname{Sp}(B), \operatorname{Im} a \geq 0\} \end{cases}$$

Ker $\operatorname{ad}_{\mathbb{C}} B$ is the kernel of $\operatorname{ad}_{\mathbb{C}} B$. It is a Cartan subalgebra of $L_{\mathbb{C}}$.

As a consequence any $A \in L_{\not{c}}$ has a decomposition:

$$(1) \quad A = A_0 + \Sigma\{A_a | a \in \operatorname{Sp}(B)\},\ A_0 \in \operatorname{Ker} \operatorname{ad}_{\not{c}} B \quad \text{and} \quad A_a \in L_a,$$

Any $A \in L$ has a real decomposition:

$$(2) \qquad A = A(0) + \Sigma\{A(a) | a \in \operatorname{Sp}(B),\ \operatorname{Im} a \geq 0\}.$$

Finally we endow $\not{c}$ with the lexicographic ordering: $a > b$ if $\operatorname{Re} a > \operatorname{Re} b$ or $\operatorname{Re} a = \operatorname{Re} b$ and $\operatorname{Im} a > \operatorname{Im} b$.

DEFINITION 1. – An eigenvalue $a \in \operatorname{Sp}(B)$ is called maximal (resp. minimal) if for any $b \in \operatorname{Sp}(B)$, $b > 0$ (resp. $b < 0$), $[L_a, L_b] = \{0\}$.

($[L_a, L_b]$ is the space of all brackets $[X, Y]$, $X \in L_a$, $Y \in L_b$).

Now we can state our main result.

THEOREM 1. – *Let G be a real connected semi-simple Lie group with finite center and Lie algebra L.*

Then for $A, B \in L$, the union of the one-parameter semigroup $\{\exp t A | t \in \mathbb{R}_+\}$ generated by A with the one-parameter group $\{\exp t B | t \in \mathbb{R}\}$ generates G if the following conditions are satisfied:

(H1) B is strongly regular.

(H2) The couple (A, B) generates the Lie algebra L.

(H3) Let $A = A_0 + \Sigma\{A_a | a \in \operatorname{Sp}(B)\}$ be the decomposition of A along the eigenspaces of $\operatorname{ad}_{\not{c}} B$ [*see* (1) above]. Then $A_a \neq 0$ if a is either maximal or minimal.

(H4) If $a \in \operatorname{Sp}(B)$ is maximal and the real part $r = \operatorname{Re} a$ is a non zero eigenvalue of $\operatorname{ad}_{\not{c}} B$, then $\operatorname{Trace}(\operatorname{ad} A_r \circ \operatorname{ad} A_{-r}) < 0$ provided that L_r and L_a belong to the same simple ideal of $L_{\not{c}}$.

Remark 0 . – All the conditions (Hi), $i = 1, 2, 3, 4$, define semi-algebraic subsets of $L \times L$. Moreover the subsets defined by (Hi), $i = 1, 2, 3$, are open and dense in $L \times L$.

Now we state the control theoretic version of theorem 1:

THEOREM 2. – *Under the same notations and assumptions as in theorem* 1, *the semigroup generated by the set* $\{\exp t(A + u B) | u \in \mathbb{R},\ t \in \mathbb{R}_+\}$ *is* G.

In other words if $g_0, g_1 \in G$, there exists a piecewise C^1 curve $g : [0, T] \to G$, $T > 0$, such that $g(0) = g_0$, $g(T) = g_1$ and there exists a partition $0 = t_0 < t_1 < \ldots < t_{N+1} = T$ such that on $[t_i, t_{i+1}]$, $g(t) = \exp(t - t_i)(A + u_i B)\ g(t_i)$ for some $u_i \in \mathbb{R}$.

Theorem 1 is the culmination of a series of papers (*see* [12], [5], [6], [4], [15]) beginning with the result [12]. The **improvement** between theorem 1 and the basic result of [12] lies in the condition (H2). In [12], (H2) was replaced by a much stronger and very unnatural condition. The condition (H2) given here is **necessary** for the generation of G by the semigroup $\{\exp t\, A | t \in \mathbb{R}_+\}$ and the group $\{\exp t\, B | t \in \mathbb{R}\}$ as is easily seen. Let us stress that (H2) is not implied by the conditions (H1), (H3), (H4).

In the thesis [3] and in [5], [6], [4], [15], some intermediate results were proved.

Some results for other types of Lie groups can be found for instance in [9], [8], [14], [1].

1. CLOSED SUBSEMIGROUPS OF LIE GROUPS

To prove our result, it is sufficient to show that the closure of the semigroup S generated by $\{\exp t\, A | t \in \mathbb{R}_+\}$ and $\{\exp s\, B | s \in \mathbb{R}\}$ is the whole group G. This follows applying the following simple lemma to the set $\Gamma = \{A, B, -B\}$.

LEMMA 0. – *Let Γ be a subset of L which generates L as a Lie algebra. Let S be the semigroup generated by the union $\{\exp t\, X | X \in \Gamma,\ t \in \mathbb{R}_+\}$ of the one-parameter semigroups generated by the elements of Γ. If the closure of S is G then S itself is G.*

Proof. – By a classical result (*see* [12], for instance), the interior of S, $\operatorname{int}(S)$, is nonempty. Let S^{-1} be the semigroup $\{x^{-1} | x \in S\}$. Then for any $g \in G$, $S^{-1}\, g$ has closure G. Hence $\operatorname{int}(S) \cap S^{-1}\, g$ is nonempty: there exist $s_1,\ s_2 \in S$ such that $s_1^{-1}\, g = s_2$. Hence $g = s_1\, s_2$.

These considerations lead us to consider closed semigroups of a Lie group. As is the case with closed subgroups of a Lie group, closed subsemigroups of Lie groups have a better structure than general subsemigroups of a Lie group that can be pretty wild.

Now, as is well known, a closed subgroup of a Lie group is a Lie subgroup and hence has a Lie algebra. On the same way, closed subsemigroups of a Lie group possess a tangent object similar to a Lie algebra.

DEFINITION 2. – Let S be a closed subsemigroup of a Lie group. Its Lie-saturate (*see* [12]) or Lie-wedge (*see* [10]), denoted by $W(S)$, is the set of all $X \in L$ such that $\exp t\, X \in S$ for all real $t \geq 0$. The edge $E(s)$

of S is the largest vector subspace contained in $W(S)$: it is also the set of all $X \in L$ such that $\exp tX \in S$ for all $t \in \mathbb{R}$.

Note that the Lie algebra of a closed subgroup of a Lie group is defined in a totally similar fashion.

$W(S)$ has some nice properties very reminiscent of those of a Lie algebra. Let us list them here:

A) $W(S)$ is a closed convex positive cone in L.

B) $E(S)$ is a Lie subalgebra of L.

C) For any $X \in E(S)$ and for any $t \in \mathbb{R}$, the inner automorphism $e^{t \operatorname{ad} X}$ of L maps $W(S)$ into itself and preserves $E(S)$.

These properties are easy to prove (*see* for instance [12]).

