Groupes réductifs I: groupes auto-adjoints

Un traitement raisonnablement complet de la théorie des groupes réductifs nous occuperait facilement pendant un trimestre, je suis donc obligé de me limiter au strict minimum, en essayant de tirer profit de la topologie complexe, et en évitant la théorie des schémas. Les puristes ne trouveront donc rien à leur goût dans ce qui suit...

Pour ceux qui voient ces choses la première fois, un conseil: garder toujours en tête les groupes $\mathbf{GL}_n(\mathbf{C})$ et $\mathbf{SL}_n(\mathbf{C})$ comme exemple typique de groupe réductif, et le groupe des matrices triangulaires supérieures (ou unipotentes supérieures) comme un exemple typique de groupe non réductif.

Le résultat principal de ce cours est le magnifique théorème de Cartan, Chevalley et Mostow affirmant que les sous-groupes algébriques réductifs de $\mathbf{GL}_n(\mathbf{C})$ sont précisément les adhérences de Zariski des sous-groupes compacts de $\mathbf{GL}_n(\mathbf{C})$. Ce résultat fondamental est fort délicat et nous en donnons une preuve complète. Références très bien: le livre canonique de Borel sur les groupes algébriques, le livre de Wallach sur la théorie géométrie des invariants et le livre de Procesi sur les groupes de Lie et leurs invariants sont excellents.

Convention: A^T désigne la transposée de la matrice A.

1 Groupes algébriques-généralités

1.1 Topologie de Zariski

Commençons par quelques rappels de géométrie algébrique "à la grand papa". Soit $n \geq 0$ un entier. On dispose sur $\mathbf{C}^n$ d'au moins deux topologies:

• celle standard (ou "naturelle"), euclidienne.

• celle de Zariski, dont les fermés sont les **variétés affines (ou simplement variétés) dans $\mathbf{C}^n$**, i.e. les zéros communs d'une famille de polynômes dans $\mathbf{C}[X_1, ..., X_n]$. Tout fermé Zariski est clairement un fermé pour la topologie standard.

Si $Z \subset \mathbf{C}^n$ est une variété affine, une fonction $\varphi : Z \to \mathbf{C}$ est dite **régulière** s'il existe $P \in \mathbf{C}[X_1, ..., X_n]$ tel que $\varphi(z) = P(z)$ pour $z \in Z$. Les fonctions régulières sur Z forment une $\mathbf{C}$-algèbre réduite de type fini $\mathbf{C}[Z]$, isomorphe à $\mathbf{C}[X_1, ..., X_n]/I_Z$, où $I_Z = \{f \in \mathbf{C}[X_1, ..., X_n] | f(Z) = \{0\}\}$ est **l'idéal de** Z. De plus Z s'identifie à $\mathrm{Hom}_{\mathbf{C}-\mathrm{alg}}(\mathbf{C}[Z], \mathbf{C})$ via $z \to (f \to f(z))$, ou encore à l'ensemble des idéaux maximaux de $\mathbf{C}[Z]$.

Un **morphisme de variétés affines** $f : X \to Y$ (avec $X \subset \mathbf{C}^n$, $Y \subset \mathbf{C}^m$) est une application de la forme $f(x) = (P_1(x), ..., P_m(x))$ avec $P_i \in \mathbf{C}[X]$. De manière équivalente, c'est une application $f : X \to Y$ telle que $\varphi \circ f \in \mathbf{C}[X]$ pour tout $\varphi \in \mathbf{C}[Y]$. Un tel f est continu (pour les deux topologies). Tout morphisme

$f : X \to Y$ induit un morphisme de $\mathbf{C}$-algèbres $\mathbf{C}[Y] \to \mathbf{C}[X]$ et tout morphisme de $\mathbf{C}$-algèbres $\mathbf{C}[Y] \to \mathbf{C}[X]$ est ainsi obtenu. Un isomorphisme est ce que l'on pense[1].

Une variété affine X est dite **irréductible** si tout ouvert (Zariski) non vide de X est dense dans X. Cela équivaut au fait que $\mathbf{C}[X]$ est intègre. Toute variété affine possède une décomposition unique en réunion finie de fermés irréductibles maximaux, qu'on appelle les **composantes irréductibles de** X.

La catégorie des variétés affines admet des produits finis. Noter que la topologie produit sur $\mathbf{C}\times\mathbf{C}$ n'est pas celle sur $\mathbf{C}^2$. On munira toujours $\mathbf{C}^n \times \mathbf{C}^m$ de la structure de variété affine induite par l'identification avec $\mathbf{C}^{n+m}$. Si $X \subset \mathbf{C}^n$, $Y \subset \mathbf{C}^m$ sont des variétés, $X \times Y$ devient une variété dans $\mathbf{C}^{n+m}$ telle que

$$\mathbf{C}[X \times Y] \simeq \mathbf{C}[X] \otimes_{\mathbf{C}} \mathbf{C}[Y].$$

1.2 Variétés définies sur un sous-corps de C

Si k est un sous-corps de $\mathbf{C}$, on dit qu'une variété $Z \subset \mathbf{C}^n$ est **définie sur** k **(ou une** k**-variété)** si l'idéal I_Z de Z dans $\mathbf{C}[\mathbf{C}^n] = \mathbf{C}[X_1, ..., X_n]$ est engendré par $I_Z \cap k[X_1, ..., X_n]$. Dans ce cas

$$k[Z] = k[X_1, ..., X_n]/(I_Z \cap k[X_1, ..., X_n])$$

est une sous-k-algèbre de $\mathbf{C}[Z]$ telle que $k[Z] \otimes_k \mathbf{C} = \mathbf{C}[Z]$. Un morphisme $f : Z_1 \to Z_2$ entre des k-variétés est dit **défini sur** k **(ou** k**-morphisme)** si $\varphi \circ f \in k[Z_1]$ pour $\varphi \in k[Z_2]$, i.e. f est défini par des polynômes à coefficients dans k.

Si $Z \subset \mathbf{C}^n$ est une k-variété, il est clair que l'on peut écrire

$$Z = \{x \in \mathbf{C}^n | f_1(x) = ... = f_k(x) = 0\}$$

pour une famille de polynômes $f_i \in k[X_1, ..., X_n]$. Réciproquement:

Théorème 1.1. *Pour une variété $Z \subset \mathbf{C}^n$ les assertions suivantes sont équivalentes:*

a) Z est définie sur k.

b) Il existe $f_1, ..., f_d \in k[X_1, ..., X_n]$ tels que $Z = \{x \in \mathbf{C}^n | f_i(x) = 0, i = 1, ..., d\}$.

c) $\sigma(Z) \subset Z$ pour tout $\sigma \in \mathrm{Aut}(\mathbf{C}/k)$.

