N. Bergeron

GROUPES DE LIE ET GROUPES ALGÉBRIQUES

N. Bergeron

GROUPES DE LIE ET GROUPES ALGÉBRIQUES

N. Bergeron

Une grande partie de ces notes de cours sont des “copier-coller” des notes des cours des années précédentes par Patrick Polo. En plus des références mentionées dans le texte je me suis également servi de notes de cours de Frédéric Paulin et d’Yves Benoist.

TABLE DES MATIÈRES

CHAPITRE 1

MESURE DE HAAR

1.1. Groupes topologiques

Un **groupe topologique** est un groupe G muni d'une topologie telle que les deux applictions :

$$\begin{array}{rcl} G \times G & \to & G, \\ (g,h) & \mapsto & gh \end{array} \qquad \text{et} \qquad \begin{array}{rcl} G & \to & G, \\ g & \mapsto & g^{-1} \end{array}$$

soient continues. Ceci équivaut à la continuité de l'application $(g,h) \mapsto gh^{-1}$.

Dans ce cas tout sous-groupe de G muni de la topologie induite est un groupe topologique.

Exemple 1.1 **(Groupes discrets)**. — Tout groupe Γ, muni de la topologie discrète, est un groupe topologique. Par exemple, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, tout groupe fini, etc.

Exemple 1.2 **(Groupes additifs et multiplicatifs)**. — 1) $(\mathbb{R}, +)$ est un groupe topologique, puisque l'application $(x,y) \mapsto x - y$ est continue. De même, $(\mathbb{C}, +)$ est un groupe topologique, isomorphe à $(\mathbb{R}^2, +)$. Plus généralement, $(\mathbb{R}^n, +)$ est un groupe topologique.

2) $(\mathbb{R}^*, \times)$ est un groupe topologique, puisque l'application $(x,y) \mapsto xy^{-1}$ est continue. Il n'est pas connexe : $\mathbb{R}_+^*$ est un sous-groupe ouvert et fermé.

De même, $(\mathbb{C}^*, \times)$ est un groupe topologique. Le cercle $\mathbb{S}^1 = \{z \in \mathbb{C} \ : \ z\bar{z} = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$. On le note ausi $U(1)$. Comme espace topologique, il est compact. On a un isomorphisme de groupes topologiques $\mathbb{C}^* \cong \mathbb{S}^1 \times \mathbb{R}_+^*$.

Exemple 1.3 **(Groupes linéaires)**. — Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On munit $M_n(\mathbb{K}) \cong \mathbb{K}^{n^2}$ de la topologie usuelle. L'application $A \mapsto \det A$ est continue, puisque c'est un polynôme en les coefficients $a_{i,j}$ de A. Donc le groupe

$$GL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) \ : \ \det A \neq 0\}$$

est un ouvert de $M_n(\mathbb{K})$. L'application $(A, B) \mapsto AB$ est continue, puisque chaque coefficient

$$(AB)_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}$$

est une fonction continue (un polynôme quadratique) en les coefficients de A et B. Soit $C(A)$ la matrice des cofacteurs de A, c'est-à-dire $C(A)_{i,j}$ est le déterminant de la matrice de taille $n-1$ obtenue à partir de A en supprimant la i-ème ligne et la j-ème colonne; c'est un polynôme homogène de degré $n-1$ en les coefficients de A. D'après la formule

$$A^{-1} = \frac{1}{\det A}\, {}^t C(A),$$

où ^{t} désigne la transposée, on voit que $A \mapsto A^{-1}$ est une application continue. Donc $GL_n(\mathbb{K})$ est un groupe topologique. Le groupe

$$SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) \ : \ \det A = 1\}$$

est un sous-groupe fermé. Ni $GL_n(\mathbb{K})$ ni $SL_n(\mathbb{K})$ ne sont compacts, car $SL_n(\mathbb{K})$ contient, par exemple, les matrices $I + xE_{i,j}$, pour $i < j$ et $x \in \mathbb{K}$ arbitraire, donc les fonctions continues $A \mapsto A_{i,j}$ ne sont pas bornées sur $SL_n(\mathbb{K})$.

***Exemple 1.4* (Groupes classiques)**. — Ce sont les groupes orthogonaux, unitaires ou symplectiques, c'est-à-dire les sous-groupes de $GL_n(\mathbb{K})$ qui préservent une forme bilinéaire symétrique, une forme hermitienne, ou une forme bilinéaire antisymétrique (forme alternée). En particulier, on a les deux exemples suivants.

1) On munit $\mathbb{R}^n$ du produit scalaire usuel :

$$\langle x, y\rangle = \sum_i x_i y_i \quad \text{et} \quad ||x|| = \sqrt{\langle x, x\rangle} = \sqrt{\sum_i x_i^2}.$$

Alors, on définit le groupe orthogonal

$$\begin{aligned} O(n) &= \{A \in GL_n(\mathbb{R}) \ : \ \langle Ax, Ay\rangle = \langle x, y\rangle, \quad \forall x, y \in \mathbb{R}^n\} \\ &= \{A \in GL_n(\mathbb{R}) \ : \ {}^t A A = I\} \\ &= \{A = (a_{i,j}) \in M_n(\mathbb{R}) \ : \ \sum_{k=1}^{n} a_{k,i} a_{k,j} = \delta_{i,j}, \quad \forall i, j\}. \end{aligned}$$

Alors, $O(n)$ est un sous-groupe fermé de $GL_n(\mathbb{R})$ et aussi un sous-espace fermé de $M_n(\mathbb{R})$. De plus, $\sum_k a_{k,i}^2 = 1$ entraîne $|a_{k,i}| \leq 1$ pour tout k, i; donc $O(n)$ est un fermé borné de $M_n(\mathbb{R})$. Le groupe $O(n)$ est donc compact.

D'autre part, comme $\det({}^t A) = \det A$, pour tout $A \in O(n)$ on a $(\det A)^2 = 1$ d'où $\det A = \pm 1$. Ceci conduit à introduire le groupe spécial orthogonal

$$SO(n) = \{A \in O(n) \ : \ \det A = 1\}.$$

C'est un sous-groupe fermé de $O(n)$, il est donc également compact. Pour $n = 2$, on a

$$SO(2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a^2 + b^2 = 1 \right\} \cong \mathbb{S}^1.$$

2) On munit $\mathbb{C}^n$ du produit scalaire hermitien usuel :

$$\langle x, y \rangle = \sum_k x_k \overline{y_k} \quad \text{et} \quad ||x|| = \sqrt{\langle x, x \rangle} = \sqrt{\sum_k |x_k|^2}.$$

Alors, on définit le groupe unitaire

$$\begin{aligned} U(n) &= \{A \in GL_n(\mathbb{C}) \ : \ \langle Ax, Ay \rangle = \langle x, y \rangle, \quad \forall x, y \in \mathbb{C}^n\} \\ &= \{A \in GL_n(\mathbb{C}) \ : \ {}^t A \overline{A} = I\} \\ &= \{A = (a_{i,j}) \in M_n(\mathbb{C}) \ : \ \sum_{k=1}^n a_{k,i} \overline{a_{k,j}} = \delta_{i,j}, \quad \forall i, j\}. \end{aligned}$$

Alors, $U(n)$ est un sous-groupe fermé de $GL_n(\mathbb{C})$ et aussi un sous-espace fermé de $M_n(\mathbb{C})$. De plus, $\sum_k |a_{k,i}|^2 = 1$ entraîne $|a_{k,i}| \leq 1$ pour tout k, i; donc $U(n)$ est un fermé borné de $M_n(\mathbb{C})$. Le groupe $U(n)$ est donc compact.

D'autre part, l'image de $U(n)$ par l'application continue det est un sous-groupe compact de $\mathbb{C}^*$, donc contenu dans $\mathbb{S}^1$. En fait, on peut voir que l'image est exactement $\mathbb{S}^1$. On introduit aussi le groupe spécial unitaire

$$SU(n) = \{A \in U(n) \ : \ \det A = 1\}.$$

C'est un sous-groupe fermé de $O(n)$, il est donc également compact. Pour $n = 1$, on a

$$U(1) = \{z \in \mathbb{C}^* \ : \ z\bar{z} = 1\} = \mathbb{S}^1.$$

***Exemple 1.5* (Groupes p-adiques).** — Soit $\mathbb{Z}_p$ l'anneau des entiers p-adiques. Alors $(\mathbb{Z}_p, +)$ et $(\mathbb{Z}_p^*, \times)$ sont des groupes topologiques compacts.

1.2. Composante connexe d'un groupe topologique

Soit G un groupe topologique. On note G^0 la **composante connexe** de l'élément neutre e, c'est-à-dire la plus grande partie connexe de G contenant e.

Lemme 1.6. — *Le sous-ensemble G^0 est fermé et distingué dans G.*

Si, de plus, e possède un voisinage connexe, alors G^0 est un sous-groupe ouvert et fermé.

Démonstration. — Le sous-ensemble G^0 est fermé, puisque c'est la composante connexe de e. Le produit $G^0 \times G^0$ est un ensemble connexe et son image par l'application continue $(x, y) \mapsto xy^{-1}$ est une partie connexe contenant e, donc contenue dans G^0. Ceci montre que G^0 est un sous-groupe.

De plus, G^0 est stable par toute application continue $f : G \to G$ telle que $f(e) = e$; en particulier par toutes les conjugaisons $x \mapsto gxg^{-1}$. Ainsi, G^0 est un sous-groupe fermé normal.

Supposons enfin que e admette un voisinage connexe V. Soit $g \in G^0$. Alors $G^0 \cup V$ est connexe, donc égal à G^0. Donc G^0 contient le voisinage gV de g. Ceci montre que G^0 est ouvert. □

Lemme 1.7. — *Soit G un groupe topologique. Tout sous-groupe ouvert H est aussi fermé.*

Démonstration. — Le groupe G est la réunion disjointe de classes g_iH et chacune est ouverte. Le complémentraire de H, étant la réunion des classes g_iH distinctes de H, est donc ouvert. Par conséquent H est fermé. □

On aura besoin plus loin de la proposition suivante.

Proposition 1.8. — *Supposons G connexe et soit V un voisinage arbitraire de e. Alors le sous-groupe engendré par V égale G.*

Démonstration. — Soit H le sous-groupe engendré par V et $W = V \cap V^{-1}$. Alors

$$H = \cup_{n \geq 1} W^n$$

est un sous-groupe de G, et il est ouvert. En effet, pour tout $x \in H$ il existe un entier n tel que $x \in W^n$ et alors xW est un voisinage de x contenu dans H.

Ainsi, H est un sous-groupe ouvert, donc aussi fermé. Comme G est connexe, il vient $H = G$. □

1.3. Mesures de Haar

1.3.1. Opérateurs de translation à gauche et à droite. — Soit G un groupe topologique compact que nous supposerons pour simplifier *métrisable*. Soit $\mathcal{C}(G)_{\mathbb{R}}$ l'espace de Banach des fonctions continues réelles sur G muni de la norme

$$||f|| := \sup_{g \in G} |f(g)|.$$

On écrit $f \geq 0$ si f est à valeurs dans $\mathbb{R}_+$. La loi de groupe fournit des opérateurs de translation à droite et à gauche sur $\mathcal{C}(G)_{\mathbb{R}}$:

$$T_a f(g) = f(ga) \quad \text{et} \quad \check{T}_a f(g) = f(a^{-1}g).$$

Ce sont des isométries :

$$||T_a f|| = ||\check{T}_a f|| = \sup_{g \in G} |f(g)| = ||f||.$$

À toute suite finie $A = (a_1, \dots, a_n)$ d'éléments de G, on peut associer les opérateurs "moyenne de translations" :

$$T_A = \frac{1}{n}\sum_{i=1}^{n} T_{a_i} \quad \text{et} \quad \check{T}_A = \frac{1}{n}\sum_{i=1}^{n} \check{T}_{a_i}.$$

Ces opérateurs commutent et sont de norme ≤ 1. Les familles $\{T_A\}_A$ et $\{\check{T}_A\}_A$ sont donc équicontinues. Pour toute $f \in \mathcal{C}(G)_{\mathbb{R}}$ et, par exemple pour les opérateurs de translation à droite, on a plus précisemment

$$\inf f \leq \inf T_A f \leq \sup T_A f \leq \sup f.$$

En posant $\operatorname{osc}(f) = \sup f - \inf f$, on a donc

$$\operatorname{osc}(T_A f) \leq \operatorname{osc}(f). \tag{1}$$

Lemme 1.9. — *Pour toute fonction $f \in \mathcal{C}(G)_{\mathbb{R}}$,*

$$\inf_A \operatorname{osc}(T_A f) = 0.$$

Démonstration. — La fonction f étant uniformément continue et bornée (le groupe G est compact), la famille $\{T_A f\}_A \subset \mathcal{C}(G)_{\mathbb{R}}$ est équicontinue et bornée. Le théorème d'Ascoli implique donc que son adhérence est compacte. Si $\operatorname{osc}(T_{A_n} f) \to \inf_A \operatorname{osc}(T_A f)$ pour $n \to +\infty$, on peut donc supposer, quitte à extraire une sous-suite, que $T_{A_n} f$ converge uniformément vers une ceraine fonction $\varphi \in \mathcal{C}(G)_{\mathbb{R}}$.

Pour toute famille finie B d'éléments de G,

$$\operatorname{osc}(T_B \varphi) = \lim \operatorname{osc}(T_B T_{A_n} f) = \lim \operatorname{osc}(T_{BA_n} f) \geq \inf_A \operatorname{osc}(T_A f) = \operatorname{osc}(\varphi),$$

avec

$$BA_n = \{ba \ : \ b \in B \text{ et } a \in A_n\}.$$

Il découle donc de (1) que

$$\operatorname{osc}(T_B \varphi) = \operatorname{osc}(\varphi).$$

En particulier, $\sup T_B \varphi = \sup \varphi$, et si $T_B \varphi$ atteint son maximum en $g \in G$, φ l'atteint en tout point de gB. Pour une suite $(b_i)_{i \geq 1}$ dense dans G, en prenant successivement $B = B_n = (b_1, \dots, b_n)$, on obtient des g_n tels que $\varphi = \sup \varphi$ sur $g_n B_n$.

En prenant une sous-suite convergente $g_{n_k} \to g$, on voit que $\varphi = \sup \varphi$ sur l'ensemble dense des gb_i. Donc φ est constante, et $\inf_A \operatorname{osc}(T_A f) = \operatorname{osc}(\varphi) = 0$. □

1.3.2. Intégration invariante et mesures de Radon. — On veut définir une théorie de l'intégration sur G qui soit invariante par translation à gauche ou à droite (en fait, on aura les deux simultanément, ce qui est une particularité du cas compact). Pour toute fonction $f \in \mathcal{C}(G)_{\mathbb{R}}$ on voudrait donc pouvoir définir une intégrale

$$\mu(f) = \int_G f(g) dg$$

de sorte que, pour tout $h \in G$, on ait

$$\int_G f(hg)dg = \int_G f(g)dg.$$

L'existence d'une telle intégrale pour tout groupe topologique G localement compact a été démontrée en 1933 par Alfred Haar; on parle donc d'intégrale (ou de mesure) de Haar. L'année suivante a paru un article dans lequel John Von Neumann obtient l'existence *et l'unicité* (à un facteur près) pour les groupes compacts (métrisables) [(1)], et c'est sa très belle démonstration que nous reproduisons ici en suivant l'exposé qu'en fait Bruno Sévennec dans [**12**]. Commençons par rappeler la notion de mesure de Radon positive sur un groupe topologique G localement compact, qui permet d'avoir une bonne théorie de l'intégration.

Notons $\mathcal{C}_c(G)_{\mathbb{R}}$ l'espace des fonctions continues à support compact sur G que l'on munit de la norme infini. Soit $\nu : \mathcal{C}_c(G)_{\mathbb{R}} \to \mathbb{R}$ une forme linéaire. On dit que ν est **positive** si $\nu(f) \geq 0$ pour tout $f \geq 0$.

Lemme 1.10. — *Supposons G compact. Soit $\nu : \mathcal{C}(G)_{\mathbb{R}} \to \mathbb{R}$ une forme linéaire positive. Alors, pour toute $f \in \mathcal{C}(G)_{\mathbb{R}}$, on a*

$$|\nu(f)| \leq \nu(|f|) \leq \nu(1_G)||f||,$$

(où 1_G est la fonction de valeur constante égale à 1). Donc ν est continue.

Démonstration. — On a $\nu(f) = \pm|\nu(f)|$, posons alors $u = \pm f$. La fonction $u \in \mathcal{C}(G)_{\mathbb{R}}$ et l'on a $|\nu(f)| = \nu(u)$. De plus, on a

$$u \leq |f| \leq ||f|| \cdot 1_G,$$

d'où

$$|\nu(f)| = \nu(u) \leq \nu(|f|) \leq \nu(1_G)||f||.$$

□

Une **mesure de Radon** sur G est une forme linéaire continue $\nu : \mathcal{C}_c(G)_{\mathbb{R}} \to \mathbb{R}$. D'après le lemme précédent, lorsque G est compact toute forme linéaire positive est continue, donc est une mesure de Radon positive. Dans la suite *toute les mesures seront des mesures de Radon positives.*

Remarque 1.11. — Se donner une mesure de Radon positive sur G permet d'avoir une bonne théorie de l'intégration sur G. De façon plus précise, on a une correspondance bijective entre mesures de Radon positives et mesures boreliennes positives régulières et finies sur les compacts, voir par exemple [**10**, Chap. 2].

---

(1) Il faut attendre 1936 pour qu'il obtienne (en même temps qu'André Weil) l'unicité en général.

Une mesure ν sur un groupe topologique localement compact G est dite **invariante à gauche** si

$$\int_G f(hg)d\nu(g) = \int_G f(g)d\nu(g)$$

pour tout $h \in G$ et toute fonction $f \in \mathcal{C}_c(G)_{\mathbb{R}}$.

Théorème 1.12. — *Étant donné un groupe G localement compact, il existe une mesure invariante à gauche non nulle. Elle est unique à un facteur strictement positif près.*

Une telle mesure s'appelle **mesure de Haar** à gauche. Nous admettons le théorème 1.12 en général. Nous montrons néanmoins l'unicité dans le cas général puis l'existence lorsque G est compact.

Si G est compact, la mesure de Haar μ est dite **normalisée** si

$$\int_G d\mu(g) = 1.$$

1.3.3. Fonction module et unicité de la mesure de Haar. — Supposons fixée une mesure de Haar à gauche μ sur G. Pour h fixé dans G, la forme linéaire

$$f \mapsto \int_G f(hgh^{-1})d\mu(g)$$

définit une mesure invariante à gauche. Il devrait donc exister un nombre réel positif $\Delta(h)$ tel que

$$\int_G f(hgh^{-1})d\mu(g) = \Delta(h)\int_G f(g)d\mu(g)$$

ou encore :

$$\int_G f(gh^{-1})d\mu(g) = \Delta(h)\int_G f(g)d\mu(g).$$

Cela découlera de l'unicité de la mesure de Haar mais nous ne pouvons pas encore l'utiliser. Fixons donc $f \in \mathcal{C}_c(G)_{\mathbb{R}}$ positive et telle que

$$\int_G f d\mu = 1.$$

Et posons :

$$\Delta(g) = \int_G f(xg^{-1})d\mu(x).$$

A priori la fonction $\Delta : G \to \mathbb{R}_+^*$ dépend de f.

Lemme 1.13. — *Soit ν une mesure de Haar à gauche sur G. Alors pour tout $h \in \mathcal{C}_c(G)_{\mathbb{R}}$, on a :*

$$\int_G h d\nu = \left(\int_G f d\nu\right) \times \int_G h(x^{-1})\Delta(x)^{-1}d\mu(x).$$

Démonstration. — On considère le groupe $G \times G$ muni de la mesure de Haar à gauche $\mu \otimes \nu$. Les transformations

$$S(x, y) = (x, xy) \quad \text{et} \quad T(x, y) = (yx, y)$$

préservent la mesure. La transformation

$$S^{-1}T : (x, y) \mapsto (yx, x^{-1})$$

préserve donc également la mesure $\mu \otimes \nu$. En particulier :

$$\begin{aligned}\left(\int_G f d\nu\right)\left(\int_G g d\mu\right) &= \int_{G\times G} f(yx)g(x^{-1})d\nu(x)d\mu(y) \\ &= \int_G \Delta(x^{-1})g(x^{-1})d\nu(x).\end{aligned}$$

Appliquée à la fonction $g(y) = h(y^{-1})\Delta(y)^{-1}$ cette dernière égalité implique :

$$\left(\int_G f d\nu\right)\left(\int_G g d\mu\right) = \int_G h d\nu.$$

□

Corollaire 1.14. — *On a :*

$$d\mu(xg) = \Delta(g)d\mu(x).$$

Démonstration. — La mesure $d\nu = d\mu(xg)$ est invariante à gauche et non nulle; c'est donc une mesure de Haar à gauche. On a :

$$\int_G f d\nu = \int_G f(x)d\mu(xg) = \int_G f(xg^{-1})d\mu(x) = \Delta(g).$$

Le lemme 1.13 implique donc :

$$\int_G h(x)d\mu(xg) = \Delta(g)\int_G h(x^{-1})\Delta(x)^{-1}d\mu(x).$$

Mais le lemme 1.13 pour $\nu = \mu$ implique finalement que

$$\int_G h(x^{-1})\Delta(x)^{-1}d\mu(x) = \int_G h d\mu.$$

On obtient donc, comme annoncé, que

$$\int_G h(x)d\mu(xg) = \Delta(g)\int_G h d\mu.$$

□

Il découle en particulier du corollaire ci-dessus que Δ ne dépend pas de f et est un morphisme multiplicatif :

Proposition 1.15. — *La fonction Δ est un morphisme continu*

$$\Delta : G \to \mathbb{R}_+^*$$

et vérifie que pour tout $h \in \mathcal{C}_c(G)_\mathbb{R}$, on a :

$$\int_G h(xg^{-1})d\mu(x) = \Delta(g)\int_G h(x)d\mu(x).$$

Démonstration. — Il ne reste plus qu'à montrer que Δ est continue. Mais

$$\Delta(h) = \int_G f(gh^{-1})d\mu(g)$$

et f est uniformément continue à gauche. Le résultat est donc immédiat. $\square$

La fonction Δ s'appelle le **module** du groupe G. Si $\Delta \equiv 1$, le groupe G est dit **unimodulaire**. Un groupe commutatif est unimodulaire.

Proposition 1.16. — *Un groupe compact est unimodulaire. Un groupe discret est unimodulaire.*

Démonstration. — 1) Si G est compact, alors $\Delta(G)$ est un sous-groupe compact du groupe $\mathbb{R}_+^*$, et $\{1\}$ est le seul sous-groupe compact de $\mathbb{R}_+^*$.

2) Si G est discret, alors une fonction continue de support compact est une fonction de support fini. La mesure μ définie sur G par

$$\int_G f(g)d\mu(g) = \sum_{g\in G} f(g)$$

est invariante à gauche et à droite. $\square$

On peut maintenant démontrer l'unicité de la mesure de Haar :

Proposition 1.17. — *Soit ν une mesure de Haar à gauche sur G. Alors il existe une constante $c > 0$ telle que $\nu = c\mu$.*

Démonstration. — Étant donné deux fonctions $f, h \in \mathcal{C}_c(G)_\mathbb{R}$, il découle du lemme 1.13, d'une part que

$$(\int_G f d\mu) \times (\int_G h d\nu) = \left(\int_G f d\nu\right) \times \int_G h(x^{-1})\Delta(x)^{-1}d\mu(x)$$

puis (en prenant $\mu = \nu$ dans le lemme 1.13) que

$$\int_G h(x^{-1})\Delta(x)^{-1}d\mu(x) = \int_G h d\mu.$$

On en déduit que

$$(\int_G f d\mu) \times (\int_G h d\nu) = \left(\int_G f d\nu\right) \times \left(\int_G h d\mu\right).$$

On choisit alors h positive et non nulle de sorte que :

$$\int_G f d\nu = \left(\frac{\int_G h d\nu}{\int_G h d\mu}\right) \int_G f d\mu.$$

quelque soit f. □

Remarquons pour finir que l'on passe facilement de l'étude des mesures de Haar à gauche à celle des mesures de Haar à droite :

Proposition 1.18. — *La mesure $\Delta(g^{-1})d\mu(g)$ est une mesure de Haar à droite. De plus, pour $f : G \to \mathbb{R}$ continue et à support compact,*

$$\int_G f(g^{-1})d\mu(g) = \int_G f(g)\Delta(g^{-1})d\mu(g).$$

Démonstration. — Il découle du lemme 1.13 que pour toute fonction $f \in \mathcal{C}_c(G)_{\mathbb{R}}$, on a :

$$\int_G f(g^{-1})\Delta(g^{-1})d\mu(g) = \int_G f(g)d\mu(g).$$

En appliquant cette relation à la fonction $f_1(g) = f(g)\Delta(g^{-1})$ on obtient la proposition. □

Sur un groupe unimodulaire, et donc en particulier sur un groupe compact, une mesure de Haar à gauche est donc également une mesure de Haar à droite.

1.3.4. Exemples. —

1.3.4.1. $\mathbb{R}^{\mathbf{n}}$. — Une mesure de Lebesgue sur $\mathbb{R}^n$ est une mesure de Haar (à droite et à gauche) sur le groupe additif $(\mathbb{R}^n, +)$.

1.3.4.2. Le groupe affine. — Il s'identifie au sous-groupe de $GL_2(\mathbb{R})$ des matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \quad a, b \in \mathbb{R}, \quad a \neq 0.$$

Il est homéomorphe à l'ouvert de $\mathbb{R}^2$

$$\{(a,b) \in \mathbb{R}^2 \;:\; a \neq 0\} = \mathbb{R}^* \times \mathbb{R}.$$

Étant donnés deux éléments $h = (a, b)$ et $g = (u, v)$ dans G, la multiplication à gauche (resp. à droite) de g par h est donnée par

$$hg = (au, av + b) \qquad (\text{resp.} \quad gh = (au, bu + v)).$$

La mesure μ_g définie par

$$\int_G f(g)d\mu_g(g) = \int_{\mathbb{R}^* \times \mathbb{R}} f(a,b)\frac{dadb}{a^2}$$

est une mesure de Haar à gauche. La mesure μ_d définie par

$$\int_G f(g)d\mu_d(g) = \int_{\mathbb{R}^* \times \mathbb{R}} f(a,b)\frac{dadb}{|a|}$$

est une mesure de Haar à droite. La fonction module est donnée par

$$\Delta(g) = \frac{1}{|a|}.$$

1.3.4.3. Groupes linéaires. — Soit $G = GL_n(\mathbb{R})$. C'est par définition l'ouvert de $M_n(\mathbb{R})$ des matrices inversibles. Si $c_1, \ldots, c_n$ sont les vecteurs colonnes d'une matrice $x \in M_n(\mathbb{R})$, alors pour $g \in G$, $gx = (gc_1, \ldots, gc_n)$ et donc la mesure

$$|\det x|^{-n} \prod_{i,j=1}^{n} dx_{i,j}$$

sur G est invariante à gauche. De même, en considérant les lignes au lieu des colonnes, on vérifie qu'elle est également invariante à droite. Le groupe $GL_n(\mathbb{R})$ est unimodulaire.

1.3.4.4. Groupes triangulaires stricts. — Soit $G = T_0(n, \mathbb{R})$ le groupe triangulaire strict. Il s'identifie à $\mathbb{R}^{\frac{n(n-1)}{2}}$ et la mesure

$$\prod_{i<j} dx_{i,j}$$

est une mesure de Haar à gauche et à droite. Le groupe G est unimodulaire.

1.3.4.5. Groupes triangulaires. — Soit $G = T(n, \mathbb{R})$ le groupe triangulaire. Il s'identifie à

$$(\mathbb{R}^*)^n \times \mathbb{R}^{\frac{n(n-1)}{2}} \subset \mathbb{R}^{\frac{n(n+1)}{2}}.$$

Dans ces coordonnées, la mesure μ_g définie par

$$\prod_{i=1}^{n} |x_{i,i}|^{i-n-1} dx_{i,i} \prod_{i<j} dx_{i,j}$$

est une mesure de Haar à gauche, et la mesure μ_d définie par

$$\prod_{i=1}^{n} |x_{i,i}|^{i} dx_{i,i} \prod_{i<j} dx_{i,j}$$

est une mesure de Haar à droite. La fonction module est donnée par

$$\Delta(x) = \prod_{i=1}^{n} |x_{i,i}|^{2i-n-1}.$$

1.3.5. Mesure de Haar sur un groupe compact. — Supposons maintenant G compact. On voudrait pouvoir définir la mesure de Haar μ à l'aide du lemme 1.9 en posant $\mu(f) = \int_G f d\mu = c$ dès que la constante c est limite d'une suite $T_{A_n} f$. Von Neumann appelle alors c une **moyenne à droite** de f. *A priori* elle n'est pas unique. L'astuce est de moyenner aussi à gauche, c'est-à-dire de considérer les opérateurs $\check{T}_A$.

Lemme 1.19. — *Si* $T_{A_n} f \to c$ *et* $\check{T}_{A'_n} f \to c'$ *avec* c *et* c' *deux constantes arbitraires, alors* $c = c'$*. Autrement dit, toute moyenne à gauche coïncide avec toute moyenne à droite.*

Démonstration. — Les T_A commutent aux $\check{T}_B$, fixent les constantes et sont équicontinus (de norme ≤ 1). On a donc

$$c = \lim \check{T}_{A'_n} T_{A_n} f = \lim T_{A_n} \check{T}_{A'_n} f = c'.$$

□

Remarque 1.20. — Notons $\mu(f)$ la valeur commune des moyennes à droite et à gauche de f. Par le même argument de commutation, on obtient aussi

$$\mu(T_A f) = \mu(f) = \mu(\check{T}_B f).$$

Théorème 1.21. — *Soit* G *un groupe compact (métrisable). Il existe une unique mesure de Haar à gauche* μ *normalisée sur* G*. De plus* μ *est invariante à droite et invariante par inversion :*

$$\int_G f(g) d\mu(g) = \int_G f(g^{-1}) d\mu(g).$$

Démonstration. — L'unicité vient de ce que $\lambda(f) = \lim \lambda(T_{A_n} f) = \mu(f)$ pour toute forme linéaire candidate λ.

Inversement, $f \mapsto \mu(f)$ définie une application continue $\mu : \mathcal{C}(G)_{\mathbb{R}} \to \mathbb{R}$. On a clairement $\mu(\alpha f) = \alpha \mu(f)$. Montrons que μ est également additive, à savoir que

$$\mu(f + f') = \mu(f) + \mu(f').$$

Si $\mu(f) = \lim T_{A_n} f$, on a pour tout n

$$\mu(T_{A_n} f') = \mu(f')$$

d'où pour des A'_n convenables

$$\mu(f') = \lim T_{A'_n} T_{A_n} f'.$$

Comme $\mu(f) = \lim T_{A'_n} T_{A_n} f$ est aussi vérifiée, on peut écrire

$$\mu(f) + \mu(f') = \lim T_{A'_n A_n} (f + f') = \mu(f + f').$$

La positivité de μ est immédiate. Le reste provient de l'unimodularité du groupe (compact) G. □

1.3.6. Espaces homogènes de groupes compacts. — Si $H \subset G$ est un sous-groupe fermé du groupe compact G, le quotient $X = G/H$ est naturellement un espace compact sur lequel G agit continûment et transitivement.

Théorème 1.22. — *Il existe sur X une unique mesure de probabilité invariante par G. Elle est obtenue en projetant sur X la mesure de Haar normalisée de G.*

Démonstration. — Il suffit de prouver l'unicité. Elle suit le même schéma que la preuve d'unicité des moyennes à gauche et à droite sur un groupe compact, à ceci près qu'on ne peut translater ici que d'un côté, le rôle des moyennes de l'autre côté étant tenu par la moyenne invariante à gauche ν donnée.

Plus précisément, si $f \in \mathcal{C}(X)_{\mathbb{R}}$ l'ensemble des moyennes de translatées $\{T_A f\}_A$ est relativement compact dans $\mathcal{C}(X)_{\mathbb{R}}$, et on montre plus haut (lemme 1.9) que $\inf_A \operatorname{osc}(T_A f) = 0$. Il suffit alors de remarquer que toute limite constante $c = \lim T_{A_n} f$ coïncide avec $\nu(f)$ pour toute mesure de probabilité invariante ν sur X. □

En particulier la mesure de Lebesgue sur la sphère $\mathbb{S}^n = SO(n+1)/SO(n)$ est l'unique mesure de probabilité invariante par le groupe des rotations $SO(n+1)$.

1.4. Algébrisation des groupes compacts

Dans cette section nous donnons une application intéressante de l'existence d'une mesure de Haar sur un groupe compact.

1.4.1. Topologie de Zariski et groupes algébriques. — Soit k un corps, $V = k^n$ et $k[V]$ l'anneau des polynômes sur V. Pour toute partie F de V et tout idéal I de $k[V]$, on note

$$I(F) := \{P \in k[V] \ : \ \forall v \in F, \quad P(v) = 0\},$$

$$Z(I) := \{v \in V \ : \ \forall P \in I, \quad P(v) = 0\}.$$

L'ensemble F est un **fermé de Zariski** si F est l'ensemble des zéros d'une famille de polynômes, c'est-à-dire s'il existe un idéal I de $k[V]$ tel que $F = Z(I)$. Ces fermés définissent une topologie sur V appelée **topologie de Zariski**. L'ensemble $\overline{F} := Z(I(F))$ est l'**adhérence de Zariski** de F, c'est le plus petit fermé de Zariski contenant F. Une partie F' de F est dite **Zariski dense** dans F si $\overline{F'} = F$, c'est-à-dire si tout polynôme nul sur F' est nul sur F.

Remarquons que le groupe $SL(V) \subset \operatorname{End}(V) \cong k^{n^2}$ est un fermé de Zariski et que $GL(V)$ est un ouvert de Zariski.

Un sous-groupe G de $M_n(k)$ est dit **k-algébrique** si G est un fermé de Zariski. Par exemple, les groupes orthogonaux rencontrés au premier paragraphe sont tous algébriques.

1.4.2. Sous-groupes compacts de $\mathbf{GL_n}(\mathbb{R})$. —

Théorème 1.23. — *Soit G un sous-groupe compact de $GL_n(\mathbb{R})$; alors G est un groupe algébrique (réel).*

Démonstration. — (Voir Mneimné-Testard [**9**]) Considérons l'idéal I formé par les polynômes, à coefficients réels, en les n^2 indéterminées correspondant aux coefficients des matrices dans $M_n(\mathbb{R})$, qui s'annulent sur G. Il s'agit de montrer que si M est une matrice n'appartenant pas à G, il existe un polynôme Q dans I tel que $Q(M)$ soit non nul.

Puisque M n'appartient pas à G, les deux compacts G et $G \cdot M$ sont disjoints; soit K un compact de $M_n(\mathbb{R})$ contenant G et $G \cdot M$.

Le théorème de Tietze-Urysohm, appliqué au compact métrique K, implique qu'il existe une fonction f continue sur K, égale à 0 sur G et à 1 sur $G \cdot M$. Puisque K est compact, le théorème de Stone-Weierstrass implique par ailleurs de f est limite uniformes de polynômes en n^2 indéterminées.

Il existe donc un polynôme P sur $M_n(\mathbb{R})$ tel que

$$\forall g \in G, \quad |P(g)| < \frac{1}{2} \quad \text{et} \quad \forall x \in G \cdot M, \quad |P(x) - 1| < \frac{1}{2}.$$

Considérons le polynôme Q défini par

$$Q(x) = \int_G P(gx) dg,$$

où dg est la mesure de Haar normalisée sur G. Alors Q est clairement une fonction polynômiale, égale à $Q(e)$ (ici e désigne l'élément neutre de G) sur G et à $Q(M)$ sur $G \cdot M$, d'après l'invariance de la mesure de Haar. Or,

$$|Q(e)| = |\int_G P(g) dg| < \frac{1}{2} \quad \text{et} \quad |Q(M) - 1| < \frac{1}{2}.$$

De sorte que $Q(M) \neq Q(e)$, et le polynôme $P = Q - Q(e)$ est un élément de I non nul au point M. □

Remarque 1.24. — Ce théorème n'est valable ni sur le corps de base $\mathbb{C}$ ni sur $\mathbb{Q}_p$. Par exemple le groupe unitaire $U(n)$ est Zariski dense dans $GL_n(\mathbb{C})$ et $SL_n(\mathbb{Z}_p)$ est Zariski dense dans $SL_n(\mathbb{Q}_p)$.