Unhappily they do not characterize the Lie wedges. Otherwise our problem would have a very simple answer. In the following we shall supplement conditions A), B), C) by three other conditions on a set Γ in order that the semigroup generated by the set $\{\exp tX | X \in \Gamma, t \geq 0\}$ is the whole group G.

We shall consider subsets Γ of L verifying the following conditions:

A) Γ is a closed convex positive cone.

B) The largest vector subspace $E(\Gamma)$ contained in Γ called the edge of Γ is a Lie subalgebra of L.

C) For any $X \in E(\Gamma)$, any $t \in \mathbb{R}$, $e^{t \operatorname{ad} X}$ maps Γ into itself.

D) $E(\Gamma)$ contains a strongly regular element B.

E) If $s \in \operatorname{Sp}(B)$ and s is maximal, (respectively minimal), there exists a X_+ (resp. X_-) such that $X_+(s) \neq 0$ (resp. $X_-(s) \neq 0$).

F) If $r \in \operatorname{Sp}(B)$ is the real part of a maximal s and if L_r and L_s belong to the same simple ideal of $L_{\not{c}}$, then there exist $X_+, X_- \in \Gamma$ such that:

$$\operatorname{Trace}(\operatorname{ad} X_+(r) \circ \operatorname{ad} X_-(-r)) < 0.$$

THEOREM 3. – *If a subset Γ of L satisfies the conditions A) to F), and if Γ generates L as a Lie algebra, then the subsemigroup of G geenrated by the set $\{\exp tX | X \in \Gamma, t \in \mathbb{R}_+\}$ is the whole G.*

In fact we can prove the following apparently more general result:

THEOREM 4. – *If a subset Γ of L satisfies the conditions D), E), F) and if Γ generates L as a Lie algebra, then the subsemigroup of G generated by the set $\{\exp tX | X \in \Gamma, t \in \mathbb{R}_+\}$ is the whole G.*

Clearly Theorem 4 implies Theorem 1 if we take $\Gamma = \{A, B, -B\}$.

Proof of Theorem 4 *and* 2 *using Theorem* 3. – For Theorem 4: let S be the closure of the semigroup generated by the set $\{\exp t X, \exp t B, \exp - t B | X \in \Gamma, t \in \mathbb{R}_+\}$. Its wedge $W(S)$ satisfies the assumptions of Theorem 3.

For Theorem 2: let S be the closure of the semigroup generated by the set $\{\exp t(A + u B) | t \in \mathbb{R}_+, u \in \mathbb{R}\}$. Its wedge $W(S)$ satisfies all the assumptions of Theorem 3, the only point that may not be clear is that $B \in E(S)$, the edge of $W(S)$. But by property A), the limits $\lim_{u \to \pm\infty} \frac{A + u B}{|u|}$ belong to $W(S)$. But these limits are B and $-B$.

To prove Theorem 3, we shall show that $\Gamma = L$. Theorem 3 follows then immediately.

2. PREPARATIONS FOR THE PROOF OF THEOREM 3

In this section we collect, for the benefit of the reader a number of well known facts which we shall use in the proof.

Let L be a semi-simple real finite dimensional Lie algebra, $L_{\mathbb{C}} = L \otimes_{\mathbb{R}} \mathbb{C}$ its complexification, $\sigma : L_{\mathbb{C}} \to L_{\mathbb{C}}$ the semilinear involution associated to L (conjugation). Let $\mathrm{Sim}(L)$ (resp. $\mathrm{Sim}(L_{\mathbb{C}})$) denote the set of all simple ideals in L (resp. $L_{\mathbb{C}}$). Then we have the direct algebra decompositions:

$$L = \oplus \{\Sigma | \Sigma \in \mathrm{Sim}(L)\} \qquad \text{and} \qquad L_{\mathbb{C}} = \oplus\{S | S \in \mathrm{Sim}(L_{\mathbb{C}})\}.$$

σ permutes the elements of $\mathrm{Sim}(L_{\mathbb{C}})$. The connection between $\mathrm{Sim}(L)$ and $\mathrm{Sim}(L_{\mathbb{C}})$ is as follows:

(1) $\mathrm{Sim}(L) = \{(S + \sigma S) \cap L | S \in \mathrm{Sim}(L_{\mathbb{C}})\}$.

(2) If $\Sigma \in \mathrm{Sim}(L)$ and $\Sigma_{\mathbb{C}}$ denotes its complexification then either $\Sigma_{\mathbb{C}}$ is a simple ideal in $L_{\mathbb{C}}$ (inner case) or $\Sigma_{\mathbb{C}} = S_1 \oplus S_2$, $S_i \in \mathrm{Sim}(L_{\mathbb{C}})$, $i = 1, 2$ (outer case). In the outer case σ induces a real Lie algebra isomorphism $S_1 \to S_2 \cdot \Sigma$ can be identified with the graph of σ in $S_1 \oplus S_2$ ($\Sigma = \{(x, \sigma(x)) | x \in S_1\}$). In fact, Σ is isomorphic to S_1 as a real Lie algebra.

Now let $B \in L$ be a strongly regular element in L. The set of all these elements is an open dense semi-algebraic subset in L. $\mathrm{Ker}\, \mathrm{ad}_{\mathbb{C}} B$ is a Cartan subalgebra of $L_{\mathbb{C}}$.

The Cartan algebra $L_0 = \mathrm{Ker}\, \mathrm{ad}_{\mathbb{C}} B$ of $L_{\mathbb{C}}$ splits: $L_0 = \oplus \{L_0 \cap S | S \in \mathrm{Sim}(L_{\mathbb{C}})\}$. Each $L_0 \cap S$ is a Cartan algebra of S. The root system R of $L_{\mathbb{C}}$

in the complex dual space L_0^* of L_0 is the union of the root systems R_S, $S \in \mathrm{Sim}\,(L_{\not{c}})$, $(L_0 \cap S)^*$ being identified canonically to a subspace of L_0^*.

Since B is strongly regular the mapping $R \to \mathrm{Sp}\,(B)$, $\alpha \to \alpha\,(B)$ is a bijection and the root space L_α associated with $\alpha \in R$ coincides with the $\alpha\,(B)$-eigenspace $L_{\alpha\,(B)}$ of $\mathrm{ad}_{\not{c}}\, B$. Hence, from now on, we shall write L_α and $L\,(\alpha)$ in stead of $L_{\alpha\,(B)}$ and $L\,(\alpha\,(B))$. σ operates on R as follows: $\sigma\,(\alpha) = * \circ \alpha \circ \sigma$ where $* : \not{c} \to \not{c}$ is the conjugation, that is $\sigma\,(\alpha)\,(X) = \alpha\,(\sigma\,(X))^*$, for $X \in L_{\not{c}}$.

Order structure on R defined by B. – We endow $R \cup \{0\}$ with the total order structure pull back of the order structure on $\mathrm{Sp}\,(B) \cup \{0\}$ by the bijection: $\alpha \in R \cup \{0\} \to \alpha\,(B) \in \mathrm{Sp}\,(B) \cup \{0\}$.