1.3 La notion de groupe algébrique

Si $f \in \mathbf{C}[X_1, ..., X_n]$, l'ensemble $D(f) = \{x \in \mathbf{C}^n | f(x) \neq 0\}$ est ouvert Zariski de $\mathbf{C}^n$, mais possède une structure naturelle de fermé Zariski de $\mathbf{C}^{n+1}$, d'algèbre de fonctions régulières $\mathbf{C}[D(f)] = \mathbf{C}[X_1, ..., X_n][1/f]$, via l'identification $D(f)$" = "$\{(y, t) \in \mathbf{C}^{n+1} | f(y)t = 1\}$. On considère toujours $\mathbf{GL}_n(\mathbf{C})$ comme $D(\det g) \subset M_n(\mathbf{C}) \simeq \mathbf{C}^{n^2}$ et donc comme un fermé Zariski de $\mathbf{C}^{n^2+1}$, défini sur $\mathbf{Q}$.

Définition 1.1. Un sous-groupe $G \subset \mathbf{GL}_n(\mathbf{C})$ est dit **algébrique** si G est un fermé Zariski de $\mathbf{GL}_n(\mathbf{C})$. Si k est un sous-corps de $\mathbf{C}$, un k**-groupe algébrique (ou groupe algébrique défini sur** k**)** est un groupe algébrique $G \subset \mathbf{GL}_n(\mathbf{C})$ défini sur k en tant que sous-variété de $\mathbf{GL}_n(\mathbf{C})$.

[1] à condition de ne pas penser qu'il s'agit d'un morphisme bijectif!

Définition 1.2. Si $G \subset \mathbf{GL}_n(\mathbf{C})$ est un sous-groupe algébrique, et $A \subset \mathbf{C}$ un sous-anneau, le groupe des **points A-rationnels de G** est

$$G(A) = G \cap \mathbf{GL}_n(A).$$

Donc $G(\mathbf{R})$ (resp. $G(\mathbf{Z})$) est le **groupe des points réels (resp. entiers) de** G.

Il faut faire très attention car $G(A)$ dépend vraiment de la manière dont on réalise G comme sous-groupe de $\mathbf{GL}_n(\mathbf{C})$. Si G est défini sur k et A est une k-algèbre, on vérifie que $G(A)$ ne dépend plus des choix, et s'identifie à $\mathrm{Hom}_{k-\mathrm{alg}}(k[G], A)$.

Les deux théorèmes suivants sont délicats et reposent sur le théorème de constructibilité de Chevalley et le "main theorem" de Zariski, cf. le livre de Borel.

Théorème 1.2. *(Chevalley, Zariski) Soit $f : G \to H$ un morphisme de groupes algébriques.*

a) $f(G)$ est un sous-groupe fermé (Zariski) de H, défini sur k si G, H, f le sont.

b) Si f est bijectif, alors f est un isomorphisme.

Théorème 1.3. *(Borel, Chevalley) Soit G un groupe algébrique. Alors*

a) Le groupe dérivé[2] G' est un sous-groupe fermé (Zariski) de G, connexe (resp. défini sur k) si G l'est.

b) Si H_i sont des sous-groupes (Zariski) fermés ***connexes*** *de G, le sous-groupe abstrait H engendré par les H_i est (Zariski) fermé, connexe. Si G et les H_i sont définis sur k, H l'est aussi.*

c) Si H est un sous-groupe Zariski fermé et distingué de G, G/H est un groupe algébrique. Si G, H sont définis sur k, alors G/H l'est aussi.

Si G est un groupe algébrique, la **composante neutre** G^0 de G est la composante connexe de $1 \in G$, pour la topologie usuelle ou bien celle de Zariski (on utilise implicitement un résultat hautement nontrivial: si $X \subset \mathbf{C}^n$ est une variété affine, alors X est connexe pour la topologie de Zariski si et seulement si X l'est pour la topologie usuelle).

Proposition 1.1. *G^0 est un sous-groupe distingué d'indice fini dans G, défini sur k si G l'est.*

Exercice 1.4. Démontrer la proposition ci-dessus.

1.4 L'algèbre de Lie d'un groupe algébrique

Tout groupe algébrique $G \subset \mathbf{GL}_n(\mathbf{C})$ est un sous-groupe fermé de $\mathbf{GL}_n(\mathbf{C})$ pour la topologie euclidienne et on dispose de son algèbre de Lie

$$\mathfrak{g} = \{X \in M_n(\mathbf{C}) |\, e^{tX} \in G,\ \forall t \in \mathbf{R}\}.$$

Proposition 1.2. *$\mathfrak{g}$ est un sous-$\mathbf{C}$-espace vectoriel de $M_n(\mathbf{C})$.*

Proof. Il suffit de voir que si $X \in \mathfrak{g}$ et P est un polynôme nul sur G, alors $z \to P(e^{zX})$ est nulle. Or cette application est holomorphe et nulle sur $\mathbf{R}$, donc nulle. □

[2] i.e. engendré par les commutateurs $xyx^{-1}y^{-1}$, $x, y \in G$.

Exercice 1.5. Montrer que tout morphisme continu $f : \mathbf{R} \to \mathbf{GL}_n(\mathbf{C})$ est de la forme $f(t) = e^{tA}$ pour une unique matrice $A \in M_n(\mathbf{C})$. En déduire que si $G \subset \mathbf{GL}_n(\mathbf{C})$ et $H \subset \mathbf{GL}_m(\mathbf{C})$ sont des sous-groupes fermés (pour la topologie usuelle) et $f : G \to H$ est un morphisme continu, alors f induit naturellement un morphisme d'algèbres de Lie $df : \mathrm{Lie}(G) \to \mathrm{Lie}(H)$, **la dérivée de** f, tel que $f(e^X) = e^{df(X)}$ pour $X \in \mathrm{Lie}(G)$.

Pour pratiquer la gymnastique "groupes algébriques-algèbre de Lie", je conseille fortement de faire les exercices suivants, utilisés tout le temps.

Exercice 1.6. Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un groupe algébrique, d'algèbre de Lie $\mathfrak{g} \subset M_n(\mathbf{C})$.

a) Soit $g \in G$. Montrer que $gXg^{-1} \in \mathfrak{g}$ pour $X \in \mathfrak{g}$, et que la dérivée de $G \to G, x \to gxg^{-1}$ est $\mathrm{Ad}(g) : \mathfrak{g} \to \mathfrak{g}, X \to gXg^{-1}$.

b) Montrer que $\mathrm{Ad} : G \to \mathbf{GL}(\mathfrak{g}),\quad \mathrm{Ad}(g)(X) = gXg^{-1}$ est un morphisme de groupes algébriques (la **représentation adjointe** de G), dont la dérivée est $\mathrm{ad} = d(\mathrm{Ad}) : \mathfrak{g} \to \mathrm{End}(\mathfrak{g}), \mathrm{ad}(X)(Y) = [X,Y] = XY - YX$.