CHAPITRE 2

GROUPES DE LIE

2.1. Sous-groupes fermés de $GL_n(\mathbb{R})$

Considérons la $\mathbb{R}$-algèbre de Lie $M_n(\mathbb{R})$ muni du crochet de Lie définit par le commutateur :

$$[A, B] = AB - BA.$$

Remarquons que l'on a évidemment

$$[A, A] = 0, \quad [B, A] = -[A, B]$$

et

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0. \tag{2}$$

Cette relation est l'**identité de Jacobi**.

Une **sous-algèbre de Lie** de $M_n(\mathbb{R})$ est un sous-espace vectoriel E qui est stable par le crochet, c'est-à-dire tel que $[X, Y] \in E$ pour tout $X, Y \in E$.

2.1.1. Application exponentielle. — On munit $\mathbb{R}^n$ de la norme euclidienne $||\cdot||$. On munit alors $M_n(\mathbb{R})$ de la norme correspondante, c'est-à-dire

$$||A|| = \sup_{x \neq 0} \frac{||Ax||}{||x||}.$$

Pour tout $A, B \in M_n(\mathbb{R})$ on a $||AB|| \leq ||A||||B||$. Par conséquent, pour tout $A \in M_n(\mathbb{R})$, la série

$$\sum_{k \geq 0} \frac{A^k}{k!}$$

est absolument convergente; on note $\exp(A)$ sa limite.

Proposition 2.1. — *L'application* $\exp : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ *est* C^∞.

Démonstration. — Soient $A, B \in M_n(\mathbb{R})$ et $\rho = \sup\{||A||, ||B||\}$. On montre par récurrence [1] que

$$||A^k - B^k|| \leq k\rho^{k-1}||A - B||. \tag{3}$$

Il en résulte

$$|| \exp(A) - \exp(B)|| \leq \exp(\rho)||A - B||.$$

Et donc exp est continue. En fait l'application exponentielle étant définie par une série entière de rayon de convergence infini, elle est C^∞ et sa différentielle est obtenue par dérivation terme à terme. [2] □

Si A et B commutent alors

$$\exp(A + B) = \exp(A) \exp(B).$$

En particulier, $\exp(A) \exp(-A) = \exp(0) = I$, ce qui montre que $\exp(A) \in GL_n(\mathbb{R})$ et $\exp(A)^{-1} = \exp(-A)$. Donc :

$$\forall k \in \mathbb{Z}, \quad \exp(A)^k = \exp(kA). \tag{4}$$

La différentielle de l'exponentielle en la matrice nulle est facile à déterminer : comme $\exp(A) = I+A+O(||A||^2)$, l'application linéaire $d_0 \exp$ est l'identité. Il résulte alors du théorème d'inversion locale que *l'exponentielle réalise un difféomorphisme d'un voisinage de* 0 *dans* $M_n(\mathbb{R})$ *sur un voisinage de* I *dans* $GL_n(\mathbb{R})$.

Notons $\mathcal{V}_0 = \{A \in M_n(\mathbb{R}) \ : \ ||A - I|| < 1\}$. Pour tout $A \in \mathcal{V}_0$, la série

$$\sum_{k\geq 0}(I - A)^k$$

converge absolument, et sa limite B vérifie $AB = I$, c'est-à-dire $B = A^{-1}$. Ceci montre que $\mathcal{V}_0 \subset GL_n(\mathbb{R})$.

Pour tout $A \in \mathcal{V}_0$, la série

$$\log(A) = \sum_{k\geq 1} \frac{(-1)^{k-1}}{k}(A - I)^k$$

converge absolument, et l'on peut facilement vérifier (voir [**6**, Lemme II.2.2]) :

$$\exp(\log(A)) = A. \tag{5}$$

---

[1] On peut remarquer que

$$\begin{aligned} A^k - B^k &= A^k - BA^{k-1} + BA^{k-1} - B^2A^{k-2} + \ldots + B^{k-1}A - B^k \\ &= (A - B)A^{k-1} + B(A - B)A^{k-2} + \ldots + B^{k-1}(A - B). \end{aligned}$$

[2] Attention : la différentielle de l'application polynomiale $A \mapsto A^k$ est l'application linéaire $M_n(\mathbb{R}) \to M_n(\mathbb{R})$, $B \mapsto A^{k-1}B + A^{k-2}BA + \ldots + ABA^{k-2} + BA^{k-1}$.

Théorème 2.2. — *1) L'application* $\log : \mathcal{V}_0 \to M_n(\mathbb{R})$ *est* C^∞*.*

2) Les applications exp *et* log *sont des difféomorphismes réciproques entre un voisinage ouvert de* 0 *dans* $M_n(\mathbb{R})$ *et un voisinage ouvert de* I *dans* $GL_n(\mathbb{R})$*.*

Démonstration. — 1) L'application $\log : \mathcal{V}_0 \to M_n(\mathbb{R})$ est C^∞. En effet : soient $g, h \in \mathcal{V}_0$; posons

$$\delta = \sup\{||g - I||, ||h - I||\} < 1.$$

Il résulte encore de (3) que

$$||\log(g) - \log(h)|| \leq \sum_{k\geq 1} \frac{1}{k}||(g-I)^k - (h-I)^k|| \leq \sum_{k\geq 1} \delta^{k-1}||g-h|| \leq \frac{||g-h||}{1-\delta}.$$

Ceci montre que log est uniformément continue sur la boule de centre I et de rayon δ. Comme somme d'une série entière on montre même que log est C^∞.

2) Posons

$$\mathcal{U}_0 = \{X \in M_n(\mathbb{R}) \ : \ ||X|| < \log 2\}.$$

Pour tout $X \in \mathcal{U}_0$, on a

$$||\exp(X) - I|| \leq \exp(||X||) - 1 < \exp(\log 2) - 1 = 1,$$

et $\exp(X) \in \mathcal{V}_0$. On peut alors facilement vérifier (voir encore [**6**, Lemme II.2.2]) :

$$\log(\exp(X)) = X, \quad \forall X \in \mathcal{U}_0. \tag{6}$$

Les applications exp et log sont donc des bijections réciproques entre $\mathcal{U}_0$ et $\exp(\mathcal{U}_0)$. Et puisque exp est C^∞, le 2) découle de 1). □

Proposition 2.3. — *Soient* $X, Y \in M_n(\mathbb{R})$ *et* $t \in \mathbb{R}$*. Pour* $t \to 0$*, on a :*

$$\exp(tX)\exp(tY) = \exp\left(t(X+Y) + \frac{t^2}{2}[X,Y] + O(t^3)\right) \tag{7}$$

et

$$\exp(tX)\exp(tY)\exp(-tX)\exp(-tY) = \exp\left(t^2[X,Y] + O(t^3)\right). \tag{8}$$

Démonstration. — Posons $F(t) = \exp(tX)\exp(tY)$. Alors

$$\begin{aligned} F(t) &= \left(I + tX + \frac{t^2}{2}X^2 + O(t^3)\right)\left(I + tY + \frac{t^2}{2}Y^2 + O(t^3)\right) \\ &= I + t(X+Y) + \frac{t^2}{2}(X^2 + 2XY + Y^2) + O(t^3). \end{aligned}$$

Pour t assez petit, on a $||F(t) - I|| < 1$ et

$$\begin{aligned} \log F(t) &= t(X+Y) + \frac{t^2}{2}(X^2 + 2XY + Y^2) - \frac{t^2}{2}(X+Y)^2 + O(t^3) \\ &= t(X+Y) + \frac{t^2}{2}[X,Y] + O(t^3). \end{aligned}$$

Ceci prouve (7). Posons $G(t) = F(t)F(-t)$. Alors,

$$G(t) = I - t^2(X+Y)^2 + t^2(X^2 + 2XY + Y^2) + O(t^3) = I + t^2[X,Y] + O(t^3),$$

d'où $\log G(t) = t^2[X,Y] + O(t^3)$, et (8) en découle. □

Corollaire 2.4. — *Soient $X, Y \in M_n(\mathbb{R})$ et $t \in \mathbb{R}$. Pour $k \in \mathbb{N}$, $k \to +\infty$, on a :*

$$\left(\exp(\frac{tX}{k})\exp(\frac{tY}{k})\right)^k = \exp\left(t(X+Y) + O(\frac{1}{k})\right) \to \exp(t(X+Y)) \tag{9}$$

et

$$\left(\exp(\frac{tX}{k})\exp(\frac{tY}{k})\exp(-\frac{tX}{k})\exp(-\frac{tY}{k})\right)^{k^2} = \exp\left(t^2[X,Y] + O(\frac{1}{k})\right) \to \exp(t^2[X,Y]). \tag{10}$$

2.1.2. L'algèbre de Lie d'un sous-groupe fermé de $GL_n(\mathbb{R})$. — Soit G un sous-groupe fermé de $GL_n(\mathbb{R})$. On lui associe le sous-ensemble de $M_n(\mathbb{R})$ suivant :

$$\mathfrak{g} = \{X \in M_n(\mathbb{R}) \ : \ \forall t \in \mathbb{R}, \quad \exp(tX) \in G\}.$$

Théorème 2.5. — *L'ensemble $\mathfrak{g}$ est une sous-algèbre de Lie de $M_n(\mathbb{R})$. On la notera* Lie(G).

Démonstration. — Commençons par montrer que $\mathfrak{g}$ est un sous-espace vectoriel de $M_n(\mathbb{R})$. Soient $X, Y \in \mathfrak{g}$. Il est clair que $sX \in \mathfrak{g}$ pour tout $s \in \mathbb{R}$, donc il suffit de montrer que $X + Y \in \mathfrak{g}$, c'est-à-dire que

$$\forall t \in \mathbb{R}, \quad \exp(t(X+Y)) \in G.$$

Fixons $t \in \mathbb{R}$ et soit $k \in \mathbb{N}$, $k > 0$. Comme $X, Y \in \mathfrak{g}$, alors $\exp(tX/k)$ et $\exp(tY/k)$ appartiennent à G, et comme G est un groupe, il contient aussi le produit

$$\left(\exp(\frac{tX}{k})\exp(\frac{tY}{k})\right)^k = \exp\left(t(X+Y) + O(\frac{1}{k})\right),$$

et comme G est fermé dans $GL_n(\mathbb{R})$ il contient aussi la limite $\exp(t(X+Y))$.

Montrons maintenant que $[X,Y] \in \mathfrak{g}$. Comme $\exp(-A) = \exp(A)^{-1}$, il suffit de montrer que

$$\exp\left(s[X,Y]\right) \in G \quad \text{pour tout } s \geq 0, \quad \text{disons } s = t^2.$$

Pour $t \in \mathbb{R}$ fixé et $k \in \mathbb{N}$, $k \to +\infty$, on a

$$\left(\exp(\frac{tX}{k})\exp(\frac{tY}{k})\exp(\frac{-tX}{k})\exp(\frac{-tY}{k})\right)^{k^2} \to \exp(t^2[X,Y]).$$

Comme $X, Y \in \mathfrak{g}$, alors G contient le terme de gauche pour tout k, et comme G est fermé il contient aussi la limite $\exp(t^2[X,Y])$. Ceci montre que $[X,Y] \in \mathfrak{g}$. □

On a ainsi associé à tout sous-groupe fermé $G \subset GL_n(\mathbb{R})$ une sous-algèbre de Lie $\mathrm{Lie}(G) \subset M_n(\mathbb{R})$. D'après la définition, le lemme suivant est immédiat.

Lemme 2.6. — *1) On a :* $\mathrm{Lie}(GL_n(\mathbb{R})) = M_n(\mathbb{R})$.
2) Si $H \subset G$, alors $\mathrm{Lie}(H) \subset \mathrm{Lie}(G)$.

On appelle **dimension** d'un sous-groupe fermé $G \subset GL_n(\mathbb{R})$ la dimension de son algèbre de Lie.

2.1.3. Sous-groupes fermés de $GL_n(\mathbb{R})$. — D'après le théorème 2.5, la restriction à $\mathfrak{g}$ de l'application exponentielle définit une application

$$\exp_G : \mathfrak{g} \to G.$$

Lemme 2.7. — *L'image de* $\exp_G$ *contient un voisinage de I dans G.*

Démonstration. — Soit $\mathfrak{m}$ un supplémentaire de $\mathfrak{g}$ dans $M_n(\mathbb{R})$ et considérons l'application

$$\phi : \mathfrak{g} \oplus \mathfrak{m} \to GL_n(\mathbb{R}), \quad (X, Y) \mapsto \exp(X)\exp(Y).$$

Elle est C^∞ et sa différentielle en $(0,0)$ est $\mathrm{id}_\mathfrak{g} \oplus \mathrm{id}_\mathfrak{m}$, qui est un isomorphisme. Donc d'après le théorème d'inversion local, il existe des voisinages ouverts U, V, resp. W, de 0 dans $\mathfrak{g}$, $\mathfrak{m}$, resp. de I dans $GL_n(\mathbb{R})$, tels que ϕ induise un difféomorphisme

$$\psi : U \times V \to W.$$

Supposons que le lemme soit faux. Il existe alors une suite $(g_k)_{k\geq 1}$ d'éléments de G qui converge vers I et telle que g_k n'appartient pas à $\exp_G(\mathfrak{g})$, pour tout k. Pour k assez grand, on peut écrire $g_k = \exp(X_k)\exp(Y_k)$ où $X_k \in \mathfrak{g}$ et $Y_k \in \mathfrak{m}$ tendent vers 0. Par hypothèse $Y_k \neq 0$ et quitte à remplacer g_k par $\exp(-X_k)g_k$ on peut supposer que $g_k = \exp(Y_k)$ appartient pour tout k.

Posons $B_k = \frac{Y_k}{||Y_k||}$; c'est un élément de la sphère unité $\mathbf{S}$ de $M_n(\mathbb{R})$, qui est compacte. Donc la suite $(B_k)_{k\geq 1}$ possède une valeur d'adhérence $B \in \mathbf{S}$.

Fait. On a : $B \in \mathbf{S} \cap \mathfrak{g}$.

Démonstration du fait. — Remplaçant $(B_k)_{k\geq 1}$ par une sous-suite, on peut supposer que

$$\lim_{k\to+\infty} B_k = B.$$

Fixons $t \in \mathbb{R}$ et posons $t_k = t/||Y_k||$. Alors $tB_k = t_kY_k$ et l'on a

$$\exp(tB) = \lim_{k\to+\infty} \exp(tB_k) = \lim_{k\to+\infty} \exp(t_kY_k).$$

Notons n_k la partie entière de t_k et $t'_k = t_k - n_k$. Pour tout k, on a

$$\exp(t_kY_k) = \exp(Y_k)^{n_k} \cdot \exp(t'_kY_k) = g_k^{n_k} \cdot \exp(t'_kY_k).$$

Comme $|t'_k| < 1$ et $Y_k \to 0$, alors $\exp(t'_k Y_k)$ converge vers I, et donc $\exp(tB)$ est la limite de la suite $(g_k^{n_k})$. Comme G est un sous-groupe fermé, cette limite appartient à G. On a donc

$$\exp(tB) \in G, \quad \forall t \in \mathbb{R}$$

soit $B \in \mathfrak{g}$. □

Mais B appartient également à $\mathfrak{m}$ qui est un supplémentaire de $\mathfrak{g}$ dans $M_n(\mathbb{R})$. C'est absurde. □

Il découle du lemme 2.7 que l'application $\exp_G$ munit un voisinage de l'identité dans G d'une structure de sous-variété de $GL_n(\mathbb{R})$. Comme $\exp(A) = I + A + O(||A||^2)$, l'espace tangent à G en I s'identifie à $\mathfrak{g}$.

Soit maintenant g un élément quelconque de G. L'application $A \mapsto g\exp(A)$ de $M_n(\mathbb{R})$ dans $GL_n(\mathbb{R})$ est C^∞ et induit donc un difféomorphisme d'un voisinage de 0 dans $M_n(\mathbb{R})$ vers un voisinage de g dans $GL_n(\mathbb{R})$. La restriction de cette application à $\mathfrak{g}$ munit un voisinage de g dans G d'une structure de sous-variété de $GL_n(\mathbb{R})$. On obtient donc le théorème suivant (dû à von Neumann) :

Théorème 2.8. — *Tout sous-groupe fermé de $GL_n(\mathbb{R})$ est une sous-variété de $GL_n(\mathbb{R})$.*

Proposition 2.9. — *Soient $H \subset G$ des sous-groupes fermés de $GL_n(\mathbb{R})$. Si G est connexe et si* $\mathrm{Lie}(H) = \mathrm{Lie}(G)$ *(c'est-à-dire si* $\dim H = \dim G$*), alors $H = G$.*

Démonstration. — D'après le lemme 2.7 le groupe H contient un voisinage de l'identité dans G. D'après la proposition 1.8 il contient donc G tout entier. □

2.1.4. Groupes classiques. — Soient n, p et q des entiers naturels. On note I_n la matrice identité $n \times n$, et

$$I_{p,q} = \begin{pmatrix} -I_p & 0 \\ 0 & I_q \end{pmatrix}, \quad J_n = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \quad \text{et} \quad K_{p,q} = \begin{pmatrix} -I_p & 0 & 0 & 0 \\ 0 & I_q & 0 & 0 \\ 0 & 0 & -I_p & 0 \\ 0 & 0 & 0 & I_q \end{pmatrix}.$$

On appelle **groupes classiques (réels)** les sous-groupes réels de la liste suivante; ce sont tous des sous-groupes fermés de $GL_m(\mathbb{C}) \subset GL_{2m}(\mathbb{R})$ pour un entier m convenable.

$$\begin{aligned}
SL_n(\mathbb{C}) &= \{x \in GL_n(\mathbb{C}) \ : \ \det x = 1\} \\
SL_n(\mathbb{R}) &= \{x \in GL_n(\mathbb{R}) \ : \ \det x = 1\} \\
O(n) &= \{x \in GL_n(\mathbb{R}) \ : \ {}^t x x = I_n\} \\
SO(n) &= O(n) \cap SL_n(\mathbb{R}) \\
O(p,q) &= \{x \in GL_{p+q}(\mathbb{R}) \ : \ {}^t x I_{p,q} x = I_{p,q}\} \\
SO(p,q) &= O(p,q) \cap SL_{p+q}(\mathbb{R}) \\
U(n) &= \{x \in GL_n(\mathbb{C}) \ : \ {}^t \overline{x} x = I_n\} \\
SU(n) &= U(n) \cap SL_n(\mathbb{C}) \\
U(p,q) &= \{x \in GL_{p+q}(\mathbb{C}) \ : \ {}^t \overline{x} I_{p,q} x = I_{p,q}\} \\
SU(p,q) &= U(p,q) \cap SL_{p+q}(\mathbb{C}) \\
Sp_{2n}(\mathbb{R}) &= \{x \in GL_{2n}(\mathbb{R}) \ : \ {}^t x J_n x = J_n\} \\
O_n(\mathbb{C}) &= \{x \in GL_n(\mathbb{C}) \ : \ {}^t x x = I_n\} \\
SO_n(\mathbb{C}) &= O_n(\mathbb{C}) \cap SL_n(\mathbb{C}) \\
Sp_{2n}(\mathbb{C}) &= \{x \in GL_{2n}(\mathbb{C}) \ : \ {}^t x J_n x = J_n\} \\
Sp(p,q) &= \{x \in Sp_{p+q}(\mathbb{C}) \ : \ {}^t \overline{x} K_{p,q} x = K_{p,q}\} \\
SL(n,\mathbb{H}) &= \{x \in SL_{2n}(\mathbb{C}) \ : \ J_n x = \overline{x} J_n\} \\
SO(n,\mathbb{H}) &= \{x \in SO_{2n}(\mathbb{C}) \ : \ {}^t \overline{x} J_n x = J_n\}.
\end{aligned}$$

2.2. Groupes de Lie

Un **groupe de Lie** est une variété G de classe C^∞, munie d'une structure de groupe telle que l'application

$$G \times G \to G, \quad (x,y) \mapsto xy^{-1}$$

soit de classe C^∞. Il revient au même de demander que les applications de composition $(x,y) \mapsto xy$ et d'inverse $x \mapsto x^{-1}$ soient de classes C^∞.

Tout groupe de Lie, quand on oublie son atlas maximal de cartes, est un groupe topologique.

Il découle facilement de la définition que, dans un groupe de Lie G, les translations à gauche

$$L_g : G \to G, \quad x \mapsto gx$$

et à droite

$$R_g : G \to G, \quad x \mapsto xg^{-1},$$

sont des difféomorphismes de classe C^∞.

Un **morphisme (de groupes de Lie réels)** entre deux groupes de Lie est un morphisme de groupes qui est de classe C^∞. Notons qu'un morphisme de groupes entre deux groupes de Lie est de classe C^∞ si et seulement s'il est C^∞ en e. Un **isomorphisme (de groupes de Lie réels)** est un isomorphisme de groupes qui est un difféomorphisme de classe C^∞. Deux groupes de Lie sont **isomorphes** s'il existe un isomorphisme de l'un sur l'autre.

Soit G un groupe de Lie. Un **sous-groupe de Lie** de G est une partie de G qui est à la fois un sous-groupe de G et une sous-variété de classe C^∞ de G. Comme les translations à gauche sont des difféomorphismes de classe C^∞, il suffit de vérifier que cette partie est un sous-groupe et une sous-variété de classe C^∞ au voisinage de l'élément neutre. Une sous-groupe de Lie est évidemment un groupe de Lie. Un **plongement (de groupes de Lie)** d'un groupe de Lie H dans un groupe de Lie G est un morphisme de groupes de H dans G qui est un plongement de variétés C^∞. L'image de H est alors un sous-groupe de Lie de G.

***Exemple 2.10* (Groupes discrets).** — Soit G un groupe. Muni de la topologie discrète, G est un groupe topologique, que l'on appelle **groupe discret**. Si G est dénombrable, alors le groupe G, muni de son atlas de cartes de variété de dimension 0 évident, est un groupe de Lie.

***Exemple 2.11* (Groupes additifs et multiplicatifs).** — Les groupes $(\mathbb{R},+)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C},+)$, $(\mathbb{C}^*,\times)$, munis de leur structure de variété analytique réelle, donc C^∞, évidente, sont des groupes de Lie.

***Exemple 2.12* (Groupes linéaires).** — Soit V un espace vectoriel (réel ou complexe) de dimension finie. Alors, le groupe

$$GL(V)$$

des automorphismes linéaires de V, muni de sa structure d'ouvert de l'espace vectoriel de dimension finie $\mathrm{End}(V)$ des applications linéaires de V dans lui-même, est un groupe de Lie.

Montrons, en effet, que la composition et l'inverse sont C^∞. La composition $(f,g)\mapsto f\circ g$ est la restriction à l'ouvert $GL(V)$ d'une application bilinéaire de $\mathrm{End}(V)$, donc C^∞. Si g est un élément de $GL(V)$, alors son inverse est l'unique application f vérifiant l'équation $g\circ f-\mathrm{id}=0$. Le théorème des fonctions implicites, appliqué à la fonction $F(g,f)=g\circ f-\mathrm{id}$, dont la différentielle partielle par rapport à la seconde variable en un point (g,f) est l'application linéaire inversible $Y\mapsto g\circ Y$ de $\mathrm{End}(V)$ dans lui-même, montre que l'inverse $g\mapsto g^{-1}$ est de classe C^∞.

L'espace tangent en tout point de $GL(V)$ est identifié à $\mathrm{End}(V)$.

L'application Φ qui à un automorphisme linéaire de $\mathbb{R}^n$ associe sa matrice dans la base canonique induit un isomorphisme du groupe $GL(\mathbb{R}^n)$ vers le groupe $GL_n(\mathbb{R})$. Ce dernier, en tant qu'ouvert de $M_n(\mathbb{R})\cong\mathbb{R}^{n^2}$, est naturellement une variété C^∞. La multiplication de deux matrices carrées est polynomiale en les coefficients et donc

C^∞. Par la formule

$$M^{-1} = \frac{1}{\det M} {}^t\text{Comatrice}(M),$$

l'inverse d'une matrice carrée inversible est rationnelle (de dénominateur ne s'annulant pas) en les coefficients, donc C^∞. On obtient donc une structure naturelle de groupe de Lie sur $GL_n(\mathbb{R})$. L'application Φ est naturellement un isomorphisme de groupes de Lie. Il en est de même pour $GL(\mathbb{C}^n)$ et $GL_n(\mathbb{C})$. Notons que $GL_n(\mathbb{R})$ est un sous-groupe de Lie de $GL_n(\mathbb{C})$.

Exemple 2.13 **(Quelques morphismes)**. — L'application exponentielle $x \mapsto e^x$ de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, \times)$ est un isomorphisme de groupes de Lie. L'application déterminant $x \mapsto \det x$ de $GL_n(\mathbb{R})$ dans $(\mathbb{R}^*, \times)$ est un morphisme de groupes de Lie. Pour tout g dans G, la **conjugaison** $i_g : G \to G$ définie par $x \mapsto gxg^{-1}$ est un isomorphisme de groupes de Lie.

2.2.1. Propriétés élémentaires. —

Proposition 2.14. —
1. *Un morphisme de groupes de Lie est une application de rang constant.*
2. *Un morphisme de groupes de Lie, qui est bijectif, est un isomorphisme de groupes de Lie.*

Démonstration. — Soit $f : G \to H$ un morphisme de groupes de Lie.

1) Pour tout g dans G on a

$$f \circ L_g = L_{f(g)} \circ f. \tag{11}$$

Puisque $f(e) = e$, le théorème de dérivation des applications composées montre que :

$$d_g f \circ d_e L_g = d_e L_{f(g)} \circ d_e f.$$

Les translations à gauche sont des C^∞-difféomorphismes, donc $d_e L_g$ et $d_e L_{f(g)}$ sont des isomorphismes linéaires. Par conséquent, $d_g f$ et $d_e f$ ont même rang.

2) Supposons f bijectif. D'après (11), il suffit de vérifier que f est un C^∞-difféomorphisme local en e. Mais d'après le théorème du rang constant et l'injectivité de f, sinon il existerait un voisinage V de e dans G tel que $f(V)$ serait d'intérieur vide dans H. Comme G est séparable (c'est une variété !), l'image $f(G)$ de f serait une union dénombrable de parties de H d'intérieur vide. Comme H est métrisable, le théorème de Baire contredirait alors la surjectivité de f. □

Toute variété est localement connexe (par arcs). Il découle donc du lemme 1.6 que G^0, la composante connexe de l'élément neutre dans un groupe de Lie G est ouverte.

Proposition 2.15. — *Tout sous-groupe de Lie d'un groupe de Lie est fermé.*

Démonstration. — Soit H un sous-groupe de Lie d'un groupe de Lie G. Comme sous-variété de G, le groupe H est localement fermé dans G. Il est donc ouvert dans son adhérence. Mais si $g \in \overline{H}$, alors gH est ouvert dans $\overline{H}$, car la multiplication par g est un homéomorphisme de $\overline{H}$ dans lui-même. Donc gH rencontre H, et g appartient à H. □

2.2.2. Algèbre de Lie d'un groupe de Lie. — Soit G un groupe de Lie et T_eG l'espace tangent à G en son élément neutre e. Le groupe G agit sur lui-même par conjugaison, car l'application

$$\mu : G \times G \to G, \quad (g, x) \mapsto gxg^{-1}$$

est C^∞. Pour tout $g \in G$, l'application μ_g correspondante est notée $\mathrm{Int}(g)$; c'est l'**automorphisme intérieur** de conjugaison par g. Alors e est un point fixe de cette action. Notons

$$\mathrm{Ad}g = d_e\mu_g : T_eG \to T_eG$$

la différentielle en e de μ_g. Puisque μ_g est un difféomorphisme, $\mathrm{Ad}g \in GL(T_eG)$. L'application $\mathrm{Ad} : G \to GL(T_eG)$, définie par $g \mapsto \mathrm{Ad}g$, est un morphisme de groupes de Lie : c'est clairement un morphisme de groupes et il est C^∞ par le théorème de dérivation des applications composées et le fait que μ soit C^∞. On appelle cette application la **représentation adjointe**.

Notons

$$\mathrm{ad} = d_e\mathrm{Ad} : T_eG \to \mathrm{End}(T_eG)$$

la différentielle de Ad. Pour tout $X, Y \in T_eG$ on pose alors

$$[X, Y] = \mathrm{ad}X(Y).$$

***Exemple 2.16* (Groupes linéaires).** — Soit $G = GL_n(\mathbb{R})$. Puisque G est un ouvert de $M_n(\mathbb{R})$, l'espace tangent à G en l'élément neutre I_n est $M_n(\mathbb{R})$. Comme $\mathrm{Int}(g) : G \to G$ est la restriction à l'ouvert G de $M_n(\mathbb{R})$ de l'application linéaire $X \mapsto gXg^{-1}$ de $M_n(\mathbb{R})$ dans elle-même, on a

$$\mathrm{Ad}g(X) = gXg^{-1}.$$

Enfin pour tous $X, Y \in M_n(\mathbb{R})$,

$$\mathrm{ad}X(Y) = ((d_e\mathrm{Ad})(X))(Y) = \frac{d}{dt}\Big|_{t=0} (\exp(tX)Y\exp(-tX)) = XY - YX.$$

Donc $\mathrm{ad}X(Y)$ est le crochet de Lie $[X, Y]$ des matrices X et Y, et les notations sont cohérentes.

Proposition 2.17. — *L'espace vectoriel T_eG, muni de l'application $(X, Y) \mapsto [X, Y]$ est une algèbre de Lie. De plus, pour tout g dans G, l'application $\mathrm{Ad}g : T_eG \to T_eG$ est un morphisme d'algèbre de Lie :*

$$\mathrm{Ad}g([X, Y]) = [\mathrm{Ad}g(X), \mathrm{Ad}g(Y)].$$

Cette algèbre de Lie est appelée l'**algèbre de Lie de groupe** G; elle est notée $\mathfrak{g}$. L'application

$$\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$$

est un morphisme d'algèbres de Lie, appelé la **représentation adjointe** de $\mathfrak{g}$.

Démonstration. — Soit (U, φ) une carte locale (de classe C^∞) de G au voisinage de l'élément neutre e et telle que $\varphi(e) = 0$. Cette carte fournit aussi une carte locale $(\pi^{-1}(U), d\varphi)$ pour le fibré tangent $\pi : TG \to G$. On note $\overline{x}$ l'image d'un point x de U par φ, ainsi que l'image d'un point x de $\pi^{-1}(U)$ par $d_{\pi(x)}\varphi$.

Le produit dans G est C^∞ et les applications

$$U \times U \to \mathbb{R}^n,\ (x, y) \mapsto \varphi(xy)$$

et

$$U \times U \to \mathbb{R}^n,\ (x, y) \mapsto \varphi(x) + \varphi(y)$$

coïncident et ont la même différentielle en (e, e). De sorte que l'application

$$\varphi(U) \times \varphi(U) \to \mathbb{R}^n$$

qui à $(\varphi(x), \varphi(y))$ associe $\varphi(xy) - \varphi(x) - \varphi(y)$ est de différentielle nulle. On en déduit que, pour tous x, y dans G proches de e,

$$\overline{xy} = \overline{x} + \overline{y} + B(\overline{x}, \overline{y}) + \varepsilon(\overline{x}, \overline{y}), \tag{12}$$

où B est une application bilinéaire, et, ici comme plus bas, l'application ε est une application de plusieurs variables réelles de classe C^∞, définie sur un voisinage de 0, dont chaque terme du développement limité en 0 contient une puissance d'ordre au moins 2 dans au moins l'une des variables.

En appliquant (12) avec $y = x^{-1}$, on obtient $0 = \overline{x} + \overline{x^{-1}} + B(\overline{x}, \overline{x^{-1}}) + \varepsilon(\overline{x}, \overline{x^{-1}})$. Donc

$$\overline{x^{-1}} = -\overline{x} + \varepsilon(\overline{x}).$$

Donc, pour tous g, x dans G proches de e,

$$\overline{gxg^{-1}} = \overline{(gx)g^{-1}} = \overline{x} + B(\overline{g}, \overline{x}) - B(\overline{x}, \overline{g}) + \varepsilon(\overline{x}, \overline{g}).$$

D'où, pour tout g dans G proche de e et tout X dans T_eG,

$$\overline{\mathrm{Ad}g(X)} = \overline{X} + B(\overline{g}, \overline{X}) - B(\overline{X}, \overline{g}) + \varepsilon(\overline{g}).$$

Par conséquent, pour tous X, Y dans T_eG,

$$\overline{\mathrm{ad}X(Y)} = B(\overline{X}, \overline{Y}) - B(\overline{Y}, \overline{X}). \tag{13}$$

L'anticommutativité de l'application $(X, Y) \mapsto \mathrm{ad}X(Y)$ s'en déduit immédiatement. Enfin il découle de sa définition que le produit $(X, Y) \mapsto B(X, Y)$ est associatif et la formule de Jacobi découle elle aussi de (13). $\square$

Proposition 2.18. — *Si G et G' sont des groupes de Lie, d'algèbres de Lie $\mathfrak{g}$ et $\mathfrak{g}'$, si $f : G \to G'$ est un morphisme de groupes de Lie, alors $d_e f : \mathfrak{g} \to \mathfrak{g}'$ est un morphisme d'algèbres de Lie.*

Démonstration. — Pour tout g dans G, puisque f est un morphisme,

$$f \circ \mu_g = \mu_{f(g)} \circ f.$$

Donc pour tout g dans G et tout X dans $\mathfrak{g}$, par le théorème de dérivation des applications composées,

$$d_e f \circ (\mathrm{Ad} g) = (\mathrm{Ad} f(g)) \circ d_e f$$

et

$$d_e f \circ (\mathrm{ad} X) = (\mathrm{ad} d_e f(X)) \circ d_e f.$$

D'où, pour tous X, Y dans $\mathfrak{g}$,

$$d_e f([X,Y]) = [d_e f(X), d_e f(Y)].$$

□

En particulier, l'espace tangent en l'élément neutre à un sous-groupe de Lie H d'un groupe de Lie G est une sous-algèbre de Lie de l'algèbre de Lie de G, qui s'identifie avec l'algèbre de Lie de H.

Notons que l'algèbre de Lie d'un produit de groupes de Lie s'identifie avec l'algèbre de Lie produit des algèbres de Lie de ces groupes de Lie.

Il découle aussi de la proposition 2.18 que si $f : G \to G'$ est un isomorphisme de groupes de Lie, alors $d_e f : \mathfrak{g} \to \mathfrak{g}'$ est un isomorphisme d'algèbres de Lie.

Proposition 2.19. — *Soit $f : G \to G'$ un morphisme de groupes de Lie. Alors* $\mathrm{Ker} f$ *est un sous-groupe de Lie (fermé) de G et l'on a*

$$\mathrm{Lie}(\mathrm{Ker} f) = \mathrm{Ker} d_e f.$$

Démonstration. — Le morphisme f étant de rang constant $r = \mathrm{rang}(d_e f)$, le sous-groupe $\mathrm{Ker} f = f^{-1}(e)$ est une sous-variété de dimension

$$d = \dim \mathrm{Lie}(G) - r = \dim \mathrm{Ker} d_e f.$$

C'est donc un sous-groupe de Lie de G. De plus, f étant identiquement égale à e sur $\mathrm{Ker} f$, on a

$$\mathrm{Lie}(\mathrm{Ker} f) \subset \mathrm{Ker} d_e f,$$

d'où l'égalité puisque ces deux espaces ont même dimension. □

Retour aux sous-groupes fermés de $GL_n(\mathbb{R})$. — D'après le théorème de Von Neuman, tout sous-groupe fermé G de $GL_n(\mathbb{R})$ est un groupe de Lie. Par ailleurs, pour tout

$$X \in \mathfrak{g} = \{X \in M_n(\mathbb{R}) \ : \ \forall t \in \mathbb{R}, \ \exp(tX) \in G\},$$

la courbe $f(t) = \exp(tX)$ est C^∞, à valeurs dans G, vérifie $f(0) = 1$ et

$$f'(0) = \lim_{t \to 0} \frac{\exp(tX) - I}{t} = X.$$

Donc $X \in T_e G = \mathrm{Lie}(G)$, et ceci montre que $\mathfrak{g} \subset \mathrm{Lie}(G)$. Comme

$$\dim \mathrm{Lie}(G) = \dim(G) = \dim \mathfrak{g},$$

on a en fait égalité $\mathfrak{g} = \mathrm{Lie}(G)$.