Notation. – We set $\mathrm{Re}\,\alpha = (\alpha + \sigma\,(\alpha))/2$, $\mathrm{Im}\,\alpha = \sqrt{-1}\,(\sigma\,(\alpha) - \alpha)/2$. These are linear forms in L_0^*.

Maximal, minimal roots. – A root α is maximal (resp. minimal) if $\alpha\,(B)$ is maximal (resp. minimal) in the sense of definition 1. This is equivalent to the more classical definition: α is maximal (resp. minimal) if $\alpha + \beta \notin R$ whenever $\beta \in R$ and $\beta > 0$ (resp. $\beta < 0$).

Now we state a lemma collecting some very well known facts we shall need all the time.

LEMMA 1. – 1) *R is stable under σ and under the map $\alpha \to -\alpha$.*

$$L_{\not{c}} = L_0 \oplus \bigoplus \{L_\alpha | \alpha \in R\},\ L_0 = \mathrm{Ker\,ad}_{\not{c}}\, B.$$

$$L = L\,(0) \oplus \bigoplus\{L\,(\alpha) | \alpha \in R,\ \mathrm{Im}\,\alpha\,(B) \geq 0\},\ L\,(0) = \mathrm{Ker\,ad}\, B.$$

For each $S \in \mathrm{Sim}\,(L_{\not{c}})$, $S = L_0 \cap S \oplus \bigoplus \{L_\alpha | \alpha \in R_S\}$.

For each

$\Sigma \in \mathrm{Sim}\,(L)$, $\Sigma = L\,(0) \cap \Sigma \oplus \bigoplus\{L\,(\alpha) | \alpha \in R\,\Sigma_{\not{c}},\ \mathrm{Im}\,\alpha\,(B) \geq 0\}$.

2) *For* $\alpha \in R$, $\mathrm{Re}\,\alpha\,(B) = 0$ *(resp.* $\mathrm{Im}\,\alpha\,(B) = 0$*) if and only if* $\mathrm{Re}\,\alpha = 0$ *(resp.* $\mathrm{Im}\,\alpha = 0$*) (as linear forms on* L_0*)* $\cdot$ *α and $\sigma\,(\alpha)$ have the same sign if* $\alpha + \sigma\,(\alpha) \neq 0$.

3) *Each R_S contains one maximal root s and one minimal root $-s$. For all* $\alpha \in R_S$, $\mathrm{Re}\,s\,(B) \geq \mathrm{Re}\,\alpha\,(B) \geq -\mathrm{Re}\,s\,(B)$.

4) $[L_\alpha,\ L_\beta]$

$$= \begin{cases} 0, & if\ \alpha + \beta \notin R \cup \{0\}; \\ \{L_{\alpha+\beta}\}, & if\ \alpha + \beta \in R; \\ a\ one\ dimensional\ subspace\ H_\alpha\ of\ L_0, & if\ \alpha + \beta = 0. \end{cases}$$

A reduced sum of roots is a root if and only if all the roots belong to the same R_S.

5) *If* $\alpha, \beta \in R$, $\alpha + k\beta \in R$ *if and only if* k *is an integer and* $-p(\alpha, \beta) \leq k \leq q(\alpha, \beta)$, $p(\alpha, \beta)$, $q(\alpha, \beta)$ *non negative integers.*

6) $\sigma(L_\alpha) = L_{\sigma(\alpha)}$ *for all* $\alpha \in R$ *and* $\dim L_\alpha = 1$. $L(\alpha) = (L_\alpha + L_{\sigma(\alpha)}) \cap L$. $\dim L(\alpha) = 1$ *if* $\sigma(\alpha) = \alpha$, 2 *if* $\sigma(\alpha) \neq \alpha$.

7) *If* $X \in L$ *and:* $X = X_0 + \Sigma\{X_\alpha | \alpha \in R\}$,

$$X = X(0) + \Sigma\{X(\alpha) | \alpha \in R, \operatorname{Im}\alpha(B) \geq 0\},$$

are the decompositions of X along the root space then: $X(0) = X_0$ *and:*

$$X(\alpha) = \begin{cases} X_\alpha + X_{\sigma(\alpha)} = X_\alpha + \sigma X_\alpha & \text{if } \alpha \in R,\ \sigma(\alpha) \neq \alpha, \\ X_\alpha & \text{if } \alpha \in R,\ \sigma(\alpha) = \alpha. \end{cases}$$

Also, $X(\alpha) = X(\sigma(\alpha))$ *for all* $\alpha \in R$.

Before the last statement of Lemma 1, we introduce a useful convention.

Convention. – If α is a linear form on L_0 and $\alpha \notin R \cup \{0\}$, $L(\alpha)$ will be understood to be $\{0\}$. Similar convention for $X(\alpha) : X(\alpha) = 0$ if $\alpha \notin R \cup \{0\}$.

8) For $\alpha, \beta \in R$:

$$[L(\alpha), L(\beta)] = \begin{cases} L(\alpha+\beta) + L(\alpha+\sigma(\beta)) & \text{if } \alpha \neq \sigma(\alpha) \text{ and } \beta \neq \sigma(\beta), \\ L(\alpha+\beta) & \text{otherwise.} \end{cases}$$

The next proposition comes from Joseph [11]. (*See* also [3]). Let S be a simple component of $L_{\not{t}}$, s (resp. $-s$) its maximal (resp. minimal) root.

DEFINITION 3. – Let us denote by R'_S the set of roots $\alpha \in R_S$ such that $\alpha + s$ or α–s is a root. R''_S will denote the complement $R_S \backslash (R'_S \cup \{s, -s\})$.

PROPOSITION 0. – 1) *If* $\alpha, \beta \in R'_S$ *have the same sign and if* $\alpha + \beta \in R_S$, *then* $\alpha + \beta \in \{s, -s\}$.

2) *If* $\alpha \in R'_S$, $\beta \in R''_S$ *and* $\alpha + \beta \in R_S$, *then* $\alpha + \beta \in R'_S$ *and* α, $\alpha + \beta$ *have the same sign.*

3) *If* $\alpha, \beta \in R''_S$ *and* $\alpha + \beta \in R_S$, *then* $\alpha + \beta \in R''_S$.

COROLLARY 0. – 1) *If* $\alpha, \beta \in R'_S$ *have the same sign then for all* $\gamma \in R''_S$ *such that* $\alpha + \beta + \gamma \in R_S$ *and either* $\alpha + \gamma$ *or* $\beta + \gamma$ *is a root then* $\alpha + \beta + \gamma \in \{s, -s\}$.

2) *If* $\alpha \in R'_S$, $\beta, \gamma \in R''_S$, *if* $\alpha + \beta + \gamma \in R_S$ *and one at least of the three linear forms* $\alpha + \beta$, $\beta + \gamma$, $\alpha + \gamma$ *is a root, then* $\alpha + \beta + \gamma \in R'_S$ *and* α, $\alpha + \beta + \gamma$ *have the same sign.*

Proof of corollary 0. – 1) Since α, β play a symmetric role we can assume that $\alpha+\gamma$ is a root by Proposition 0.2 $\alpha+\gamma \in R'_S$ and α, $\alpha+\gamma$ have the same sign. Then by proposition 0.1 $\alpha+\beta+\gamma \in \{s, -s\}$.