Exercice 1.7. Si H est un sous-groupe fermé (Zariski) d'un groupe algébrique G, montrer que $\mathfrak{h}$ est une sous-algèbre de Lie de G (i.e. $[\mathfrak{h},\mathfrak{h}] \subset \mathfrak{h}$). Si H est distingué, montrer que $\mathfrak{h}$ est un **idéal** de $\mathfrak{g}$ (i.e. $[\mathfrak{h},\mathfrak{g}] \subset \mathfrak{h}$). On a noté $[U,V] = \mathrm{Vect}_{X\in U, Y\in V}[X,Y]$.

Exercice 1.8. Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un groupe algébrique **connexe**.

1. Si $f, g : G \to H$ sont deux morphismes tels que $df = dg$, alors $f = g$.
2. Si H_1, H_2 sont des sous-groupes algébriques **connexes** de G, alors $H_1 \subset H_2$ si et seulement si $\mathfrak{h}_1 \subset \mathfrak{h}_2$.
3. Un sous-groupe fermé **connexe** H de G est distingué dans G si et seulement si $\mathfrak{h}$ est un **idéal** de $\mathfrak{g}$ (i.e. $[\mathfrak{h},\mathfrak{g}] \subset \mathfrak{h}$).
4. Le centre Z de G a pour algèbre de Lie le **centre**[3] de $\mathfrak{g}$.
5. Soit $G \to \mathbf{GL}(V)$ un morphisme de groupes algébriques. Alors G et $\mathfrak{g}$ laissent stables les mêmes sous-espaces de V. Un tel sous-espace est fixé par G si et seulement s'il est tué par $\mathfrak{g}$.

La description suivante de l'algèbre de Lie d'un groupe algébrique sera très utile dans le corollaire ci-dessus[4].

Théorème 1.9. *Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un sous-groupe algébrique et soit $I \subset \mathbf{C}[\mathbf{GL}_n(\mathbf{C})]$ l'idéal des polynômes s'annulant sur G. On a*

$$\mathfrak{g} = \{A \in M_n(\mathbf{C}) | \ \frac{df}{dt}|_{t=0} f(1+tA) = 0, \forall f \in I\}.$$

Proof. Si $f \in C^\infty(\mathbf{GL}_n(\mathbf{C}))$ et $A \in M_n(\mathbf{C})$ on pose comme d'habitude

$$A.f(g) = \frac{d}{dt}|_{t=0} f(ge^{tA}),$$

[3] I.e. les $X \in \mathfrak{g}$ tels que $[X,Y] = 0$ pour tout $Y \in \mathfrak{g}$.

[4] Pouvez-vous le démontrer directement? pas moi ...

i.e. on voit A comme endomorphisme de $C^\infty(\mathbf{GL}_n(\mathbf{C}))$. Pour tout $f \in \mathbf{C}[\mathbf{GL}_n(\mathbf{C})]$ et $A \in M_n(\mathbf{C})$

$$(A.f)(1) = \frac{d}{dt}|_{t=0} f(e^{tA}) = \frac{df}{dt}|_{t=0} f(1+tA) = \sum_{i,j} A_{ij} \frac{\partial f}{\partial T_{ij}}(1)$$

car $e^{tA} = 1 + tA + O(t^2)$. On en déduit facilement que $A.f \in \mathbf{C}[\mathbf{GL}_n(\mathbf{C})]$ pour $f \in \mathbf{C}[\mathbf{GL}_n(\mathbf{C})]$ et $A \in M_n(\mathbf{C})$.

Si $X \in \mathfrak{g}$, on a clairement $f(e^{tA}) = 0$ pour $f \in I$ et $t \in \mathbf{R}$ (car $e^{tA} \in G$), donc $\frac{df}{dt}|_{t=0} f(1+tA) = 0$, ce qui montre une inclusion. Supposons que $A \in M_n(\mathbf{C})$ vérifie $(A.f)(1) = 0$ pour $f \in I$ et montrons que $A.I \subset I$. En effet, si $f \in I$ alors $f(g\cdot) \in I$ pour $g \in G$, donc $(A.f)(g) = (A.f(g\cdot))(1) = 0$ pour $g \in G$, donc $A.f \in I$. Par récurrence[5] $A^k.f \in I$ pour $f \in I$, donc $(A^k.f)(1) = 0$ pour tout k. Ainsi pour $f \in I$ la fonction $\varphi(t) = f(e^{tA})$ a toutes ses dérivées nulles en 0 et est analytique, donc est nulle et $e^{tA} \in G$ pour $t \in \mathbf{R}$, ce qui montre que $A \in \mathfrak{g}$. □

Le résultat suivant n'est pas évident, même pour $k = \mathbf{R}$:

Corollaire 1.1. *Si $G \subset \mathbf{GL}_n(\mathbf{C})$ est un k-groupe algébrique, alors $\mathfrak{g}_k := \mathfrak{g} \cap M_n(k)$ est une k-forme de $\mathfrak{g}$, i.e. $\mathfrak{g}_k \otimes_k \mathbf{C} \simeq \mathfrak{g}$.*

Proof. Le théorème 1.9 montre que $\mathfrak{g}$ est définie par des égalités de la forme

$$\sum_{i,j} \frac{\partial f}{\partial T_{ij}}(1) X_{ij} = 0,$$

avec $f \in I$, I étant l'idéal de G dans $\mathbf{C}[\mathbf{GL}_n(\mathbf{C})]$. Comme G est défini sur k, $I_k = I \cap k[\mathbf{GL}_n(\mathbf{C})]$ engendre I, donc il suffit de se restreindre aux $f \in I_k$, pour lesquels $\frac{\partial f}{\partial T_{ij}}(1) \in k$. Ainsi $\mathfrak{g}$ est l'ensemble des solutions d'un système linéaire à coefficients dans k, et donc $\mathfrak{g}_k \otimes_k \mathbf{C} = \mathfrak{g}$. □

2 Groupes réductifs et semi-simplicité

Nous allons isoler maintenant une classe remarquable de groupes algébriques: les groupes réductifs.

2.1 Actions algébriques d'un groupe algébrique

Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un groupe algébrique et soit X une variété affine.

Définition 2.1. a) Une **action algébrique (ou simplement action...)** de G sur X est une action du groupe G sur X au sens usuel, telle que l'application naturelle $G \times X \to X, (g,x) \to g.x$ soit un morphisme de variétés affines.

b) Une **représentation algébrique** de G dans un $\mathbf{C}$-espace vectoriel V est une représentation linéaire de G dans V (i.e. un morphisme de groupes $G \to \mathbf{GL}(V)$) telle que tout $v \in V$ soit contenu dans un sous-espace de dimension finie $W \subset V$, stable par G et tel que le morphisme induit $G \to \mathbf{GL}(W)$ soit un morphisme de variétés affines (i.e. l'action de G sur la variété affine W est algébrique).