Corollaire 2.20. — *Tout sous-groupe fermé G de $GL_n(\mathbb{R})$ est un groupe de Lie et l'on a*

$$\mathrm{Lie}(G) = \{X \in M_n(\mathbb{R}) \ : \ \exp(tX) \in G, \quad \forall t \in \mathbb{R}\}.$$

Nous verrons plus loin une généralisation, à tout groupe de Lie, due à É. Cartan. Remarquons qu'en général un sous-groupe H d'un groupe de Lie G qui est un groupe de Lie n'est pas une sous-variété ! La condition d'être fermé est donc essentielle.

Exemple 2.21. — Soit $\alpha \in \mathbb{R}$ tel que $\alpha \notin 2\pi\mathbb{Q}$. Alors :

1) Le sous-groupe H de $\mathbb{S}^1$ engendré par $\exp(i\alpha)$ est isomorphe à $\mathbb{Z}$, mais c'est un sous-groupe dense de $\mathbb{S}^1$, donc ce n'est pas une sous-variété, et de plus la topologie induite par celle de $\mathbb{S}^1$ n'est pas la topologie discrète de $\mathbb{Z}$. En d'autres termes, le morphisme

$$\phi : \mathbb{Z} \to \mathbb{S}^1, \quad : n \mapsto \exp(ni\alpha)$$

est C^∞ (trivialement) et injectif mais son image n'est pas un sous-groupe de Lie. En fait ϕ n'est pas un homéomorphisme sur son image.

2) De même, le morphisme de groupes

$$\psi : \mathbb{R} \to \mathbb{S}^1 \times \mathbb{S}^1, \quad t \mapsto (\exp(it), \exp(it\alpha))$$

est C^∞ et injectif. Mais $\psi(\mathbb{R})$ est dense dans $\mathbb{S}^1 \times \mathbb{S}^1$, donc n'en est pas un sous-variété, et ψ n'est pas un homéomorphisme sur son image.

2.3. Exponentielle d'un groupe de Lie

Soit G un groupe de Lie, d'élément neutre e, et d'algèbre de Lie $\mathfrak{g}$.

Rappelons que la translation à gauche (resp. à droite) par un élément g de G est le C^∞-difféomorphisme $L_g : G \to G$ (resp. $R_g : G \to G$) défini par $L_g : x \mapsto gx$ (resp. $R_g : x \mapsto xg^{-1}$), et que les applications L_g et R_h commutent.

2.3.1. Champs de vecteurs invariants. —

2.3.1.1. Rappels sur les champs de vecteurs. — Un **champ de vecteur** C^∞ X sur G est la donnée, pour tout $g \in G$, d'un élément de T_gG noté X_g ou $X(g)$, de telle sorte que : pour tout $f \in C^\infty$, l'application

$$D_X(f) : g \mapsto d_g f(X_g) \text{ soit } C^\infty.$$

Dans ce cas, l'application $f \mapsto D_X(f)$ est une **dérivation** de $C^\infty(G)$, c'est-à-dire que $D_X : C^\infty(G) \to C^\infty(G)$ est une application linéaire telle que

$$D_X(fg) = D_X(f)g + fD_X(g), \quad \forall f, g \in C^\infty(G).$$

Maintenant, rappelons (voir [**13**]) que si D une dérivation de $C^\infty(G)$ et $f \in C^\infty(G)$, le germe en g de $D(f)$ ne dépend que de celui de f. L'application

$$D_g(f) = D(f)(g)$$

définit donc une dérivation ponctuelle de l'ensemble des germes de fonctions C^∞ en g. La variété G est localement difféomorphe à $\mathbb{R}^n$, l'espace tangent T_gG s'identifie donc naturellement à l'espace des dérivations ponctuelles des germes de fonctions C^∞ en g. Notons toujours D_g le vecteur de T_gG correspondant. Alors

$$X : g \mapsto X(g) = D_g$$

est un champs de vecteurs C^∞. Donc : *une dérivation de $C^\infty(G)$ est la même chose qu'un champ de vecteurs C^∞ sur G.* On notera plus simplement $X(f) = D_X(f)$.

Proposition 2.22. — *Soient X, Y deux champs de vecteurs C^∞, considérés comme des dérivations de $C^\infty(G)$. Alors,*

$$[X, Y] := X \circ Y - Y \circ X$$

est une dérivation, donc un champ de vecteurs, appelé le **crochet de Lie des champs de vecteurs X et Y**.

Démonstration. — Soient f et $g \in C^\infty(G)$. On calcule :

$$(X \circ Y)(fg) = X(Y(f)g + fY(g) = (X \circ Y)(f)g + Y(f)X(g) + X(f)Y(g) + f(X \circ Y)(g).$$

Les deux termes du milieu étant symétriques en X et Y, on obtient que

$$(X \circ Y - Y \circ X)(fg) = (X \circ Y - Y \circ X)(f)g + f(X \circ Y - Y \circ X)(g).$$

Ceci montre que $[X, Y]$ est une dérivation. L'ensemble des dérivations est donc une sous-algèbre de Lie de l'espace des endomorphismes de $C^\infty(G)$. $\square$

2.3.1.2. Champs de vecteurs invariants. — Un champ de vecteurs X sur G est dit **invariant à gauche** si l'on a :

$$\forall g \in G, \quad X_g = d_e L_g(X). \tag{14}$$

Ceci équivaut à :

$$\forall g, h \in G, \quad X_{gh} = d_h L_g(X_h) \tag{15}$$

puisque $d_e L_{gh} = d_e(L_g \circ L_h) = d_h L_g \circ d_e L_h$. Notons $\mathcal{V}(G)^G$ l'espace vectoriel des champs de vecteurs invariants à gauche

L'application qui à un vecteur tangent à l'origine $X \in \mathfrak{g}$ associe le champ de vecteurs invariant X défini par

$$X(g) = d_e L_g(X)$$

induit des isomorphismes d'espaces vectoriels

$$\mathfrak{g} \cong \mathcal{V}(G)^G.$$

Proposition 2.23. — *1) L'ensemble $\mathcal{V}(G)^G$ est un sous-algèbre de Lie de l'algèbre de Lie des champs de vecteurs sur G.*

2) L'isomorphisme d'espaces vectoriels $\mathfrak{g} \cong \mathcal{V}(G)^G$ est un isomorphisme d'algèbres de Lie.

Dans la suite de ces notes, nous identifierons souvent l'algèbre de Lie $\mathfrak{g}$ d'un groupe de Lie G avec l'algèbre de Lie $\mathcal{V}(G)^G$ des champs de vecteurs invariants à gauche sur G, par l'application précédente.

Démonstration. — 1) Notons λ_g l'action correspondant à L_g sur $C^\infty(G)$:

$$\lambda_g(f) = f \circ L_{g^{-1}}, \quad \text{c'est-à-dire} \quad \lambda_g(f)(h) = f(g^{-1}h), \quad \forall h \in G.$$

(On met g^{-1} pour avoir $\lambda_g \circ \lambda_{g'} = \lambda_{gg'}$.) Alors, pour $f \in C^\infty(G)$ et $g, h \in G$, on a :

$$d_h(\lambda_{g^{-1}}(f)) = d_h(f \circ L_g) = d_{gh} f \circ d_h L_g. \tag{16}$$

Lemme 2.24. — *Un champ de vecteur X sur G est invariant à gauche si et seulement si la dérivation correspondante D_X sur $C^\infty(G)$ vérifie :*

$$\forall g \in G, \quad : \lambda_g \circ D_X = D_X \circ \lambda_g. \tag{17}$$

Démonstration. — Commençons par rappeler que

$$(D_X f)(h) = d_h f(X_h)$$

de sorte que

$$\begin{aligned}(\lambda_{g^{-1}} \circ D_X)(f)(h) &= \lambda_{g^{-1}}(h \mapsto d_h f(X_h)) \\ &= d_{gh} f(X_{gh}).\end{aligned}$$

Le lemme résulte alors du calcul suivant, où l'égalité (18) équivaut à (15), tandis que l'égalité (19) résulte de (16) :

$$\begin{aligned}
(\lambda_{g^{-1}} \circ D_X)(f)(h) &= d_{gh}f(X_{gh}) \\
&= d_{gh}f(d_hL_g(X_h)) \qquad (18)\\
&= d_h(\lambda_{g^{-1}}(f))(X_h) \qquad (19)\\
&= (D_X \circ \lambda_{g^{-1}})(f)(h).
\end{aligned}$$

□

Maintenant si X et Y sont deux champs de vecteurs invariants à gauche, il résulte de (17) que pour tout g l'on a

$$\lambda_g \circ D_X \circ D_Y = D_X \circ \lambda_g \circ D_Y = D_X \circ D_Y \circ \lambda_g,$$

et de même pour $D_Y \circ D_X$, donc $[X, Y]$ est un champ de vecteurs invariant à gauche.

2) Soit $X \in \mathfrak{g}$. Écrivons $X = \frac{d}{dt}\Big|_{t=0} c_X(t)$ avec c_X un chemin C^∞ passant par e à l'instant $t = 0$. Alors

$$X(g)(= d_eL_g(X)) = \frac{d}{dt}\Big|_{t=0} gc_X(t).$$

Notons D_X la dérivation associée à ce champ de vecteurs (invariant à gauche). Remarquons que si $f \in C^\infty(G)$, on a :

$$\frac{d}{dt}\Big|_{t=0} f(gc(t)) = d_gf(d_eL_g(X)) = d_gf(X_g) = (D_Xf)(g). \qquad (20)$$

Étant donné $X, Y \in \mathfrak{g}$, c_X, c_Y comme au-dessus et $f \in C^\infty(G)$, l'application

$$(s, t) \mapsto f(gc_X(s)c_Y(t)c_X(s)^{-1})$$

est de classe C^∞. En utilisant (20) et d'après le lemme de Schwarz, on peut calculer de deux manière différente l'expression

$$A = \frac{d^2}{dsdt}\Big|_{s=0,\ t=0} f(gc_X(s)c_Y(t)c_X(s)^{-1}).$$

En dérivant d'abord par rapport à t, on obtient :

$$\begin{aligned}
A &= \frac{d}{ds}\Big|_{s=0} d_gf \circ d_eL_g \circ (\mathrm{Ad}\ c_X(s))(Y) \\
&= d_gf \circ d_eL_g([X, Y]) \\
&= D_{[X,Y]}f(g).
\end{aligned}$$

Puis en dérivant d'abord par rapport à s, on obtient :

$$\begin{aligned}
A &= \frac{d}{dt}\Big|_{t=0} d_g(f \circ R_{c_Y(t)^{-1}}) \circ d_eL_g(X) - \frac{d}{dt}\Big|_{t=0} d_{gc_Y(t)}f \circ d_eL_{gc_Y(t)}(X) \\
&= \frac{d}{dt}\Big|_{t=0} D_X(f \circ R_{c_Y(t)^{-1}})(g) - \frac{d}{dt}\Big|_{t=0} D_Xf(gc_Y(t)) \\
&= D_XD_Yf(g) - D_YD_Xf(g).
\end{aligned}$$

□

2.3.2. Application exponentielle. — Pour tout $X \in \mathfrak{g}$, on désignera par $\mathbf{X}$ le champ de vecteurs invariant à gauche associé, c'est-à-dire

$$\mathbf{X}_e = X \quad \text{et} \quad \mathbf{X}_g = d_e L_g(X), \quad \forall g \in G.$$

Rappelons qu'un champ de vecteurs $\mathbf{X}$ de classe C^∞ sur une variété M est **complet** si son flot local ϕ est défini sur $\mathbb{R} \times M$, ce qui implique que $(\phi_t)_{t\in\mathbb{R}}$ est un groupe à un paramètre C^∞ de C^∞-difféomorphismes de M, voir [**4**].

Un **sous-groupe à un paramètre** de G (en abrégé : **1-psg**) est un morphisme de groupes de Lie $\alpha : \mathbb{R} \to G$.

Théorème 2.25. — *Soient $X \in \mathfrak{g}$ et $\mathbf{X}$ le champ de vecteurs invariant à gauche associé. Alors $\mathbf{X}$ est complet et, si $(\phi_t)_{t\in\mathbb{R}}$ est le flot de $\mathbf{X}$, alors pour tous t dans $\mathbb{R}$ et g dans G, on a :*

$$\phi_t(g) = g\phi_t(e).$$

Par conséquent, l'application

$$\alpha_X : \mathbb{R} \to G, \quad t \mapsto \phi_t(e)$$

est un morphisme de groupes de Lie.

Réciproquement, si β est un 1-psg alors $\beta = \alpha_X$, où $X = \beta'(0)$. Par conséquent, on a une bijection

$$\mathfrak{g} \leftrightarrow \{1\text{-}psg\ de\ G\}.$$

Démonstration. — Notons $\Phi : (g,t) \mapsto \phi_t(g)$ le flot (local) associé à $\mathbf{X}$. Puisque $\mathbf{X}$ est invariant à gauche, et par la propriété d'unicité du flot local de $\mathbf{X}$, pour tout g dans G, le point $\phi_t(g)$ est défini si et seulement si $\phi_t(e)$ l'est, et alors

$$\phi_t(g) = g\phi_t(e). \tag{21}$$

Soit $I = I_e$ le domaine de définition de la courbe intégrale maximale $\alpha : t \mapsto \phi_t(e)$ telle que $\alpha(0) = e$. Alors I est un intervalle ouvert contenant 0 et il s'agit de montrer que $I = \mathbb{R}$. Mais d'après (21), $\phi_t(g)$ est défini pour $t \in I$ et pour tout g dans G. Soit $s \in I$. Prenant $g = \phi_s(e)$, on obtient que α se prolonge à l'intervalle $I \cup (s+I)$. Par maximalité de I, ceci entraîne que

$$s + I \subset I, \quad \forall s \in I,$$

et on déduit que $I = \mathbb{R}$. Penant toujours $g = \phi_s(e)$, il découle en outre de (21) que

$$\alpha_X(s+t) = \phi_{t+s}(e) = \phi_t(\phi_s(e)) = \phi_s(e)\phi_t(e) = \alpha_X(s)\alpha_X(t).$$

Comme $\alpha_X : t \mapsto \alpha_X(t)$ est C^∞, c'est donc un morphisme de groupes de Lie $\mathbb{R} \to G$. Enfin, comme $\alpha'_X(0) = X$, l'application $X \mapsto \alpha_X$ est injective.

Réciproquement, soit β un 1-psg et soient $X = \beta'(0)$ et $\mathbf{X}$ le champ de vecteurs invariant à gauche associé. Alors, en dérivant par rapport à s, en $s = 0$, l'égalité

$$\beta(s+t) = \beta(t)\beta(s) = (L_{\beta(t)} \circ \beta)(s)$$

on obtient

$$\beta'(t) = d_e L_{\beta(t)}(\beta'(0)) = d_e L_{\beta(t)}(X) = \mathbf{X}(\beta(t)).$$

Donc β est la courbe intégrale de $\mathbf{X}$ passant par e en $t = 0$, d'où $\beta = \alpha_X$. □

Corollaire 2.26. — *Pour tous $X \in \mathfrak{g}$ et $t \in \mathbb{R}$, on a $\alpha_{tX}(1) = \alpha_X(t)$.*

Démonstration. — L'application $\phi : s \mapsto \alpha_X(ts)$ est un 1-psg, et $\phi'(0) = t\alpha'_X(0) = tX$. Donc ϕ coïncide avec α_{tX}. □

On appelle **application exponentielle**, et on note

$$\exp = \exp_G : \mathfrak{g} \to G$$

l'application définie par $\exp(X) = \alpha_X(1)$. Alors $\exp(0) = e$ et , d'après le corollaire précédent,

$$\exp((s+t)X) = \alpha_X(s+t) = \alpha_X(s)\alpha_X(t) = \exp(sX)\exp(tX), \quad \forall s, t \in \mathbb{R}.$$

Exemple 2.27. — Pour $G = GL_n(\mathbb{R})$, on a $\mathfrak{g} = M_n(\mathbb{R})$ et pour tout $X \in M_n(\mathbb{R})$, l'application exponentielle usuelle :

$$\mathbb{R} \to GL_n(\mathbb{R}), \quad t \mapsto \sum_{k \geq 0} \frac{t^k}{k!} X^k$$

est un 1-psg, dont la dérivée en 0 est X. Ceci montre que pour $G = GL_n(\mathbb{R})$, l'exponentielle de Lie définie ci-dessus coïncide avec l'exponentielle usuelle des matrices.

Théorème 2.28. — *1) L'application* $\exp : \mathfrak{g} \to G$ *est C^∞.*

2) La différentielle en 0 de l'application exponentielle de G est l'application identité de $\mathfrak{g}$:

$$d_0 \exp = \mathrm{id}_{\mathfrak{g}}.$$

Par conséquent, $\exp$ *est un C^∞-difféomorphisme d'un voisinage ouvert U de 0 dans $\mathfrak{g}$ sur un voisinage ouvert V de e dans G.*

3) Le sous-groupe engendré par V (ou par $\exp(\mathfrak{g})$*) est égal à G^0 - la composante connexe du neutre dans G.*

Démonstration. — 1) Cela découle des propriétés de régularité du flot local Φ.

Montrons le point 2). Pour toute courbe C^∞ $f : \mathbb{R} \to \mathfrak{g}$ telle que $f(0) = 0$, on a

$$\left.\frac{d}{dt}\right|_{t=0} \exp(f(t)) = (d_0 \exp)(f'(t)).$$

Appliquant ceci à la courbe $f(t) = tX$, on obtient que

$$(d_0 \exp)(X) = \frac{d}{dt}\Big|_{t=0} \alpha_X(t) = X, \quad \forall X \in \mathfrak{g}.$$

Ceci montre que $d_0 \exp = \mathrm{id}_{\mathfrak{g}}$. La dernière asertion du point 2) résulte alors du théorème d'inversion locale.

Enfin, comme exp est continue et $\mathfrak{g}$ connexe, alors $\exp(\mathfrak{g}) \subset G^0$. D'autre part, comme V est un voisinage ouvert de e, le sous-groupe engendré par V est égal à G^0, d'après la proposition 1.8. □

Proposition 2.29. — *Soit $\phi : G \to H$ un morphisme de groupes de Lie. Alors, pour tout $X \in \mathfrak{g}$, on a :*

$$\exp_H(d_e\phi(X)) = \phi(\exp_G(X)).$$

Démonstration. — L'application $\alpha : t \mapsto \phi(\exp_G(tX))$ est un 1-psg de H, tel que $\alpha'(0) = d_e\phi(X)$, donc α est le 1-psg associé à $d_e\phi(X)$. □

2.4. Sous-groupes de Lie immergés et sous-algèbres de Lie

Soit G un groupe de Lie, d'élément neutre e, et soit $\mathfrak{g}$ son algèbre de Lie.

Le théorème suivant est important. En suivant Warner [**13**] nous le déduisons ici du théorème d'intégrabilité de Frobenius. Pour d'autres démonstrations, voir [**7, 5**].

Théorème 2.30. — *Soit $\mathfrak{h}$ une sous-algèbre de Lie de $\mathfrak{g}$. Il existe un* **unique** *sous-groupe de Lie immergé* **connexe** *H dans G tel que* Lie$(H) = \mathfrak{h}$*, c'est-à-dire qu'il existe un groupe de Lie connexe H et une immersion injective*

$$\tau : H \hookrightarrow G \quad \text{telle que} \quad d_e\tau = \sigma,$$

où σ désigne l'inclusion $\mathfrak{h} \subset \mathfrak{g}$. De plus, le couple (H, τ) est unique à isomorphisme unique près. On dit que H est le sous-groupe **associé à** *$\mathfrak{h}$.*

Attention : *un sous-groupe de Lie immergé n'est pas un sous-groupe de Lie en général*, voir exemple 2.21.

2.4.1. Théorème d'intégrabilité de Frobénius. — (Voir cours introductif de Biquard.)

Soit M une variété de classe C^∞ de dimension $n \geq 1$ et soit p un entier, $1 \leq p \leq n$. Un **champ de p-plans** $\mathcal{D}$ sur M est la donnée, pour tout point x de M, d'un sous-espace $\mathcal{D}(x)$ de dimension p dans T_xM, de telle manière que pour tout point x de M, il existe un voisinage U de x et p champs de de vecteurs $X_1, \dots, X_p$ de classes C^∞ sur U qui engendrent $\mathcal{D}$ en chaque point de U. On dit d'un champ de vecteur X sur M qu'il **appartient** au champ de plans $\mathcal{D}$, ce que l'on notera $X \in \mathcal{D}$, si $X(x) \in \mathcal{D}(x)$ pour tout $x \in M$.

Une sous-variété immergée $\psi : N \to M$ est une **variété intégrale** du champ de plan $\mathcal{D}$ sur M si

$$d_x\psi(T_xN) = \mathcal{D}(\psi(x)) \quad \text{pour tout } x \in N.$$

***Théorème 2.31* (Théorème de Frobénius)**. — *Soit $\mathcal{D}$ un champ de p-plan sur une variété M de classe C^∞. Supposons que quelque soient X et Y champs de vecteurs sur M appartenant à $\mathcal{D}$, le crochet de Lie $[X,Y]$ sur M appartient également à $\mathcal{D}$. Soit $x \in M$. Alors, il existe une unique variété intégrale de $\mathcal{D}$ connexe maximale qui passe par x.*

Démonstration. — On se ramène facilement au problème local correspondant au cas où M est un voisinage ouvert de 0 dans $\mathbb{R}^n$. Par définition d'un champ de plans, il existe $(X_1, \dots, X_p)$ un p-uplet de champs de vecteurs de classe C^∞, qui, en tout point x de M, est une base de $\mathcal{D}(x)$.

On se ramène tout d'abord au cas où $[X_i, X_j] = 0$ pour $i, j \in \{1, \dots, p\}$. Quitte à faire un changement linéaire de coordonnées, on peut supposer que $X_i(0) = \frac{\partial}{\partial x_i}(0)$ pour $i \in \{1, \dots, p\}$. Si $X_i = \sum_{j=1}^n a_{i,j} \frac{\partial}{\partial x_j}$, alors, quitte à réduire M, on peut supposer que la matrice $(a_{i,j}(x))_{1 \leq i,j \leq p}$ qui vaut la matrice identité en $x = 0$, est inversible. À nouveau, un changement linéaire de coordonnées permet de se ramener au cas où $X_i = \frac{\partial}{\partial x_i} + \sum_{j=p+1}^n c_{i,j} \frac{\partial}{\partial x_j}$. Et, en utilisant que par hypothèse chaque $[X_i, X_j]$ est combinaison linéaire des X_k, un calcul simple implique que $[X_i, X_j] = 0$ pour $i, j \in \{1, \dots, p\}$.

Il s'agit maintenant de montrer par récurrence sur p que si $(X_1, \dots, X_p)$ est un p-uplet de champs de vecteurs C^∞ linéairement indépendants et commutants (*i.e.* $[X_i, X_j] = 0$ pour tous i, j), alors il existe un C^∞-difféomorphisme local φ en 0 tel que, au voisinage de 0, on ait $\varphi^*(X_i) = \frac{\partial}{\partial x_i}$ pour $i \in \{1, \dots, p\}$.

Le cas $p = 1$ découle du théorème de redressement des champs de vecteurs. Supposons le résultat vrai pour $p - 1$. Alors nous pouvons supposer, quitte à utiliser un difféomorphisme local en 0, que $X_i = \frac{\partial}{\partial x_i}$ pour $i \in \{1, \dots, p-1\}$. Comme ci-dessus on peut de plus supposer que

$$X_p = \frac{\partial}{\partial x_p} + \sum_{j=p+1}^n c_j \frac{\partial}{\partial x_j}.$$

Comme $[X_p, X_i] = 0$ pour tout $i \in \{1, \dots, p-1\}$, on a $\frac{\partial c_j}{\partial x_i} = 0$ pour tout j, c'est-à-dire que c_j est une fonction des coordonnées $x_p, \dots, x_n$ seulement. Le théorème de redressement appliqué au champ de vecteur X_p sur $\{0\} \times \mathbb{R}^{n-p+1}$ permet de conclure. □

2.4.2. Démonstration du théorème 2.30. — Soit p la dimension de $\mathfrak{h}$. L'application qui à un élément g de G associe le p-plan

$$\mathcal{D}(g) = d_eL_g(\mathfrak{h})$$

de T_gG définit un champ de p-plans. En effet, soit $(X_1, \ldots, X_p)$ une base de $\mathfrak{h}$. Alors les champs de vecteurs invariants à gauche associés à $X_1, \ldots, X_p$ sont C^∞ et forment en tout point g de G une base de $\mathcal{P}(g)$.

Puisque $\mathfrak{h}$ est une sous-algèbre de Lie, le théorème de Frobénius implique que le champ de p-plans $\mathcal{P}$ est intégrable. Soit H la variété intégrale de $\mathcal{D}$ connexe maximale passant par e. L'injection $\tau : H \hookrightarrow G$ est une immersion injective C^∞ de H dans G.

Montrons que H est un sous-groupe de G. Comme pour tout g dans G, le C^∞-difféomorphisme L_g préserve le champ de p-plans $\mathcal{P}$, la sous-variété immergée $L_g(H)$ est donc la variété intégrale de $\mathcal{D}$ connexe maximale passant par g. En particulier, si g appartient à H, alors $L_g(H) = H$. On en déduit que H est stable par multiplication, ainsi qu si g appartient à H, alors il existe h dans H tel que $gh = e$, ce qui implique que $g^{-1} \in H$.

Enfin, la restriction à H de l'application $(x, y) \mapsto xy^{-1}$ est encore C^∞, car cette propriété est locale, et car H est une sous-variété immergée C^∞ dans G.

L'unicité découle de l'unicité dans le théorème de Frobénius.

2.4.3. Applications. — Il découle immédiatement du théorème 2.30 que *l'application qui à un sous-groupe de Lie immergée de G associe son algèbre de Lie est une bijection de l'ensemble des sous-groupes de Lie immergés connexes de G sur l'ensemble des sous-algèbres de Lie de $\mathfrak{g}$.*

Montrons maintenant la généralisation annoncée du corollaire 2.20.

***Théorème 2.32* (Cartan).** — *Tout sous-groupe fermé H de G est un sous-groupe de Lie de G.*

Démonstration. — Notons

$$\mathfrak{h} = \{X \in \mathfrak{g} \ : \ \forall t \in \mathbb{R}, \quad \exp(tX) \in H\}.$$

C'est le candidat pour être l'algèbre de Lie de H.

La démonstration du théorème 2.5 se transpose facilement (en utilisant une carte locale) et implique que $\mathfrak{h}$ est une sous-algèbre de Lie de $\mathfrak{g}$.

La restriction à $\mathfrak{h}$ de l'exponentielle est à valeur dans H. Soit $\mathfrak{m}$ un supplémentaire de $\mathfrak{h}$ dans $\mathfrak{g}$. L'application de $\mathfrak{h} \times \mathfrak{m}$ dans G qui à (X, Y) associe $\exp(X)\exp(Y)$ est un difféomorphisme d'un voisinage U de 0 dans $\mathfrak{h} \times \mathfrak{m}$ sur un voisinage de e dans G. L'image de $U \cap \mathfrak{h}$ est alors une sous-variété de G au voisinage de e. La démonstration du lemme 2.7 se généralise immédiatement pour montrer que – quitte à diminuer U – l'image de $U \cap \mathfrak{h}$ est l'intersection de H avec un voisinage de e dans G.

Cela montre que H est une sous-variété de G au voisinage de e et donc – par translation à gauche – en tout point de H. □

Une conséquence du théorème 2.32 est la suivante.

Théorème 2.33. — *Soient H et H' deux groupes de Lie et $f : H \to H'$ un morphisme de groupes* **continu**. *Alors f est une application C^∞.*

Démonstration. — Comme f est un morphisme continu, son graphe

$$\Gamma_f = \{(h, f(h)) \ : \ h \in H\}$$

est un sous-groupe fermé du groupe de Lie $G = H \times H'$. Donc, d'après le théorème 2.32, Γ_f est un sous-groupe de Lie fermé de G. Notons ϕ la restriction à Γ_f de la projection $\mathrm{pr}_1 : G \to H$. Alors ϕ est C^∞, bijective, et sa différentielle en tout point est bijective. Donc ϕ est un difféomorphisme local, et puisqu'il est bijectif c'est donc un difféomorphisme. Alors f égale $\mathrm{pr}_2 \circ \phi^{-1}$ est C^∞. □

2.5. Retour sur l'action adjointe

Soit G un groupe de Lie, d'élément neutre e, et soit $\mathfrak{g}$ son algèbre de Lie.

Lemme 2.34. — *1) Soient $g \in G$ et $X \in \mathfrak{g}$. Pour tout $t \in \mathbb{R}$, on a*

$$g \exp(tX) g^{-1} = \mathrm{Int}(g)(\exp(tX)) = \exp(t\mathrm{Ad}(g)(X)).$$

2) Pour tout $X \in \mathfrak{g}$ et $t \in \mathbb{R}$, on a

$$\mathrm{Ad}(\exp_G(tX)) = \exp_{GL(\mathfrak{g})}(\mathrm{ad}(tX)).$$

Démonstration. — 1) Fixons $g \in G$. Alors, $\mathrm{Int}(g) : G \to G$ est un morphisme de groupes de Lie dont la différentielle est $\mathrm{Ad}(g) : \mathfrak{g} \to \mathfrak{g}$. Donc 1) découle de la proposition 2.29, appliquée à $\phi = \mathrm{Ad}(g)$.

2) De même, $\mathrm{Ad} : G \to GL(\mathfrak{g})$ est un morphisme de groupes de Lie dont la différentielle est $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$. Donc 2) découle de la proposition 2.29, appliquée à $\phi = \mathrm{Ad}$. □

On note $\mathrm{Z}(G)$ le **centre** de G, c'est-à-dire,

$$\mathrm{Z}(G) = \{g \in G \ : \ gh = hg, \quad \forall h \in G\}.$$

C'est un sous-groupe fermé de G, invariant par tout automorphisme de G. On note $\mathfrak{z}(\mathfrak{g})$ le centre de $\mathfrak{g}$, c'est-à-dire,

$$\mathfrak{z}(\mathfrak{g}) = \{X \in \mathfrak{g} \ : \ [X, Y] = 0, \quad \forall Y \in \mathfrak{g}\}.$$

C'est un idéal de $\mathfrak{g}$, stable par tout automorphisme de $\mathfrak{g}$. Nous dirons qu'un sous-groupe Λ de G est **central** s'il est contenu dans $\mathrm{Z}(G)$.

Théorème 2.35. — *1) Pour tout $X \in \mathfrak{g}$, on a*

$$\mathrm{Ad}(\exp_G(X)) = \exp_{GL(\mathfrak{g})}(\mathrm{ad}(X)) = \sum_{k \geq 0} \frac{\mathrm{ad}(X)^k}{k!}.$$

2) Supposons G **connexe**. *Alors*

$$\mathrm{Ker}(\mathrm{Ad}) = \mathrm{Z}(G) \quad \textit{et} \quad \mathrm{Lie}(\mathrm{Z}(G)) = \mathrm{Ker}(\mathrm{ad}) = \mathfrak{z}(\mathfrak{g}).$$

Démonstration. — Le point 1) découle du lemme précédent et du fait que l'application exponentielle pour $GL(\mathfrak{g})$ est l'exponentielle usuelle d'une matrice.

Montrons le point 3). Pour tout morphisme $\phi : G \to H$ de groupes de Lie, on a

$$\mathrm{Lie}(\mathrm{Ker}\phi) = \mathrm{Ker}(d_e\phi),$$

d'après la proposition 2.19. Appliquant ceci à $\phi = \mathrm{Ad}$ et tenant compte du point 1), on obtient :

$$\mathrm{Lie}(\mathrm{Ker\ Ad}) = \mathrm{Ker\ ad} = \mathfrak{z}(\mathfrak{g}).$$

Il reste à montrer l'égalité $\mathrm{Ker}(\mathrm{Ad}) = \mathrm{Z}(G)$, lorsque G est connexe. On a toujours l'inclusion $\mathrm{Z}(G) \subset \mathrm{Ker}(\mathrm{Ad})$. En effet, si $g \in \mathrm{Z}(G)$, alors $\mathrm{Int}(g) = \mathrm{id}_G$ et donc $\mathrm{Ad}(g) = \mathrm{id}_{\mathfrak{g}}$, d'où $g \in \mathrm{Ker}(\mathrm{Ad})$.

Réciproquement, supposons G connexe et soit $g \in \mathrm{Ker}(\mathrm{Ad})$. Alors, pour tout $X \in \mathfrak{g}$, on a

$$g \exp(X) g^{-1} = \exp(\mathrm{Ad}(g)(X)) = \exp(X),$$

et donc g commute au sous-groupe de G engendré par $\exp(\mathfrak{g})$, qui égale $G^0 = G$. □

2.6. Revêtements et groupes de Lie

Rappelons qu'une application $f : X \to Y$ entre deux espaces topologiques est un **revêtement** si tout $y \in Y$ possède un voisinage ouvert V tel que $f^{-1}(V)$ soit une réunion disjointe d'ouverts de X, chacun homéomorphe à V par f.

Un groupe de Lie G est **simplement connexe** si tout revêtement connexe de G (vu comme espace topologique ou variété) est trivial [(3)].

Théorème 2.36. — *Soit G un groupe de Lie connexe. Il existe un groupe de Lie connexe et simplement connexe $\widetilde{G}$ et un morphisme de groupes de Lie $\pi : \widetilde{G} \to G$ qui est un revêtement (en particulier surjectif); alors $d\pi$ induite un isomorphisme entre* $\mathrm{Lie}(\widetilde{G})$ *et* $\mathfrak{g}$ *et* $\mathrm{Ker}\ \pi$ *est un sous-groupe normal discret donc central* Λ *de telle manière que $G \cong \widetilde{G}/\Lambda$.*

Démonstration. — Considérons $\pi : \widetilde{G} \to G$ un revêtement universel de la variété lisse G. Soit $\tilde{e}$ un point de la fibre au-dessus de l'élément neutre $e \in G$. Montrons qu'il existe une et une seule structure de groupe de Lie sur $\widetilde{G}$, d'élément neutre $\tilde{e}$, telle que π soit un morphisme de groupes.

Soit $m : G \times G \to G$ la multiplication $m : (x, y) \mapsto xy$ de G. Remarquons que $\widetilde{G} \times \widetilde{G}$ est simplement connexe. L'application composée de $\pi \times \pi : \widetilde{G} \times \widetilde{G} \to G \times G$ et de $m : G \times G \to G$ se relève en une unique application lisse $\tilde{m} : \widetilde{G} \times \widetilde{G} \to \widetilde{G}$ telle

(3) Cette définition est équivalente à la définition en termes de lacets, voir [**7**].

que $\tilde{m}(\tilde{e},\tilde{e}) = \tilde{e}$. De même, l'application $x \mapsto (\pi(x))^{-1}$ de $\widetilde{G}$ dans G se relève en une unique application, notée $x \mapsto x^{-1}$, de $\widetilde{G}$ dans $\widetilde{G}$ telle que $\tilde{e}^{-1} = \tilde{e}$.

L'unicité des relèvements permet de montrer que la loi $\tilde{m}$ est associative, a pour élément neutre $\tilde{e}$ et pour inverse d'un élément x de $\widetilde{G}$ l'élément x^{-1}. En effet, les applications $(x,y,z) \mapsto \tilde{m}(\tilde{m}(x,y),z)$ et $(x,y,z) \mapsto \tilde{m}(x,\tilde{m}(y,z))$ de l'espace simplement connexe $\widetilde{G} \times \widetilde{G} \times \widetilde{G}$ dans $\widetilde{G}$ sont deux relèvements par π de l'application $(x,y,z) \mapsto \pi(x)\pi(y)\pi(z)$, qui coïncident en $\tilde{e}$, donc sont égales. De plus, les trois applications $x \mapsto \tilde{m}(x,\tilde{e})$, $x \mapsto \tilde{m}(\tilde{e},x)$ et $x \mapsto x$ de l'espace simplement connexe $\widetilde{G}$ dans $\widetilde{G}$ sont trois relèvements par π de l'application $x \mapsto \pi(x)$, qui coïncident en $\tilde{e}$, donc sont égales. Enfin, les trois applications $x \mapsto \tilde{m}(x,x^{-1})$, $x \mapsto \tilde{m}(x^{-1},x)$ et $x \mapsto \tilde{e}$ de l'espace simplement connexe $\widetilde{G}$ dans $\widetilde{G}$ sont trois relèvements par π de l'application $x \mapsto e$, qui coïncident en $\tilde{e}$, donc sont égales.