2) β and γ play a symmetric role. Hence we have to consider the cases $\alpha+\beta \in R_S$ and $\beta+\gamma \in R_S$ only. If $\alpha+\beta \in R_S$, by Proposition 0.2, $\alpha+\beta \in R'_S$ and α, $\alpha+\beta$ have the same sign. Applying again Proposition 0.2, we get that $\alpha+\beta+\gamma \in R'_S$ and α, $\alpha+\beta+\gamma$ have the same sign. If $\beta+\gamma \in R_S$, by Proposition 0.3 $\beta+\gamma \in R''_S$ and then by Proposition 0.2 $\alpha+\beta+\gamma \in R'_S$ and α, $\alpha+\beta+\gamma$ have the same sign.

Remark 2. – R'_S and R''_S are stable by the mapping $\alpha \to -\alpha$ but not by σ in general.

In the case of a simple Lie algebra, Joseph used these sets R'_S, (which correspond to Heisenberg subalgebras of *S*), to characterize the minimum orbit of the adjoint representation.

Now we state some lemmas about Γ which will be of great help in the proof of the theorem:

LEMMA 2. – *Under the assumptions A) to F) on* Γ:

1) *If* $X \in \Gamma$ *and* $Y \in E(\Gamma)$, $X-Y \in \Gamma$.

2) $E(\Gamma)$ *is a split Lie subalgebra of* L, i.e. *if* $X \in E(\Gamma)$, *then* $L(\alpha) \subset E(\Gamma)$ *for all* $\alpha \in R$ *such that* $X(\alpha) \neq 0$.

3) *Let* $r_m = \max\{\mathrm{Re}\, a | a \in \mathrm{Sp}(B)\} = \max\{\mathrm{Re}\,\alpha(B) | \alpha \in R\}$. *Then* $L(\alpha) \subset \Gamma$ *for all* $\alpha \in R$ *such that* $|\mathrm{Re}\,\alpha(B)| = r_m$ *and there exists an* $X \in \Gamma$ *with* $X(\alpha) \neq 0$. *In particular, by F), if* $\rho \in R$ *and* $\rho(B) = r_m$ *or* $-r_m$, $L(\rho) \subset \Gamma$.

4) L *is generated, as a Lie algebra, by the set* $\{X(\alpha) | X \in \Gamma, \alpha \in R\}$ *if* Γ *generates* L *as a Lie algebra.*

For the proof *see* the appendix.

LEMMA 3. – *Let* $B \in L$ *be strongly regular. Let* $\alpha \in R$, $X \in L(\alpha)$ *and* $Y \in L$. *For any finite set of roots* $\beta_1, \beta_2, \ldots, \beta_N$ *such that* $Y(\beta_i) \neq 0$ *for all* $1 \leq i \leq N$ *and* $\alpha+\beta_i \in R$, $1 \leq i \leq N$, *outside a discrete, possibly empty, subset of* $\mathbb{R}$:

$$[e^{t\,\mathrm{ad}\,B}(X), Y](\alpha+\beta_i) \neq 0,\ 1 \leq i \leq N. \text{ (Note that } e^{t\,\mathrm{ad}\,B}(X) \in L(\alpha).\text{)}$$

For the sake of completeness, we give the easy proof of this lemma in the appendix.

LEMMA 4. – *Under the assumptions A) to F) on* Γ, *for any* $X \in E(\Gamma)$ *and any* $Y \in \Gamma$, $L(\alpha) \subset \Gamma$ *for all* $\alpha \in R$ *such that* $[X, Y](\alpha) \neq 0$, *provided that* $\mathrm{ad}^2 X(Y) \in E(\Gamma)$.

Proof. – By property C) of Γ, $e^{t\,\mathrm{ad}\,X}(Y) \in \Gamma$ for all $t \in \mathbb{R}$. $e^{t\,\mathrm{ad}\,X}(Y) = \sum_{n \geq 0} \frac{t^n}{n!} \mathrm{ad}^n X(Y)$. Since X and $\mathrm{ad}^2 X(Y) \in E(\Gamma)$, $\mathrm{ad}^n X(Y) \in E(\Gamma)$ for all $n \geq 2$. By Lemma 2.1, $Y + t[X, Y] \in \Gamma$ and by property A) of Γ, $\lim_{t \to \pm\infty} \frac{Y + t[X, Y]}{|t|} \in \Gamma$. Then shows that $[X, Y] \in E(\Gamma)$. Then we apply Lemma 2.2.

In order to help the reader, let us explain the main ideas of the proof that will be given in Section 3, in the simple case. The semisimple case is a bit more complicated but the basic ideas are the same.

Observe, by Proposition 0, 1.2, that $L' = L(R'_S \cup \{\pm s\})$, the Lie algebra generated by $\{L_\alpha | \alpha \in R'_S \cup \{\pm s\}\}$, is "almost" an ideal.

We will consider I, the Lie algebra generated by elements X of L' such that $\mathbb{R}X \subset \Gamma$.

I is nonempty and we will show that it is an ideal of L, hence $\Gamma = L$.

To prove that I is an ideal we just check on the generators $X(\alpha)$ of I and $Y(\alpha)$ of L that $[X(\alpha), Y(\beta)] \in I$. This is mainly obtained on the basis of the properties of $R_{S'}$, $R_{S''}$ given by propositon 0 and corollary 0, by checking all cases. Some of these cases are very simple: $\alpha = s$, for instance; the most difficult case being: $\alpha \in R_{S'}$ and $\sigma(\alpha) \in R''_S$.

3. PROOF OF THEOREM 3

First we reduce the general case to the special one where the maximal ideal of L contained in Γ is zero: Let J be this maximal ideal. Since L is semi-simple we have a direct algebra decomposition $L = J \oplus K$, where K is a second ideal. We have $J \subset E(\Gamma)$ and we have a decomposition: $\Gamma = J \oplus \Gamma_0$ where $\Gamma_0 = \Gamma \cap K$, in an obvious sense. Clearly Γ_0 generates K as a Lie algebra since otherwise Γ could not generate L. Γ_0 satisfies all the conditions A) to F) if we take for B the component B_0 of B in Γ_0. Finally note that $E(\Gamma_0) = E(\Gamma) \cap K$. Substituting K for L and Γ_0 for Γ we can assume that the maximal ideal of L in Γ, is zero. To prove the theorem, it is enough to prove that Γ contains a nontrivial ideal, which will lead to a contradiction.

Let $r_m = \max\{\operatorname{Re} s(B) | s \in R,\ s \text{ maximal}\}$. By Lemma 1.3, $r_m \geq \operatorname{Re}\alpha(B)$ for all $\alpha \in R$.