[5] A^k désigne la composition k fois de l'opérateur de dérivation par rapport à A, pas la puissance k-ième de A!

On dispose du très utile résultat de linéarisation suivant:

Proposition 2.1. *Soit G un groupe algébrique agissant sur une variété affine X.*
a) $\mathbf{C}[X]$ est une représentation algébrique de G pour $g.f(x) = f(g^{-1}x)$.
b) Il existe n, une immersion fermée $\varphi : X \to \mathbf{C}^n$ et une représentation algébrique $\rho : G \to \mathbf{GL}_n(\mathbf{C})$ tels que $\varphi(g.x) = \rho(g)\varphi(x)$ pour tous g, x.

Proof. a) Soit $f \in \mathbf{C}[X]$. Nous allons montrer que le sous-espace W de G engendré par les translatés $g.f$ ($g \in G$) de f est de dimension finie et une représentation algébrique de G. Comme $(g,x) \to f(g.x)$ est dans $\mathbf{C}[G \times X] \simeq \mathbf{C}[G] \otimes_{\mathbf{C}} \mathbf{C}[X]$, on peut écrire $f(g.x) = \sum_{i=1}^n a_i(g) b_i(x)$, avec $a_i \in \mathbf{C}[G], b_i \in \mathbf{C}[X]$, donc $W \subset \mathrm{Vect}(b_1, ..., b_n)$ est de dimension finie.

Il reste à voir que l'action de G sur W est algébrique. Prenons une base $u_i = g_i.f$ de W, avec $g_i \in G$, $1 \le i \le d$. Alors

$$(g.u_i)(x) = (gg_i).f(x) = f((gg_i)^{-1}.x) = \sum_{j=1}^n a_j((gg_i)^{-1}) b_j(x),$$

donc $g.u_i = \sum_{j=1}^n F_{ij}(g) b_j$ avec $F_{ij} \in \mathbf{C}[G]$. Si $l \in W^*$, on prolonge l à $\mathbf{C}[X]^*$ et on a $l(g.u_i) = \sum_{j=1}^n F_{ij}(g) l(b_j)$, donc $g \to l(g.u_i) \in \mathbf{C}[G]$. Cela permet de conclure.

b) Soit $f_1, ..., f_m$ un système de générateurs de $A = \mathbf{C}[X]$ en tant que $\mathbf{C}$-algèbre et considérons $W = \mathrm{Vect}_{1 \le i \le m, g \in G}(g.f_i)$. Alors W est une représentation algébrique de G et l'application naturelle

$$X \to W^*, x \to (f \to f(x))$$

est G-équivariante et une immersion fermée, car W engendre $\mathbf{C}[X]$. □

Les mêmes idées fournissent aussi le résultat fondamental suivant:

Théorème 2.1. *(Chevalley) Soient $H \subset G$ des k-groupes, avec H fermé (Zariski) dans G. Il existe une représentation fidèle $\rho : G \to \mathrm{GL}(W)$, définie sur k et une droite $L \subset W$ définie sur k telle que $H = \{g \in G |\, \rho(g)L = L\}$.*

Proof. Pour simplifier supposons $k = \mathbf{C}$ (le cas général est identique...). Faisons agir G par translation à gauche sur lui-même, d'où une action de G sur $\mathbf{C}[G]$ par $g.f(x) = f(g^{-1}x)$. Soit I l'idéal de $\mathbf{C}[G]$ des fonctions s'annulant sur H. On vérifie sans mal que $H = \{g \in G |\, g.I \subset I\}$. Comme I est de type fini ($\mathbf{C}[G]$ est noethérien) et $\mathbf{C}[G]$ est une représentation algébrique de G, il existe $V \subset \mathbf{C}[G]$ de dimension finie, stable par G et contenant une famille de générateurs de I. Soit alors $W = I \cap V$. On vérifie sans problème que $H = \{g \in G |\, g.W \subset W\}$. Si $f_1, ..., f_m$ est une base de W et $Z = \wedge^m W$, $v = f_1 \wedge ... \wedge f_m$, alors $H = \{g \in G |\, g.v \in \mathbf{C}v\}$ (exercice d'algèbre linéaire), ce qui permet de conclure. □

2.2 Groupes réductifs et semi-simplicité

La théorie des modules semi-simples montre que pour un groupe algébrique G et une représentation algébrique V les assertions suivantes sont équivalentes, dans quel cas on dit que V est **semi-simple**:

a) V est la somme de ses sous-représentations irréductibles.
b) V est isomorphe à une somme directe de représentations irréductibles.
c) Tout sous-espace G-stable $W \subset V$ possède un supplémentaire G-stable.

Définition 2.2. Un groupe algébrique G est dit **réductif** si toutes ses représentations algébriques sont semi-simples.

D'après la discussion ci-dessus, il suffit de tester la semi-simplicité des représentations algébriques de dimension finie. Soit $\hat{G}$ l'ensemble des classes d'isomorphisme de représentations algébriques irréductibles, forcément de dimension finie de G. Pour toute représentation algébrique V de G on a un isomorphisme canonique

$$\bigoplus_{\pi \in \hat{G}} \pi \otimes_{\mathbf{C}} \mathrm{Hom}_G(\pi, V) \simeq V.$$

Pour $V = \mathbf{C}[G]$ on a $\mathrm{Hom}_G(\pi, \mathbf{C}[G]) \simeq \pi^*$ (réciprocité de Frobenius), d'où un isomorphisme

$$\mathbf{C}[G] \simeq \bigoplus_{\pi \in \hat{G}} \pi \otimes_{\mathbf{C}} \pi^*,$$

analogue d'un résultat standard quand G est fini[6] et analogue algébrique de l'isomorphisme

$$L^2(K) \simeq \widehat{\bigoplus}_{\pi \in \hat{K}} \pi \otimes_{\mathbf{C}} \pi^*.$$

Nous verrons plus tard que ces deux isomorphismes sont étroitement liés!