L'application π est lisse, est un morphisme de groupes et est un revêtement, elle convient donc. Notons que c'est un difféomorphisme local au voisinage des éléments neutres, la différentielle induit donc un isomorphisme entre $\mathrm{Lie}(\widetilde{G})$ et $\mathfrak{g}$. Enfin, comme π est un morphisme de groupes, la fibre $\Lambda = \pi^{-1}(e)$ est un sous-groupe distingué de $\widetilde{G}$. Comme π est un revêtement, elle est discrète dans $\widetilde{G}$ et le lemme suivant permet de conclure la démonstration. □

Lemme 2.37. — *Soit G un groupe topologique connexe et Λ un sous-groupe discret normal. Alors Λ est central.*

Démonstration. — Pour tout $\gamma \in \Lambda$, l'application continue $g \mapsto g\gamma g^{-1}$ de l'espace connexe G à valeurs dans l'espace discret Λ est constante, donc égale à $e\gamma e^{-1} = \gamma$. Donc γ commute avec tout élément de G. □

Théorème 2.38. — *Soient G_1 et G_2 deux groupes de Lie connexes, $\mathfrak{g}_1$ et $\mathfrak{g}_2$ leurs algèbres de Lie, et $\phi : \mathfrak{g}_1 \to \mathfrak{g}_2$ un morphisme d'algèbres de Lie.*

1) Il existe **au plus un** *morphisme de groupes de Lie $\sigma : G_1 \to G_2$ tel que $d\sigma = \phi$. Dans ce cas* $\mathrm{Lie}(\mathrm{Ker}\sigma) = \mathrm{Ker}\phi$.

2) Si G_1 est simplement connexe, il **existe** *un unique morphisme de groupes de Lie $\sigma : G_1 \to G_2$ tel que $d\sigma = \phi$.*

Démonstration. — Posons $G = G_1 \times G_2$; son algèbre de Lie est $\mathfrak{g} = \mathfrak{g}_1 \times \mathfrak{g}_2$. Notons $\mathfrak{h}$ le graphe de ϕ, c'est-à-dire,

$$\mathfrak{h} = \{(x,\phi(x)) \; : \; x \in \mathfrak{g}_1\}.$$

C'est une sous-algèbre de Lie de $\mathfrak{g}_1 \times \mathfrak{g}_2 = \mathrm{Lie}(G)$, isomorphe à $\mathfrak{g}_1$ par la première projection pr_1.

D'après le théorème 2.30, il existe un unique sous-groupe de Lie immergé connexe $\tau : H \hookrightarrow G$ avec τ injective et $d\tau = (\mathrm{id}_{\mathfrak{g}_1}, \phi)$.

1) Soit $\sigma : G_1 \to G_2$ un morphisme tel que $d\sigma = \phi$. Alors le morphisme graphe

$$\tilde{\sigma} : G_1 \to G_1 \times G_2, \quad x \mapsto (x,\sigma(x))$$

est une immersion injective, et l'on a

$$d\tilde{\sigma} = (\mathrm{id}_{\mathfrak{g}_1}, d\sigma) = (\mathrm{id}_{\mathfrak{g}_1}, \phi).$$

Donc, d'après le résultat d'unicité dans le théorème 2.30, il existe un (unique) isomorphisme

$$\psi : G_1 \xrightarrow{\sim} H \quad \text{tel que} \quad \tau \circ \psi = \tilde{\sigma}.$$

Le graphe de σ, égal à $\tilde{\sigma}(G_1)$, est donc égal à $\tau(H)$, donc uniquement déterminé par $\mathfrak{h}$, c'est-à-dire, par ϕ. Ceci montre que σ, s'il existe, est unique. De plus, s'il existe, on a

$$\mathrm{Lie}(\mathrm{Ker}\sigma) = \mathrm{Ker}d\sigma = \mathrm{Ker}d\phi,$$

d'après la proposition 2.19. Ceci prouve 1).

Montrons 2). Soit $\pi = \mathrm{pr}_1 \circ \tau$, c'est un morphisme de groupes de Lie de H vers G_1, et

$$d\pi = \mathrm{pr}_1 \circ (\mathrm{id}_{\mathfrak{g}_1}, \phi) = \mathrm{id}_{\mathfrak{g}_1} \tag{22}$$

est un isomorphisme. Donc, d'après le théorème d'inversion local, il existe des voisinages ouverts U, resp. V, de l'identité dans H, resp., G_1, tels que π induise un difféomorphisme de U vers V.

Alors, $\pi(H)$ est un sous-groupe de G_1 contenant un voisinage de l'identité. Comme G_1 est connexe, ceci entraîne que $\pi(H) = G_1$.

De plus, $\mathrm{Ker}\pi \cap U = \{1\}$ et donc $K := \mathrm{Ker}\pi$ est un sous-groupe discret de H, et $\pi : H \to G_1$ est un *revêtement*. En effet, soit $g \in G_1$ et $h \in \pi^{-1}(g)$ arbitraire. Alors $\pi^{-1}(gV) = hUK$ et, comme $K \cap U = \{1\}$, alors $\pi^{-1}(gV)$ est la réunion disjointe :

$$\bigcup_{k \in K} hUk,$$

et chaque hUk est difféomorphe par π à $g\pi(U) = gV$. Ceci montre que π est un revêtement, connexe puisque H est connexe.

Donc, sous l'hypothèse que G_1 est simplement connexe, π est un homéomorphisme. Comme c'est un difféomorphisme local en e et donc en tout point, c'est en fait un difféomorphisme. On peut donc poser

$$\sigma = \mathrm{pr}_2 \circ \tau \circ \pi^{-1}.$$

C'est un morphisme de groupes de Lie $G_1 \to G_2$ et, *via* l'identification (22) de $\mathfrak{h}$ à $\mathfrak{g}_1$ *via* $d\pi$, on obtient que $d\sigma = \phi$. Ceci montre l'existence, lorsque G_1 est supposé simplement connexe. □

Corollaire 2.39. — *Un groupe de Lie simplement connexe est complètement déterminé (à isomorphisme près) par son algèbre de Lie.*

Démonstration. — Soient G et G' deux groupes de Lie simplement connexes, nous allons plus généralement montrer que si $\mathrm{Lie}(G) \cong \mathrm{Lie}(G')$, alors $G \cong G'$.

Soit ϕ un isomorphisme $\mathrm{Lie}(G) \to \mathrm{Lie}(G')$. D'après le théorème 2.38, il existe alors un (unique) morphisme de groupes de Lie

$$\sigma : G \to G', \qquad (\text{resp.} \quad \tau : G' \to G)$$

tel que $d\sigma = \phi$, (resp. $d\tau = \phi^{-1}$). Alors $\tau\sigma$ est un morphisme $G \to G$ tel que

$$d(\tau\sigma) = \mathrm{id}_{\mathfrak{g}} = d(\mathrm{id}_G).$$

L'unicité dans le théorème 2.38 implique $\tau\sigma = \mathrm{id}_G$, et de même $\sigma\tau = \mathrm{id}_G$. Ceci montre que $G \cong G'$. $\square$

Nous terminons ce chapitre en revenant sur quelques groupes classiques. Comme au-dessus, on note Λ le sous-groupe distingué central de $\widetilde{G^0}$ tel que l'application $\widetilde{G^0} \to G^0$ induise un isomorphisme de groupes de Lie $\widetilde{G^0}/\Lambda \cong G^0$. On note par ailleurs $\mathbb{U}_n$ le groupe des racines n-ième de l'unité.

G	$\mathrm{Z}(G)$	G/G^0	Λ
$SL_n(\mathbb{R})$	$\begin{cases} \{\pm \mathrm{Id}\} & \text{si } n \text{ pair} \\ e & \text{sinon} \end{cases}$	e	$\begin{cases} \mathbb{Z} & \text{si } n = 2 \\ \mathbb{Z}/2\mathbb{Z} & \text{si } n \geq 3 \end{cases}$
$SO(p,q)$	$\begin{cases} SO(2) & \text{si } pq = 0 \text{ et } p+q = 2 \\ \{\pm \mathrm{Id}\} & \text{si } n = p+q \text{ pair} \\ e & \text{sinon} \end{cases}$	$\begin{cases} e & \text{si } pq = 0 \\ \mathbb{Z}/2\mathbb{Z} & \text{sinon} \end{cases}$	$\begin{cases} e & \text{si } p = q = 1 \\ \mathbb{Z} & \text{si } 0 \leq p < q = 2 \\ \mathbb{Z}/2\mathbb{Z} & \text{si } p \leq 1 \text{ et } q \geq 3 \\ \mathbb{Z}^2 & \text{si } p = q = 2 \\ \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{si } p = 2,\ q \geq 3 \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{si } p, q \geq 3 \end{cases}$
$SU(p,q)$	$\mathbb{U}_n \mathrm{Id}$	e	$\begin{cases} e & \text{si } pq = 0 \\ \mathbb{Z} & \text{sinon} \end{cases}$
$Sp_{2n}(\mathbb{R})$	$\{\pm \mathrm{Id}\}$	e	$\mathbb{Z}$
$Sp(p,q)$	$\{\pm \mathrm{Id}\}$	e	$\begin{cases} e & \text{si } pq = 0 \\ \mathbb{Z} \times \mathbb{Z} & \text{sinon} \end{cases}$
$SL_n(\mathbb{C})$	$\mathbb{U}_n \mathrm{Id}$	e	e
$SO_n(\mathbb{C})$	$\begin{cases} \{\pm \mathrm{Id}\} & \text{si } n \text{ pair} \\ e & \text{sinon} \end{cases}$	$\mathbb{Z}/2\mathbb{Z}$	$\begin{cases} \mathbb{Z} & \text{si } n = 2 \\ \mathbb{Z}/2\mathbb{Z} & \text{si } n \geq 3 \end{cases}$
$Sp_{2n}(\mathbb{C})$	$\{\pm \mathrm{Id}\}$	e	e

CHAPITRE 3

GROUPES DE LIE SEMISIMPLES

3.1. Groupes de Lie compacts

Étant donné un groupe de Lie G, on note $\mathfrak{g}$ son algèbre de Lie, $[\cdot,\cdot]$ son crochet de Lie et $\mathfrak{g}_{\mathbb{C}} := \mathfrak{g} \otimes \mathbb{C}$ l'algèbre de Lie complexifiée. On note Ad l'**action adjointe** : pour g dans G, Adg est la dérivée de la conjugaison $x \mapsto gxg^{-1}$.

Soit $\mathrm{Aut}(\mathfrak{g})$ le **groupe des automorphismes de** $\mathfrak{g}$, c'est-à-dire

$$\mathrm{Aut}(\mathfrak{g}) = \{g \in GL(\mathfrak{g}) \ : \ \forall X, Y \in \mathfrak{g}, \quad [g(X), g(Y)] = g([X,Y])\}.$$

C'est un sous-groupe fermé de $GL(\mathfrak{g})$, donc un sous-groupe de Lie, et Ad est un morphisme de groupes de Lie de G dans $\mathrm{Aut}(\mathfrak{g})$.

Théorème 3.1. — *L'application $G \mapsto \mathfrak{g}_{\mathbb{C}}$ établit une bijection :*

$$\left\{ \begin{array}{c} \textit{groupes de Lie compacts} \\ \textit{connexes à centre trivial} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{algèbres de Lie} \\ \textit{semisimples complexes} \end{array} \right\}.$$

Il s'agit bien sûr d'une bijection "modulo isomorphisme".

Démonstration. — L'image $\mathrm{Ad}(G)$ est un sous-groupe compact d'un groupe linéaire.

Lemme 3.2. — *Soit U un sous-groupe compact d'un groupe linéaire $GL(V)$. Il existe une forme bilinéaire symétrique définie positive sur V qui est U-invariante.*

Démonstration. — Choisissant une base de V, on identifie $V = \mathbb{R}^n$. On munit V du produit scalaire hermitien usuel, qu'on désigne par $\langle \cdot, \cdot \rangle$. Pour $x, y \in V$, l'application $u \in U \mapsto \langle ux, uy \rangle$ est continue; on pose

$$(x, y) = \int_U \langle ux, uy \rangle du,$$

où du est la mesure de Haar normalisée sur U. Alors $(\cdot,\cdot)$ est une forme bilinéaire symétrique qui est U-invariante; elle est définie positive puisque pour $x \neq 0$ on a

$$(x,x) = \int_U \langle ux, ux \rangle du > 0.$$

□

Il existe donc une forme bilinéaire symétrique définie positive B_0 sur $\mathfrak{g}$ qui est $\mathrm{Ad}(G)$-invariante. Pour tout $X \neq 0$ dans $\mathfrak{g}$, l'opérateur $\mathrm{ad}X$ est antisymétrique pour B_0, donc $\mathrm{tr}((\mathrm{ad}X)^2) < 0$: la forme de Killing [(1)] est définie négative. Elle est en particulier non dégénérée et $\mathfrak{g}$ est semisimple et donc $\mathfrak{g}_\mathbb{C}$ aussi. L'injectivité de l'application $G \mapsto \mathfrak{g}_\mathbb{C}$ sera démontrée au cours de la section suivante. Dans cette partie nous montrons la surjectivité (voir proposition 3.7). □

Remarque 3.3. — Il découle du théorème 3.1 et la classification des algèbres de Lie semisimples complexes (voir cours introductif) que les groupes simples compacts sont soit (au centre près) un des groupes classiques $A_r = SU(r+1)$, $B_r = SO(2r+1)$, $C_r = Sp(2r)$, $D_r = SO(2r)$ ou un des cinq groupes exceptionnels E_6, E_7, E_8, F_4, G_2.

Soit dorénavant $\mathfrak{g}$ une algèbre de Lie semisimple complexe. On appelle **forme réelle** de $\mathfrak{g}$ une sous-algèbre de Lie réelle $\mathfrak{g}_\mathbb{R}$ telle que $\mathfrak{g} = \mathfrak{g}_\mathbb{R} \oplus i\mathfrak{g}_\mathbb{R}$, ce qui équivaut à dire que $\mathfrak{g}_\mathbb{R}$ est engendré, comme $\mathbb{R}$-espace vectoriel, par une $\mathbb{C}$-base de $\mathfrak{g}$. La forme réelle $\mathfrak{g}_\mathbb{R}$ est dite **compacte** si la forme de Killing de $\mathfrak{g}_\mathbb{R}$ est définie négative.

Exemple 3.4. — Soit $\mathfrak{g} = \mathfrak{sl}_2(\mathbb{C})$, avec la base standard

$$E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad F = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

On a $[E,F] = H$ et $[H,E] = 2E$, $[H,F] = -2F$. Alors $\mathfrak{sl}_2(\mathbb{R})$, dont (E,H,F) est une $\mathbb{R}$-base, est une forme réelle de $\mathfrak{sl}_2(\mathbb{C})$. Dans la base (E,H,F), on a :

$$\mathrm{ad}(E)\mathrm{ad}(F) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \mathrm{ad}(H)^2 = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Donc la forme de Killing de $\mathfrak{sl}_2(\mathbb{R})$ a pour matrice dans la base (E,H,F) la matrice suivante :

$$\begin{pmatrix} 0 & 0 & 4 \\ 0 & 8 & 0 \\ 4 & 0 & 0 \end{pmatrix};$$

[(1)] On rappelle que la forme de Killing de $\mathfrak{g}$ est définie par

$$(X,Y) \mapsto \mathrm{tr}((\mathrm{ad}X)(\mathrm{ad}Y)).$$

elle est de signature $(2,1)$, sa matrice dans la base $(E+F)/2$, $H/2$, $(E-F)/2$ est

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

D'autre part, posons $X = E - F$, $H' = iH$, $Y = i(E+F)$. Alors (X, H', Y) est une $\mathbb{C}$-base de $\mathfrak{sl}_2(\mathbb{C})$, et l'on a :

$$[H', X] = 2Y, \quad [H', Y] = -2X, \quad [X, Y] = 2H'.$$

Donc $\mathbb{R}X \oplus \mathbb{R}H' \oplus \mathbb{R}Y$ est une forme réelle de $\mathfrak{sl}_2(\mathbb{C})$, notée [(2)] $\mathfrak{su}_2$. Les matrices $\mathrm{ad}(X)\mathrm{ad}(H')$, $\mathrm{ad}(Y)\mathrm{ad}(H')$ et $\mathrm{ad}(Y)\mathrm{ad}(X)$ sont de trace nulle, et le tableau ci-dessous décrit $\mathrm{ad}(X)^2$, etc.

	X	H'	Y
$\mathrm{ad}(X)^2$	0	$-4H'$	$-4Y$
$\mathrm{ad}(Y)^2$	$-4X$	$-4H'$	0
$\mathrm{ad}(H')^2$	$-4X$	0	$-4Y$

Par conséquent; la forme de Killing de $\mathfrak{su}_2$ a pour matrice dans la base (X, H', Y) :

$$\begin{pmatrix} -8 & 0 & 0 \\ 0 & -8 & 0 \\ 0 & 0 & -8 \end{pmatrix};$$

elle est définie négative, l'algèbre de Lie $\mathfrak{su}_2$ est une forme réelle compact de $\mathfrak{sl}_2(\mathbb{C})$. En particulier, les algèbres de Lie réelles $\mathfrak{sl}_2(\mathbb{R})$ et $\mathfrak{su}_2$ ne sont pas isomorphes (puisque leur formes de Killing ont des signatures différentes).

Pour montrer la surjectivité de l'application considérée dans le théorème 3.1 il suffit de montrer que $\mathfrak{g}$ a une forme réelle compacte $\mathfrak{g}_{\mathbb{R}}$. Il découle en effet du lemme suivant que la composante connexe $\mathrm{Aut}^0(\mathfrak{g}_{\mathbb{R}})$ du groupe des automorphismes de $\mathfrak{g}_{\mathbb{R}}$ convient : c'est un groupe compact car il est fermé et préserve la forme de Killing.

Lemme 3.5. — *Soit* $\mathfrak{g}$ *une* $\mathbb{R}$*-algèbre de Lie semisimple et* $G = \mathrm{Aut}^0(\mathfrak{g})$. *C'est un sous-groupe de Lie fermé connexe à centre trivial de* $GL(\mathfrak{g})$ *et l'on a* $\mathrm{Lie}(G) \cong \mathfrak{g}$.

Dans ce cas on dira que G est le groupe de Lie **adjoint** de $\mathfrak{g}$; on le notera $\mathrm{Ad}(\mathfrak{g})$.

Démonstration. — Afin de déterminer l'algèbre de Lie de $\mathrm{Aut}(\mathfrak{g})$, notons θ le crochet de Lie de $\mathfrak{g}$, considéré comme application linéaire $\mathfrak{g} \otimes \mathfrak{g} \to \mathfrak{g}$. Posons $E = \mathrm{Hom}_{\mathbb{R}}(\mathfrak{g} \otimes \mathfrak{g}, \mathfrak{g}) = \mathfrak{g} \otimes (\mathfrak{g} \otimes \mathfrak{g})^*$ de sorte que $\theta \in E$. Le groupe $H = GL(\mathfrak{g})$ opère sur E :

$$(h \cdot \varphi)(X \otimes Y) = h(\varphi((h^{-1}X) \otimes (h^{-1}Y))) \quad (h \in H,\ \varphi \in E).$$

[(2)] La notation signifie évidemment que c'est l'algèbre de Lie du groupe unitaire $SU(2)$.

Et le groupe $\mathrm{Aut}(\mathfrak{g})$ est le groupe d'isotropie H_θ de θ dans H. L'action infinitésimale de $\mathfrak{h} = \mathrm{End}(\mathfrak{g})$ sur E est donnée par :

$$u \cdot \varphi = u \circ \varphi - \varphi \circ u, \quad \forall u \in \mathfrak{h},\ \varphi \in E,$$

c'est-à-dire

$$(u \cdot \varphi)(X \otimes Y) \quad = \quad u(\varphi(X \otimes Y)) - \varphi(u(X) \otimes Y + X \otimes u(Y)).$$

Donc, $u \in \mathfrak{h}_\theta$ si et seulement si

$$u([X,Y]) = [u(X), Y] + [X, u(Y)]$$

c'est-à-dire si et seulement si $u \in \mathrm{End}(\mathfrak{g})$ est une **dérivation**.

Lemme 3.6. — *Soit* $\mathfrak{g}$ *une* $\mathbb{R}$*-algèbre de Lie semisimple. Alors, toute dérivation est intérieure, i.e. appartient à* $\mathrm{ad}(\mathfrak{g}) \subset \mathrm{End}(\mathfrak{g})$.

Démonstration. — L'application $\mathrm{ad} : \mathfrak{g} \to \mathrm{End}(\mathfrak{g})$ est un morphisme d'algèbre de Lie de noyau le centre de $\mathfrak{g}$ – elle est donc injective ici – et d'image contenue dans la sous-algèbre de Lie $\mathrm{Der}(\mathfrak{g}) \subset \mathrm{End}(\mathfrak{g})$ constituée des dérivations de $\mathfrak{g}$. Posons $\mathfrak{a} = \mathrm{ad}(\mathfrak{g})$ c'est un idéal de l'algèbre de Lie $\mathrm{Der}(\mathfrak{g})$:

$$[D, \mathrm{ad} X] = \mathrm{ad}(DX). \tag{23}$$

Puisque $\mathfrak{a} \cong \mathfrak{g}$ est semisimple, sa forme de Killing est non dégénérée. Écrivons :

$$\mathrm{Der}(\mathfrak{g}) = \mathfrak{a} \oplus \mathfrak{a}^\perp.$$

Mais $\mathfrak{a}^\perp$ est encore un idéal et si $D \in \mathfrak{a}^\perp$ et $X \in \mathfrak{g}$ on a

$$\mathrm{ad}(DX) = [D, \mathrm{ad} X] \in \mathfrak{a} \cap \mathfrak{a}^\perp = \{0\}.$$

Donc $\mathfrak{a}^\perp = \{0\}$ et $\mathrm{Der}(\mathfrak{g}) = \mathfrak{a}$. □

On a donc :

$$\mathrm{Lie}(G) \cong \mathrm{Lie}(H_\theta) \cong \mathfrak{h}_\theta \cong \mathfrak{g}.$$

Il reste à montrer que G est à centre trivial. Mais G est connexe et

$$\mathrm{Ad} : G \to GL(\mathfrak{g})$$

est donc un morphisme de groupes de Lie dont le noyau est exactement le centre de G. Par ailleurs la différentielle de Ad en e est égale ad. Elle est donc injective et d'image $\mathrm{ad}(\mathfrak{g}) = \mathrm{Lie}(\mathrm{Aut}(\mathfrak{g}))$. L'image $\mathrm{Ad}(G)$ coïncide donc avec $\mathrm{Aut}^0(\mathfrak{g})$ et le centre de G est nécessairement trivial. □

Pour montrer que $\mathfrak{g}$ a une forme réelle compacte, considérons $\mathfrak{h}$ une sous-algèbre de Cartan et

$$\Delta = \{\alpha \in \mathfrak{h}^* \ :\ \alpha \neq 0 \text{ et } \mathfrak{g}_\alpha \neq 0\}$$

le [3] **système de racines** de $\mathfrak{g}$, où pour $\alpha \in \mathfrak{h}^*$, on a noté

$$\mathfrak{g}_\alpha = \{X \in \mathfrak{g} \ : \ \forall H \in \mathfrak{h}, \quad [H, X] = \alpha(H)X\}.$$

Notons B la forme de Killing de $\mathfrak{g}$. Pour tout $\alpha \in \Delta$, soit H_α l'unique [4] élément de $\mathfrak{h}$ défini par

$$B(H_\alpha, H) = \alpha(H), \quad \forall H \in \mathfrak{h}. \tag{24}$$

Rappelons que pour $X_{\pm\alpha}$ dans $\mathfrak{g}_{\pm\alpha}$, on a $[X_\alpha, X_{-\alpha}] = B(X_\alpha, X_{-\alpha})H_\alpha$. Pour $\alpha \in \Delta$, choisissons donc X_α dans $\mathfrak{g}_\alpha$ tels que $[X_{-\alpha}, X_\alpha] = H_\alpha$ et définissons, pour α, β dans Δ, le nombre $\mathrm{N}_{\alpha,\beta}$ par [5]

$$[X_\alpha, X_\beta] = \mathrm{N}_{\alpha,\beta} X_{\alpha+\beta} \quad \text{si} \quad \alpha + \beta \in \Delta \tag{25}$$

et par $\mathrm{N}_{\alpha,\beta} = 0$ sinon.

Proposition 3.7. — *On peut choisir les X_α de sorte que $\mathrm{N}_{\alpha,\beta} = -\mathrm{N}_{-\alpha,-\beta}$. Chaque $\mathrm{N}_{\alpha,\beta}$ est alors réel.*

Il nous suffit de montrer cette proposition, car on peut prendre

$$\mathfrak{g}_\mathbb{R} = i\mathfrak{h}_\mathbb{R} \oplus \bigoplus_{\alpha\in\Delta} \mathbb{R}i(X_\alpha + X_{-\alpha}) \oplus \bigoplus_{\alpha\in\Delta} \mathbb{R}(X_\alpha - X_{-\alpha}), \tag{26}$$

où $\mathfrak{h}_\mathbb{R} = \sum_{\alpha\in\Delta} \mathbb{R}H_\alpha$ (cette dernière somme n'est pas directe, il faudrait se restreindre à une base de Δ).

Lemme 3.8. — *La restriction de la forme de Killing $B_{|\mathfrak{h}_\mathbb{R}\times\mathfrak{h}_\mathbb{R}}$ est définie positive et $\mathfrak{h} = \mathfrak{h}_\mathbb{R} \oplus i\mathfrak{h}_\mathbb{R}$.*

Démonstration. — On sait déjà que $B_{|\mathfrak{h}_\mathbb{R}\times\mathfrak{h}_\mathbb{R}}$ est non dégénérée montrons qu'elle est positive. Pour $H \in \mathfrak{h}_\mathbb{R}$, on a

$$B(H, H) = \sum_{\alpha\in\Delta} \alpha(H)^2 = \sum_{\alpha\in\Delta} B(H_\alpha, H)^2.$$

Il suffit donc de voir que, pour α, β dans Δ, $B(H_\alpha, H_\beta)$ est réel. Cela résulte par exemple du théorème d'intégralité (voir cours introductif). La dernière partie du lemme résulte également de ce dernier résultat. □

---

[3] Rappelons que toutes les sous-algèbres de Cartan sont conjuguées. Donc à chaque algèbre de Lie semisimple complexe est associé un unique système de racines abstrait réduit.

[4] Rappelons que, l'algèbre de Lie complexe $\mathfrak{g}$ étant semisimple, $B_{|\mathfrak{h}\times\mathfrak{h}}$ est non dégénérée.

[5] Rappelons que chaque $\mathfrak{g}_\alpha$ ($\alpha \in \Delta$) est de dimension un et que pour $\alpha, \beta \in \mathfrak{h}^*$,

$$[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] \subset \mathfrak{g}_{\alpha+\beta} \quad \text{avec égalité lorsque } \alpha, \beta \text{ et } \alpha + \beta \in \Delta.$$

Par construction, les facteurs de la somme directe (26) sont orthogonaux [(6)]. De plus le lemme 3.8 et les relations $B(X_\alpha, X_{-\alpha}) = 1$ impliquent que $B_{|\mathfrak{g}_\mathbb{R}\times\mathfrak{g}_\mathbb{R}}$ est définie négative. Enfin, l'égalité $\mathrm{N}_{\alpha,\beta} = -\mathrm{N}_{-\alpha,-\beta}$ assure que $\mathfrak{g}_\mathbb{R}$ est une algèbre de Lie réelle.

Remarque 3.9. — Dans l'exemple 3.4 la forme réelle ainsi obtenue est bien $\mathfrak{su}_2$.

Lemme 3.10. — 1. *Pour* α, β *dans* Δ, *on a* $\mathrm{N}_{\alpha,\beta} = -\mathrm{N}_{\beta,\alpha}$.

2. *Pour* α, β, γ *dans* Δ *avec* $\alpha+\beta+\gamma = 0$, *on a*
$$\mathrm{N}_{\alpha,\beta} = \mathrm{N}_{\beta,\gamma} = \mathrm{N}_{\gamma,\alpha} \quad \textit{et} \quad \mathrm{N}_{\alpha,\beta}\mathrm{N}_{-\alpha,-\beta} < 0.$$

3. *Pour* $\alpha, \beta, \gamma, \delta$ *dans* Δ *non deux à deux colinéaires* [(7)] *et de somme* $\alpha+\beta+\gamma+\delta = 0$, *on a*
$$\mathrm{N}_{\alpha,\beta}\mathrm{N}_{\gamma,\delta} + \mathrm{N}_{\beta,\gamma}\mathrm{N}_{\alpha,\delta} + \mathrm{N}_{\gamma,\alpha}\mathrm{N}_{\beta,\delta} = 0.$$

Démonstration. — 1) Cela résulte de la définition des $\mathrm{N}_{\alpha,\beta}$ et de l'antisymétrie du crochet de Lie.

2) Comme $\alpha+\beta+\gamma = 0$, on a
$$H_\alpha + H_\beta + H_\gamma = 0. \tag{27}$$
Or l'identité de Jacobi
$$[X_\alpha, [X_\beta, X_\gamma]] = [[X_\alpha, X_\beta], X_\gamma] + [X_\beta, [X_\alpha, X_\gamma]] \tag{28}$$
donne
$$-\mathrm{N}_{\beta,\gamma}H_\alpha = \mathrm{N}_{\alpha,\beta}H_\gamma - \mathrm{N}_{\alpha,\gamma}H_\beta$$
soit, d'après le 1),
$$\mathrm{N}_{\beta,\gamma}H_\alpha + \mathrm{N}_{\gamma,\alpha}H_\beta + \mathrm{N}_{\alpha,\beta}H_\gamma = 0. \tag{29}$$
Puisque α est non nul et que les racines β et γ ne sont donc pas colinéaires, on déduit finalement de (27) et (29) que $\mathrm{N}_{\alpha,\beta} = \mathrm{N}_{\beta,\gamma} = \mathrm{N}_{\gamma,\alpha}$.

D'autre part, si pour α dans Δ on pose $H'_\alpha = \frac{2H_\alpha}{\alpha(H_\alpha)}$ et on choisit X'_α multiples de X_α tels que $B(X'_\alpha, X'_{-\alpha}) = \frac{2}{\alpha(H_\alpha)}$ alors $(X'_{-\alpha}, H'_\alpha, X'_\alpha)$ est un $\mathfrak{sl}_2$-triplet [(8)]. La théorie des $\mathfrak{sl}_2$-modules implique alors que
$$[X'_{-\alpha}, [X'_\alpha, X_\beta]] = a_{\alpha,\beta}X_\beta,$$
où $a_{\alpha,\beta}$ est un entier strictement positif. On en déduit que $\mathrm{N}_{\alpha,\beta}\mathrm{N}_{-\alpha,\alpha+\beta} > 0$. Le 1) et la première partie du 2) permettent de conclure.

---

(6) Rappelons que $B(\mathfrak{g}_\alpha, \mathfrak{g}_\beta) = 0$ si $\alpha+\beta \neq 0$.

(7) Rappelons que α et $-\alpha$ sont les seules racines proportionnelles à α.

(8) En effet :
$$[H'_\alpha, X'_\alpha] = 2X'_\alpha,\ [H'_\alpha, X'_{-\alpha}] = -2X'_{-\alpha} \text{ et } [X'_\alpha, X'_{-\alpha}] = H'_\alpha.$$

3) L'identité de Jacobi (28) implique que

$$\mathrm{N}_{\beta,\gamma}[X_\alpha, X_{-\alpha-\delta}] = \mathrm{N}_{\alpha,\beta}[X_{-\gamma-\delta}, X_\gamma] + \mathrm{N}_{\alpha,\gamma}[X_\beta, X_{-\beta-\delta}]$$

soit

$$\mathrm{N}_{\beta,\gamma}\mathrm{N}_{\alpha,-\alpha-\delta}X_{-\delta} = \mathrm{N}_{\alpha,\beta}\mathrm{N}_{-\gamma-\delta,\gamma}X_{-\delta} + \mathrm{N}_{\alpha,\gamma}\mathrm{N}_{\beta,-\beta-\delta}X_{-\delta}.$$

Mais d'après 2) on a :

$$\mathrm{N}_{\alpha,-\alpha-\delta} = \mathrm{N}_{\delta,\alpha}, \quad \mathrm{N}_{-\gamma-\delta,\gamma} = \mathrm{N}_{\gamma,\delta} \quad \text{et} \quad \mathrm{N}_{\beta,-\beta-\delta} = \mathrm{N}_{\delta,\beta}.$$

Il découle donc du point 1) que

$$(\mathrm{N}_{\alpha,\beta}\mathrm{N}_{\gamma,\delta} + \mathrm{N}_{\beta,\gamma}\mathrm{N}_{\alpha,\delta} + \mathrm{N}_{\gamma,\alpha}\mathrm{N}_{\beta,\delta})X_{-\delta} = 0.$$

Ce qui conclut la démonstration du lemme. □

Démonstration de la proposition 3.7. — Choisissons un ordre total sur $\mathfrak{h}_{\mathbb{R}}^*$ tel que la somme de deux éléments positifs est positive; par exemple l'ordre lexicographique pour les coordonnées dans une base de $\mathfrak{h}_{\mathbb{R}}$. On note

$$\Delta^+ = \{\alpha \in \Delta \ : \ \alpha > 0\}$$

les racines positives correspondantes. Pour ρ dans Δ^+, posons

$$\Delta_\rho = \{\alpha \in \Delta \ : \ -\rho \leq \alpha \leq \rho\}$$

et montrons par récurrence sur le cardinal de Δ_ρ que l'on peut choisir les X_α, pour α dans Δ_ρ, tels que

$$\forall \alpha, \beta, \ \alpha + \beta \in \Delta_\rho, \quad \mathrm{N}_{\alpha,\beta} = -\mathrm{N}_{-\alpha,-\beta}. \tag{30}$$

Remarquons immédiatement que $\mathrm{N}_{\alpha,\beta}$ est alors réel d'après le 2) du lemme 3.10.

Par hypothèse de récurrence, il ne reste à choisir que X_ρ car $X_{-\rho}$ s'en déduit. Si on ne peut pas écrire $\rho = \gamma + \delta$ avec γ, δ dans Δ^+, on choisit X_ρ arbitrairement. Si on peut écrire $\rho = \gamma + \delta$ avec γ, δ dans Δ^+, on prend

$$X_\rho = \lambda[X_\gamma, X_\delta] \quad \text{et} \quad X_{-\rho} = -\lambda[X_{-\gamma}, X_{-\delta}],$$

où $\lambda \in \mathbb{C}^*$ est choisi de sorte que $B(X_\rho, X_{-\rho}) = 1$. Il reste à vérifier (30). D'après l'hypothèse de récurrence il suffit de le vérifier lorsque $\alpha + \beta = \rho$. Ce qui résulte de l'égalité du 3) du lemme 3.10 appliquée à $\alpha, \beta, -\gamma, -\delta$ et à $-\alpha, -\beta, \gamma, \delta$ et de l'hypothèse de récurrence. □

Remarque 3.11. — La démonstration de la proposition se généralise facilement (il s'agit essentiellement d'utiliser la théorie des $\mathfrak{sl}_2$-modules pour préciser le point 2) du lemme 3.10) pour démontrer le théorème suivant (pour plus de détails, voir Serre [**11**]). La base construite dans ce théorème est appelée une **base de Chevalley**.