Special case: $r_m = 0$. – Then $\operatorname{Re}\alpha = 0$ for all $\alpha \in R$. By Lemma 2, 3.4, $L = \Gamma$: a contradiction.

General case: $r_m > 0$. – Let S be a simple factor of $L_{\not{c}}$ such that $\operatorname{Re} s(B) = r_m$ for the unique maximal root s in R_S. Call I the subalgebra of the simple factor $\Sigma = L \cap (S + \sigma S)$ of L, generated by $L(s)$, $L(-s)$ and all the $L(\alpha)$ such that $\alpha \in R'_S$ and $L(\alpha) \subset \Gamma$. Clearly $I \subset \Gamma$ since $L(s)$, $L(-s)$ are contained in Γ by Lemma 2.3 [in fact, $L(s)$, $L(-s)$, $L(\alpha)$ are contained in $E(\Gamma)$].

Suppose that we can prove that I is an ideal. Since I is not the zero ideal we get a contradiction with the definition of Γ.

To prove that I is an ideal we shall prove first that:

LEMMA 5. – *$L(\alpha) \subset \Gamma$ if $\alpha \in R'_S$ and if there exists a $Y \in \Gamma$ such that $Y(\alpha) \neq 0$.*

To see this assume we can show that $L(\alpha+\varepsilon s) \subset \Gamma$, $\varepsilon \in \{\pm 1\}$ choosen so that $\alpha + \varepsilon s \in R$. Then $L(-\varepsilon s)$, $L(\alpha + \varepsilon s)$ are contained in $E(\Gamma)$. Since $L(\alpha) \subset [L(-\varepsilon s), L(\alpha+\varepsilon s)]$ by Lemma 1.8, $L(\alpha) \subset \Gamma$.

To prove that $L(\alpha+\varepsilon s) \subset \Gamma$ we use Lemma 4. Choose an $X \in L(\varepsilon s)$ so that $[X, Y](\alpha + \varepsilon s) \neq 0$. This is possible by Lemma 3. Then:

$$\operatorname{ad}^2 X(Y) \in \Sigma\{L(p\varepsilon s + q\varepsilon\sigma(s) + \beta) | \beta \in R_S \cup \{0\},\ p+q = 2,\ p,\ q \geq 0\}.$$

Now $|\operatorname{Re}(p\varepsilon s + q\varepsilon\sigma(s) + \beta)(B)| \geq (p+q-1) r_m \geq r_m$. Lemma 2.3 applied to $Z_t = e^{t \operatorname{ad} X}(Y) \in \Gamma$ and to the root $p\varepsilon s + q\varepsilon\sigma(s)+\beta$, shows that $L(p\varepsilon s + q\varepsilon\sigma(s)+\beta) \subset \Gamma$ for all β such that $\operatorname{ad}^2 X(Y)(p\varepsilon s + q\varepsilon\sigma(s) + \beta) \neq 0$ since $\dfrac{d^2}{(dt)^2} Z_t(p\varepsilon s + q\varepsilon\sigma(s) + \beta)_{|t=0} = \operatorname{ad}^2 X(Y)(p\varepsilon s + q\varepsilon\sigma(s) + \beta)$.

Now we shall prove that I is an ideal. For simplicity let us denote by $R(I)$ the set $\{s, -s\} \cup \{\alpha \in R'_S | L(\alpha) \subset \Gamma\}$ and by $R(\Gamma)$ the set of all $\beta \in R_S$ such that there exists a $Y \in \Gamma$, $Y(\beta) \neq 0$. Since I is generated by the set $\cup\{L(\alpha) | \alpha \in R(I)\}$ and Σ by the set $\{L(\beta) | \beta \in R(\Gamma)\}$, by Lemma 2.4, it is sufficient to show that $[L(\alpha), L(\beta)] \subset \Gamma$ for $\alpha \in R(I)$ and $\beta \in R(\Gamma)$. If $\beta \in R(\Gamma)$ and β or $\sigma(\beta)$ belongs to R'_S then $L(\beta) = L(\sigma(\beta)) \subset I$ by Lemma 5, and $[L(\alpha), L(\beta)] \subset I$. The remaining case is when $\beta \in R''(\Gamma) = \{\beta | \beta \in R(\Gamma),\ \beta \text{ and } \sigma(\beta) \in R''_S\}$. Since $[L(\alpha), L(\beta)] \subset L(\alpha+\beta) + L(\alpha+\sigma(\beta))$ it is sufficient to prove that $L(\alpha+\beta) \subset \Gamma$ and $L(\alpha+\sigma(\beta)) \subset \Gamma$. This we shall do in several steps.

1) If α or $\sigma(\alpha) \in \{s, -s\}$, then neither $\alpha + \beta$ nor $\alpha + \sigma(\beta)$ is a root or is zero by definition of R''_S. Hence $L(\alpha + \beta) = L(\alpha + \sigma(\beta)) = 0$.

2) Now let $\alpha \in R'_S$ and $\sigma(\alpha) \in R'_S \cup R''_S$. We shall apply Lemma 4. Choose a Y such that $Y(\beta) \neq 0$. By Lemma 5, $L(\gamma) \subset E(\Gamma)$ if $\gamma \in \{s, -s\} \cup R'_S$ and $Y(\gamma) \neq 0$. Using Lemma 2.1, we can assume that $Y(\gamma) = 0$ for $\gamma \in \{s, -s\} \cup R'_S$. Now, by Lemma 3, we can choose an X such that $[X, Y](\alpha + \beta) \neq 0$ (resp. $[X, Y](\alpha + \sigma(\beta)) \neq 0$) if $\alpha + \beta \in R'_S$ (resp. $\alpha + \sigma(\beta) \in R'_S$).

To apply Lemma 4, we have to show that $\mathrm{ad}^2 X(Y) \in E(\Gamma)$.

$$\mathrm{ad}^2 X(Y) = \mathrm{ad}^2 X(Y(0)) + \Sigma\{\mathrm{ad}^2 X(Y(\gamma)) | \gamma,\ \sigma(\gamma) \in R''_S,\ \mathrm{Im}\,\gamma(B) \geq 0\},$$

$$\mathrm{ad}^2 X(Y(0)) \subset [L(\alpha), L(\alpha)] \subset E(\Gamma) \text{ since } L(\alpha) \subset \Gamma.$$

$$\mathrm{ad}^2 X(Y(\gamma)) \in \begin{cases} L(2\alpha + \gamma) + L(2\alpha + \sigma(\gamma)) + L(\alpha + \sigma(\alpha) + \gamma) \\ \quad \text{if } \alpha \neq \sigma(\alpha) \text{ and } \gamma \neq \sigma(\gamma); \\ L(2\alpha + \gamma) + L(\alpha + \sigma(\alpha) + \gamma) \\ \quad \text{if } \alpha \neq \sigma(\alpha) \text{ and } \gamma = \sigma(\gamma); \\ L(2\alpha + \gamma) \text{ if } \alpha = \sigma(\alpha). \end{cases}$$

In paragraphs 3-4-5-6, we shall assume that both γ and $\sigma(\gamma)$ belongs to R''_S.