Proposition 2.2. *Un groupe algébrique G est réductif si et seulement si le G-module $\mathbf{C}[G]$ est semi-simple (pour l'action naturelle de G via $g.f(x) = f(xg)$).*

Proof. Un sens étant évident, supposons que $\mathbf{C}[G]$ est semi-simple et montrons que toute représentation algébrique de dimension finie W est semi-simple. Si $l_1, ..., l_n$ est une base de W^*, l'application $W \to \mathbf{C}[G]^n, v \to (g \to l_i(g.v))$ est G-équivariante et trivialement injective. Or $\mathbf{C}[G]^n$ est semi-simple comme G-module, donc W aussi (un sous-G-module d'un module semi-simple l'est encore). $\square$

Par exemple soit $D_n(\mathbf{C})$ le sous-groupe des matrices diagonales dans $\mathbf{GL}_n(\mathbf{C})$, alors

$$\mathbf{C}[D_n(\mathbf{C})] = \mathbf{C}[X_1^{\pm 1}, ..., X_n^{\pm 1}] = \bigoplus_{k_1, ..., k_n \in \mathbf{Z}} \mathbf{C} \cdot X_1^{k_1} ... X_n^{k_n}$$

et le $\mathbf{C}$-espace vectoriel $\mathbf{C} \cdot X_1^{k_1} ... X_n^{k_n}$ de dimension 1 est stable sous $D_n(\mathbf{C})$, qui y agit par le caractère

$$\chi_{k_1, ..., k_n}(\mathrm{diag}(t_1, ..., t_n)) = t_1^{k_1} ... t_n^{k_n}.$$

Les groupes algébriques isomorphes à un $D_n(\mathbf{C})$ jouent un rôle primordial dans la théorie des groupes algébriques et sont appelés **tores algébriques**. Nous les étudierons plus en détail dans le cours prochain. La proposition 2.2 fournit le résultat important suivant. Nous verrons dans le cours prochain que les tores sont précisément les groupes réductifs connexes et commutatifs.

Corollaire 2.1. *Les tores algébriques sont réductifs.*

Exercice 2.2. Soit T un tore algébrique. Montrer que toute représentation algébrique V de dimension finie de T possède une base dans laquelle l'action de T est diagonale.

[6]En fait, tout groupe fini est algébrique et réductif!

Théorème 2.3. *Soit G un groupe algébrique réductif et soit N un sous-groupe fermé (Zariski) distingué de G. Alors N et G/N sont des groupes réductifs.*

Proof. Pour G/N c'est évident, car les représentations de G/N sont les représentations de G sur lesquelles N agit trivialement, donc elles sont semi-simples. Pour N c'est moins évident. Par la proposition ci-dessus il suffit de voir que $\mathbf{C}[H]$ est un H-module semi-simple, or $\mathbf{C}[G] \to \mathbf{C}[H]$ est surjective et un quotient d'un H-module semi-simple l'est encore. Il suffit donc de voir que $\mathbf{C}[G]$ est H-semi-simple. Soit X la somme des sous-H-modules irréductibles de $\mathbf{C}[G]$. Comme H est distingué dans G, X est stable sous G, donc on peut écrire $\mathbf{C}[G] = X \oplus Y$, avec Y G-stable. Si $Y \neq 0$, alors Y possède un sous-H-module irréductible, qui doit être dans X, une contradiction. Donc $Y = 0$ et $\mathbf{C}[G]$ est semi-simple comme H-module. □

Exercice 2.4. a) Un groupe algébrique G est réductif si et seulement si G^0 l'est.

b) Si G, H sont réductifs, alors $G \times H$ l'est aussi. Indication: commencer par vérifier que le produit tensoriel $V \otimes_{\mathbf{C}} W$ est une représentation irréductible de $G \times H$ si V, W sont des représentations algébriques irréductibles de G, resp. H.

2.3 Invariants d'un groupe réductif

Nous allons voir que l'action d'un groupe réductif G sur une variété affine X est particulièrement sympathique. Soit G un tel groupe et V une représentation algébrique de G. Puisque

$$V^G = \{v \in V |\, g.v = v,\ \forall g \in G\}$$

est stable par G et V est semi-simple, on peut écrire $V = V^G \oplus W$, avec W G-stable. En fait, W est l'unique supplémentaire de V^G stable par G, et c'est la somme des sous-G-modules irréductibles non-triviaux de V (exercice facile). On en déduit facilement que la projection $R_V : V \to V^G$ sur V^G le long de W est naturelle en V: si $f : V \to W$ est un morphisme de G-représentations algébriques, sa restriction $f^G : V^G \to W^G$ vérifie $R_W \circ f = f^G \circ R_V$. En particulier si f est surjectif, alors f^G l'est. Ainsi **le foncteur $V \to V^G$ est exact sur les représentations algébriques de G**. La projection $R_V : V \to V^G$ est appelée **opérateur de Reynolds**.

Si G agit sur une variété affine X, alors $\mathbf{C}[X]$ est une représentation algébrique de G et la discussion ci-dessus fournit:

Proposition 2.3. *Soit G un groupe réductif agissant sur une variété affine X. L'opérateur de Reynolds $R_X := R_{\mathbf{C}[X]} : \mathbf{C}[X] \to \mathbf{C}[X]^G$ vérifie:*

a) $(R_X(f))|_Y = R_Y(f|_Y)$ pour $Y \subset X$ sous-variété fermée G-stable, $f \in \mathbf{C}[X]$.

b) $R_X(fF) = fR_X(F)$ si $f \in \mathbf{C}[X]^G$ et $F \in \mathbf{C}[X]$.

Exercice 2.5. Démontrer cette proposition.

On va utiliser ces projecteurs pour démontrer le résultat fondamental suivant:

Théorème 2.6. *(Hilbert) Si un groupe réductif G agit sur une variété affine X, alors $\mathbf{C}[X]^G$ est une $\mathbf{C}$-algèbre de type fini.*

Proof. Prenons (prop. 2.1) une immersion fermée $\varphi : X \to \mathbf{C}^n$ et une représentation algébrique $\rho : G \to \mathbf{GL}_n(\mathbf{C})$ tels que $\varphi(g.x) = \rho(g)\varphi(x)$. On fait agir G sur $\mathbf{C}^n$ via ρ. La surjection $\mathbf{C}[\mathbf{C}^n] \to \mathbf{C}[X]$ est G-équivariante et induit une surjection

$\mathbf{C}[\mathbf{C}^n]^G \to \mathbf{C}[X]^G$. Il suffit donc de montrer que $\mathbf{C}[\mathbf{C}^n]^G$ est une $\mathbf{C}$-algèbre de type fini, i.e. on peut supposer que $X = \mathbf{C}^n$, G agissant via une représentation algébrique $\rho : G \to \mathbf{GL}_n(\mathbf{C})$.