***Théorème 3.12* (Constantes de structures).** — *Pour tout élément α d'une base* $\mathbf{b}$ *de* Δ *fixons* $X_\alpha \in \mathfrak{g}_\alpha$ *et* $X_{-\alpha} \in \mathfrak{g}_{-\alpha}$ *tels que* $[X_\alpha, X_{-\alpha}] = H'_\alpha$ *(avec toujours* $H'_\alpha = \frac{2H_\alpha}{\alpha(H_\alpha)}$*). Alors, il existe des éléments* $E_\beta \in \mathfrak{g}_\beta$*, pour tout* $\beta \in \Delta$*, uniques au signe près, tels que* $[E_\beta, E_{-\beta}] = H'_\beta$*,* $E_\alpha = X_\alpha$ *pour* $\alpha \in \mathbf{b}$*, et, chaque fois que* $\beta, \gamma, \beta + \gamma \in \Delta$ *:*

$$[E_\beta, E_\gamma] = \mathrm{N}_{\beta,\gamma} E_{\beta+\gamma}, \quad \mathrm{N}_{-\beta,-\gamma} = -\mathrm{N}_{\beta,\gamma}, \quad \mathrm{N}_{\beta,\gamma} = \pm(r+1),$$

où r est le plus grand entier naturel tel que $\beta - r\gamma \in \Delta$. Par conséquent,

$$\mathfrak{g}_\mathbb{Z} := \mathfrak{h}_\mathbb{Z} \oplus \bigoplus_{\beta \in \Delta} \mathbb{Z} E_\beta,$$

avec

$$\mathfrak{h}_\mathbb{Z} := \bigoplus_{\alpha \in \mathbf{b}} \mathbb{Z} H_\alpha,$$

est une $\mathbb{Z}$-forme de $\mathfrak{g}$, c'est-à-dire un réseau qui est stable par le crochet de Lie.

3.2. Involution de Cartan

Une **involution de Cartan** d'une algèbre semisimple réelle $\mathfrak{g}$ est un automorphisme θ tel que $\theta^2 = 1$ et tel que la forme bilinéaire symétrique B_θ donnée par

$$B_\theta(X, Y) = B(\theta X, Y)$$

est définie négative. On a alors la **décomposition de Cartan** $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ où

$$\mathfrak{k} = \{X \in \mathfrak{g} \ : \ \theta(X) = X\} \quad \text{et } \mathfrak{p} = \{X \in \mathfrak{g} \ : \ \theta(X) = -X\}.$$

Les sous-espaces $\mathfrak{k}$ et $\mathfrak{p}$ sont orthogonaux pour la forme de Killing B qui est définie négative sur $\mathfrak{k}$ et définie positive sur $\mathfrak{p}$.

Exemple 3.13. — Si $\mathfrak{g} = \mathfrak{sl}_n(\mathbb{R})$ - l'algèbre de Lie du groupe spécial linéaire - ou $\mathfrak{g} = \mathfrak{so}(p, q)$ - l'algèbre de Lie du groupe orthogonal associé à une forme bilinéaire symétrique de signature (p, q) - alors, on peut prendre $\theta(X) = -{}^tX$. Dans le premier cas $\mathfrak{k} = \mathfrak{so}(n)$ et dans le deuxième cas $\mathfrak{k} = \mathfrak{so}(p) \times \mathfrak{so}(q)$.

Exemple 3.14. — Le complexifié $\mathfrak{g}_\mathbb{C}$ d'une algèbre de Lie réelle compacte $\mathfrak{g}$ est une algèbre de Lie que l'on peut considérer comme une algèbre de Lie réelle. Elle admet alors une involution de Cartan σ égale à la conjugaison complexe par rapport à la forme réelle $\mathfrak{g}$. On a alors $\mathfrak{k} = \mathfrak{g}$ et $\mathfrak{p} = i\mathfrak{g}$. On vérifie que pour $X + iY \neq 0$ dans $\mathfrak{k} + i\mathfrak{k}$ on a

$$B_\sigma(X + iY, X + iY) = B(X, X) + B(Y, Y) < 0.$$

Proposition 3.15. — 1. *Toute algèbre de Lie semisimple réelle $\mathfrak{g}$ admet une involution de Cartan θ.*

2. *Deux involutions de Cartan de $\mathfrak{g}$ sont toujours conjuguées (par un élément de* $\mathrm{Aut}^0(\mathfrak{g})$*).*

Remarque 3.16. — Le 2) prouve l'injectivité de l'application $G \mapsto \mathfrak{g}_{\mathbb{C}}$ du théorème 3.1.

Démonstration de la remarque. — Soient G et G' deux groupes de Lie compacts connexes à centres triviaux tels que $\mathrm{Lie}(G) \otimes \mathbb{C}$ soit isomorphe à $\mathrm{Lie}(G') \otimes \mathbb{C}$. Notons $\mathfrak{g}_{\mathbb{C}}$ l'algèbre de Lie complexe correspondante. Les sous-algèbre de Lie réelles $\mathfrak{g} = \mathrm{Lie}(G)$ et $\mathfrak{g}' = \mathrm{Lie}(G')$ sont deux formes réelles auxquelles correspondent deux involutions de Cartan σ et σ'. D'après la proposition 3.15 ces deux involutions sont conjuguées par un élément de $\mathrm{Aut}^0(\mathfrak{g}_{\mathbb{C}})$; cet élément induit en particulier un isomorphisme entre $\mathfrak{g}$ et $\mathfrak{g}'$. Pour conclure il suffit donc de remarquer que

$$\mathrm{Ad} : G \to GL(\mathfrak{g})$$

est un morphisme de groupes de Lie injectif – puisque G est connexe et à centre trivial – et d'image $\mathrm{Aut}^0(\mathfrak{g})$ d'après le lemme 3.5. □

Démonstration de la proposition 3.15. — 1) Considérons $\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \otimes \mathbb{C}$ et $\mathfrak{u}$ une forme réelle compacte de $\mathfrak{g}_{\mathbb{C}}$ - une telle forme réelle existe toujours d'après le paragraphe précédent (voir proposition 3.7). Soient τ la conjugaison complexe par rapport à $\mathfrak{g}$, σ la conjugaison complexe par rapport à $\mathfrak{u}$ (voir exemple 3.14) et N l'automorphisme de $\mathfrak{g}_{\mathbb{C}}$ égal à $\sigma\tau$. On a

$$B_\sigma(NX, Y) = B(\tau X, Y) = B(X, \tau Y) = B_\sigma(X, NY).$$

Ceci montre (voir exemple 3.14) que N est un opérateur hermitien pour le produit scalaire hermitien B_σ. Par conséquent, N est diagonalisable, à valeurs propres réelles, non nulles puisque N est inversible.

Pour toute la suite, on fixe une base $\mathcal{B} = (e_1, \dots, e_n)$ de $\mathfrak{g}_{\mathbb{C}}$ dans laquelle N est diagonale, et l'on considèrera des matrices relativement à cette base. Pour commencer, soit

$$P = N^2,$$

c'est une matrice diagonale dont les coefficients diagonaux $\lambda_1, \dots, \lambda_n$ sont des réls strictement positifs. On peut donc considérer leur logarithme $\mu_i = \log(\lambda_i)$ et la matrice diagonale

$$D = \begin{pmatrix} \mu_i & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mu_n \end{pmatrix}.$$

Pour tout $t \in \mathbb{R}$, on pose alors $\lambda_i^t = \exp(t\mu_i)$ et

$$P^t = \exp(tD) = \begin{pmatrix} \lambda_i^t & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n^t \end{pmatrix}.$$

Alors $P^t N = NP^t$, pour tout $t \in \mathbb{R}$. Comme N appartient à $\mathrm{Aut}(\mathfrak{g}_{\mathbb{C}})$, il en est de même de $P = N^2$. Montrons que $P^t \in \mathrm{Aut}(\mathfrak{g}_{\mathbb{C}})$, pour tout $t \in \mathbb{R}$.

Écrivons $[e_i, e_j] = \sum_{k=1}^n c_{i,j,k} e_k$. En appliquant l'automorphisme P, on obtient les égalités

$$\forall i, j, k, \quad (\lambda_i \lambda_j - \lambda_k) c_{i,j,k} = 0.$$

Donc, chaque fois que $c_{i,j,k} \neq 0$ on a $\lambda_i \lambda_j = \lambda_k$ et donc aussi

$$\lambda_i^t \lambda_j^t c_{i,j,k} = \lambda_k^t c_{i,j,k}, \quad \forall t \in \mathbb{R},$$

et bien sûr cette égalité est aussi vérifiée lorsque $c_{i,j,k} = 0$. Ceci montre que P^t est un automorphisme de $\mathfrak{g}_{\mathbb{C}}$, pour tout $t \in \mathbb{R}$. On pose alors, pour tout t,

$$\sigma_t = P^t \circ \sigma \circ P^{-t};$$

c'est la conjugaison par rapport à la forme compacte $P^t(\mathfrak{u})$. Montrons que, pour t bien choisi, σ_t commute à τ. Observons d'abord que

$$\sigma N \sigma^{-1} = \tau\sigma = N^{-1} \quad \text{d'où} \quad \sigma P \sigma^{-1} = P^{-1} \quad \text{et } \sigma P = P^{-1}\sigma.$$

Par un calcul matriciel analogue au précédent (facile car P et P^t sont diagonales), on obtient que

$$\forall t \in \mathbb{R}, \quad \sigma P^{-t} = P^t \sigma.$$

Alors :

$$\begin{cases} \sigma_t \tau = P^t \sigma P^{-t} \tau = P^{2t} N, \\ \tau \sigma_t = \tau P^t \sigma P^{-t} = N^{-1} P^{-2t}. \end{cases}$$

Par conséquent, si $Q = P^{-1/4} = \exp(D/4)$ alors $\phi = Q\sigma Q^{-1}$ est un automorphisme qui commute à τ. On en déduit que $\phi(\mathfrak{g}) \subset \mathfrak{g}$ et $\theta := \phi_{|\mathfrak{g}}$ est une involution de Cartan.

2) Soient θ et θ_1 deux involutions de Cartan de $\mathfrak{g}$. Comme en 1), on peut poser

$$Q = ((\theta\theta_1)^2)^{-1/4} \in \mathrm{Aut}(\mathfrak{g}), \quad \theta' = Q\theta_1 Q^{-1}$$

et prouver que θ et θ' commutent.

On diagonalise alors simultanément θ et θ' : on a

$$\mathfrak{g} = (\mathfrak{k} \cap \mathfrak{k}') \oplus (\mathfrak{k} \cap \mathfrak{p}') \oplus (\mathfrak{p} \cap \mathfrak{k}') \oplus (\mathfrak{p} \cap \mathfrak{p}'),$$

où $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ et $\mathfrak{g}' = \mathfrak{k}' \oplus \mathfrak{p}'$ sont les décompositions de Cartan de $\mathfrak{g}$ relativement à θ et θ'. La forme de Killing est définie négative sur $\mathfrak{k}$ et $\mathfrak{k}'$ et définie positive sur $\mathfrak{p}$ et $\mathfrak{p}'$. Donc $\mathfrak{k} \cap \mathfrak{p}' = \mathfrak{k}' \cap \mathfrak{p} = 0$ et $\mathfrak{k} = \mathfrak{k}'$, $\mathfrak{p} = \mathfrak{p}'$. C'est-à-dire $\theta = \theta'$. □

3.3. Sous-algèbres de Cartan

Soit $\mathfrak{g}$ une algèbre de Lie semisimple réelle. Un élément $X \in \mathfrak{g}$ est dit **semisimple** (resp. **nilpotent**) si $\mathrm{ad}(X)$ l'est [9]. Une **sous-algèbre de Cartan** $\mathfrak{h}$ de $\mathfrak{g}$ est une sous-algèbre commutative formée d'éléments semisimples et maximale pour cette propriété.

Proposition 3.17. — *Soient $\mathfrak{h}$ une sous-algèbre de Cartan de $\mathfrak{g}$ et θ une involution de Cartan de $\mathfrak{g}$. Alors,*

1. *$\mathfrak{h}_{\mathbb{C}}$ est une sous-algèbre de Cartan de $\mathfrak{g}_{\mathbb{C}}$;*
2. *il existe un conjugué de $\mathfrak{h}$ qui est θ-stable.*

Démonstration. — 1) Considérons

$$\mathrm{N}_{\mathfrak{g}}(\mathfrak{h}) = \{X \in \mathfrak{g} \, : \, \forall H \in \mathfrak{h}, \quad [H, X] = 0\}$$

le normalisateur de $\mathfrak{h}$ dans $\mathfrak{g}$ et son analogue $\mathrm{N}_{\mathfrak{g}_{\mathbb{C}}}(\mathfrak{h}_{\mathbb{C}})$ l'analogue sur le corps des nombres complexes. Puisque $\mathfrak{h}$ est une sous-algèbre de Cartan, on a

$$\mathrm{N}_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{h}$$

(la démonstration, donnée dans le cours introductif sur le corps des nombres complexes, reste valable sur $\mathbb{R}$). Donc $\mathfrak{h}$ est commutative maximale et

$$\mathrm{N}_{\mathfrak{g}_{\mathbb{C}}}(\mathfrak{h}_{\mathbb{C}}) = \mathrm{N}_{\mathfrak{g}}(\mathfrak{h}) \otimes \mathbb{C} = \mathfrak{h}_{\mathbb{C}}.$$

Donc $\mathfrak{h}_{\mathbb{C}}$ est une sous-algèbre de Cartan de $\mathfrak{g}_{\mathbb{C}}$.

2) D'après le 2) de la proposition 3.15, il suffit de construire une involution de Cartan θ' de $\mathfrak{g}$ telle que $\theta'(\mathfrak{h}) = \mathfrak{h}$. Soit $\mathfrak{u}$ une forme réelle compacte de $\mathfrak{g}_{\mathbb{C}}$ construite à partir de $\mathfrak{h}_{\mathbb{C}}$ par la méthode du §4.1. Notons σ (resp. τ) la conjugaison complexe par rapport à $\mathfrak{u}$ (resp. $\mathfrak{g}$). Comme dans démonstration du point 1) de la proposition 3.15, on peut poser

$$Q = ((\sigma\tau)^2)^{-1/4}, \quad \sigma' = Q \circ \sigma \circ Q^{-1}, \quad \theta' = \sigma'_{|\mathfrak{g}}$$

et montrer que θ' est une involution de Cartan de $\mathfrak{g}$. Comme $Q(\mathfrak{h}_{\mathbb{C}}) = \mathfrak{h}_{\mathbb{C}}$, on a $\theta'(\mathfrak{h}) = \mathfrak{h}$. □

3.4. Sous-espaces de Cartan

Soit $\mathfrak{g}$ une algèbre de Lie semisimple réelle. Un élément $X \in \mathfrak{g}$ est dit **hyperbolique** (resp. **elliptique**) si $\mathrm{ad}(X) \in \mathrm{End}(\mathfrak{g})$ est semisimple à valeurs propres réelles (resp. imaginaires pures). Un **sous-espace de Cartan** $\mathfrak{a}$ de $\mathfrak{g}$ est une sous-algèbre commutative formée d'éléments hyperboliques et maximale pour cette propriété.

Par définition, tout élément hyperbolique fait partie d'un sous-espace de Cartan.

[9] Rappelons que $\mathrm{ad}(X) \in \mathrm{End}(\mathfrak{g})$ est **semisimple** si et seulement s'il est diagonalisable sur $\mathbb{C}$.

On peut diagonaliser $\mathfrak{g}$ sous l'action de $\mathfrak{a}$. Pour λ dans $\mathfrak{a}^*$, on note

$$\mathfrak{g}_\lambda = \{Y \in \mathfrak{g} \ : \ \forall X \in \mathfrak{a}, \quad [X,Y] = \lambda(X)Y\}, \quad m_\lambda = \dim \mathfrak{g}_\lambda$$

et

$$\Sigma = \{\lambda \neq 0 \ : \ \mathfrak{g}_\lambda \neq 0\}$$

l'ensembles des **racines restreintes**. On peut montrer, nous n'en aurons pas besoin, que Σ est un système de racines abstrait (au sens du cours introductif) - pas toujours réduit. On a la décomposition

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\lambda\in\Sigma} \mathfrak{g}_\lambda.$$

Soient $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ une décomposition de Cartan associée à une involution de Cartan θ et

$$K = \{g \in \mathrm{Aut}(\mathfrak{g}) \ : \ \theta g = g\theta\}.$$

Lemme 3.18. — *Le groupe K est compact; son algèbre de Lie est $\mathfrak{k}$.*

Démonstration. — Le groupe K est fermé dans $\mathrm{Aut}(\mathfrak{g})$ et préserve la forme bilinéaire symétrique définie négative B_θ; c'est donc un groupe compact. Notons $\mathfrak{l}$ son algèbre de Lie. La sous-algèbre $\mathfrak{l} \subset \mathfrak{g}$ est stable par θ, se projette surjectivement sur $\mathfrak{k}$ et est compacte. Cela force $\mathfrak{l} = \mathfrak{k}$. □

Remarque 3.19. — Les éléments de $\mathfrak{k}$ sont elliptiques. Ceux de $\mathfrak{p}$ sont hyperboliques.

Démonstration. — Soit $X \in \mathfrak{p}$ (resp. $X \in \mathfrak{k}$). Il resulte de l'égalité

$$B([X,Y],Z) + B(Y,[X,Z]) = 0$$

que l'élément $\mathrm{ad}(X) \in \mathrm{End}(\mathfrak{g})$ est un opérateur symétrique (resp. antisymétrique) relativement à la forme bilinéaire symétrique B_θ. □

Remarque 3.20. — Notons $G = \mathrm{Aut}^0(\mathfrak{g})$. Le sous-groupe $K = \{g \in G \ : \ \theta g = g\theta\}$ est un sous-groupe compact maximal de G. L'espace G/K, muni de la métrique riemannienne G-invariante induite par la forme de Killing sur $\mathfrak{p}$ est un "espace symétrique riemannien simplement connexe à courbure négative ou nulle sans facteur euclidien". L'application $\mathfrak{g} \mapsto G/K$ est une bijection entre les algèbres de Lie semisimples réelles et ces espaces symétriques. Cette bijection est due à Cartan.

Proposition 3.21. —
1. *Tout sous-espace de Cartan $\mathfrak{a}$ est conjugué à un sous-espace de Cartan dans $\mathfrak{p}$.*
2. *Deux sous-espaces de Cartan dans $\mathfrak{p}$ sont toujours conjugués par un élément de K^0.*

Démonstration. — 1) Mettons $\mathfrak{a}$ dans une sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{g}$. D'après le point 2) de la proposition 3.17, on peut supposer que $\mathfrak{h}$ est θ-stable. Mais alors

$$\mathfrak{h} = (\mathfrak{h} \cap \mathfrak{k}) \oplus (\mathfrak{h} \cap \mathfrak{p}).$$

Comme, d'après la remarque 3.19, $\mathfrak{h} \cap \mathfrak{p}$ est l'ensemble des éléments hyperboliques de $\mathfrak{h}$. On a $\mathfrak{a} \subset \mathfrak{p}$.

2) Soient $\mathfrak{a}_1$ et $\mathfrak{a}_2$ deux sous-espaces de Cartan dans $\mathfrak{p}$. Choisissons X_i dans $\mathfrak{a}_i$ en dehors des noyaux des racines restreintes. Alors, un élément X de $\mathfrak{g}$ qui commute à X_i, commute à $\mathfrak{a}_i$.

Quitte à conjuguer $\mathfrak{a}_2$ par un élément de K^0, on peut supposer que la fonction définie sur K^0 : $g \mapsto B(X_1, gX_2)$ atteint son minimum pour $g = 1$. On a alors, pour tout Z dans $\mathfrak{k}$, $B(X_1, [Z, X_2]) = 0$. D'où $B(Z, [X_1, X_2]) = 0$. Comme $[X_1, X_2]$ est dans $\mathfrak{k}$, on en déduit $[X_1, X_2] = 0$, puis $[\mathfrak{a}_1, \mathfrak{a}_2] = 0$ et enfin $\mathfrak{a}_1 = \mathfrak{a}_2$. □

Remarque 3.22. — La dernier point de la démonstration montre que : *Si $\mathfrak{a} \subset \mathfrak{p}$ est un sous-espace abélien maximal, c'est un sous-espace de Cartan dans $\mathfrak{g}$.*

Démonstration. — Soient $\mathfrak{a}_1 = \mathfrak{a}$ et $\mathfrak{a}_2$ une sous-algèbre de Cartan dans $\mathfrak{p}$. Et considérons X_1 et X_2 comme au-dessus. Là encore, on peut supposer que la fonction $g \in K^0 \mapsto B(X_1, gX_2)$ atteint son minimum pour $g = 1$. On en déduit que $[X_1, X_2]$ et donc que $[\mathfrak{a}_1, \mathfrak{a}_2] = 0$ et donc que $\mathfrak{a}_1 = \mathfrak{a}_2$. □

Corollaire 3.23. — *Soit $\mathfrak{g}_{\mathbb{C}}$ (resp. $\mathfrak{g}$, $\mathfrak{u}$) une algèbre de Lie semisimple complexe (resp. réelle, réelle compacte).*

1. *Toutes les sous-algèbres de Cartan de $\mathfrak{u}$ sont conjuguées.*
2. *Toutes les sous-algèbres de Cartan de $\mathfrak{g}_{\mathbb{C}}$ sont conjuguées.*
3. *$\mathfrak{g}$ n'a qu'un nombre fini de classes de conjugaison de sous-algèbres de Cartan.*

La dimension commune des sous-algèbres de Cartan de $\mathfrak{g}$ est appelée le **rang de** $\mathfrak{g}$. La dimension des sous-espaces de Cartan de $\mathfrak{g}$ est appelée le **rang réel de** $\mathfrak{g}$.

***Exemple 3.24* (Le groupe spécial linéaire).** — Soit $\mathfrak{g} = \mathfrak{sl}_n(\mathbb{R})$. Pour $0 \leq j \leq [n/2]$, on note $\mathfrak{h}_j$ l'ensemble des matrices de la forme

$$\begin{pmatrix} \begin{pmatrix} t_1 & \theta_1 \\ -\theta_1 & t_1 \end{pmatrix} & & & & & \\ & \ddots & & & & \\ & & \begin{pmatrix} t_j & \theta_j \\ -\theta_j & t_j \end{pmatrix} & & & \\ & & & s_{2j+1} & & \\ & & & & \ddots & \\ & & & & & s_n \end{pmatrix}$$

et de trace nulle. Les $\mathfrak{h}_j$ sont des sous-algèbres de Cartan θ-stable de $\mathfrak{g}$ (avec $\theta(X) = -{}^tX$). Et toute sous-algèbre de Cartan θ-stable de $\mathfrak{g}$ est conjuguée à l'une d'entre elles. Remarquons que

$$\dim(\mathfrak{h}_j \cap \mathfrak{k}) = j \quad \text{et} \quad \dim(\mathfrak{h}_j \cap \mathfrak{p}) = n - j - 1.$$

Les sous-algèbres $\mathfrak{h}_j$ sont deux à deux non-conjuguées : les valeurs propres sont différentes.

L'ensemble des matrices diagonales de trace nulle constitue un sous-espace de Cartan $\mathfrak{a}$ de $\mathfrak{g}$ qui est donc de rang réel $n-1$.

Démonstration du corollaire 3.23. — 1) L'égalité $\mathfrak{u}_{\mathbb{C}} = \mathfrak{u} \oplus i\mathfrak{u}$ est une décomposition de Cartan. Si $\mathfrak{t}$ est une sous-algèbre de Cartan de $\mathfrak{u}$, $i\mathfrak{t}$ est un sous-espace de Cartan de $\mathfrak{u}_{\mathbb{C}}$ dans $i\mathfrak{u}$. On peut appliquer le 2) de la proposition 3.21.

2) Soient $\mathfrak{h}_1$ et $\mathfrak{h}_2$ deux sous-algèbres de Cartan de $\mathfrak{g}_{\mathbb{C}}$. D'après le §4.1, il existe des formes réelles compactes $\mathfrak{u}_i$ telles que chaque $\mathfrak{t}_i := \mathfrak{u}_i \cap \mathfrak{h}_i$ soit une sous-algèbre de Cartan de $\mathfrak{u}_i$. Quitte à conjuguer $\mathfrak{u}_2$, on peut, d'après le 2) de la proposition 3.15, supposer $\mathfrak{u}_1 = \mathfrak{u}_2$. On applique alors le premier point.

3) Fixons un sous-espace de Cartan $\mathfrak{a}$ dans $\mathfrak{p}$. Chaque classe de conjugaison de sous-algèbre de Cartan contient, d'après le 2) de la proposition 3.17, une sous-algèbre de Cartan θ-stable $\mathfrak{h}_1$. D'après le 2) de la proposition 3.21, on peut supposer que $\mathfrak{a}_1 := \mathfrak{h} \cap \mathfrak{p}$ est inclus dans $\mathfrak{a}$. Soient

$$\Sigma_1 = \{\alpha \in \Sigma \ : \ \alpha(\mathfrak{a}_1) = 0\} \quad \text{et} \quad \mathfrak{a}_1' = \{X \in \mathfrak{a} \ : \ \forall \alpha \in \Sigma_1, \quad \alpha(X) = 0\}.$$

Par définition $\mathfrak{a}_1'$ contient $\mathfrak{a}_1$. Mais tout élément de $\mathfrak{a}_1'$ commute au commutant de $\mathfrak{a}_1$ et par maximalité de $\mathfrak{h}$, on a en fait égalité $\mathfrak{a}_1 = \mathfrak{a}_1'$. Donc $\mathfrak{a}_1$ est entièrement déterminé par le sous-ensemble $\Sigma_1 \subset \Sigma$ qui ne peut prendre qu'un nombre fini de valeurs.

Pour conclure il reste à montrer que si $\mathfrak{h}_2$ est une autre sous-algèbre de Cartan θ-stable telle que $\mathfrak{h}_2 \cap \mathfrak{p} = \mathfrak{a}_1$, alors $\mathfrak{h}_1$ et $\mathfrak{h}_2$ sont conjuguées. Soient

$$\mathfrak{m}_1 = \{X \in \mathfrak{k} \ : \ [X, \mathfrak{a}_1] = 0\}, \quad \mathfrak{z}_1 \text{ le centre de } \mathfrak{m}_1 \quad \text{et} \quad \mathfrak{m}_1' = \mathfrak{m}_1/\mathfrak{z}_1.$$

L'algèbre de Lie réelle $\mathfrak{m}_1$ est l'algèbre de Lie d'un sous-groupe de $\mathrm{Aut}(\mathfrak{k})$. L'algèbre de Lie réelle $\mathfrak{m}_1'$ est donc l'algèbre de Lie d'une groupe de Lie compact à centre trivial, par suite elle est semisimple et compacte. Dans une représentation linéaire on vérifie que $[\mathfrak{m}_1, \mathfrak{m}_1]$ et $\mathfrak{z}_1$ sont orthogonales pour la forme de Killing. L'algèbre produit $[\mathfrak{m}_1, \mathfrak{m}_1] \oplus \mathfrak{z}_1$ est donc une sous-algèbre de Lie de $\mathfrak{m}_1$. Mais modulo $\mathfrak{z}_1$ le centre $[\mathfrak{m}_1, \mathfrak{m}_1]$ se projette sur $[\mathfrak{m}_1', \mathfrak{m}_1']$ qui est un idéal de $\mathfrak{m}_1'$ semisimple. On en désuit que $\mathfrak{m}_1' = [\mathfrak{m}_1, \mathfrak{m}_1]$. Les

$$\mathfrak{t}_i' := (\mathfrak{h}_i \cap \mathfrak{k})/\mathfrak{z}_1$$

sont en particulier des sous-algèbres de Cartan de $\mathfrak{m}_1'$ et le 1) permet de conclure. $\square$

Remarque 3.25. — Comme $\theta(\mathfrak{g}_\lambda) = \mathfrak{g}_{-\lambda}$, on a l'égalité

$$\Sigma = -\Sigma.$$

Soit Σ^+ un **système de racines positives** de Σ, c'est-à-dire une partie de Σ telle que

- $\Sigma^+ \cup (-\Sigma^+) = \Sigma$,
- $\Sigma^+ \cap (-\Sigma^+) = \emptyset$, et
- $\forall \alpha, \beta \in \Sigma^+$, $\alpha + \beta \notin \Sigma^- := (-\Sigma^+)$.

Une telle partie existe toujours : on choisit une base de $\mathfrak{a}^*$, on munit $\mathfrak{a}^*$ de l'ordre lexicographique des coefficients dans cette base et on prend

$$\Sigma^+ = \{\alpha \in \Sigma \ : \ \alpha > 0\}.$$

Soit

$$\mathfrak{n} = \bigoplus_{\lambda \in \Sigma^+} \mathfrak{g}_\lambda.$$

Il découle de l'inclusion $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] \subset \mathfrak{g}_{\alpha+\beta}$ et du troisième point de la définition de Σ^+ que l'algèbre $\mathfrak{n}$ est une algèbre de Lie nilpotente.

***Lemme 3.26* (Décomposition d'Iwasawa)**. — *On a l'égalité*

$$\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n}.$$

Démonstration. — Cela résulte de l'égalité $\theta(\mathfrak{g}_\lambda) = \mathfrak{g}_{-\lambda}$. □

Remarque 3.27. — La dimension de $\mathfrak{n}$ ne dépend que de $\mathfrak{g}$.

La proposition suivante permet de déterminer facilement la forme de Killing d'une algèbre de Lie simple.

Proposition 3.28. — *Soit $\mathfrak{g}$ une algèbre de Lie réelle telle que $\mathfrak{g}_\mathbb{C}$ soit simple. Alors la forme de Killing est (à un multiple réel près) la seule forme bilinéaire symétrique non-dégénérée sur $\mathfrak{g}$ qui est* ad$(\mathfrak{g})$*-invariante.*

Démonstration. — Soit B_0 la forme de Killing de $\mathfrak{g}$ et soit B une forme bilinéaire invariante sur $\mathfrak{g}$. Considérons l'endomorphisme f de l'espace vectoriel $\mathfrak{g}_\mathbb{C}$ défini par

$$B_0(f(X), Y) = B(X, Y).$$

Pour tous $X, Y \in \mathfrak{g}_\mathbb{C}$, on a :

$$f([X, Y]) = [X, f(Y)].$$

Autrement dit, l'application linéaire f commute aux $\mathrm{ad}(X)$. Soit λ une valeur propre de f. Alors $\mathrm{Ker}(f - \lambda \mathrm{Id}_{\mathfrak{g}_\mathbb{C}})$ est un sous-espace de $\mathfrak{g}_\mathbb{C}$ laissé stable par tous les $\mathrm{ad}(X)$. C'est donc un idéal non nul et par suite il égal à $\mathfrak{g}_\mathbb{C}$ tout entier. On en conclut que B est soit nulle soit un multiple de B_0. □

On prendra garde que dans la proposition précédente il est nécessaire que $\mathfrak{g}$ soit simple sur $\mathbb{C}$. Ainsi l'algèbre de Lie simple réelle $\mathfrak{sl}_2(\mathbb{C})$ admet un espace de dimension 2 de formes invariantes : considérer les formes

$$(X, Y) \mapsto a\mathrm{Retr}(XY) + b\mathrm{Imtr}(\overline{XY}).$$

3.5. Groupes de Lie semisimples

Soit G un groupe de Lie connexe. On dit que G est **semisimple** si son algèbre de Lie $\mathfrak{g}$ est semisimple. On dit que G est **quasi-simple** si $\mathfrak{g}$ est simple.

Théorème 3.29. — *Soit G un groupe de Lie semi-simple réel et connexe.*

1. *Il existe un groupe de Lie connexe et simplement connexe $\widetilde{G}$ et un morphisme de groupes de Lie $\pi : \widetilde{G} \to G$ qui est un revêtement (en particulier surjectif); alors $d\pi$ induite un isomorphisme entre $\mathrm{Lie}(\widetilde{G})$ et $\mathfrak{g}$ et $\mathrm{Ker}\,\pi$ est un sous-groupe normal discret donc central Λ de telle manière que $G \cong \widetilde{G}/\Lambda$.*
2. *Le centre Z de G est discret* (10) *et l'application adjointe* Ad *identifie le quotient $\overline{G} = G/Z$ avec le groupe adjoint $\mathrm{Ad}(\mathfrak{g}) = \mathrm{Aut}^0(\mathfrak{g})$.*
3. *Si G est simplement connexe, il est complètement déterminé (à isomorphisme près) par son algèbre de Lie $\mathfrak{g}$.*
4. *Si G est simplement connexe (resp. adjoint) - c'est-à-dire $G = \widetilde{G}$ (resp. $G = \overline{G}$) - il est le produit direct de ses sous-groupes distingués et connexes minimaux, qui, de plus, sont quasi-simples et également simplement connexes (resp. adjoints).*

Remarque 3.30. — D'après le 2), au centre près, et à quelques composantes connexes près, le groupe G s'identifie à un groupe algébrique réel.

Démonstration du théorème 3.29. — Les points 1) et 3), valides dans le contexte plus général des groupes de Lie, ont été démontrés plus haut, ce sont respectivement le théorème 2.36 et le corollaire 2.39.

2) Puisque G est connexe le noyau du morphisme adjoint $\mathrm{Ad} : G \to \mathrm{Aut}(\mathfrak{g})$ est exactement le centre Z de G. Par ailleurs son image est connexe - donc contenue dans $\mathrm{Aut}^0(\mathfrak{g})$ - et contient l'image par l'application exponentielle de

$$\mathrm{ad}(\mathfrak{g}) \cong \mathrm{Lie}(\mathrm{Ad}(\mathfrak{g})).$$

On a donc $\overline{G} = G/Z$. Enfin puisque les algèbres de Lie de G et $\overline{G}$ sont isomorphes, le centre Z de G (qui est un sous-groupe fermé, et donc de Lie, dans G) est nécessairement discret.

(10) Nous verrons qu'il est même souvent fini - c'est le cas si les groupes et les morphismes considérés sont algébriques.

4) Écrivons
$$\mathfrak{g} = \mathfrak{g}_1 \oplus \ldots \oplus \mathfrak{g}_n,$$
où chaque $\mathfrak{g}_i$ est une algèbre de Lie simple.

Notons G le revêtement universel de $\mathrm{Ad}(\mathfrak{g})$; alors on a
$$\mathrm{Lie}(G) = \mathrm{Lie}(\mathrm{Ad}(\mathfrak{g})) = \mathfrak{g}.$$
De plus, d'après le point 3) ci-dessus, G est l'unique groupe de Lie simplement connexe (à isomorphisme près) tel que $\mathrm{Lie}(G) = \mathfrak{g}$.

On obtient de même, pour chaque $\mathfrak{g}_i$, un unique groupe de Lie quasi-simple simplement connexe G_i tel que $\mathrm{Lie}(G_i) = \mathfrak{g}_i$. Alors
$$G_1 \times \cdots \times G_n$$
est un groupe de Lie simplement connexe dont l'algèbre de Lie est
$$\mathfrak{g}_1 \oplus \ldots \oplus \mathfrak{g}_n = \mathfrak{g},$$
d'où, par unicité, $G_1 \times \cdots \times G_n \cong G$. On en déduit le point 4) dans le cas simplement connexe. Remarquons finalement que le centre de G est le produit direct des centres des G_i, le groupe adjoint $\overline{G}$ est donc les produit des groupes adjoints $\overline{G}_i$ et on conclut de la même manière. $\square$

L'application $G \mapsto \mathrm{Lie}(G)$ établit donc une bijection :
$$\left\{ \begin{array}{c} \text{groupes de Lie semisimples} \\ \text{simplement connexes} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{algèbres de Lie réelles} \\ \text{semisimples} \end{array} \right\}.$$
Il s'agit bien sûr d'une bijection "modulo isomorphisme". La bijection réciproque associe à $\mathfrak{g}$ le revêtement universel de $\mathrm{Aut}^0(\mathfrak{g})$. De plus, cette bijection induit une bijection entre groupes quasi-simples et algèbres de Lie simples, et préserve les produits. Pour conclure montrons que cette bijection induit une bijection :
$$\left\{ \begin{array}{c} \text{groupes de Lie simplement connexes} \\ \text{semisimples compacts} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{algèbres de Lie réelles} \\ \text{semisimples compactes} \end{array} \right\}.$$
Cela découle du théorème suivant.

Théorème 3.31. — *Soit G un groupe de Lie compact connexe semisimple. Alors, son revêtement universel $\widetilde{G}$ est compact (et semisimple, puisque* $\mathrm{Lie}(\widetilde{G}) = \mathrm{Lie}(G)$.