3) Here we show that $L(2\alpha + \gamma)) \subset \Gamma$, $L(2\alpha + \sigma(\gamma)) \subset \Gamma$:

Since the role of γ and $\sigma(\gamma)$ is symmetric it is sufficient to prove that $L(2\alpha + \gamma) \subset \Gamma \cdot 2\alpha + \gamma \neq 0$ since 2α is not a root. If $L(2\alpha + \gamma) \neq \{0\}$, $2\alpha + \gamma \in R_S$ and by Lemma 1.5, $\alpha + \gamma \in R'_S$. Hence by Corollary 0.1, $2\alpha + \gamma \in \{s, -s\}$ and hence $L(2\alpha + \gamma) \subset I \subset E(\Gamma)$.

From these considerations it follows that $\mathrm{ad}^2 X(Y(\gamma)) \in E(\Gamma)$ if the component $Z = \mathrm{ad}^2 X(Y(\gamma))(\alpha + \sigma(\alpha) + \gamma)$ of $\mathrm{ad}^2 X(Y(\gamma))$ along $L(\alpha + \sigma(\alpha) + \gamma)$ is zero. Let us assume hence that $Z \neq 0$. Note that since $\mathrm{ad}^2 X(Y(\gamma)) \neq 0$, $\mathrm{ad}\, X(Y(\gamma)) \neq 0$ and one, at least, of $\alpha + \gamma$ and $\sigma(\alpha) + \gamma$ is a root. Neither can be zero: since $\alpha \in R'_S$, $\gamma \in R''_S$ and $R'_S \cap R''_S = \varnothing$, $\alpha + \gamma \neq 0$. If $\sigma(\alpha) + \gamma = 0$, then $\alpha = -\sigma(\gamma)$. Again, since $R'_S \cap R''_S = \varnothing$ this is impossible.

In the next steps we show that $Z \in E(\Gamma)$.

4) Since either $\alpha + \gamma \in R_S$ or $\sigma(\alpha) + \gamma \in R_S$, and since $L(\alpha + \sigma(\alpha) + \gamma) \neq 0$, $\alpha + \sigma(\alpha) + \gamma \in R_S$. In fact, the only other possibility would be $\alpha + \sigma(\alpha) + \gamma = 0$, but in this case, we have a contradiction: $\alpha + \sigma(\alpha) \in R'_S$ (resp. $\{s, -s\}$) if $\sigma(\alpha) \in R''_S$ (resp. R'_S)

by Proposition 0.2 (resp. Proposition 0.1). This contradicts the fact that $\alpha + \sigma(\alpha) = -\gamma \in R''_S$.

In Steps 5 and 6 we prove that $\mathrm{ad}^2 X(Y) \in E(\Gamma)$ if $\alpha \neq -\sigma(\alpha)$.

5) Let $\sigma(\alpha) \in R'_S$ and $\alpha + \sigma(\alpha) \neq 0$. $\alpha, \sigma(\alpha)$ have the same sign by Lemma 1.2. Applying Corollary 0.1 since we have seen that $\alpha + \sigma(\alpha) + \gamma \in R_S$ and either $\alpha + \gamma$ or $\sigma(\alpha) + \gamma$ belongs to R_S, we get $\alpha + \sigma(\alpha) + \gamma \in \{s, -s\}$. By Lemma 2.3, $L(\alpha + \sigma(\alpha) + \gamma) \subset E(\Gamma)$ and hence $Z \in E(\Gamma)$.

6) Let $\sigma(\alpha) \in R''_S$. Again Corollary 0.2 tells us that $\alpha + \sigma(\alpha) + \gamma \in R'_S$. Since for all $t \in \mathbb{R}$, $e^{t\,\mathrm{ad}\,X}(Y) \in \Gamma$, if we show that for some $t \in \mathbb{R}$, $e^{t\,\mathrm{ad}\,X}(Y)(\alpha+\sigma(\alpha)+\gamma) \neq 0$, then by Lemma 5, $L(\alpha+\sigma(\alpha)+\gamma) \subset E(\Gamma)$. But:

$$\frac{d^2}{(dt)^2}\left(e^{t\,\mathrm{ad}\,X}(Y)(\alpha + \sigma(\alpha) + \gamma)\right)_{|t=0} = Z \neq 0.$$

Thus we have proved that $Z \in E(\Gamma)$, if $\alpha \neq -\sigma(\alpha)$. This shows that $\mathrm{ad}^2 X(Y) \in E(\Gamma)$ in that case. Hence $L(\alpha + \beta) + L(\alpha + \sigma(\beta)) \subset E(\Gamma)$ for all β, such that $\beta, \sigma(\beta) \in R''_S$ and all $\alpha \in \{s, -s\} \cup R'_S$ such that $\alpha + \sigma(\alpha) \neq 0$. We shall deduce the case where $\alpha + \sigma(\alpha) = 0$ from this as follows:

7) Since $\alpha \in R'_S$, $\alpha + \varepsilon s \in R'_S$ for $\varepsilon = -\mathrm{sign}(\alpha)$ (*i.e.* $\varepsilon = -\mathrm{sign}(\alpha(B))$). Let $\hat{\alpha}$ denote the root $\alpha + \varepsilon s$, then $\hat{\alpha} \in R'_S$ and $\mathrm{Re}\,\hat{\alpha}(B) = \varepsilon r_m \neq 0$. So $\hat{\alpha} + \sigma(\hat{\alpha}) \neq 0$ by Lemma 1.2. Since $L(\alpha) \subset E(\Gamma)$ and $L(\varepsilon s) \subset E(\Gamma)$ by Lemma 2.3, $L(\hat{\alpha}) \subset [L(\varepsilon s), L(\alpha)] \subset E(\Gamma)$.

We claim that $\hat{\alpha} + \beta \in R_S$ (resp. $\hat{\alpha} + \sigma(\beta) \in R_S$): In fact by Proposition 0.2, if $\alpha + \beta \in R_S$ (resp. $\alpha + \sigma(\beta) \in R_S$), then $\alpha + \beta \in R'_S$ (resp. $\alpha + \sigma(\beta) \in R'_S$) and $\alpha, \alpha + \beta$ (resp. $\alpha, \alpha + \sigma(\beta)$) have the same sign $-\varepsilon$. This shows that $\hat{\alpha} + \beta = \alpha + \varepsilon s + \beta \in R_S$ (resp. $\hat{\alpha} + \sigma(\beta) = \alpha + \varepsilon s + \sigma(\beta) \in R_S$). By what has been proved in the case $\alpha + \sigma(\alpha) \neq 0$, $L(\hat{\alpha} + \beta) \subset E(\Gamma)$ and $L(\hat{\alpha} + \sigma(\beta)) \subset E(\Gamma)$. Finally by Lemma 2.2, $L(\alpha + \beta) \subset [L(-\varepsilon s), L(\hat{\alpha} + \beta)] \subset E(\Gamma)$, $L(\alpha + \sigma(\beta)) \subset [L(-\varepsilon s), L(\hat{\alpha} + \sigma(\beta))] \subset E(\Gamma)$.