Notons $A = \mathbf{C}[\mathbf{C}^n] \simeq \mathbf{C}[X_1, ..., X_n]$ et remarquons que $A^G = \{f \in A |\, f(v) = f(\rho(g)v),\ g \in G\}$ est graduée, i.e. si $f \in A^G$, alors les composantes homogènes de f dans A sont aussi dans A^G. Considérons $I = \{f \in A^G | f(0) = 0\}$ et prenons une famille de générateurs non nuls et homogènes $f_1, ..., f_r \in I$ de IA (cela est possible: on part d'une famille $F_1, ..., F_d \in IA$ qui engendre IA, on écrit chaque $F_i = \sum_j F_{ij} a_{ij}$ avec $F_{ij} \in I$ et on prend pour $f_1, ..., f_r$ la famille des composantes homogènes non nulles des F_{ij}). Nous allons montrer par récurrence sur $d \geq 0$ que si $f \in A^G$ est homogène de degré d, alors $f \in \mathbf{C}[f_1, ..., f_r]$, ce qui donnera $A^G = \mathbf{C}[f_1, ..., f_r]$. Cela est clair si $d = 0$, supposons donc que $d \geq 1$ et que c'est vrai pour $d - 1$. Comme $f \in IA$, on peut écrire $f = f_1 F_1 + ... + f_r F_r$, et on peut supposer que F_i est homogène, de degré $d - \deg(f_i) < d$. Alors

$$f = R_X(f) = R_X(f_1 F_1 + ... + f_r F_r) = f_1 R_X(F_1) + ... + f_r R_X(F_r).$$

Mais $R_X(F_i) \in A^G$ et $R_X(F_i)$ est homogène du même degré que F_i (car l'espace des polynômes homogènes de degré fixé est stable par G et donc laissé stable par R_X). On a $R_X(F_i) \in \mathbf{C}[f_1, ..., f_r]$ (hypothèse de récurrence), d'où le résultat. $\square$

Remarque 2.7. On peut naturellement se demander (comme l'a fait Hilbert au congress ICM en 1900 à Paris) si $\mathbf{C}[X]^G$ est une $\mathbf{C}$-algèbre de type fini pour tout groupe algébrique G agissant sur une variété affine X. La réponse est négative en général: Nagata a construit des contre-exemples et Mukai a montré qu'il y en a même avec G un groupe algébrique isomorphe au groupe additif $(\mathbf{C}^3, +)$.

Gardons les hypothèses du théorème. L'algèbre $\mathbf{C}[X]^G$ est de type fini et réduite, l'ensemble $X//G$ des idéaux maximaux de $\mathbf{C}[X]^G$ est une variété affine, appelée le **quotient catégorique de X par G**: si $\mathbf{C}[X]^G = \mathbf{C}[T_1, ..., T_n]/I$ pour un idéal radical I, $X//G$ est a variété $V(I)$ de $\mathbf{C}^n$. On a une identification canonique

$$\mathbf{C}[X//G] = \mathbf{C}[X]^G$$

et l'inclusion $\mathbf{C}[X//G] = \mathbf{C}[X]^G \to \mathbf{C}[X]$ induit un morphisme de variétés affines

$$\pi_X : X \to X//G,$$

qui envoie $x \in X$ sur l'idéal de $\mathbf{C}[X]^G$ des fonctions nulles sur x.

Théorème 2.8. *a) L'application $\pi_X : X \to X//G$ est surjective.*

b) Si Y, Z sont des sous-variétés fermées disjointes de X et stables par G, alors il existe $f \in \mathbf{C}[X]^G$ nulle sur Y et qui vaut 1 sur Z.

Proof. a) Soit m_0 un idéal maximal de $\mathbf{C}[X]^G$. On veut trouver un idéal maximal m de $\mathbf{C}[X]$ tel que $m_0 = m \cap \mathbf{C}[X]^G$. En posant $I = m_0 \mathbf{C}[X]$, nous montrons d'abord que $m_0 = I \cap \mathbf{C}[X]^G$, en particulier $I \neq \mathbf{C}[X]^G$. Une inclusion étant évidente, soit $f \in I \cap \mathbf{C}[X]^G$ et écrivons $f = \sum f_i \alpha_i$, avec $f_i \in m_0$ et $\alpha_i \in \mathbf{C}[X]$, alors $f = R_X(f) = \sum f_i R_X(\alpha_i) \in m_0$. Soit m un idéal maximal de $\mathbf{C}[X]$ contenant I, alors $\mathbf{C}[X]^G/(m \cap \mathbf{C}[X]^G) \to \mathbf{C}[X]/m \simeq \mathbf{C}$ est injective, donc $m \cap \mathbf{C}[X]^G$ est un idéal maximal de $\mathbf{C}[X]^G$ (il n'est pas $\mathbf{C}[X]^G$ car $1 \notin m$), contenant m_0, donc égal à m_0. Cela permet de conclure.

c) Le Nullstellensatz montre[7] qu'il existe $f \in \mathbf{C}[X]$ nulle sur Y et qui vaut 1 sur Z. En posant $F = R_X(f)$ on obtient une fonction dans $\mathbf{C}[X]^G$ qui est nulle sur Y et vaut 1 sur Z. $\square$

Corollaire 2.2. *Soit H un sous-groupe fermé et réductif d'un groupe algébrique G. Alors $\pi_G : G \to G//H$ induit une bijection $G/H \simeq G//H$.*

Proof. π_G est surjective par le théorème ci-dessus. Il faut voir que ses fibres sont les H-orbites dans G (H agit sur G par $h.g = gh^{-1}$). Si $g_1 H \neq g_2 H$, puisque $g_1 H$ et $g_2 H$ sont des sous-variétés fermées de G (car H l'est), stables par H, le théorème 2.8 fournit une fonction $f \in \mathbf{C}[G]^H$ nulle sur $g_1 H$ et qui vaut 1 sur $g_2 H$, donc $\pi_G(g_1) \neq \pi_G(g_2)$. $\square$

Exercice 2.9. Gardons les mêmes hypothèses sur G et X.

a) Montrer que tout morphisme G-invariant $f : X \to Z$, avec Z une variété affine se factorise de manière unique en un morphisme $X//G \to Z$.

b) Soit $Y \subset X$ une sous-variété fermée G-stable de X. Montrer que l'on dispose d'un morphisme naturel $Y//G \to X//G$, qui est une immersion fermée. Si Y' est une autre sous-variété fermée G-stable de X, alors $\pi_X(Y \cap Y') = \pi_X(Y) \cap \pi_X(Y')$.

c) Montrer que chaque fibre de π_X contient une unique G-orbite fermée (donc $X//G$ s'identifie à l'ensemble des G-orbites fermées dans X).

3 Sous-groupes auto-adjoints de $\mathbf{GL}_n(\mathbf{C})$

Nous avons vu que les tores sont des groupes algébriques réductifs, mais pour l'instant nous n'avons pas vraiment d'exemple plus frappant. Pour remédier à cela, introduisons une nouvelle classe de groupes algébriques:

Définition 3.1. Un sous-groupe algébrique G de $\mathbf{GL}_n(\mathbf{C})$ est dit **auto-adjoint** si G est stable par $g \to g^* := \bar{g}^T$ ($\bar{g}$ est le conjugué complexe de g).