La démonstration utilise les deux lemmes suivants, pour lesquels on renvoie à [**2**, §VII.3, Prop. 4 & Lemme 3].

Lemme 3.32. — *Soient G un groupe de Lie connexe, Z un sous-groupe fermé central tel que G/Z soit compact. Alors tout morphisme de groupes de Lie $\phi : Z \to \mathbb{R}$ s'étend en un morphisme de groupes de Lie $\widetilde{\phi} : G \to \mathbb{R}$.*

Lemme 3.33. — *Soient G un groupe de Lie connexe et Λ un sous-groupe discret central tel que G/Λ soit compact. Alors Λ est un groupe abélien de type fini.*

Démonstration du théorème 3.31. — Soit $\Lambda = \mathrm{Ker}(\widetilde{G} \to G)$. C'est un sous-groupe discret, normal, donc central (lemme 2.37). Par hypothèse, $\widetilde{G}/\Lambda \cong G$ est compact. Donc, d'après le lemme 3.33, Λ est un groupe abélien de type fini, donc de la forme

$$\Lambda = \mathbb{Z}^r \oplus F, \quad \text{où } F \text{ est un groupe fini.}$$

Montrons que $r = 0$. Supposons $r \geq 1$. Alors, on a un morphisme de groupes (de Lie)

$$\phi : \Lambda \overset{\mathrm{pr}_1}{\to} \mathbb{Z} \hookrightarrow \mathbb{R}$$

tel que $\phi(\Lambda) = \mathbb{Z}$. D'après le lemme 3.32, ϕ s'étend en un morphisme de groupes de Lie

$$\widetilde{\phi} : \widetilde{G} \to \mathbb{R}.$$

Alors $d\widetilde{\phi} : \mathfrak{g} \to \mathbb{R}$ est nulle car $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$ et (par homogénéité) $d_g\widetilde{\phi} = 0$ pour tout $g \in \widetilde{G}$. Donc $\widetilde{\phi}$ est le morphisme constant $\widetilde{G} \to \{0\}$, d'après la proposition plus bas. Mais ceci est une contradiction, puisque $\widetilde{\phi}(\widetilde{G})$ contient $\phi(\Lambda) = \mathbb{Z}$. Cette contradiction montre que $r = 0$, et donc $\Lambda = F$ est un groupe (abélien) fini. Il en résulte que $\widetilde{G}$ est compact. Ceci prouve le théorème, modulo la proposition ci-dessous. □

Proposition 3.34. — *Soit $f : M \to N$ une application lisse entre deux variétés (lisses), avec M connexe. On suppose que $d_m f = 0$, pour tout $m \in M$. Alors f est constante.*

Démonstration. — Comme M est supposée connexe, il suffit de montrer que f est localement constante. En prenant des cartes locales, on se ramène ainsi à montrer qu'une application $f : \mathbb{R}^n \to \mathbb{R}$ telle que $d_x f = 0$ pour tout $x \in \mathbb{R}^n$, est constante. Ceci ne présente pas de difficulté, voir par exemple [**13**, 1.24]. □

3.6. Aperçu de la classification

Pour terminer donnons un aperçu de la classification des groupes quasi-simples classiques. Quitte à passer au revêtement universel un tel groupe correspond à une algèbre de Lie réelle simple. Commençons par le lemme suivant.

Lemme 3.35. — *Soit $\mathfrak{g}$ une algèbre de Lie complexe simple vue comme algèbre de Lie réelle. Alors $\mathfrak{g}$ est simple.*

Démonstration. — On a déjà remarqué que $\mathfrak{g}$ est semisimple (regarder la forme de Killing). Et un idéal non nul $\mathfrak{h}$ de $\mathfrak{g}$ est somme directe d'algèbres de Lie simples. On a donc

$$[\mathfrak{g}, \mathfrak{h}] \subset \mathfrak{h} = [\mathfrak{h}, \mathfrak{h}], \quad \text{d'où} \quad \mathfrak{h} = [\mathfrak{g}, \mathfrak{h}].$$

Donc, tout $H \in \mathfrak{h}$ s'écrit $H = \sum_{k=1}^{n}[X_k, Y_k]$, avec $X_k \in \mathfrak{g}$, $Y_k \in \mathfrak{h}$. Alors

$$iH = \sum_{k=1}^{n}[iX_k, Y_k] \in [\mathfrak{g}, \mathfrak{h}] = \mathfrak{h}.$$

Ceci montre que $\mathfrak{h}$ est stable par multiplication par i donc est un idéal complexe de $\mathfrak{g}$. Comme $\mathfrak{g}$ est simple sur $\mathbb{C}$, il vient $\mathfrak{h} = \mathfrak{g}$. Ceci prouve que l'algèbre de Lie réelle $\mathfrak{g}$ est simple. □

Donc, parmi les algèbres de Lie réelles simples, on trouve toutes les algèbres de Lie complexe simples considérées comme algèbres de Lie réelles. Les groupes semi-simples réels classiques qui correspondent sont énumérés dans le tableau suivant, ce sont des groupes complexes que l'on considère comme des groupes réels. Pour chaque type on indique le groupe classique correspondant, ce sont tous des groupes connexes, on donne leur centres et leur groupes fondamentaux.

type	G	$Z(G)$	$\pi_1(G)$
A_{r-1}	$SL_r(\mathbb{C})$	$\mathbb{U}_n \cdot \mathrm{Id}$	$\{1\}$
B_r	$SO_{2r+1}(\mathbb{C})$	$\{1\}$	$\mathbb{Z}/2\mathbb{Z}$
C_r	$Sp_{2r}(\mathbb{C})$	$\{\pm\mathrm{Id}\}$	$\{1\}$
D_r	$SO_{2r}(\mathbb{C})$	$\{\pm\mathrm{Id}\}$	$\begin{cases} \mathbb{Z} & \text{si } r = 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{si } r \geq 2 \end{cases}$

Il y a bien sûr d'autres algèbres de Lie simples réelles que celles rencontrées ci-dessus. Soit $\mathfrak{g}$ une algèbre de Lie simple réelle. On dit que $\mathfrak{g}$ est **absolument simple** si $\mathfrak{g} \otimes \mathbb{C}$ est une algèbre de Lie complexe simple.

Théorème 3.36 **(L'alternative "complexe/absolument simple")**
Soit $\mathfrak{g}$ une algèbre de Lie simple réelle. Alors, de deux choses l'une :

1. *ou bien $\mathfrak{g}$ est* **complexe**, *c'est-à-dire qu'il existe une structure, unique à isomorphisme près, d'algèbre de Lie complexe sur $\mathfrak{g}$ qui prolonge la structure d'algèbre de Lie réelle;*
2. *ou bien $\mathfrak{g}$ est absolument simple, et donc $\mathfrak{g}$ est une forme réelle de l'algèbre de Lie complexe $\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \otimes \mathbb{C}$.*

Démonstration. — Commençons par remarquer que si $\mathfrak{g}$ est complexe alors, vue comme algèbre de Lie complexe, elle admet une forme réelle compact $\mathfrak{u}$ et $\mathfrak{g} \cong \mathfrak{u} \otimes \mathbb{C}$. Comme $\mathbb{C} \otimes \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$, on obtient que

$$\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathfrak{u} \otimes (\mathbb{C} \oplus \mathbb{C}) \cong \mathfrak{g} \oplus \mathfrak{g}.$$

En particulier elle n'est pas simple. Montrons la réciproque : soit $\mathfrak{g}$ une algèbre de Lie simple réelle telle que $\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \otimes \mathbb{C}$ ne soit pas simple, nous allons montrer que

$$\mathfrak{g}_{\mathbb{C}} \cong \mathfrak{s} \oplus \mathfrak{s},$$

où $\mathfrak{s}$ est une algèbre de Lie simple complexe uniquement déterminée et qui, vue comme algèbre de Lie réelle est isomorphe à $\mathfrak{g}$.

Notons τ la conjugaison complexe de $\mathfrak{g}_{\mathbb{C}}$ (relativement à la sous-algèbre réelle $\mathfrak{g}$). On sait déjà que $\mathfrak{g}_{\mathbb{C}}$ est semisimple (regarder la forme de Killing). Soit $\mathfrak{s}$ un idéal simple (non-abélien !) de $\mathfrak{g}_{\mathbb{C}}$. Alors $\tau(\mathfrak{s})$ est un idéal de $\mathfrak{g}_{\mathbb{C}}$.

Lemme 3.37. — *Soient $\mathfrak{h}_{\mathbb{C}}$ un idéal (ou plus généralement, sous-espace vectoriel complexe) de $\mathfrak{g}_{\mathbb{C}}$ et $\mathfrak{h} = \mathfrak{h}_{\mathbb{C}} \cap \mathfrak{g}$. Alors :*

$$\tau(\mathfrak{h}_{\mathbb{C}}) = \mathfrak{h}_{\mathbb{C}} \Leftrightarrow \mathfrak{h}_{\mathbb{C}} = \mathfrak{h} \otimes \mathbb{C}.$$

Démonstration. — L'implication $\Leftarrow$ est claire. D'autre part, l'application composée

$$\mathfrak{h} \otimes \mathbb{C} \xrightarrow{f} \mathfrak{h}_{\mathbb{C}} \hookrightarrow \mathfrak{g}_{\mathbb{C}}$$

est injective, donc f aussi. Montrons que f est surjective si $\tau(\mathfrak{h}_{\mathbb{C}}) = \mathfrak{h}_{\mathbb{C}}$. Soit $x \in \mathfrak{h}_{\mathbb{C}}$. Comme $\mathfrak{h}_{\mathbb{C}}$ est τ-stable, alors

$$\mathrm{Re}(x) := \frac{x + \tau(x)}{2} \quad \text{et} \quad \mathrm{Im}(x) := i\frac{\tau(x) - x}{2}$$

appartiennent à $\mathfrak{h}_{\mathbb{C}}$ et sont fixés par τ. Ils appartiennent donc à $\mathfrak{h}$ et l'on a

$$x = \mathrm{Re}(x) + i\mathrm{Im}(x) \in \mathfrak{h} \otimes \mathbb{C}.$$

Ceci montre que f est surjective. Le lemme est démontré. □

Les idéaux

$$\mathfrak{s} \cap \tau(\mathfrak{s}) \quad \text{et} \quad \mathfrak{s} + \tau(\mathfrak{s})$$

de $\mathfrak{g}_{\mathbb{C}}$ sont τ-stables, donc d'après le lemme 3.37 on a :

$$\mathfrak{s} \cap \tau(\mathfrak{s}) = \mathfrak{a} \otimes \mathbb{C}, \quad \mathfrak{s} + \tau(\mathfrak{s}) = \mathfrak{b} \otimes \mathbb{C},$$

où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de l'algèbre de Lie réelle $\mathfrak{g}$, nuls ou égaux à $\mathfrak{g}$ puisque $\mathfrak{g}$ est simple. Comme $\mathfrak{s} \neq 0$, on a $\mathfrak{b} \neq 0$, d'où

$$\mathfrak{b} = \mathfrak{g} \quad \text{et} \quad \mathfrak{s} + \tau(\mathfrak{s}) = \mathfrak{g}.$$

D'autre part, on ne peut avoir $\mathfrak{a} = \mathfrak{g}$, car sinon on aurait

$$\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \otimes \mathbb{C} \subset \mathfrak{s}, \quad \text{d'où } \mathfrak{g}_{\mathbb{C}} = \mathfrak{s},$$

contredisant la non-simplicité de $\mathfrak{g}_{\mathbb{C}}$. Donc $\mathfrak{a} = 0 = \mathfrak{s} \cap \tau(\mathfrak{s})$ et l'on a

$$\mathfrak{g}_{\mathbb{C}} = \mathfrak{s} \oplus \tau(\mathfrak{s}).$$

Comme τ est un automorphisme de $\mathfrak{g}_{\mathbb{C}}$, vue comme algèbre de Lie réelle, il induit un isomorphisme entre les algèbres de Lie $\mathfrak{s}$ et $\tau(\mathfrak{s})$ considérées comme algèbres de Lie réelles et

$$\mathfrak{g} = \{x + \tau(x) \ : \ x \in \mathfrak{g}_{\mathbb{C}}\} = \{x + \tau(x) \ : \ x \in \mathfrak{s}\} \cong \mathfrak{s}.$$

On obtient donc les isomorphismes d'algèbres de Lie réelles :

$$\mathfrak{g} \oplus \mathfrak{g} \cong \mathfrak{g}_{\mathbb{C}} \cong \mathfrak{s} \oplus \mathfrak{s}.$$

Finalement $\mathfrak{g}_{\mathbb{C}} \cong \mathfrak{s} \oplus \mathfrak{s}$, vues comme algèbres de Lie complexes et le théorème est démontré. □

Il nous reste donc à classifier les algèbres de Lie réelles absolument simples classiques, c'est-à-dire les formes réelles des algèbres de Lie simples complexes de type A, B, C ou D.

3.6.1. Formes réelles d'espaces vectoriels. — Soit $V_{\mathbb{R}}$ un $\mathbb{R}$-espace vectoriel de dimension n et $V_{\mathbb{C}} = V_{\mathbb{R}} \otimes \mathbb{C}$. Notons σ la conjugaison complexe sur $V_{\mathbb{C}}$ dont l'ensemble des points fixes est V. L'automorphisme σ opère également sur le dual $V'_{\mathbb{C}}$ ainsi que sur n'importe quel produit tensoriel $T_{\mathbb{C}}$ de la forme $(V_{\mathbb{C}} \otimes V_{\mathbb{C}} \otimes \ldots) \otimes (V'_{\mathbb{C}} \otimes V'_{\mathbb{V}} \otimes \ldots)$. Alors l'ensemble des points fixes $T_{\mathbb{R}}$ s'obtient de la même manière comme produit tensoriel de $V_{\mathbb{R}}$ et $V'_{\mathbb{R}}$. Si $t \in T_{\mathbb{C}}$ nous notons t^{σ} son image par σ. En particulier tout automorphisme F de $V_{\mathbb{C}}$ définit un élément de $V'_{\mathbb{C}} \otimes V_{\mathbb{C}}$ et l'on pourra parler de F^{σ}.

Lemme 3.38. — *Soit F un automorphisme de $V_{\mathbb{C}}$ tel que $F^{\sigma} = F^{-1}$. Alors, il existe un automorphisme Φ de $V_{\mathbb{C}}$ tel que*

$$F = \Phi^{\sigma} \circ \Phi^{-1}.$$

Démonstration. — L'ensemble

$$W = \{x \in V_{\mathbb{C}} \ : \ x^{\sigma} = F(x)\}$$

est clairement un $\mathbb{R}$-espace vectoriel. Montrons $W \otimes \mathbb{C} = V_{\mathbb{C}}$.

1. Si $a_1, \ldots, a_m$ sont des vecteurs de W linéairement indépendants sur $\mathbb{R}$, montrons par récurrence sur m qu'ils sont encore linéairement indépendants sur $\mathbb{C}$ dans $V_{\mathbb{C}}$. En effet, par l'absurde on aurait une relation de dépendance linéaire $\sum_i \lambda_i a_i = 0$ avec les λ_i dans $\mathbb{C}$ et pas tous dans $\mathbb{R}$, et $\lambda_m = 1$. En lui appliquant σ on obtiendrai alors $\sum_i \lambda_i^{\sigma} a_i = 0$ et donc $\sum_i (\lambda_i^{\sigma} - \lambda_i) a_i = 0$; une absurdité d'après l'hypothèse de récurrence.

2. Soit $(a_1, \ldots, a_m)$ une base de W sur $\mathbb{R}$, montrons que c'est une base de $V_{\mathbb{C}}$ sur $\mathbb{C}$. Soit $x \in V_{\mathbb{C}}$ alors $x + F^{-1}(x^{\sigma})$ et $i(x - F^{-1}(x^{\sigma}))$ sont dans W. On peut donc écrire

$$x + F^{-1}(x^{\sigma}) = \lambda_1 a_1 + \ldots + \lambda_m a_m$$

et

$$x - F^{-1}(x^{\sigma}) = -i(\mu_1 a_1 + \ldots + \mu_m a_m -,$$

avec $\lambda_i, \mu_j \in \mathbb{R}$. Soit

$$x = (\lambda_1 - i\mu_1) a_1 + \ldots + (\lambda_m - i\mu_m) a_m.$$

En particulier $m = n$. Pour conclure la démonstration du lemme fixons maintenant $(b_1, \dots, b_n)$ une base (réelle) de $V_{\mathbb{R}}$. Soit Φ l'automorphisme de $V_{\mathbb{C}}$ qui envoie les b_i sur les a_i; c'est un automorphisme complexe. En combinant les relations

$$a_i = \Phi(b_i), \quad a_i^\sigma = F(a_i), \quad b_i^\sigma = b_i,$$

on obtient $F(\Phi(b_i)) = \Phi^\sigma(b_i)$ pour tout i, soit

$$F = \Phi^\sigma \circ \Phi^{-1}.$$

□

Remarque 3.39. — Soient maintenant $t, t', \dots$ des tenseurs appartenant à des "espaces de tenseurs" $T, T', \dots$ comme avant le lemme. Supposons $t \in T_{\mathbb{R}}$, $t' \in T'_{\mathbb{R}}$, …, et que tous ces tenseurs sont invariants sous l'automorphisme F du lemme [11]. Soit Φ l'automorphisme donné par le lemme et $t_1 = \Phi^{-1}(t)$, etc. On a alors :

$$t_1^\sigma = (\Phi^\sigma)^{-1}(t) = \Phi^{-1}(F^{-1}(t)) = t_1$$

soit $t_1 \in T_{\mathbb{R}}$ et de même $t'_1 \in T'_{\mathbb{R}}$, etc.

La principale application que l'on a en vue concerne le cas des algèbres à involutions. Une **algèbre** A est un espace vectoriel V muni d'une application bilinéaire de $V \times V$ dans V, ou, ce qui revient au même, un élément t de $T = V' \otimes V' \otimes V$. Une **involution** sur A est alors la donnée d'un endomorphisme τ de V, ou, ce qui revient au même, d'un élément t' dans $T' = V' \otimes V$, tel que τ soit un antiautomorphisme [12] d'ordre deux de l'algèbre A. On parle alors d'**algèbre à involution**. On parlera naturellement d'algèbres à involution réelles $A_{\mathbb{R}}$ ou complexes $A_{\mathbb{C}}$. Comme cas particulier du lemme et de la remarque qui précèdent on a le théorème suivant.

Théorème 3.40. — *Soit $A_{\mathbb{C}}$ une algèbre à involution définie sur $\mathbb{R}$, σ la conjugaison complexe correspondante et F un automorphisme [13] de $A_{\mathbb{C}}$ tel que $F^\sigma = F^{-1}$. Alors, il existe une algèbre réelle à involution $B_{\mathbb{R}}$ et un isomorphisme Φ de $B_{\mathbb{C}} = B_{\mathbb{R}} \otimes \mathbb{C}$ sur $A_{\mathbb{C}}$ tels que*

$$F = \Phi^\sigma \circ \Phi^{-1}.$$

Démonstration. — Soit $V_{\mathbb{C}}$ l'espace vectoriel sous-jacent à $A_{\mathbb{C}}$ et soit $t \in T_{\mathbb{C}}$ et $t' \in T'_{\mathbb{C}}$ les tenseurs sur $V_{\mathbb{C}}$ correspondant à la structure d'algèbre à involution de $A_{\mathbb{C}}$. Puisque $A_{\mathbb{C}}$ est définie sur $\mathbb{R}$, l'espace $V_{\mathbb{C}}$ aussi et on a en fait $t \in T_{\mathbb{R}}$ et $t' \in T'_{\mathbb{R}}$. Soient t_1, t'_1 et Φ comme dans la remarque 3.39 et soit $B_{\mathbb{R}}$ l'algèbre réelle à involution définie sur $V_{\mathbb{R}}$ par t_1 et t'_1. Le lemme 3.38 et la remarque 3.39 impliquent que $B_{\mathbb{R}}$ et Φ vérifient les conclusions du théorème. □

[11] L'automorphisme F de $V_{\mathbb{C}}$ s'étend naturellement en un automorphisme de $T_{\mathbb{C}}, T_{\mathbb{C}}, \dots$.
[12] C'est-à-dire que $\tau(xy) = \tau(y)\tau(x)$.
[13] F préserve donc l'involution de $A_{\mathbb{C}}$.

3.6.2. Automorphismes d'algèbres à involution. — Soit $\mathfrak{g}_{\mathbb{C}}$ une algèbre de Lie simple complexe. On note $G_{\mathbb{C}} = \mathrm{Aut}^0_{\mathbb{C}}(\mathfrak{g}_{\mathbb{C}})$ le groupe adjoint correspondant. Le groupe des automorphismes de $G_{\mathbb{C}}$ s'identifie naturellement au groupe $\mathrm{Aut}_{\mathbb{C}}(\mathfrak{g}_{\mathbb{C}})$. Rappelons alors (voir cours introductif ou [**3**, Ch. VIII, §5, Corollaire 2]) que $\mathrm{Aut}_{\mathbb{C}}(\mathfrak{g}_{\mathbb{C}})/\mathrm{Aut}^0_{\mathbb{C}}(\mathfrak{g}_{\mathbb{C}})$ est isomorphe au groupe de symétries du diagramme de Dynkin de $\mathfrak{g}_{\mathbb{C}}$, il est en particulier d'ordre 1 lorsque $\mathfrak{g}_{\mathbb{C}}$ est une algèbre de Lie simple de type A_1, B_r $(r \geq 1)$, C_r $(r \geq 1)$ et d'ordre 2 lorsque $\mathfrak{g}_{\mathbb{C}}$ est de type A_r $(r \geq 2)$, D_r $(r \geq 2$ et $\neq 4)$. Nous laisserons de côté le cas de l'algèbre D_4 dont le diagramme de Dynkin a pour groupe de symétries $\mathfrak{S}_3$ et complétons la classification des formes réelles dans chacun des autres cas en suivant une méthode due à Weil qui, dans le cas des autres groupes classiques, passe par l'identification de $\mathrm{Aut}(G_{\mathbb{C}})$ avec le groupe des automorphismes d'une certaine algèbre à involution.

Commençons par considérer le cas du groupe $G_{\mathbb{C}} = PGL(n, \mathbb{C})$. Soit A l'algèbre $M_n(\mathbb{C}) \oplus M_n(\mathbb{C})$ muni de l'involution τ définie par

$$(X, Y) \mapsto ({}^tY, {}^tX).$$

Lemme 3.41. — *Supposons $n \geq 3$. Alors, le groupe des automorphismes de A qui commutent à l'involution τ est naturellement isomorphe au groupe des automorphismes de $PGL(n, \mathbb{C})$.*

Démonstration. — Un automorphisme de A envoie l'idéal $M_n(\mathbb{C}) \oplus \{0\}$ de A sur un idéal de A, c'est-à-dire sur lui même ou sur $\{0\} \oplus M_n(\mathbb{C})$. Le groupe G des automorphismes de A qui commutent à l'involution τ a donc deux composantes connexes G_0 et G_1, où G_0 est le sous-groupe des automorphismes qui laisse stable chaque composante $M_n(\mathbb{C})$ de A. On sait, d'après le théorème de Skolem-Noether, que tout automorphisme de $M_n(\mathbb{C})$ est intérieur. Le groupe G_0 est donc constitué des automorphismes $\phi(M)$ définis par

$$(X, Y) \mapsto (M^{-1}XM, {}^tMY{}^tM^{-1}),$$

où M est une matrice inversible quelconque. L'application $M \mapsto \phi(M)$ est alors un morphisme surjectif du groupe $GL(n, \mathbb{C})$ vers G_0 dont le noyau est le centre de $GL(n, \mathbb{C})$. Le groupe G_0 est donc naturellement isomorphe au groupe adjoint $PGL(n, \mathbb{C})$. Quand à G_1, il est constitué des automorphismes de A qui échangent ses deux composantes; c'est donc la classe de l'automorphisme $(X, Y) \mapsto (Y, X)$ modulo G_0.

Maintenant, les automorphismes intérieurs de G induisent des automorphismes de G_0 qui sont soit des automorphismes intérieurs soit des produits de tels automorphismes avec l'automorphisme induit sur G_0 par $(X, Y) \mapsto (Y, X)$; ce dernier n'est autre que $\phi(M) \mapsto \phi({}^tM^{-1})$, et il est facile de vérifier que pour $n \geq 3$, ce n'est pas un automorphisme intérieur. On obtient ainsi tous les automorphismes de $PGL(n, \mathbb{C})$. $\square$

De manière à décrire de manière similaire les groupes d'automorphismes des groupes orthgonaux et symplectiques, on considère maintenant l'algèbre matricielle $A = M_n(\mathbb{C})$ muni de l'involution $\tau(X) = {}^tX$ ou de l'involution $\tau(X) = J^{-1}{}^tXJ$, où dans le deuxième cas n est pair et J est la matrice antisymétrique

$$J = \begin{pmatrix} 0 & I_{n/2} \\ -I_{n/2} & 0 \end{pmatrix}.$$

Notons $F = I_n$ dans le premier cas et $F = J$ dans le second. D'après le théorème de Skolem-Noether, tout automorphisme de $M_n(\mathbb{C})$ est intérieur et donc de la forme

$$X \mapsto M^{-1}XM$$

avec $M \in M_n(\mathbb{C})$ inversible. Un tel automorphisme commute à l'involution τ si et seulement si $F = {}^tMFM$. Soit G le groupe de ces automorphismes.

Lemme 3.42. — *Supposons n pair égal à $2r$ et $F = J$. Alors, le groupe G des automorphismes de A qui commutent à l'involution τ est naturellement isomorphe au groupe (des automorphismes de) $PSp(n, \mathbb{C})$ - le groupe adjoint associé à l'algèbre de Lie simple complexe de type B_r.*

Démonstration. — Les matrices M vérifiant

$${}^tMJM = J$$

forment le groupe symplectique $Sp(n, \mathbb{C})$. Le groupe G est donc le quotient $PSp(n, \mathbb{C})$ du groupe $Sp(n, \mathbb{C})$ par son centre et nous avons rappeleé que dans ce cas tout automorphisme est inérieur. □

Lemme 3.43. — *Supposons $n \geq 3$, $\neq 8$ et $F = I_n$. Alors, le groupe des automorphismes de A qui commutent à l'involution τ est naturellement isomorphe au groupe des automorphismes de $PSO(n, \mathbb{C})$.*

Démonstration. — Les matrices $M \in M_n(\mathbb{C})$ vérifiant

$${}^tMM = I_n$$

forment le groupe orthogonal $O(n, \mathbb{C})$. Le groupe G est le quotient $PO(n, \mathbb{C})$ de $O(n, \mathbb{C})$ par son centre. Notons que le groupe ortogonal $O(n, \mathbb{C})$ a deux composantes connexes : la composante de l'identité $SO(n, \mathbb{C})$ et l'ensemble $O^-(n, \mathbb{C})$ des matrices de déterminant -1. Notons $PSO(n, \mathbb{C})$ le groupe adjoint correspondant, quotient de $SO(n, \mathbb{C})$ par son centre. Il convient alors de distinguer le cas n impair égal à $2r + 1$ - l'algèbre de Lie correspondante est de type B_r - où

$$G = PO(n, \mathbb{C}) = PSO(n, \mathbb{C}) \cong SO(n, \mathbb{C})$$

et tout automorphisme de $PSO(n, \mathbb{C})$ est intérieur, du cas n pair égal à $2r$ - l'algèbre de Lie correspondante est de type D_r - où d'un côté le groupe G n'est pas connexe et contient $G_0 = PSO(n, \mathbb{C})$ comme sous-groupe d'indice deux et d'un autre côté le groupe des automorphismes intérieurs est d'indice deux [14] dans le groupe de tous les automorphismes de $PSO(n, \mathbb{C})$. Pour conclure dans ce dernier cas il suffit que les automorphismes inérieurs de G correspondant à des éléments de $G_1 = PO^-(n, \mathbb{C})$ induisent sur G_0 des automorphismes qui ne sont pas intérieurs; c'est immédiat et cela conclut la démonstration du lemme. □

Rappelons qu'il y a parmi les groupes des différentes familles des isomorphismes exceptionnels :

1. Tous les automorphismes et antiautomorphismes de l'algèbre $M_2(\mathbb{C})$ commutent à l'involution $M \mapsto J^{-1t}MJ$; cela découle du fait que pour toute matrice inversible $M \in M_2(\mathbb{C})$, on a
$$J^{-1t}MJ = \det(M)M^{-1}.$$
De cette manière on obtient que $SL(2, \mathbb{C}) = Sp(2, \mathbb{C})$, et donc que
$$PGL(2, \mathbb{C}) = PSp(2, \mathbb{C}).$$
2. Le groupe $PSO(3, \mathbb{C})$ est isomorphe au groupe $PSp(2, \mathbb{C})$.
3. Le groupe $PSO(4, \mathbb{C})$ est isomorphe au groupe $PSO(3, \mathbb{C}) \times PSO(3, \mathbb{C})$.
4. Le groupe $PSO(5, \mathbb{C})$ est isomorphe au groupe $PSp(4, \mathbb{C})$.
5. Le groupe $PSO(6, \mathbb{C})$ est isomorphe au groupe $PGL(4, \mathbb{C})$.

Dans le paragraphe nous déterminons les différentes formes réelles des groupes simples classiques adjoints différents de $PSO(8, \mathbb{C})$.

3.6.3. Formes réelles des groupes classiques. — Soit G un groupe simple réel adjoint. D'après la remarque 3.30, le groupe G est un groupe algébrique réel et, d'après le lemme 3.35 l'ensemble de ses points complexes est un groupe simple complexe adjoint $G_{\mathbb{C}}$. Supposons dorénavant que $G_{\mathbb{C}}$ est un groupe classique différent de $PSO(8, \mathbb{C})$ et notons σ la conjugaison complexe sur $G(\mathbb{C})$ dont l'ensemble des points fixes est G.

D'après les lemmes 3.41, 3.42 et 3.43, il existe une algèbre à involution A tel que $G_{\mathbb{C}}$ soit isomorphe à la composante G_0 de l'identité dans le groupe des automorphismes de A qui commutent à l'involution. Soit f un isomorphisme de $G_{\mathbb{C}}$ vers G_0. L'application $f^\sigma \circ f^{-1}$ est alors un automorphisme du groupe (complexe) G_0. D'après les lemmes 3.41, 3.42 et 3.43 (et leur démonstrations) il correspond à f un unique automorphisme F de A qui induit l'automorphisme $f^\sigma \circ f^{-1}$ sur G_0. On a clairement $F^\sigma = F^{-1}$ et le théorème 3.40 implique donc qu'il existe une algèbre réelle à involution (B, θ) et un isomorphisme Φ de $B_{\mathbb{C}} = B \otimes \mathbb{C}$ sur A tels que
$$F = \Phi^\sigma \circ \Phi^{-1}.$$

[14] On utilise ici que $n \neq 8$.

Soit G' la composante de l'identité dans le groupe des automorphismes de B; Φ détermine un isomorphisme de $G'_{\mathbb{C}}$ sur G_0. Alors $\varphi = \Phi^{-1} \circ f$ est un isomorphisme entre $G_{\mathbb{C}}$ et $G'_{\mathbb{C}}$. Mais $\Phi^{\sigma} \circ \Phi^{-1} = F = f^{\sigma} \circ f^{-1}$ soit

$$\varphi = \varphi^{\sigma}$$

et l'isomorphisme φ induit un isomorphisme entre les groupes (réels) G et G'. On a ainsi démontré la proposition suivante.

Proposition 3.44. — *Un groupe réel G comme ci-dessus est isomorphe à la composante de l'identité du groupe des automorphismes d'une algèbre à involution (B, θ) définie sur $\mathbb{R}$.*

On est donc ramené à comprendre les différentes formes réelles des algèbres à involutions :

1. $A = M_n(\mathbb{C})$, $\tau(X) = {}^tX$;
2. $A = M_n(\mathbb{C})$, $\tau(X) = J^{-1}{}^tXJ$, avec n pair;
3. $A = M_n(\mathbb{C}) \oplus M_n(\mathbb{C})$, $\tau(X, Y) = ({}^tY, {}^tX)$.

Commençons par remarquer que d'après le théorème de Wedderburn (voir [**8**]) une algèbre réelle B telle que $B_{\mathbb{C}}$ soit isomorphe à A comme au-dessus est isomorphe à la somme directe d'algèbres de matrices sur $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$ (le corps des quaternions). On est donc respectivement dans l'une des situations suivantes :

1. si $B_{\mathbb{C}} = M_n(\mathbb{C})$, alors
   (a) $B = M_n(\mathbb{R})$, ou
   (b) $B = M_{n/2}(\mathbb{H})$ avec n pair;
2. si $B_{\mathbb{C}} = M_n(\mathbb{C}) \oplus M_n(\mathbb{C})$, alors
   (a) $B = M_n(\mathbb{R}) \oplus M_n(\mathbb{R})$,
   (b) $B = M_n(\mathbb{C})$, ou
   (c) $B = M_{n/2}(\mathbb{H}) \oplus M_{n/2}(\mathbb{H})$ avec n pair.

Examinons maintenant les possibilités pour θ. Notons tout d'abord que dans les deux cas où $A = M_n(\mathbb{C})$, la restriction de τ au centre $\mathbb{C} \cdot I_n$ de A est trivial, on dit alors que τ est de **première espèce** et qu'elle est de **seconde espèce** sinon. C'est par exemple le cas lorsque $A = M_n(\mathbb{C}) \oplus M_n(\mathbb{C})$ puisqu'alors le centre de A est $\mathbb{C} \cdot I_n \oplus \mathbb{C} \cdot I_n$ et que τ échange les deux facteurs.

Soit $\mathbb{K} = \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$ et B la $\mathbb{R}$-algèbre $M_n(\mathbb{K})$; celle-ci est de centre L égal à $\mathbb{R}$ si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{H}$ et égal à $\mathbb{C}$ si $\mathbb{K} = \mathbb{C}$.

Lemme 3.45. — *Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{H}$, toutes les involutions sur $B = M_n(\mathbb{K})$ sont de première espèce et de la forme*

$$\theta(X) = F^{-1}{}^t\overline{X}F \text{ avec } F \text{ inversible et } {}^t\overline{F} = \pm F.$$

Si $\mathbb{K} = \mathbb{C}$, les involutions sur $B = M_n(\mathbb{K})$ de première espèce sont de la forme

$$\theta(X) = F^{-1}{}^tXF \text{ avec } F \text{ inversible et } {}^tF = \pm F,$$

et les involutions sur $B = M_n(\mathbb{K})$ de seconde espèce sont de la forme

$$\theta(X) = F^{-1}{}^t\overline{X}F \text{ avec } F \text{ inversible et } {}^t\overline{F} = F.$$

Démonstration. — Soit θ une involution de B. Le sous-corps L^θ de L des points fixes par l'involution θ contient $\mathbb{R}$, l'involution θ est donc nécessairement de première espèce lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{H}$. Commençons par remarquer que l'application $\imath : X \mapsto {}^t\overline{X}$ définie toujours une involution de l'algèbre réelle $M_n(\mathbb{K})$; cette involution est de première espèce si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{H}$ et de seconde espèce si $\mathbb{K} = \mathbb{C}$. Donc si θ est une involution de B du même type, l'application $\imath \circ \theta^{-1}$ est un automorphisme de $M_n(\mathbb{K})$ qui agit trivialement sur le centre, et d'après le théorème de Skolem-Noether c'est un automorphisme intérieur. Alors, $\theta(X) = F^{-1}{}^t\overline{X}F$ avec $F \in M_n(\mathbb{K})$ inversible et la condition d'être involutif force ${}^t\overline{F} = \lambda F$ avec $\lambda \in L$; ceci implique $\lambda^2 = 1$ si $L = \mathbb{R}$ et $|\lambda|^2 = 1$ si $L = \mathbb{C}$. Dans le premier cas on a $\lambda = \pm 1$ ce qui conclut la démonstration du lemme lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{H}$. Dans le second cas on écrit $\lambda = \mu/\overline{\mu}$ et on remplace F par μF. Il reste alors à traiter le cas où θ est une involution de première espèce de $M_n(\mathbb{C})$. On procède comme au-dessus en remplaçant l'involution $\imath$ par la transposition. □

De la même manière en utilisant les involutions $(X, Y) \mapsto ({}^tX, {}^tY)$ (première espèce) et $(X, Y) \mapsto ({}^tY, {}^tX)$ (deuxième espèce) de l'algèbre $M_n(\mathbb{K}) \oplus M_n(\mathbb{K})$ et en procédant comme dans la démonstration du lemme 3.41 on montre le lemme suivant.