APPENDIX

Proof of Lemma 2. – 1) Is trivial. 2) Follows from the fact that $E(\Gamma)$ contains the strongly regular element *B*.

3) The proof is given in [12]. For the sake of completeness, let us give a proof here. First note that since *B* is strongly regular there exists at most

one root ρ such that $\rho = \sigma(\rho)$ and $\rho(B) = \operatorname{Re}\rho(B) = r_m$. Take an $X \in \Gamma$ such that $X(\alpha) \neq 0$ for some $\alpha \in R$, $\operatorname{Re}\alpha(B) = r_m$. For $\alpha \neq \rho$, then $\alpha \neq \sigma(\alpha)$ and $\alpha(B) = r_m + \omega\sqrt{-1}$. If $\alpha = \rho$ we set $\omega = 0$. For $|\eta| \leq 1, T > 0$, the element:

$$X_T^\eta = 1/T \int_0^T e^{t\,\mathrm{ad}\,B}(X)\, e^{-t\,r_m}\,(1 + \eta\cos(\omega\, t))\, dt \text{ belongs to } \Gamma.$$

Hence by property A) $\lim_{T\to\infty} X_T^\eta \in \Gamma$. But this limit is $X(\rho) + \eta/2\, X(\alpha)$, or $\eta/2\, X(\alpha)$ if ρ does not exist or $X(\rho) = 0$. Hence for all η, $|\eta| \leq 1$, $X(\rho) + \eta/2\, X(\alpha) \in \Gamma$ if ρ exists and $\eta/2\, X(\alpha) \in \Gamma$ if ρ does not exist or $X(\rho) = 0$.

In a similar manner we get that $X(-\rho) + \eta/2\, X(-\alpha) \in \Gamma$ for all η, $|\eta| \leq 1$ if ρ exists and $\eta/2\, X(-\alpha) \in \Gamma$ for all η, $|\eta| \leq 1$ if ρ does not exist or $X(-\rho) = 0$.

In particular for $\eta = 0$, we get that $X(\rho), X(-\rho) \in \Gamma$. Using the notations of condition F), we see that $X_+(\rho), X_-(-\rho)$ belong to Γ. (If ρ exists, of course). Suppose we can prove that the element $Z = X_+(\rho) + X_-(-\rho)$ of Γ is compact in the sense that the one-parameter group $\{e^{t\,Z} | t \in \mathbb{R}\}$ is relatively compact. Then this group is contained in the closure of the one-parameter semigroup $\{e^{t\,Z} | t \in \mathbb{R}_+\}$ which in turn is contained in the closed semigroup generated by Γ. This implies that $Z \in E(\Gamma)$. By Lemma 2.2, $X_+(\rho)$ and $X_-(-\rho)$ belong to $E(\Gamma)$.

By what has been proved above and by Lemma 2.1 we get that $X(\alpha) \in E(\Gamma)$ for any $\alpha \in R$ such that $|\operatorname{Re}\alpha(B)| = r_m$. If $\alpha = \sigma(\alpha)$ this implies that if $X(\alpha) \neq 0$, $L(\alpha) \subset E(\Gamma)$. If $\alpha \neq \sigma(\alpha)$, let $\alpha(B) = r_m + \omega\sqrt{-1}$, $\omega \neq 0$. By property B) of Γ, $[B, X(\alpha)] \subset E(\Gamma)$. Now $X(\alpha) = X_\alpha + \sigma(X_\alpha)$, $X_\alpha \in L_\alpha$ and $\sigma(X_\alpha) \in L_{\sigma(\alpha)}$. Then $\mathrm{ad}\,B(X(\alpha)) = r_m X(\alpha) + \omega\sqrt{-1}(X_\alpha - \sigma(X_\alpha))$. Hence $X(\alpha), \sqrt{-1}(X_\alpha - \sigma(X_\alpha)) \in E(\Gamma)$. But $(X(\alpha), \sqrt{-1}(X_\alpha - \sigma(X_\alpha))$ form a basis of $L(\alpha)$. This shows that $L(\alpha) \subset E(\Gamma)$. To end the proof of 3) we have to prove that Z is compact:

Since the projection $G \to \mathrm{Ad}\,G$ is a finite covering map, to show that $Z \in L$ is compact, it is sufficient to prove that it is compact in Ad G. Let us recall some facts: let $\tau : L_{\mathbb{C}} \to L_{\mathbb{C}}$ be the unique Weyl anti-involution commuting with σ. Then: (i) $\tau(L_\alpha) = L_{-\alpha}$ for all $\alpha \in R$,

(ii) the hermitian form: $Z \in L_{\mathbb{C}} \to \mathrm{Kil}(Z, \tau(Z))$ is negative definite,

(iii) if $Z \in L_{\mathbb{C}}$ and $\tau(Z) = Z$, Z is compact in $\mathrm{Ad}\,G_{\mathbb{C}}$.

Take any $X \in L(\rho) - \{0\} \subset L_\rho - \{0\}$, any $Y \in L(-\rho) - \{0\} \subset L_{-\rho} - \{0\}$ such that Kil $(X, Y) < 0\,.\,\tau(X) \in L_{-\rho}$. So, $\tau(X) = z\,Y$ where

$z \in \mathbb{C} - \{0\}$. Since $\tau\sigma = \sigma\tau$, $\tau(X) = \tau\sigma(X) = \sigma\tau(X) = z^* Y$. So $z^* = z$ and z is real. Also, by (ii) above, $0 > \mathrm{Kil}(X, \tau(X)) = z \,\mathrm{Kil}(X, Y)$. Hence, $z > 0$. If $z = 1$, $\tau(X+Y) = X + Y$ and so $X + Y$ is compact. If $z \neq 1$, let $\zeta = -1/2 \log z$. If $H = [X, Y]$, then $[H, X] = hX$, $[H, Y] = -hY$ where $h \in \mathbb{R} - \{0\}$. Let $Z_1 = e^{(\zeta/h)\,\mathrm{ad}\,H}(X + Y)$. Then it is easy to check that $\tau(Z_1) = Z_1$. Hence Z_1 is compact. Since $X + Y$ is conjugate to Z_1, it is also compact in Ad G.

4) Let L' be the Lie algebra generated by the set $\{X(\alpha) | X \in \Gamma, \alpha \in R\}$. Since L is generated by Γ, it is a fortiori generated by the set $\{X(\alpha) | X \in \Gamma, \alpha \in R \cup \{0\}\}$. $L' = L' \cap L(0) + \Sigma\{L(\alpha) | \alpha \in R, L(\alpha) \cap L' \neq \{0\}\}$. Then the Lie algebra generated by L' and the set $\{X(0) | X \in \Gamma\}$ is just $L' \oplus \Sigma\{\mathbb{R} X(0) | X \in \Gamma\}$. But this is L. Hence L' contains all the $L(\alpha)$, $\alpha \in R$. This implies that $L' = L$.