3.1 Le théorème de Cartan-Chevalley

Rappelons la **décomposition polaire**: les applications[8]

$$\exp : H_n := \{X \in M_n(\mathbf{C}) |\, X = X^*\} \to H_n^+ := \{X \in H_n |\, X > 0\}$$

et $U(n) \times H_n^+ \to \mathbf{GL}_n(\mathbf{C}), (u, k) \to uk$ sont des homéomorphismes[9].

Exercice 3.1. Démontrer cette assertion.

Le résultat suivant en est une vaste généralisation:

Théorème 3.2. *(Cartan, Chevalley) Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un groupe algébrique auto-adjoint, et soient*

$$K = G \cap U(n), \quad \mathfrak{p} = \{X \in \mathfrak{g} |\, X = X^*\}.$$

[7] Si I est l'idéal de Y dans X, $\{f|_Z | f \in I\}$ est un idéal de $\mathbf{C}[Z]$ qui n'est contenu dans aucun idéal maximal, donc c'est $\mathbf{C}[Z]$ tout entier.

[8] $X > 0$ signifie: X est définie positive.

[9] Même des difféomorphismes, mais c'est plus délicat à voir.

*a) (**décomposition de Cartan**) L'application $K \times \mathfrak{p} \to G, (k, X) \to ke^X$ est un homéomorphisme et $\mathfrak{p} = i \cdot \mathrm{Lie}(K)$.*

b) K est un sous-groupe compact maximal de G, Zariski dense dans G, rencontrant chaque composante connexe de G (i.e. $G = KG^0$).

Proof. a) L'application $\theta : H := \mathbf{GL}_n(\mathbf{C}) \to H, g \to (g^*)^{-1}$ est une involution de H, préservant G. De plus, la dérivée de θ est[10] $\theta : M_n(\mathbf{C}) \to M_n(\mathbf{C}), X \to -X^*$ sur l'algèbre de Lie $M_n(\mathbf{C})$ de H. Comme θ préserve G, on a $\theta(\mathfrak{g}) \subset \mathfrak{g}$ et $\theta : \mathfrak{g} \to \mathfrak{g}$ est une involution, d'où une décomposition $\mathfrak{g} = \mathfrak{g}^{\theta=1} \oplus \mathfrak{g}^{\theta=-1}$ en espaces propres. Par définition $\mathfrak{p} = \mathfrak{g}^{\theta=-1}$.

Notons que $K = G^{\theta=1}$ est compact, en tant que fermé du compact $U(n) = H^{\theta=1}$. Soit $\mathfrak{k} = \mathrm{Lie}(K)$. Comme $K = G^{\theta=1}$, une matrice $X \in M_n(\mathbf{C})$ est dans $\mathfrak{k}$ si et seulement si $\theta(e^{tX}) = e^{tX}$ pour tout $t \in \mathbf{R}$, i.e. $e^{t\theta(X)} = e^{tX}$ pour tout t, i.e. $X = \theta(X)$. On a donc $\mathfrak{k} = \mathfrak{g}^{\theta=1}$ et comme $\mathfrak{p} = \mathfrak{g}^{\theta=-1}$, on a bien $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ et $\mathfrak{k} = i\mathfrak{p}$.

Pour montrer que $K \times \mathfrak{p} \to G$ est un homéomorphisme il suffit, d'après la décomposition polaire, de montrer que si $X \in M_n(\mathbf{C})$ est hermitienne, $k \in U(n)$ et $g = ke^X \in G$, alors $k \in G$ et $X \in \mathfrak{p}$. Il suffit bien sûr de montrer que $X \in \mathfrak{p}$. Par hypothèse $\theta(g) = ke^{-X} \in G$, donc $e^{2X} \in G$. Ainsi $e^{2nX} \in G$ pour tout $n \in \mathbf{Z}$ et on veut montrer que $e^{tX} \in G$ pour tout $t \in \mathbf{R}$. On se ramène donc à démontrer (en prenant $Y = X/2$):

Lemme 3.1. *Soit $Y \in M_n(\mathbf{C})$ hermitienne et soit P une fonction polynomiale sur $M_n(\mathbf{C})$ telle que $P(e^{nY}) = 0$ pour tout $n \in \mathbf{Z}$. Alors $P(e^{tY}) = 0$ pour tout $t \in \mathbf{R}$.*

Proof. En diagonalisant Y, on se ramène à démontrer que si $x_1, ..., x_d \in \mathbf{R}$ et $f \in \mathbf{C}[X_1, ..., X_d]$ vérifie $f(e^{nx_1}, ..., e^{nx_d}) = 0$ pour tout $n \in \mathbf{Z}$, alors $f(e^{tx_1}, ..., e^{tx_d}) = 0$ pour tout $t \in \mathbf{R}$. On veut donc montrer que si $b_1, ..., b_m \in \mathbf{C}$ et $y_1, ..., y_m \in \mathbf{R}$ vérifient $b_1e^{ny_1} + ... + b_me^{ny_m} = 0$ pour tout $n \in \mathbf{Z}$, alors $b_1e^{ty_1} + ... + b_me^{ty_m} = 0$ pour tout $t \in \mathbf{R}$. C'est un exercice facile d'analyse laissé au lecteur. □

b) Le tout dernier point découle facilement de a). Montrons que K est un compact maximal de G. Soit L un sous-groupe compact de G contenant strictement K. D'après a) L contient e^X pour un $X \in \mathfrak{p}$ non nul. Donc e^{kX} reste dans le compact L quand $k \in \mathbf{Z}$. Comme X est diagonalisable, à valeurs propres réelles, on voit facilement que cela n'est pas possible pour $X \neq 0$, une contradiction. Donc K est un sous-groupe compact maximal de G.

Montrons enfin que K est Zariski dense dans G. Si $f \in \mathbf{C}[G]$ est nulle sur K, il suffit de voir que $f(ke^X) = 0$ pour tout $k \in K$ et $X \in \mathfrak{p}$. Or la fonction $z \to f(ke^{zX})$ est holomorphe sur $\mathbf{C}$ et nulle sur $i\mathbf{R}$, car $e^{zX} \in K$ pour $z \in i\mathbf{R}$. Donc cette fonction est nulle, ce qui permet de conclure. □

Corollaire 3.1. *(**astuce unitaire**) Tout sous-groupe algébrique auto-adjoint G de $\mathbf{GL}_n(\mathbf{C})$ est réductif.*

Proof. Soit V une représentation algébrique de G. Gardons les notations du théorème et prenons un produit hermitien invariant par K dans V. Si W est un sous-espace stable par G dans V, alors $W^\perp$ est un supplémentaire stable par K. Mais K étant Zariski-dense dans G et la représentation étant algébrique, $W^\perp$ est automatiquement stable par G. Cela permet de conclure. □

[10] Par abus de notation on écrit θ au lieu de $d\theta$...