Lemme 3.46. — *Supposons $\mathbb{K} = \mathbb{R}$ ou $\mathbb{H}$. Alors toutes les involutions de première espèce sur $M_n(\mathbb{K}) \oplus M_n(\mathbb{K})$ sont de la forme*

$$(X, Y) \mapsto (F_1^{-1}{}^tXF_1, F_2^{-1}{}^tYF_2) \text{ avec } F_i \text{ inversible et } {}^tF_i = \pm F_i \text{ (pour } i = 1, 2),$$

et les involutions de seconde espèce sont de la forme

$$(X, Y) \mapsto (F^{-1}{}^tYF, {}^tF^tX^tF^{-1}) \text{ avec } F \text{ inversible.}$$

Rappelons que nous cherchons les algèbres (B, θ) qui se complexifient en (A, τ) dans la liste au-dessus et que la complexification préserve l'espèce de l'involution. Nous sommes donc ramené à la liste suivante.

3.6.3.1. $B = M_n(\mathbb{R})$ et θ de première espèce. — D'après le lemme 3.45 on a alors

$$\theta(X) = F^{-1}{}^t\overline{X}F \text{ avec } F \text{ inversible et } {}^t\overline{F} = \pm F.$$

D'après le théorème de Skolem-Noether, tout automorphisme de $M_n(\mathbb{R})$ est intérieur et donc de la forme

$$X \mapsto M^{-1}XM$$

avec M inversible. Un tel automorphisme commmute à l'involution $\tau(X) = F^{-1}{}^tXF$ si et seulement si ${}^tMFM = F$ et le groupe (réel) G' (donné par la proposition 3.44) est isomorphe soit au groupe otthogonal $PSO(F)$ si ${}^tF = F$ soit au groupe symplectiques $PSp(F)$. Les différentes classes d'isomorphisme de groupes réels ainsi obtenus sont donc

$$PSO(p,q) \quad (p+q=n) \qquad \text{et} \qquad PSp_{2n}(\mathbb{R}).$$

3.6.3.2. $B = M_n(\mathbb{H})$ (n pair) et θ de première espèce. — De la même manière qu'au paragraphe pécédent, on obtient les classes d'isomorphismes suivantes :

$$PSp(p,q) \quad (p+q=n) \qquad \text{et } PSO^*(n).$$

3.6.3.3. $B = M_n(\mathbb{R}) \oplus M_n(\mathbb{R})$ et θ de seconde espèce. — D'après le lemme 3.46 on a alors

$$\theta(X,Y) = (F^{-1t}YF, {}^tF^tX^tF^{-1}) \text{ avec } F \text{ inversible.}$$

En procédant de la même manière que dans la démonstration du lemme 3.41, on montre alors que la composante de l'identité dans le groupe des automorphismes de (B,θ) est constitué des automorphismes définis par

$$(X,Y) \mapsto (M^{-1}XM, {}^tF^tM^tF^{-1}Y^tF^tM^{-1t}F^{-1}).$$

La seule classe d'isomorphisme de groupes réels ainsi obtenue est

$$PSL(n,\mathbb{R}).$$

3.6.3.4. $B = M_n(\mathbb{H}) \oplus M_n(\mathbb{H})$ (n pair) et θ de seconde espèce. — De la même manière qu'au paragraphe précédent, on obtient comme seule classe d'isomorphisme, le groupe :

$$PSL(n,\mathbb{H}).$$

Notons que le groupe $GL(n,\mathbb{H})$ des automorphismes de $\mathbb{H}^n$ s'identifie à

$$\left\{ \begin{pmatrix} A & -\overline{B} \\ B & \overline{A} \end{pmatrix} \in GL(2n,\mathbb{C}) \right\}.$$

On définit alors le groupe $SL(n,\mathbb{H})$ comme l'intersection de $GL(n,\mathbb{H})$ avec $SL(2n,\mathbb{C})$.

3.6.3.5. $B = M_n(\mathbb{C})$ et θ de seconde espèce. — D'après le lemme 3.45 on a alors

$$\theta(X) = F^{-1t}\overline{X}F \text{ avec } F \text{ inversible et } {}^t\overline{F} = F.$$

En procédant comme dans le cas réel, on obtient comme classes d'isomorphismes les groupes unitaires :

$$PSU(p,q) \quad (p+q=n).$$

Nous résumons dans le tableau suivant les différentes formes réelles des groupes simples classiques (plutôt que les groupes adjoints nous considérons les formes classiques). Remarquons que bien que nous ne l'ayons pas démontré la classification est également valable pour les groupes de type D_4.

type	complexe	formes réelles
A_{r-1}	$SL_r(\mathbb{C})$	$SL(r,\mathbb{R})$, $SU(p,q)$ $(p+q=r)$, $SL(r/2,\mathbb{H})$ (r pair)
B_r	$SO_{2r+1}(\mathbb{C})$	$SO(p,q)$ $(p+q=2r+1)$
C_r	$Sp_{2r}(\mathbb{C})$	$Sp_{2r}(\mathbb{R})$, $Sp(p,q)$ $(p+q=r)$
D_r	$SO_{2r}(\mathbb{C})$	$SO(p,q)$ $(p+q=2r)$, $SO^*(2r)$.

CHAPITRE 4

GROUPES ALGÉBRIQUES

Ce chapitre est une introduction aux groupes algébriques principalement sur le corps des réels et des complexes.

4.1. Variétés algébriques

Cette section n'est qu'une rapide introduction à un (très) vaste sujet, nous nous contentons d'énoncer et de démontrer les résultats utiles pour la suite.

Soient $k \subset K$ des corps de caractéristique 0, avec K algébriquement clos. Dans nos applications on aura principalement $k = \mathbb{R}$ et $K = \mathbb{C}$.

Une **variété (algébrique) affine** V ou un **fermé de Zariski** de K^n est l'ensemble des zéros d'une famille de polynômes. Elle est **définie sur k**, si on peut choisir ces polynômes à coefficients dans k. On note

$$V_k = V \cap k^n$$

l'ensemble des **k-points de V**, $I(V)$ l'idéal de $K[X_1, \ldots, X_n]$ formé des polynômes nuls sur V,

$$I_k(V) = I(V) \cap k[X_1, \ldots, X_n],$$

$$K[V] = K[X_1, \ldots, X_n]/I(V)$$

l'anneau des **fonctions régulières** sur V et

$$k[V] = k[X_1, \ldots, X_n]/I_k(V)$$

l'anneau des fonctions régulières définies sur k.

Ces fermées définissent une topologie sur K^n et k^n : la **topologie de Zariski**. La variété V est dite **irréductible** si on ne peut pas l'écrire comme union de deux fermés de Zariski propre. On note alors $K(V)$ le corps des fonctions de l'anneau intégre $K[V]$. Les éléments de $K(V)$ sont les **fonctions rationnelles**. Par noetherianité [(1)] de $K[V]$, tout fermé de Zariski est réunion finie de fermés irréductibles. On appelle **dimension** de V le supremum sur tous les points $x \in V$ du supremum des longueurs des suites strictement décroissantes de fermés irréductibles de V contenant x (la longueur d'une suite $X = F_0 \supset F_1 \supset \cdots \supset F_n$ étant n). Toute variété algébrique affine $V \subset K^n$ est de dimension $\geq n$, avec égalité ssi $V = K^n$.

Un ouvert **principal** U d'une variété affine $V \subset K^n$ est le complémentaire de l'ensemble des zéros d'un polynôme P. Il s'identifie à un fermé de Zariski de K^{n+1} :

$$\{(v,t) \in V \times K \ : \ P(v)t = 1\}.$$

Tout ouvert de V est réunion d'ouverts principaux. Lorsque V est irréductible, les corps $K(V)$ et $K(U)$ coïncident [(2)].

Une application $f : V \to W$ est **régulière** si la composition par f envoie $K[W]$ dans $K[V]$ et définie sur k si elle envoie $k[W]$ dans $k[V]$.

Remarquons que le produit $V \times W$ de deux variétés affines est encore une variété affine. Nous aurons besoin du lemme suivant.

Lemme 4.1. — *Le produit $V \times W$ de deux variétés affines irréductibles est encore irréductible.*

Démonstration. — Pour tout $v \in V$, $w \in W$, les applications $\tau_v : W \to V \times W$, $x \mapsto (v,x)$ et $\tau_w : V \to V \times W$, $x \mapsto (x,w)$ sont régulières. Supposons $V \times W = F_1 \cup F_2$. Alors, pour chaque $w \in W$ on a $V = \tau_w^{-1}(F_1)$ ou $V = \tau_w^{-1}(F_2)$. Par conséquent, $W = W_1 \cup W_2$, où $W_i = \{w \in W \ : \ \tau_w(V) = F_i\}$. Mais $Y_i = \bigcap_{v \in V} \tau_v^{-1}(F_i)$ et donc Y_1 et Y_2 sont fermés. Ceci implique, disons, $W = W_1$ et donc $V \times W = F_1$. □

Une **variété algébrique** V est un espace topologique recouvert par des ouverts U_i de cartes φ_i tels que

- φ_i est un homéomorphisme de U_i sur une variété affine V_i,
- $V_{ij} := \varphi_i(U_i \cap U_j)$ est un ouvert principal de V_i et $f_{ij} := \varphi_j \circ \varphi_i^{-1}$ est une application régulière de V_{ij} dans V_{ji},
- la diagonale est fermée dans $V \times V$ (muni de la topologie de Zariski !).

On appelle encore topologie de Zariski la topologie sur V.

Remarque 4.2. — La topologie de Zariski sur le produit $V_1 \times V_2 \subset K^{n_1+n_2}$ de deux variétés affines est plus fine que la topologie produit : $K^{n_1+n_2}$ contient plus d'ouverts de Zariski que ceux obtenus par produit d'un ouvert de Zariski de K^{n_1} par un ouvert de Zariski de K^{n_2}. La topologie de Zariski sur $V \times V$ est donc plus fine que la topologie

---

[(1)] Un fameux théorème, due à Hilbert, affirme que l'anneau $A = K[X_1, \ldots, X_n]$ est **noethérien**, c'est-à-dire que toute suite croissante d'idéaux de A est stationnaire. En particulier, $K[V] = K[X_1, \ldots, X_n]/I(V)$ est noethérien.

[(2)] Puisque V est irréductible, l'ouvert (non vide) U est dense dans V.

produit. C'est relativement à cette topologie que l'on demande à la diagonale d'être fermée. Relativement à la topologie produit cela impliquerait que V est séparé ce qui serait ben trop demandé.

On dit que V est **définie sur** k si les V_i, V_{ij} et f_{ij} sont tous définis sur k. Une application $f : V \to W$ est **régulière** si elle est régulière dans les cartes, **définie sur k**, si elle est définie sur k dans les cartes. On dira alors parfois que V est une **k-variété**, que f est une **k-application régulière** ... Un **k-isomorphisme** entre deux k-variétés V et W est une k-application régulière $f : V \to W$ bijective et telle que f^{-1} soit encore une k-application régulière.

Exemple 4.3. — L'espace projectif $\mathbb{P}^n = \mathbb{P}(K^{n+1})$ est une variété algébrique. Les ouverts et les fermés des variétés algébriques sont encore des variétés algébriques.

Une **variété algébrique projective** est un fermé de l'espace projectif. Une **variété algébrique quasi-projective** est un ouvert d'une variété algébrique projective.

Nous aurons besoin de deux théorèmes classiques sur les applications régulières.

***Théorème 4.4* (Chevalley)**. — *L'image $f(V)$ d'une application régulière $f : V \to W$ contient un ouvert dense de son adhérence (pour la topologie de Zariski).*

Démonstration. — En se plaçant dans des cartes, on peut se ramener au cas où V et W sont des variétés algébriques affines d'un certain K^n. Remplaçant si nécessaire W par $\overline{f(V)}$, on peut de plus supposer que $f(V)$ est dense dans W [(3)]. On peut enfin se ramener au cas où V et W sont irréductibles de la manière suivante.

Notons $V_1, \ldots, V_n$ les composantes irréductibles de V et posons $W_i = \overline{f(V_i)}$. Alors $W_1 \cup \ldots \cup W_n$ égale W, car c'est un fermé contenant $f(V)$. Or chaque W_i est irréductible, on est donc ramené au cas où V et W sont irréductibles.

L'application f induit donc une injection

$$A := K[W] \hookrightarrow B := K[V].$$

Observons que tout $x \in K^n$ définit un morphisme de K-algèbres, l'évaluation en x,

$$e_x : K[X_1, \ldots, X_n] \to K, \quad P \mapsto P(x),$$

dont le noyau contient l'idéal $I(V)$ si $x \in V$. Réciproquement, d'un morphisme de K-algèbres $\varphi : K[X_1, \ldots, X_n] \to K$ dont le noyau contient $I(V)$, on obtient un point

$$x = (\varphi(X_1), \ldots, \varphi(X_n)) \in V.$$

(3) On dit alors que l'application régulière f est **dominante**.

Un point de V équivaut donc à la donnée d'un morphisme d'algèbre $\psi : B \to K$. [4]

Le théorème 4.4 est donc une conséquence du lemme suivant avec $b = 1$, que l'on peut dans ce cas particulier reformuler de la manière suivante : il existe une fonction régulière sur W dont l'ouvert principal associé est contenu dans $f(V)$. □

Lemme 4.5. — *Soit $A \hookrightarrow B$ des anneaux tels que B est une A-algèbre de type fini intègre. Alors, pour tout b non nul dans B, il existe $a \in A$ tel que tout morphisme d'algèbre $\varphi : A \to K$ tel que $\varphi(a) \neq 0$ se prolonge en un morphisme $\varphi' : B \to K$ tel que $\varphi'(b) \neq 0$.*

Démonstration. — Par récurrence sur le nombre de générateurs de B, on peut supposer que B est engendré par un élément x. Soit

$$P(T) = \sum_{i=0}^{d} p_i T^i \in A[T]$$

un polynôme non nul de degré minimal d tel que $P(x) = 0$. [5] Soit $Q \in A[T]$ un polynôme non nul de degré minimal tel que $Q(b) = 0$.

On prend $a = a_d Q(0)$. Soit L le corps des fractions de A. L'idéal I de $L[T]$:

$$I = \{P_1 \in L[T] \ : \ P_1(x) = 0\}$$

est engendré par P. Donc si on note $\lambda \in K$ une racine [6] du polynôme

$$\sum_{i=0}^{d} \varphi(p_i) T^i \in K[T]$$

de degré d, on peut définir φ' par

$$\varphi'(\sum a_i x^i) = \sum \varphi(a_i) \lambda^i.$$

□

Remarque 4.6. — La démonstration du théorème 4.4 implique en outre que si V est irréductible, on peut choisir l'ouvert dense $\Omega \subset \overline{f(V)}$ de telle manière que pour tout $w \in \Omega$, toute composante irréductible de $f^{-1}(w)$ est de dimension $\dim V - \dim \overline{f(V)}$.

---

[4] Remarquons que, puisque K est algébriquement clos, le célèbre théorème des zéros de Hilbert (Nullstellensatz) affirme que si $I(V) \neq K[X_1, \ldots, X_n]$ alors $V \neq \emptyset$. Cela revient à démontrer que si $I(V) \neq K[X_1, \ldots, X_n]$, il existe un morphisme de K-algèbre $K[V] \to K$. On peut supposer que $I(V)$ est un idéal maximal, alors $K[V]$ est un corps et est une algèbre de type fini sur K, c'est donc une extension algébrique de K. Mais K étant algébriquement clos on a alors $K[V] = K$, le théorème des zéros de Hilbert est donc démontré.

[5] Si le polynôme P n'existe pas, le résultat est immédiat.

[6] Nous utilisons ici que K est algébriquement clos. Le théorème de Chevalley est d'ailleurs faux sans cette hypothèse, exemple : $f : \mathbb{R} \to \mathbb{R}$ donnée par $f(x) = x^2$.

Théorème 4.7. — *Soit $f : V \to W$ une k-application régulière bijective entre deux k-variétés irréductibles, alors il existe un ouvert non vide (dense) U de W tel que f induise un k-isomorphisme de $f^{-1}(U)$ sur U.*

Démonstration. — Comme f est bijective, il découle de la remarque 4.6 que $\dim V = \dim W$. Soit Y un ouvert affine non vide de W et soit X un ouvert affine non vide de V contenu dans $f^{-1}(Y)$. Alors la restriction de f à X est une k-application régulière $X \to Y$ injective et le théorème découle des deux lemmes suivants. □

Lemme 4.8. — *Soient X, Y des k-variétés affines irréductibles de même dimension et $\varphi : X \to Y$ une k-application régulière. Alors, il existe un ouvert dense $U \subset Y$ contenu dans $\varphi(X)$ tel que, pour tout $u \in U$, l'ensemble $\varphi^{-1}(u)$ est fini, de cardinal $[K(Y) : K(X)]$.*

En particulier, si φ est injective, elle induit un isomorphisme $K(Y) \cong K(X)$.

Démonstration. — Puisque $\dim V = \dim W$ les corps $M = K(Y)$ et $L = K(X)$ on même degré de transcendance et l'extension L/M est algébrique, et de type fini (car L est de type fini sur K). Donc, d'après le théorème de l'élément primitif, il existe $f \in K[X]$ tel que $L = M[f]$.

Soient $x_1, \ldots, x_n$ des générateurs de la K-algèbre de type fini $K[X]$; d'après ce qui précède, chaque x_i s'écrit comme un polynôme P_i en f, à coefficients dans $K(Y)$. Soit $a \in K[Y]$ tel que les coefficients de tous les P_i appartiennent à $K[Y]_a$. Alors l'image inverse par φ de l'ouvert principal $U \subset Y$ défini par a est l'ouvert principal $O \subset X$ défini par $a \circ \varphi$, et le morphisme φ induit un isomorphisme

$$K[O] \xrightarrow{\sim} (K[U])[f],$$

car les x_i appartiennent à $(K[U])[f]$. Soit T une indéterminée; on a donc un morphisme surjectif (de $K[U]$-algèbres) $(K[U])[T] \twoheadrightarrow K[O]$. Son noyau n'est pas nécessairement un idéal principal de $(K[U])[T]$, mais on s'y ramène de la façon suivante.

Soit $P = T^d + a_1 T^{d-1} + \cdots + a_d$ le polynôme minimal de f sur $M = K(U)$, soit $b \in K[U]$ tel que les coefficients a_i de P appartiennent à $K[U]_b$, et soit $g = ab$. Alors, l'image inverse par φ de l'ouvert principal $U' \subset Y$ défini par g est l'ouvert principal $O' \subset X$ défini par $g \circ \varphi$, on a $P \in (K[U'])[T]$ et φ induit un isomorphisme

$$\varepsilon : K[O'] \xrightarrow{\sim} (K[U'])[T]/(P). \tag{31}$$

En effet, posons $A = K[U']$ et soit $Q \in A[T]$ tel que $Q(f) = 0$. Comme P est unitaire, on peut faire la division euclidienne de Q par P; alors le reste R vérifie $R(f) = 0$ et est nul ou bien de degré $< \deg P$. Comme P est le polynôme minimal de f dans $M[T]$, la seconde possibilité est exclue, donc $R = 0$ et P divise Q dans $A[T]$. Ceci prouve (31).

Alors,

$$O' = \{(y,t) \in U' \times K \ : \ P_y(t) = 0\},$$

où $P_y = T^d + a_1(y)T^{d-1} + \cdots + a_d(y)$ désigne le polynôme P dans lequel on a spécialisé les coefficients en y. Donc O' s'identifie à une sous-variété fermée de $U' \times K$ et, *via* cette identification, l'application φ est la restriction de la projection sur le premier facteur. En chaque $y \in U'$, la fibre $\varphi^{-1}(y)$ s'identifie donc à l'ensemble des racines (dans K !) du polynôme spécialisé P_y.

Il reste à voir qu'il existe un ouvert non vide U'' de U' tel que P_y ait d racines distinctes pour tout $y \in U''$. Ceci découle du polynôme discriminant comme suit.

Soient $f_1, f_2, \ldots, f_d$ (où $d = \deg P$ et $f = f_1$) les racines de P dans une clôture algébrique $\overline{L}$ de L. Comme l'extension L/M est séparable [7], les f_i sont deux à deux distincts, et donc le discriminant de P :

$$\operatorname{disc}(P) = \prod_{i<j} (f_i - f_j)^2$$

est un élément non nul de $\overline{L}$. En fait, comme c'est un polynôme symétrique en les f_i, c'est un polynôme en les fonctions symétriques élémentaires des f_i, qui sont les coefficients de P, donc des éléments de $K[U']$. Donc $\operatorname{disc}(P)$ est un élément non nul δ de $K[U']$.

Soit $U'' \subset U'$ l'ouvert principal associé à δ. Pour tout $y \in U''$, le discriminant de P_y égale $\delta(y)$, qui est non nul, donc P_y a d racines distinctes. Le théorème est démontré. $\square$

Lemme 4.9. — *Soit $\varphi : X \to Y$ une k-application régulière entre variétés irréductibles telle que*

- *$\varphi(X)$ contient un ouvert dense $U \subset Y$, et*
- *φ induit un isomorphisme $K(Y) \cong K(X)$.*

Alors, il existe un ouvert non-vide (dense) Ω de Y tel que φ induit un k-isomorphisme de $\varphi^{-1}(\Omega)$ sur Ω.

Démonstration. — Soit Ω un ouvert affine de Y contenu dans $\varphi(X)$, et soit O un ouvert affine non vide contenu dans $\varphi^{-1}(\Omega)$. Alors $\varphi(O)$ est dense dans Ω et l'application φ induit une injection $k[\Omega] \hookrightarrow k[O]$. Comme $k[O]$ est une k-algèbre de type fini, il existe $f_1, \ldots, f_n \in k[O]$ tels que $k[O] = k[\Omega][f_1, \ldots, f_n]$. Or, d'après l'hypothèse, on a $\operatorname{Frac}(k[\Omega]) = \operatorname{Frac}(k[O])$ (φ est définie sur k). Par conséquent, il existe $g \in k[\Omega]$ tel que $gf_i \in k[\Omega]$ pour tout i. Alors, $k[\Omega]_g = k[O]_g$ et, par conséquent, φ induit un isomorphisme entre les ouverts principaux dans O et Ω respectivement associés à $g \circ \varphi$ et g. $\square$

[7] On utilise ici que K est de caractéristique zéro.

4.2. Groupes algébriques

Un **groupe algébrique affine** G défini sur k (ou un **k-groupe**) est un sous-groupe Zariski fermé de $GL(n,K)$ défini sur k. Rappelons que le groupe linéaire $GL(n,K)$ est un ouvert principal de K^{n^2}. Il s'identifie à :

$$\{(A,t) \in M_n(K) \times K \ : \ (\det A)t = 1\},$$

qui est une sous-variété fermée de K^{n^2+1}, et l'on a

$$K[GL_n] = K[X_{1,1}, \ldots, X_{n,n}, \det{}^{-1}].$$

Si $I(G)$ est l'idéal de $K[GL_n]$ constitué de tous les polynômes qui s'annulent sur G, on a

$$K[G] = K[GL_n]/I(G).$$

En particulier si $f : G \to H$ est un **morphisme** entre deux groupes algébriques affines $G \subset GL(n,K)$ et $H \subset GL(m,K)$, c'est-à-dire un morphisme de groupe qui est aussi une application régulière entre les variétés algébriques affines G et H, alors il existe des polynômes

$$f_{k,l} = f_{f,l}(X_{1,1}, \ldots, X_{n,n}, \det{}^{-1}) \quad \text{pour} \quad k,l = 1, \ldots, m \tag{32}$$

tels que

$$f(g) = (f_{k,l}(g))_{k,l=1,\ldots,m}.$$

De plus, le morphisme f est défini sur k si les polynômes (32) sont tous à coefficients dans k.

Tous les groupes algébriques que nous considèrerons seront affines, même si cela n'est pas précisé [(8)]. Si G est défini sur k, l'ensemble des k-points $G_k = GL(n,k) \cap G$ est aussi un groupe.

***Exemple 4.10* (Groupes algébriques).** — 1) Le groupe additif $\mathbb{G}_a = (K,+)$. Il s'identifie au sous-groupe fermé

$$\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \ : \ x \in K \right\}$$

de $GL(2,K)$.

2) Le groupe multiplicatif $\mathbb{G}_m = (K^*, \times)$. Il s'identifie au sous-groupe fermé

$$\left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \ : \ x \in K^* \right\}$$

de $GL(2,K)$ et

$$K[\mathbb{G}_m] = K[X, X^{-1}].$$

[(8)] On pourrait définir un groupe algébrique comme une variété algébrique munie d'une structure de groupe telle que les applications $\mu : G \times G \to G$, $(x,y) \mapsto xy$, et $\kappa : G \to G$, $x \mapsto x^{-1}$ soient des applications régulières. On peut néanmoins montrer (voir [**1**]) que pour cette définition un groupe algébrique affine est isomorphe à un sous-groupe Zariski fermé de $GL(n,K)$.

3) Le groupe linéaire $GL(n, K)$.

4) Le groupe spécial linéaire

$$SL(n, K) = \{A \in M_n(K) \ : \ \det A = 1\}$$

est un sous-groupe fermé de $GL(n, K)$.

5) Le sous-groupe des matrices triangulaires supérieures :

$$B_n(K) = \{A \in GL(n, K) \ : \ A_{i,j} = 0, \quad \text{pour } i > j\}$$

est un sous-groupe fermé de $GL(n, K)$.

6) Le sous-groupe des matrices triangulaires unipotentes :

$$B_n(K) = \{A \in B_n(K) \ : \ A_{i,i} = 1, \quad \text{pour } i = 1, \ldots, n\}$$

est un sous-groupe fermé de $B_n(K)$ (et donc de $GL(n, K)$.

7) Le sous-groupe $D_n(K)$ des matrices diagonales est un sous-groupe fermé de $B_n(K)$ (et donc de $GL(n, K)$).

8) Plus compliqué et plus intéressant est le cas de $PGL(n)$. On a vu (voir §4.6.2) que l'on peut définir $PGL(n)$ comme le sous-groupe de $GL(M_n(K))$ formé des automorphismes d'algèbre. On sait, d'après le théorème de Skolem-Noether, que tout automorphisme de $M_n(K)$ est intérieur, et donc de déterminant un. Par conséquent $PGL(n)$ est un sous-groupe de $SL(M_n(K))$. On peut en outre caractériser les élément $g = (g_{pq}^{ij})_{1 \leq i,j,p,q \leq n}$ de $SL(M_n(K))$ qui sont des automorphismes d'algèbre par certaines relations polynômiales. Le groupe $PGL(n)$ est donc algébrique. D'autre part, l'application $\mathrm{Ad} : GL(n) \to PGL(n)$, $g \mapsto \mathrm{Int}(g)$ (où $\mathrm{Int}(g)$ est l'automorphisme intérieur $X \mapsto gXg^{-1}$) est un morphisme de groupes algébriques. En effet, on vérifie que

$$X_{pq}^{ij}(\mathrm{Int}(g)) = \det(g)^{-1} a_{pi}(g) C_{qj}(g),$$

où $a_{rs}(g)$ (resp. $C_{rs}(g)$) désigne le coefficient d'indice (r, s) de g (resp. de sa matrice des cofacteurs).

De plus, la restriction de Ad à $SL(n)$ est surjective, et donc $K[PGL(n)]$ s'identifie à la sous-algèbre de $K[SL(n)]$ engendrée par les éléments

$$a_{pi} C_{qj}, \quad \text{pour } i, j, p, q = 1, \ldots, n. \tag{33}$$

Ceci montre que le point du vue abstrait peut être utile : il peut être plus simple de considérer des variétés algébriques abstraites et voir $PGL(n, K)$ comme le quotient $GL(n, K)/K^*$.

Proposition 4.11. — *Soit G un groupe algébrique.*

1. *Les composante (Zariski-)connexe de G coïncident avec les composantes irréductibles.*
2. *Soit G^0 la composante (Zariski-)connexe de l'identité. Alors G^0 est un sous-groupe fermé distingué d'indice fini. Tout sous-groupe fermé connexe est contenu dans G^0.*

3. *Tout sous-groupe fermé d'indice fini contient* G^0.

Démonstration. — Soient $X_1, \ldots, X_m$ les composantes irréductibles de G contenant e. Notons $Y = X_1 \cdots X_m$ l'image de $X_1 \times \cdots \times X_m$ par le morphisme $(x_1, \ldots, x_m) \mapsto x_1 \cdots x_m$. Il découle alors du lemme 4.1 que Y est une partie irréductible de G qui contient e; elle est donc contenue dans un certain X_i, disons X_1. Comme chaque X_i est contenu dans Y, il en résulte $m = 1$. Donc e est contenu dans une unique composante irréductible; notons-la G^0. C'est un fermé de G, stable par multiplication d'après ce qui précède.

Pour tout $g \in G$, $g^{-1}G^0$ est une composante irréductible de G, car image de G^0 par un automorphisme de la variété algébrique G. De plus, si $g \in G^0$ alors $g^{-1}G^0$ contient e et est donc égal à G^0. Ceci prouve que G^0 est un sous-groupe fermé. De même, pour tout $g \in G$, gG^0g^{-1} est une composante irréductible de G qui contient e, et donc $gG^0g^{-1} = G^0$. Par conséquent, G^0 est un sous-groupe normal.

Comme chaque classe gG^0 est une composante irréductible de G et que G n'a qu'un nombre fini de composantes irréductibles (par noetherianité de $K[G]$), on a $[G : G^0] < \infty$. Les classes gG^0, étant en nombre fini, sont aussi ouvertes, et sont donc les composantes (Zariski-)connexes de G.

Enfin, si H est un sous-groupe fermé connexe, alors $H \cap G^0$ est ouvert et fermé et non-vide (il contient e), donc égal à H, d'où $H \subset G^0$. Ceci prouve les deux premiers points.

Prouvons le troisième point. Si H est un sous-groupe fermé d'indice fini, il est aussi ouvert, et est donc une réunion de composantes connexes de G. Comme $e \in H$, alors H contient G^0. □

4.3. Algèbre de Lie d'un groupe algébrique

Si G est définie par un système d'équations $\{P = 0\}$ où chaque $P \in k[M_n(K)]$ alors les différentielles $d_eP \in k[M_n(K)]$ et le lieu des zéros est un sous-espace de $M_n(K)$ définie sur k que l'on note $L(G)$.

Supposons pour simplifier $k = \mathbb{R}$ et $K = \mathbb{C}$. Un $\mathbb{R}$-groupe est en particulier un groupe de Lie. En supposant $G \subset GL(n, \mathbb{C})$, l'algèbre de Lie $L(G)$ de G est une sous-algèbre de $M_n(\mathbb{C})$ définie sur $\mathbb{R}$, c'est-à-dire

$$T_e(G_{\mathbb{R}}) = L(G) \cap M_n(\mathbb{R}).$$

Nous noterons $L(G)_{\mathbb{R}}$ cette algèbre réelle.

Pour tout $g \in G$ on a $gL(G)g^{-1} = L(G)$. Cela donne lieu à un $\mathbb{R}$-morphisme $G \to GL(L(G))$ défini par $g \mapsto \varphi_g$, où $\varphi_g(X) = gXg^{-1}$ pour $X \in L(G)$; on l'appelle la **représentation adjointe de G** et on la note Ad. On a aussi une $\mathbb{R}$-application régulière ad : $L(G) \to \mathrm{End}(L(G))$ donnée par

$$\mathrm{ad}X(Y) = [X, Y] = XY - YX,$$

appelée la **représentation adjointe de l'algèbre de Lie L(G)**. Rappelons que ad est la différentielle de Ad. Le **forme de Killing** est la forme bilinéaire symétrique B sur $L(G)$ donnée par

$$B(X, Y) = \mathrm{tr}(\mathrm{ad}X\mathrm{ad}Y), \quad \text{pour } X, Y \in L(G),$$

où tr est la trace usuelle dans l'algèbre matricielle $\mathrm{End}(L(G))$. Rappelons que B est invariante sous l'action adjointe de G.

4.4. Actions algébriques

Une **k-action algébrique** du k-groupe G sur une k-variété V est une action $G \times V \to V$ qui est régulière et définie sur k. On dira également que V est une **G-variété**. Une telle variété est **homogène** si l'action de G est **transitive**, c'est-à-dire si l'on a $V = G \cdot v$ pour un, et donc tout, $v \in V$.

Théorème 4.12. — *Les orbites $G \cdot v$ d'une k-action algébrique sont ouvertes et denses dans leur adhérence (pour la topologie de Zariski) $\overline{G \cdot v}$.*

Démonstration. — Le théorème 4.4 implique que l'orbite $G \cdot v$ contient un ouvert dense U de son adhérence $\overline{G \cdot v}$. Mais alors $G \cdot v$ est la réunion des ouverts gU et est donc ouvert (et dense) dans $\overline{G \cdot v}$. □

Comme un sous-groupe ouvert est aussi fermé [9], on en déduit le corollaire suivant.

Corollaire 4.13. — *L'image $\varphi(G)$ d'un k-morphisme de k-groupes $\varphi : G \to H$ est un k-sous-groupe de H.*

Remarque 4.14. — De plus, $\varphi(G^0)$ est un sous-groupe fermé de $\varphi(G)$, connexe et d'indice fini. Donc $\varphi(G^0) = \varphi(G)^0$.

Remarque 4.15. — Si $\varphi : G \to H$ est un morphisme de groupes algébriques, son noyau $\mathrm{Ker}\varphi$ est un sous-groupe fermé de G. La remarque 4.6 s'applique au morphisme $\varphi : G^0 \to \varphi(G^0)$. Chaque fibre étant un translaté de $\mathrm{Ker}\varphi$, on obtient

$$\dim \varphi(G) = \dim G - \dim \mathrm{Ker}\varphi.$$

Dans le même esprit, nous aurons besoin de la proposition suivante.

[9] En effet, si H est ouvert dans G il est ouvert dans son adhérence $\overline{H}$ et

$$\overline{H} = H \cdot H = H.$$

Proposition 4.16. — *Soit G un k-groupe, V, W deux G-variétés homogènes irréductibles, et $f : V \to W$ une k-application régulière bijective et G-équivariante* [10]. *Alors f est un k-isomorphisme.*

Démonstration. — D'après le théorème 4.7, il existe un ouvert non vide U de W tel que f induise un k-isomorphisme de $f^{-1}(U)$ sur U. Alors, pour tout $g \in G$, f induit un k-isomorphisme de $f^{-1}(gU)$ sur gU, et la proposition en résulte. □

Le théorème principal de cette section est le suivant.

Théorème 4.17. — *Soit G un k-groupe et H un k-sous-groupe. Alors il existe un k-morphisme de G dans $GL(K^n)$ et $D \in \mathbb{P}(k^n)$ tels que*

$$H = \{g \in G \ : \ g \cdot D = v\}.$$

Démonstration. — On note π l'action linéaire de G sur $K[G]$ donnée par

$$(\pi_g P)(x) = P(g^{-1}x) \quad \text{pour } P \in K[G], \quad g, x \in G.$$

Restreinte aux sous-espaces de dimension finie

$$K^d[G] = \{P \in K[G] \ : \ \deg P \leq d\}$$

cette action est une k-action linéaire.

Soit

$$I_H = \{P \in K[G] \ : \ P(H) = 0\}$$

l'idéal de H dans $K[G]$. Par noetherianité de $K[G]$, l'idéal I_H est de type fini. Soit d un entier tel que

$$I_H^d = I_H \cap K^d[G]$$

engendre l'idéal I_H. Considérons l'action linéaire π de G sur $K^d[G]$ décrite plus haut.

Lemme 4.18. — *On a*

$$H = \{g \in G \ : \ \pi_g(I_H^d) = I_H^d\}.$$

Démonstration. — L'ensemble I_H^d est un sous-espace vectoriel de $K^d[G]$. On a immédiatement

$$H \subset \{g \in G \ : \ \pi_g(I_H^d) = I_H^d\}.$$

Réciproquement, si $g \in G$ est tel que pour tout $P \in I_H^d$,

$$P(g^{-1} \cdot) \in I_H,$$

on a en particulier $P(g^{-1}) = 0$ pour tout $P \in I_H^d$, soit $g^{-1} \in H$. □

[10] C'est-à-dire que $f(g \cdot v) = g \cdot f(v)$, pour tous $v \in V$ et $g \in G$.