Proof of Lemma 3. – By Lemma 1.7 if $Z \in L$,

$$Z = Z_0 + \sum_{\gamma \in R} Z_\gamma,\ Z = Z(0) + \sum \{Z(\gamma) | \gamma \in R, \mathrm{Im}\,\gamma \geq 0\},$$

where $Z_0 = Z(0)$, $Z_\gamma \in L_\gamma$, $Z(\gamma) \in L(\gamma)$, and,

$$Z(\gamma) = \begin{cases} Z_\gamma + Z_{\sigma(\gamma)} = Z_\gamma + \sigma Z_\gamma, & \text{if } \gamma \neq \sigma(\gamma), \\ Z_\gamma, & \text{if } \gamma = \sigma(\gamma), \end{cases}$$

Hence $Z(\gamma) \neq 0$ is equivalent to $Z_\gamma \neq 0$.

Let $\hat{X} \in L(\alpha)$, $\hat{Y} \in L$. Then, $[\hat{X}, \hat{Y}](\alpha + \beta) \neq 0$ if and only if $[\hat{X}, \hat{Y}]_{\alpha+\beta} \neq 0$. By Lemma 1.7):

$$\hat{X}(\alpha) = \begin{cases} \hat{X}_\alpha & \text{if } \sigma(\alpha) = \alpha \\ \hat{X}_\alpha + \sigma \hat{X}_\alpha & \text{if } \sigma(\alpha) \neq \alpha \end{cases} \qquad \text{and} \qquad \hat{Y} = \hat{Y}_0 + \sum_{\gamma \in R} \hat{Y}_\gamma.$$

It is easy to see that:

$$\text{(I)} \qquad \begin{cases} [\hat{X}, \hat{Y}]_{\alpha+\beta} = [\hat{X}_\alpha, \hat{Y}_\beta] & \text{if } \sigma(\alpha) = \alpha, \\ [\hat{X}, \hat{Y}]_{\alpha+\beta} = [\hat{X}_\alpha, \hat{Y}_\beta] + [\sigma \hat{X}_\alpha, \hat{Y}_{\beta'}] & \text{if } \sigma(\alpha) \neq \alpha, \end{cases}$$

where $\beta' = \alpha - \sigma(\alpha) + \beta$.

If $\alpha = \sigma(\alpha)$, the assertion of the lemma follows immediately from the above formulas.

Now, if $\alpha \neq \sigma(\alpha)$, apply the formula (I) by taking $\hat{X} = e^{t\,\mathrm{ad}\,B}(X)$, $\hat{Y} = Y$ where $X \in L(\alpha)$, $Y \in L$. Since $e^{t\,\mathrm{ad}\,B}(X)_\alpha = e^{t\,a} X_\alpha$, $a = \alpha(B)$, we see that $[e^{t\,\mathrm{ad}\,B}(X), Y]_{\alpha+\beta} = e^{ta}[X_\alpha, Y_\beta] + e^{ta^*}[\sigma X_\alpha, Y_{\beta'}].[X_\alpha, Y_\beta]$

and $[\sigma X_\alpha, Y_{\beta'}]$ being both nonzero, there exists a $c \in ¢ - \{0\}$ such that $[\sigma X_\alpha, Y_{\beta'}] + c[X_\alpha, Y_\beta] = 0$. Then:

$$[e^{t\,\mathrm{ad}\,B}(X), Y]_{\alpha+\beta} = (e^{ta} - c\,e^{ta^*})\,[X_\alpha, Y_\beta].$$

If $|c| \neq 1$, $[e^{t\,\mathrm{ad}\,B}(X), Y]_{\alpha+\beta} \neq 0$ for all $t \in \mathbb{R}$.
If $|c| = 1$, $[e^{t\,\mathrm{ad}\,B}(X), Y]_{\alpha+\beta} = 0$ if and only if

$$t \in \left\{ \frac{\log c}{2\sqrt{-1}\,\mathrm{Im}\,\alpha(B)} + \frac{n\,\pi}{\mathrm{Im}\,\alpha(B)} \;\middle|\; n \in \mathbb{Z} \right\}.$$

REFERENCES

[1] B. Bonnard, V. Jurdjevic, I. Kupka and G. Sallet, Transitivity of families of invariant vector fields on the semi-direct products of Lie groups, *Trans. Amer. Math. Soc.*, 1981.

[2] N. Bourbaki, *Groupes et algèbres de Lie*, Fasc. XXXVIII, chap. 7-8, Hermann, Paris, 1975.

[3] R. El Assoudi, *Accessibilité par des champs de vecteurs invariants à droite sur un groupe de Lie*, Thèse de doctorat de l'Université Joseph Fourier, Grenoble, 1991.

[4] R. El Assoudi and J. P. Gauthier, Controllability of right invariant systems on real simple Lie groups of type F_4, G_2, B_n and C_n, *Math. on Control signals systems*, Vol. **1**, 1988, pp. 293-301.

[5] J. P. Gauthier and G. Bornard, Controllabilité des systèmes bilinéaires, *SIAM Journal on Control and Optimization,* Vol. **20**, (3), 1982, pp. 377-384.

[6] J. P. Gauthier, I. Kupka and G. Sallet, Controllability of right invariant systems on real simple Lie groups, *Systems and control Letters,* Vol. **5**, 1984, pp. 187-190.

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

[8] J. Hilgert, Max. semigroups and controllability in products of Lie Groups, *Archiv der Math.,* Vol. **49**, 1987, pp. 189-195.

[9] J. Hilgert, K. Hoffman and J. D. Lawson, Controllability of systems on a nilpotent Lie Group, *Beiträge Alg. Geom.,* Vol. **30**, 1985, pp. 185-190.

[10] J. Hilgert, K. Hoffman and J. D. LawsonAwson, Lie theory of semigroups, Technische Hochschule Darmstadt, *Preprint,* 1987.

[11] A. Joseph, The minimal orbit in a simple Lie algebra and its associated maximal ideal, *Ann. Sc. de l'École Normale Sup.,* 4e série, Vol. **9** (1), 1976, pp. 1-29.

[12] V. Jurdjevic and I. Kupka, Controllability of right invariant systems on semi-simple Lie-Groups and their homogeneous spaces, *Ann. Inst. Fourier,* Grenoble, Vol. **31** (4), 1981, pp. 151-179.

[13] M. Kuranishi, On everywhere dense imbedding of free groups in Lie groups, *Nagoya Math. Journal,* Vol. **2**, 1951, pp. 63-71.

[14] J. D. Lawson, Maximal subsemigroups of Lie Groups that are total, *Proc. of Edimborough Math. Soc.,* Vol. **30**, 1987, pp. 479-501.

[15] F. S. Leite, P. E. Crouch, Controllability on classical Lie Groups, *Math. on Control, signals, systems,* Vol. **1**, 1988, pp. 31-42.

[16] G. Warner, *Harmonic analysis on semi-simple Lie groups 1*, Springer-Verlag, Berlin, 1972.