Soit p la dimension du sous-espace vectoriel $I_H^d \subset K^d[G]$. Notons

$$E = \bigwedge^p \left(K^d[G]\right) \quad \text{et} \quad D = \bigwedge^p \left(I_H^d\right).$$

Alors, G agit linéairement sur E *via* $\bigwedge^p \pi$ et

$$\bigwedge^p \pi(g) \cdot D = D \Leftrightarrow \pi_g(I_H^d) = I_H^d.$$

Donc [11]:

$$H = \{g \in G \ : \ \bigwedge^p \pi(g) \cdot D = D\}.$$

□

On déduit des théorèmes 4.17 et 4.12 que G/H a une structure de k-variété quasi-projective; on montre plus précisément le théorème suivant.

Théorème 4.19. — *Soit G un k-groupe et H un k-sous-groupe. Alors, le quotient G/H a une structure de k-variété quasi-projective, et lorsque $X(H) = \{1\}$ elle est quasi-affine* [12]. *On a unicité de G/H comme G-variété homogène.*

Démonstration. — L'existence de la structure quasi-projective (resp. quasi-affine) découle immédiatement des théorèmes 4.17 et 4.12 ainsi que de la remarque 4.21. Notons $V = G/H$ la variété algébrique ainsi obtenue; pour cette structure l'application π est régulière et définie sur k. L'unicité de la structure de G-variété homogène est un corollaire de la proposition 4.16; on montre plus généralement la propriété universelle suivante. □

***Remarque 4.20* (Propriété universelle)**. — Pour toute k-application régulière G-équivariante $\alpha : G \to W$ vers une G-variété homogène W telle que $\alpha(h) = \alpha(1)$, pour tout $h \in H$, il existe une unique k-application régulière (G-équivariante) $\beta : G/H \to W$ telle que $\alpha = \beta \circ \pi$, où π est la projection $G \to G/H$.

Démonstration. — Soit $\alpha : G \to W$ une k-application régulière G-équivariante vers une G-variété homogène W telle que $\alpha(h) = \alpha(1)$, pour tout $h \in H$. Montrons l'existence d'une k-application régulière (G-équivariante) $\beta : V \to W$ telle que $\alpha = \beta \circ \pi$ (nécessairement unique, puisque π est surjective). Considérons le morphisme $\theta = \pi \times \alpha : G \to V \times W$. Comme θ est G-équivariante, la démonstration du théorème

[11] Observons que le groupe H agit sur D par un k-morphisme $H \to k^*$.
[12] C'est-à-dire que c'est un ouvert d'une variété algébrique affine.

4.12 implique que $X = \theta(G)$ est ouvert dans son adhérence, et est donc une sous-variété localement fermée de $V \times W$. Considérons le diagramme commutatif de k-applications régulières G-équivariantes :

$$\begin{array}{ccccccc} G & \xrightarrow{\theta=(\pi,\alpha)} & X & \xrightarrow{\tau} & V \times W & \xrightarrow{\mathrm{pr}_W} & W \\ \pi \downarrow & & p \downarrow & & \mathrm{pr}_V \downarrow & & \\ V & = & V & = & V & & \end{array}$$

où p est la restriction de pr_V à X, et τ est l'immersion naturelle. Comme $p \circ \theta = \pi$, alors p est surjective. Elle est aussi injective : si $\pi(g) = \pi(g')$ alors $g' \in gH$ et donc $\alpha(g') = \alpha(g)$ (par G-équivariance). Donc p est bijective et la proposition 4.16 implique que p est un isomorphisme de k-variétés. Alors, comme $\alpha = \mathrm{pr}_W \circ \tau \circ \theta$, le morphisme $\beta = \mathrm{pr}_W \circ \tau \circ p^{-1}$ vérifie $\beta \circ \pi = \alpha$. □

Un **caractère** d'un k-groupe est un k-morphisme vers le groupe multiplicatif $\mathbb{G}_m$. On note $X_k(G)$ l'ensemble des caractères d'un k-groupe G; c'est un groupe abélien, la multiplication étant définie par $(\chi\chi')(g) = \chi(g)\chi'(g)$.

Remarque 4.21. — Si, dans le théorème 4.17 on suppose de plus $X_k(H) = \{1\}$, on peut remplacer l'action projective par l'action linéaire : il existe $v \in k^n$ tel que

$$H = \{g \in G \ : \ g \cdot v = v\},$$

(voir la note de bas de page à la fin de la démonstration du théorème 4.17).

Soit V un k-espace vectoriel sur lequel G agit *via* un k-morphisme $G \to GL(V)$. Pour tout $\chi \in X(G)$, on note

$$V_\chi = \{v \in V \ : \ gv = \chi(g)v, \quad \forall g \in G\}.$$

***Proposition 4.22* (Lemme de Dedekind)**. — *Soit G un groupe quelconque.*

1. *L'ensemble $\Theta(G) = \mathrm{Hom}_{\mathrm{gpes}}(G, k^*)$ est une partie libre de k^G (= fonctions $G \to k$).*
2. *Pour tout G-module V, la somme $\sum_{\chi \in \Theta(G)} V_\chi$ est directe.*

Démonstration. — 1) Supposons par l'absurde qu'il existe une relation de dépendance linéaire

$$a_1\chi_1 + \ldots + a_n\chi_n = 0,$$

avec n minimal (et $n \geq 2$). Soient $g, h \in G$. Alors

$$\sum_i a_i\chi_i(g)\chi_i(h) = \sum_i a_i\chi_i(gh) = 0.$$

Fixant un g tel que $\chi_1(g) \neq \chi_2(g)$, on obtient donc une nouvelle relation de dépendance linéaire non triviale :

$$\sum_{i=2}^{n} a_i(\chi_i(g) - \chi_1(g))\chi_i = 0.$$

Cette relation a au plus $n-1$ termes en contradiction avec la minimalité de n.

2) La démonstration est identique. Partant d'une relation de dépendance linéaire

$$v_{\chi_1} + \ldots + v_{\chi_n} = 0$$

avec n minimal. On utilise, comme au 1), que pour tout g,

$$\sum_i \chi_i(g) v_{\chi_i} = g\left(\sum_i v_{\chi_i}\right) = 0.$$

□

Corollaire 4.23. — *$X_k(G)$ est une partie libre de $k[G]$.*

Lorsque le sous-groupe H est normal on peut préciser la remarque 4.21 et obtenir le théorème suivant.

Théorème 4.24. — *Soit H un k-sous-groupe distingué d'un k-groupe G. Alors la k-variété G/H est un groupe algébrique (affine).*

Démonstration. — Soient E et D comme dans la démonstration du théorème 4.17. Alors H agit sur D par un caractère $\chi \in X_k(H)$. Soit $g \in G$. Comme H est distingué dans G, alors

$$h \mapsto \chi_1(ghg^{-1}) \quad \text{est un caractère de } H, \text{ noté } g\chi_1,$$

et pour tout $v \in D$ et $h \in H$, on a

$$h \cdot gv = g(g^{-1}hg)v = (g\chi_1)(h)gv.$$

Ceci montre que $g(E_{\chi_1}) \subset E_{g\chi_1}$. On montre de même que

$$g'(E_{g\chi_1}) \subset E_{g'g\chi_1}, \quad \forall g, g' \in G.$$

Par conséquent, la somme V des $E_{g\chi_1}$ est G-stable. Or cette somme est directe, d'après la proposition 4.22, donc il existe $\chi_2, \ldots, \chi_n \in X_k(H)$ tels que $V = E_{\chi_1} \oplus \ldots \oplus E_{\chi_n}$. Notons $\rho : G \to GL(V)$ la représentation de G dans V. Alors $\psi = \mathrm{Ad}_{GL(V)} \circ \rho$ est une représentation de G dans $\mathrm{End}(V)$, c'est-à-dire que pour $u \in \mathrm{End}(V)$ et $g \in G$, on a

$$\psi(g)u = \rho(g) \circ u \circ \rho(g^{-1}).$$

Soit $A = \bigoplus_i \mathrm{End}(E_{\chi_i})$, la sous-algèbre de $\mathrm{End}(V)$ formée des endomorphismes qui préservent chaque E_{χ_i}. Comme $\rho(G)$ permute les E_{χ_i}, alors A est stable par $\psi(G)$, et l'on obtient donc une représentation $\phi : G \to GL(A)$ qui est encore définie sur k. Montrons que $\mathrm{Ker}\phi = H$.

Si $h \in H$, alors $\rho(h)$ agit scalairement sur chaque E_{χ_i} et commute donc à A, d'où $\phi(h) = 1$. Donc $H \subset \mathrm{Ker}\phi$. Réciproquement, soit $g \in \mathrm{Ker}\phi$. Alors $\rho(g)$ est central dans A et donc agit scalairement sur chaque E_{χ_i}. En particulier $\rho(g)$ laisse D stable, d'o'u $g \in H$.

Notons $G' = \phi(G)$, d'après le corollaire 4.13 c'est un k-sous-groupe de $GL(V)$. Le morphisme ϕ induit une k-application régulière G-équivariante $\alpha : G \to G'$ telle que $\alpha(h) = \alpha(1)$, pour tout $h \in H$. D'après la remarque 4.20, il existe donc une k-application régulière, G-équivariante et bijective de G/H vers G'. D'après la proposition 4.16 celle-ci induit enfin un k-isomorphisme de variétés qui est aussi un isomorphisme de groupes. □

4.5. Décomposition de Jordan

Soit $g \in GL_n(K)$.

Proposition 4.25. — *L'élément g s'écrit*

$$g = g_s g_u = g_u g_s,$$

avec g_s **semisimple***, c'est-à-dire diagonalisable (sur K), et g_u* **unipotent***, c'est-à-dire $(g_u - I_n)^n = 0$.*

Démonstration. — Puisque $g \in M_n(K)$ avec K algébriquement clos, il est bien connu qu'il existe une matrice X_s semisimple et une matrice X_n nilpotente telles que

$$g = X_s + X_n \quad \text{avec} \quad X_s X_n = X_n X_s.$$

L'écriture $g = X_s + X_n$ est la décomposition de Jordan (additive) usuelle de la matrice g. Il est de plus bien connu qu'il existe des polynômes P et Q sans termes constants tels que

$$X_s = P(g) \quad \text{et} \quad X_n = Q(g).$$

Remarquons maintenant que comme g et X_s ont les mêmes valeurs propres alors $X_s \in GL_n(K)$. On pose alors

$$g_s = X_s \quad \text{et} \quad g_u = I_n + X_s^{-1} X_n.$$

□

Remarque 4.26. — Lorsque $k = \mathbb{R}$ la décomposition de Jordan additive reste valable et si $g \in GL_n(k)$ on a alors g_s et $g_u \in GL_n(k)$. Cela reste plus généralement vrai lorsque le corps est **parfait**, c'est-à-dire tel que toute extention finie de k est séparable; c'est par exemple le cas de tous les corps de caractéristique zéro. On pourra donc dorénavant parler de la décomposition de Jordan sur k.

Attention : l'élément g_s est alors semisimple (diagonalisable sur K, cloture algébrique de k) mais pas nécessairement diagonal sur k.

Lorsque $k = \mathbb{R}$ on peut de plus écrire

$$g_s = g_h g_e = g_h g_e,$$

où g_e est **elliptique** (c'est-à-dire semisimple avec $\mathrm{Sp}(g_e) \subset \{z \in \mathbb{C} \ : \ |z| = 1\}$) et g_h est **hyperbolique** (c'est-à-dire semisimple avec $\mathrm{Sp}(g_h) \subset]0, +\infty[$).

Proposition 4.27. — *Les éléments g_s et g_u (ainsi que g_e et g_h, lorsque $k = \mathbb{R}$) sont uniquement déterminés par g. Ils laissent stable tout sous-espace vectoriel invariant par g. En outre, ils commutent à tout endomorphisme qui commute à g.*

Démonstration. — Par construction, g_s et g_u laissent stable tout sous-espave vectoriel invariant par g et commutent à tout endomorphisme qui commute à g. On en déduit l'unicité : si g'_s et g'_u vérifient les mêmes conditions alors ils commutent à g et donc à g_s et g_u et par conséquent $g_s^{-1}g'_s = g_u(g'_u)^{-1}$ est à la fois semisimple et unipotent, donc égal à l'identité. □

Considérons maintenant $G \subset GL_n(K)$ un k-sous-groupe.

Lemme 4.28. — 1. *Si g est dans G, alors g_s et g_u aussi.*
2. *Supposons $k = \mathbb{R}$. Si g est dans $G_{\mathbb{R}}$, alors g_e, g_h et g_u aussi.*

Démonstration. — 1) Soient $V = k^n$,

$$I = \{P \in k[\mathrm{End}V] \ : \ P_{|G} = 0\},$$

$$k[\mathrm{End}V]^d = \{P \in k[\mathrm{End}V] \ : \ \deg P \leq d\}$$

et

$$I^d = I \cap k[\mathrm{End}V]^d.$$

On note R_g l'action de g sur $k[\mathrm{End}V]^d$ donnée par

$$R_g(P)(x) = P(xg).$$

On a $\mathrm{End}(V) \cong V \otimes V^*$, et comme G-module $k[\mathrm{End}V]$ s'identifie donc à l'algèbre symmétrique $S(E)$ où E est la somme directe de $\dim V$ copies de V. Par suite, si g est semisimple (resp. unipotent) alors R_g l'est aussi. De sorte que l'égalité

$$R_g = R_{g_s} R_{g_u}$$

est la décomposition de Jordan de R_g. Or $R_g(I^d) = I^d$. Donc $R_{g_s}(I^d) = I^d$, par la proposition ci-dessus. D'où $g_s \in G$.

2) On procède comme en 1). □

Remarque 4.29. — Soit $\mathfrak{g}$ l'algèbre de Lie de G. Écrivons $g_u = \exp(X_n)$ avec X_n nilpotent et $g_h = \exp(X_h)$ avec X_h **hyperbolique** (c'est-à-dire X_h semisimple et $\mathrm{Sp}(X_h) \subset \mathbb{R}$). Le même argument prouve que X_n et X_h sont dans $\mathfrak{g}$.

On note toujours π l'action linéaire de G sur $K[G]$ donnée par

$$(\pi_g P)(x) = P(g^{-1}x) \quad \text{pour } P \in K[G], \quad g, x \in G.$$

Proposition 4.30. — *Un élément g de G est semisimple (resp. unipotent) si et seulement si π_g l'est dans tous les $GL(K^d[G])$.*

Remarque 4.31. — Si $k = \mathbb{R}$, on a un énoncé analogue avec g hyperbolique (resp. elliptique).

Démonstration. — La démonstration du lemme 4.28 montre que si g est semisimple (resp. unipotent) alors l'application induite sur $k[\mathrm{End}V]$ l'est aussi. On en déduit facilement l'implication directe; montrons la réciproque. D'après la décomposition de Jordan et le lemme 4.28,

$$g = g_s g_u = g_u g_s$$

avec $g_s \in G$ semisimple et $g_u \in G$ unipotent. Donc

$$\pi(g) = \pi(g_s)\pi(g_u) = \pi(g_u)\pi(g_s).$$

Si $\pi(g)$ est semisimple, $\pi(g_u) = 1$ donc $g_u = 1$ et g est semisimple. On procède de même si $\pi(g)$ est unipotent. □

Corollaire 4.32. — *L'image par un k-morphisme $\varphi : G \to H$ d'un élément semisimple (resp. unipotent) est encore semisimple (resp. unipotent).*

Démonstration. — Puisque l'image $\varphi(G)$ est un k-sous-groupe de H, il suffit de considérer les deux cas :

- φ est injectif, mais alors $K[H]$ se surjecte sur $K[G]$ donc $\pi_{\varphi(g)}$ agit trivialement sur le noyau de la projection $K[H] \to K[G]$ et comme π_g sur son supplémentaire.
- φ est surjectif, mais alors $K[H]$ s'injecte dans $K[G]$ donc $\pi_{\varphi(g)}$ agit sur $K[H]$ comme la restriction de π_g.

Dans tous les cas la proposition précédente permet de conclure. □

En particulier, la décomposition de Jordan est indépendante de la réalisation matricielle du groupe G.

4.6. Théorie des répliques

Cette théorie due à Chevalley caractérise parmi les sous-algèbres de Lie $\mathrm{End}(\mathbb{R}^n)$ celles qui sont associées à un sous-groupe algébrique de $GL_n(\mathbb{R})$. Notons que cette théorie se généralise à tout corps de caractéristique 0.

Lemme 4.33. — *Soient $H_1, \ldots, H_p$ des sous-groupes algébriques irréductibles d'un groupe algébrique G et H le groupe engendré par les H_i. Alors H est un sous-groupe algébrique irréductible de G.*

Démonstration. — Soient $M^1 = H_1 \cdots H_p$ et, pour $n \geq 1$, $M^{n+1} = M^n \cdot M^1$ et F^n l'adhérence de Zariski de M^n. On a

$$H = \bigcup_{n \geq 1} M^n.$$

Comme les H_i sont irréductibles, les F^n aussi. La suite croissante F^n est donc stationnaire. Soit $F = \bigcup_{n \geq 1} F^n$ et $m \geq 1$ tel que $F = F^m$. Le sous-ensemble F est l'adhérence de Zariski de H. D'après le théorème 4.4, M^m contient un ouvert de Zariski dense de F. Donc, pour tout f dans F,

$$f(M^m)^{-1} \cap M^m \neq \emptyset.$$

D'où $F = M^{2m} = H$. □

Remarque 4.34. — La conclusion du lemme est fausse en général si les H_i ne sont pas irréductibles. Prendre par exemple le groupe engendré par deux réflexions.

La conclusion du lemme est fausse en général pour les points réels. Prendre par exemple $G = SO(n, 1)$, $H_1 = SO(n)$ et H_2 un conjugué (différent) de H_1. On a alors $H = SO^+(n, 1)$ qui n'est pas algébrique.

Supposons dorénavant $k = \mathbb{R}$ ou $\mathbb{C}$. Une sous-algèbre de Lie $\mathfrak{g}$ de $\mathrm{End}(k^n)$ est dite **algébrique** si $\mathfrak{g}$ est l'algèbre de Lie d'un sous-groupe Zariski fermé de $GL(k^n)$.

Pour X dans $\mathrm{End}(k^n)$, on note $\mathfrak{g}_X$ la plus petite algèbre de Lie algébrique de $\mathrm{End}(k^n)$ contenant X. Les éléments de $\mathfrak{g}_X$ sont appelés les **répliques** de X.

Lemme 4.35. — *1) Une sous-algèbre de Lie $\mathfrak{g}$ de $\mathrm{End}(\mathbb{R}^n)$ est algébrique si et seulement si $\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$ est algébrique.*

2) Une algèbre de Lie $\mathfrak{h} \subset \mathrm{End}(k^n)$ engendrée par des sous-algèbres de Lie algébriques est encore algébrique.

Démonstration. — 1) En effet, un groupe algébrique $G \subset GL(\mathbb{C}^n)$ défini sur $\mathbb{R}$ est stable par conjugaison complexe.

2) Par 1), on peut supposer $k = \mathbb{C}$. Cela résulte alors du lemme 4.33. □

Lemme 4.36. — *Soit $X \in \mathrm{End}(k^n)$.*

1. *Si X est nilpotent, alors $\mathfrak{g}_X$, alors $\mathfrak{g}_X = k \cdot X$.*
2. *Si X est diagonale :*

$$X = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix},$$

alors

$$\mathfrak{g}_X = \left\{ \begin{pmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{pmatrix} \; : \; \forall m_i \in \mathbb{Z}, \quad \sum_i m_i \lambda_i = 0 \Rightarrow \sum_i m_i \mu_i = 0 \right\}.$$

3. *Si $X = X_s + X_n$ (décomposition de Jordan), on a $\mathfrak{g}_X = \mathfrak{g}_{X_s} \oplus \mathfrak{g}_{X_n}$.*
4. *Si $k = \mathbb{R}$ et $X = X_e + X_h + X_n$ (décomposition de Jordan), on a $\mathfrak{g}_X = \mathfrak{g}_{X_e} \oplus \mathfrak{g}_{X_h} \oplus \mathfrak{g}_{X_n}$.*

Démonstration. — D'après le 1) du lemme 4.35, on peut supposer $k = \mathbb{C}$ (sauf pour le point 4.).

1. On peut supposer X sous forme de blocs de Jordan. Il est alors clair que

$$\{\exp(tX) \; : \; t \in \mathbb{C}\} = \{1 + tX + \ldots + t^n X^n \; : \; t \in \mathbb{C}\}$$

est Zariski fermé.

2. Soit $D \subset GL(\mathbb{C}^n)$ le groupe algébrique des matrices diagonales. Pour d dans D, on note $d_1, \ldots, d_n$ les coefficients diagonaux de D. Soient

$$A = \{m \in \mathbb{Z}^n \; : \; \sum_i m_i \lambda_i = 0\}$$

et

$$I_X = \{P \in \mathbb{C}[D] \; : \; P(\exp(tX)) = 0, \quad \forall t \in \mathbb{C}\}.$$

Si on écrit

$$P(d) = \sum_{m \in \mathbb{Z}^n} a_m d_1^{m_1} \cdots d_n^{m_n},$$

on a

$$P(\exp(tX)) = \sum_{m \in \mathbb{Z}^n} a_m e^{t(\sum_i m_i \lambda_i)}.$$

Donc

$$P \in I_X \Leftrightarrow \forall m \in \mathbb{Z}^n, \qquad \sum_{m' \in m + A} a_{m'} = 0.$$

On en déduit l'équivalence

$$Y = \begin{pmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{pmatrix} \in \mathfrak{g}_X \Leftrightarrow \forall m \in A, \quad \sum_i m_i \mu_i = 0.$$

3. Il résulte de la remarque 4.29 que X_s et X_n sont dans $\mathfrak{g}_X$. Or comme $[X_s, X_n] = 0$, on a $[\mathfrak{g}_{X_s}, \mathfrak{g}_{X_n}] = 0$. Donc $\mathfrak{g}_{X_s} \oplus \mathfrak{g}_{X_n}$ est une sous-algèbre de Lie. D'après le 2) du lemme 4.35, elle est algébrique. Donc $\mathfrak{g}_X = \mathfrak{g}_{X_s} \oplus \mathfrak{g}_{X_n}$.

4. La démonstration est similaire à celle de 3. □

***Théorème 4.37* (Chevalley).** — *($k = \mathbb{R}$ ou $\mathbb{C}$) Une sous-algèbre de Lie $\mathfrak{g}$ de* $\mathrm{End}(k^n)$ *est algébrique si et seulement si elle admet une base (X_p) telle que :*

– *soit* X_p *est nilpotent,*
– *soit* X_p *est semisimple et* $\mathrm{Sp}(X_p) \subset \mathbb{Z}$*,*
– *soit* X_p *est semisimple et* $\mathrm{Sp}(X_p) \subset i\mathbb{Z}$*.*

(Lorsque $k = \mathbb{C}$*, ce dernier cas est inutile car on peut remplacer* X_p *par* iX_p*.)*

Démonstration. — ($\Leftarrow$) D'après le lemme 4.35, on peut supposer $k = \mathbb{C}$ et $\dim \mathfrak{g} = 1$. Cela résulte alors du lemme 4.36.

($\Rightarrow$) On peut supposer $\mathfrak{g} = \mathfrak{g}_X$. D'après les points 3. et 1. du lemme 4.36, on peut supposer X semisimple.

Si $k = \mathbb{C}$, dans une bonne base de $\mathbb{C}^n$, $\mathfrak{g}_X$ est un sous-espace vectoriel des matrices diagonales défini par des équations linéaires à coefficients entiers (voir 2. du lemme 4.36). Donc il admet une base formée de matrices diagonales à coefficients entiers.

Si $k = \mathbb{R}$. Par le point 4. du lemme 4.36, on peut supposer X hyperbolique ou elliptique. Si X est hyperbolique, le même raisonnement que ci-dessus est valable. Si X est elliptique, on écrit

$$X = \begin{pmatrix} \sigma_{\lambda_1} & & & & & \\ & \ddots & & & & \\ & & \sigma_{\lambda_p} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \quad \text{où} \quad \sigma_\lambda = \begin{pmatrix} 0 & -\lambda \\ \lambda & 0 \end{pmatrix}$$

dans une base convenable de $\mathbb{R}^n$. On a alors

$$\mathfrak{g}_X = \left\{ Y = \begin{pmatrix} \sigma_{\mu_1} & & & & & \\ & \ddots & & & & \\ & & \sigma_{\mu_p} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} : \forall m_i \in \mathbb{Z}, \quad \sum_i m_i \lambda_i = 0 \Rightarrow \sum_i m_i \mu_i = 0 \right\}.$$

Donc $\mathfrak{g}_X$ admet une base formée de matrices Y pour lesquelles $\mu_1, \ldots, \mu_p$ sont entiers.

$\square$

4.7. Conclusion : un peu de vocabulaire

Pour clore ce chapitre nous donnons un peu de vocabulaire important.

Un k-groupe **unipotent** est un k-groupe dont tous les éléments sont unipotents. Il existe alors une base de k^n pour laquelle c'est un groupe de matrices triangulaires supérieures.

Un **tore** est un k-groupe abélien Zariski-connexe formé d'éléments semisimples. Un tore T défini sur $\mathbb{R}$ est dit **déployé** (resp. **anisotrope**) si $T_{\mathbb{R}}$ ne contient que des éléments hyperboliques. (resp. elliptiques).

Un groupe algébrique est dit **réductif** si sa composante neutre G^0 est égale au produit presque directe $S \cdot H$ d'un tore S central par (presque directe signifie que l'intersection $H \cap S$ est finie). Le nom de cette propriété provient de ce qu'en caractéristique 0 elle est équivalente à la complète réductibilité des représentations de G.

CHAPITRE 5

ÉPILOGUE : ESPACES SYMÉTRIQUES

5.1. Définitions

Soit X une variété riemannienne connexe.

On dit que X est *homogène* si le groupe $\mathrm{Isom}(X)$ des isométries de X opère transitivement sur X, *i.e.* pour tous $x, y \in X$, il existe $g \in \mathrm{Isom}(X)$ tel que $gx = y$.

Exemple 5.1. —

- La sphère $\mathbb{S}^n$. La composante neutre de $\mathrm{Isom}(\mathbb{S}^n)$ s'identifie au groupe $SO(n+1)$ des rotations. Un point quelconque de $\mathbb{S}^n$ peut être envoyé sur n'importe quel autre par une rotation; la sphère $\mathbb{S}^n$ est donc homogène.
- L'espace euclidien $\mathbb{R}^n$. Le groupe des isométries préservant l'orientation s'identifie au produit semi-direct $SO(n) \ltimes \mathbb{R}^n$. Tout point de $\mathbb{R}^n$ peut être translaté vers un autre; l'espace $\mathbb{R}^n$ est donc homogène.
- L'espace hyperbolique
$$\mathbb{H}^n = \{x \in \mathbb{R}^{n+1} \ : \ \underbrace{x_1^2 + \ldots + x_n^2 - x_{n+1}^2}_{=:q(x)} = -1, \ x_{n+1} > 0\}$$
muni de la métrique riemannienne induite par q sur chaque espace tangent. La composante neutre de $\mathrm{Isom}(\mathbb{H}^n)$ s'identifie au groupe $SO^+(n,1)$ des transformations qui préservent la forme quadratique q et la nappe supérieure de l'hyperboloïde $q = -1$.

La variété X est dit *symétrique* si pour tout $p \in X$, la symétrie géodésique en p, définie localement *via* l'application exponentielle par $\exp_p(v) \mapsto \exp_p(-v)$, s'étend en une isométrie s_p de X.

Lemme 5.2. — *Soit X une variété riemannienne symétrique. Alors X est un espace complet et homogène.*

Démonstration. — La variété X est géodésiquement complète : on peut prolonger les géodésiques grâce à la symétrie s_p.

Montrons que X est homogène. Soient x et y dans X. Par x et y il passe un segment géodésique (X est connexe et complet); notons p son milieu. Alors $s_p(x) = y$. □

Proposition 5.3. — *La variété X est symétrique si et seulement si X est homogène et il existe une isométrie involutive $\phi \in \mathrm{Isom}(X)$ avec un point fixe isolé.*

Démonstration. — L'implication directe est immédiate : la symétrie autour d'un point p quelconque est involutive et p est un point fixe isolé.

Montrons l'implication réciproque. Si $g \in \mathrm{Isom}(X)$ alors $g\phi g^{-1}$ est une isométrie involutive avec un point fixe isolé en gp. Il suffit donc pour conclure de montrer que ψ est (localement égale à) la symétrie géodésique en p.

Puisque $\phi(p) = p$, on a $d_p(\phi^2) = (d_p\phi)^2$. Et puisque $\phi^2 = id$ on conclut que $(d_p\phi)^2 = id$. En particulier l'application linéaire $d_p\phi : T_pX \to T_pX$ est diagonalisable et ses valeurs propres appartiennent à $\{\pm 1\}$. Montrons par l'absurde que $d_p\phi = -id$. Sinon il existe un vecteur $v \in T_pX$ tel que $d_p\phi(v) = v$. Soit γ la géodésique telle que $\gamma(0) = p$ et $\gamma'(0) = v$. Puisque ϕ est une isométrie, $\phi \circ \gamma$ est encore une géodésique. Mais $\phi \circ \gamma(0) = \phi(p) = p$ et $(\phi \circ \gamma)'(0) = d_p\phi(v) = v$. Donc $\phi \circ \gamma = \gamma$ et p n'est pas un point fixe isolé. C'est absurde.

De la même manière on montre que $\phi \circ \gamma$ est la géodésique γ parcouru dans le sens inverse. Autrement dit, ϕ est (localement égale à) la symétrie géodésique en p. □

Exemple 5.4. — Les espaces $\mathbb{S}^n$, $\mathbb{R}^n$ et $\mathbb{H}^n$ sont symétriques.

5.2. Construction

Soient X un espace symétrique, $p \in X$, $G = \mathrm{Isom}(X)^0$ et $K = \mathrm{Stab}_G(p)$. Puisque $\mathrm{Isom}(X)$ opère transitivement sur X et que X est connexe, le groupe G opère lui aussi transitivement sur X. On peut identifier X à l'espace quotient G/K; notons que le groupe K est compact.

Exemple 5.5. —

- Pour $X = \mathbb{S}^n$, on a $G = SO(n+1)$ et on peut prendre $K = \mathrm{Stab}_G(e_{n+1}) = SO(n)$ de sorte que $\mathbb{S}^n = SO(n+1)/SO(n)$. Noter que si $\sigma = \mathrm{diag}(1, \ldots, 1, -1) \in O(n)$, on a $\sigma^2 = id$ et K est le centralisateur de σ dans G.
- Pour $X = \mathbb{R}^n$, on a $G = SO(n) \ltimes \mathbb{R}^n$ et on peut prendre $K = \mathrm{Stab}_G(0) = SO(n)$ de sorte que $\mathbb{R}^n = (SO(n) \ltimes \mathbb{R}^n)/SO(n)$. Noter que l'application $\sigma : (k, v) \mapsto (k, -v)$ est un automorphisme involutif de G dont le centralisateur est K.
- Pour $X = \mathbb{H}^n$, on a $G = SO^+(n, 1)$ et on peut prendre $K = \mathrm{Stab}_G((0, \ldots, 0, 1)) = SO(n)$ de sorte que $\mathbb{R}^n = SO^+(n, 1)/SO(n)$. Noter que si $\sigma = \mathrm{diag}(1, \ldots, 1, -1) \in O(n, 1)$, on a $\sigma^2 = id$ et K est le centralisateur de σ dans G.

Proposition 5.6. — *Soient G un groupe de Lie connexe, K un sous-groupe compact et σ un automorphisme involutif de G tel que K soit un sous-groupe ouvert du centralisateur de σ dans G. Alors, le quotient $X = G/K$ a une structure d'espace symétrique telle que l'application $\tau(gK) = \sigma(g)K$ est une isométrie involutive de G/K avec eK pour point fixe isolé.*

Démonstration. — Puisque K est compact il existe une métrique riemannienne G-invariante sur G/K. Il suffit en effet de choisir un produit scalaire quelconque sur $T_{eK}X$ et de le moyenner sous l'action de K grâce au choix d'une mesure de Haar sur K. On obtient ainsi un produit scalaire K-invariant que l'on étend en une métrique riemannienne sur X en le translatant par G.

La même opération appliquée à G^+/K^+ – où $G^+ = G \rtimes \langle\sigma\rangle$ et $K^+ = K \times \langle\sigma\rangle$ – plutôt qu'à G/K permet de supposer que la métrique riemannienne sur X est en outre τ-invariante.

Il est clair que eK est un point fixe de τ. Montrons qu'il est isolé. Considérons donc gK un point fixe de τ avec $g \approx e$. Alors $\sigma(g) \in gK$ de sorte que l'on peut écrire $\sigma(g) = gk$ avec $k \in K$. Puisque σ est une involution qui centralise K (et que σ est un automorphisme), on a :

$$g = \sigma^2(g) = \sigma(gk) = \sigma(g)\sigma(k) = (gk)k = gk^2.$$

Donc $k^2 = e$. Mais puisque $g \approx e$ et $\sigma(e) = e$ on a $\sigma(g) \approx g$ donc $k = g^{-1}\sigma(g) \approx e$. Puisque $k^2 = e$ on en déduit que $k = e$. Donc $\sigma(g) = g$ et g centralise σ. Mais $g \approx e$ et K est ouvert dans le centralisateur de σ donc $g \in K$. □

Exemple 5.7. — Soient $G = SL(n,\mathbb{R})$, $K = SO(n)$ et $\sigma(g) = {}^t g^{-1}$ (qui correspond à l'involution de Cartan). La proposition implique que G/K est un espace symétrique.

De même les quotients $SL(n,\mathbb{C})/SU(n)$ et $SO(p,q)_0/(SO(p) \times SO(q))$ fournissent d'autres exemples d'espaces symétriques.

La proposition s'applique plus généralement lorsque G est un groupe semisimple réel et σ est une involution de Cartan. On peut alors montrer une sorte de réciproque (due à Cartan) :

Théorème 5.8. — *Soit X un espace symétrique simplement connexe. Alors*

$$X = X_0 \times X_1 \times \ldots \times X_n$$

où X_0 est un espace euclidien et pour tout $i > 0$, X_i est soit un espace symétrique compact soit un quotient G/K avec G groupe simple réel connexe non compact et K un sous-groupe compact maximal.

BIBLIOGRAPHIE

[1] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[2] N. Bourbaki. *Éléments de mathématique. Fascicule XXIX. Livre VI: Intégration. Chapitre 7: Mesure de Haar. Chapitre 8: Convolution et représentations.* Actualités Scientifiques et Industrielles, No. 1306. Hermann, Paris, 1963.

[3] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 7–9*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 2005. Translated from the 1975 and 1982 French originals by Andrew Pressley.

[4] Henri Cartan. *Calcul différentiel*. Hermann, Paris, 1967.

[5] J. J. Duistermaat and J. A. C. Kolk. *Lie groups*. Universitext. Springer-Verlag, Berlin, 2000.

[6] Jacques Faraut. *Analysis on Lie groups*, volume 110 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2008. An introduction.

[7] Roger Godement. *Introduction à la théorie des groupes de Lie*. Springer-Verlag, Berlin, 2004. Reprint of the 1982 original.

[8] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[9] Rached Mneimné and Frédéric Testard. *Introduction à la théorie des groupes de Lie classiques*. Collection Méthodes. [Methods Collection]. Hermann, Paris, 1986.

[10] Walter Rudin. *Analyse réelle et complexe*. Masson, Paris, 1980. Translated from the first English edition by N. Dhombres and F. Hoffman, Third printing.

[11] Jean-Pierre Serre. *Algèbres de Lie semi-simples complexes*. W. A. Benjamin, inc., New York-Amsterdam, 1966.

[12] Bruno Sévennec. Mesure invariante et équirépartition dans les groupes compacts. In *Autour du centenaire Lebesgue*, volume 18 of *Panor. Synthèses*, pages 63–84. Soc. Math. France, Paris, 2004.

[13] Frank W. Warner. *Foundations of differentiable manifolds and Lie groups*, volume 94 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1983. Corrected reprint of the 1971 edition.