3.2 Le théorème de Cartan, Chevalley, Mostow

Dans ce paragraphe nous démontrons le théorème profond suivant:

Théorème 3.3. *(Cartan, Chevalley, Mostow) Pour un sous-groupe algébrique G de $\mathbf{GL}_n(\mathbf{C})$ les assertions suivantes sont équivalentes:*

a) G est réductif.

b) G possède un sous-groupe compact[11] *Zariski dense dans G.*

c) G est conjugué à un sous-groupe auto-adjoint de $\mathbf{GL}_n(\mathbf{C})$.

Proof. Le fait que c) entraîne a) découle du cor. 3.1. Appelons **presque compact** un sous-groupe algébrique G de $\mathbf{GL}_n(\mathbf{C})$ conjugué à un sous-groupe auto-adjoint. L'équivalence entre b) et c) découle du:

Lemme 3.2. *Un sous-groupe algébrique $G \subset \mathbf{GL}_n(\mathbf{C})$ est presque compact si et seulement s'il possède un sous-groupe compact Zariski-dense.*

Proof. Si G est presque compact, le théorème 3.2 montre l'existence d'un sous-groupe compact Zariski-dense. Réciproquement, supposons que K est compact et Zariski dense dans G. Quitte à conjuguer G, on peut supposer que $K \subset U(n)$. Soit $g \in G$ et montrons que $g^* \in G$, ce qui permettra de conclure. Il suffit de voir que pour tout $f \in \mathbf{C}[\mathbf{GL}_n(\mathbf{C})]$ nulle sur G on a $f(g^*) = 0$. Mais f est nulle sur K et donc $f(k^*) = f(k^{-1}) = 0$ pour $k \in K$. Comme K est Zariski-dense, on a $f(g^*) = 0$ pour tout $g \in G$, ce qui permet de conclure. □

Il reste à voir que a) implique b) ou c). C'est la partie difficile. Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un groupe réductif et faisons agir G par translation à droite sur $H = \mathbf{GL}_n(\mathbf{C})$. La variété affine $X = H//G$ est munie d'une action transitive de H (cor. 2.2). L'idéal m des fonctions $f \in \mathbf{C}[H]^G$ nulles en 1 (et donc sur G) est un point x de X et on récupère G comme le stabilisateur $G = H_x$ de ce point. En effet, il est clair que $G \subset H_x$, et si $g \in H_x \backslash G$, alors G et gG sont des fermés disjoints de H, donc il existe $f \in \mathbf{C}[H]^G$ nulle sur G et valant 1 sur gG (théorème 2.8). On a alors $f \in m$ et $g.f \notin m$, une contradiction avec $g.m = m$. Le théorème de Matsushima ci-dessous permet alors de conclure que G est presque compact. □

Théorème 3.4. *(Matsushima) Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un groupe algébrique presque compact, agissant transitivement sur une variété affine X. Alors pour tout $x \in X$ le stabilisateur G_x de x dans G est presque compact.*

Proof. Prenons (prop. 2.1) un plongement fermé $\varphi : X \to \mathbf{C}^n$ et une représentation algébrique $\rho : G \to \mathbf{GL}_n(\mathbf{C})$ tels que $\varphi(g.x) = \rho(g)\varphi(x)$. Soit $H = \rho(G)$, un sous-groupe algébrique de $\mathbf{GL}_n(\mathbf{C})$, qui est presque compact (l'image d'un sous-groupe compact Zariski dense de G est un sous-groupe compact Zariski dense de H, et on applique le lemme ci-dessus).

Si $v = \varphi(x) \in V := \mathbf{C}^n$, le morphisme φ identifie X et Hv, donc $Hv \subset V$ est fermé Zariski, et on veut montrer que le stabilisateur H_v est presque compact. Quitte à conjuguer, on peut supposer que H est auto-adjoint, donc il possède une décomposition de Cartan $H = Ke^{\mathfrak{p}}$ (théorème 3.2). Comme Hv est fermé pour la topologie usuelle dans V, il existe $w \in Hv$ tel que

$$||w|| \leq ||x||, \ \forall x \in Hv,$$

[11] Pour la topologie usuelle!

autrement dit $||hw|| \geq ||w||$ pour tout $h \in H$, où $||\cdot||$ est la norme euclidienne sur $V = \mathbf{C}^n$. Le stabilisateur H_v de v est conjugué à celui H_w de w, et il suffit donc de montrer que H_w est auto-adjoint. Prenons $g \in H_w$ et écrivons $g = ke^X$, avec $k \in K = H \cap U(n)$ et $X \in \mathfrak{p}$. Alors $ke^X w = w$ force $||e^X w|| = ||w||$. Nous allons voir que cela entraîne $Xw = 0$, donc $e^X \in H_w$ et enfin $k \in H_w$, montrant ainsi que H_w est auto-adjoint.

Montrons donc que $Xw = 0$ sachant que $||e^X w|| = ||w||$. Soit $f(t) = ||e^{tX}w||^2$. Par hypothèse $f(t) \geq f(0)$ pour tout $t \in \mathbf{R}$. Mais

$$f'(t) = \langle e^{tX}Xw, e^{tX}w\rangle + \langle e^{tX}w, e^{tX}Xw\rangle = 2\mathrm{Re}(\langle e^{tX}Xw, e^{tX}w\rangle),$$

et (en utilisant le fait que $X = X^*$ car $X \in \mathfrak{p}$)

$$f''(t) = 4||e^{tX}Xw||^2.$$

Si $Xw \neq 0$, alors $f''(t) > 0$ pour tout t, donc f' est strictement croissante. Mais $f'(0) = 0$ et $f(0) = f(1)$, ce qui est manifestement absurde. Donc $Xw = 0$. Ouf! $\square$

Exercice 3.5. Soit G un sous-groupe algébrique de $\mathbf{GL}_n(\mathbf{C})$ tel que $g \in G$ soit unipotent (i.e. $g - 1$ est une matrice nilpotente) pour tout $g \in G$. Supposons que G est réductif.

a) Montrer que G est trivial en utilisant le théorème ci-dessus.

b) Montrer le même résultat sans utiliser ce théorème, en montrant que $V^G \neq 0$ pour toute représentation algébrique non nulle V de G.

Remarque 3.6. On déduit de l'exercice et du théorème 2.3 qu'un groupe réductif ne possède pas de sous-groupe fermé (Zariski), distingué, unipotent (i.e. dont tous les éléments sont des matrices unipotentes). La réciproque est en fait vraie, mais je ne sais pas la démontrer sans faire un tas de contorsions...

3.3 Les points réels d'un groupe auto-adjoint défini sur R

Dans tout ce paragraphe $G \subset \mathbf{GL}_n(\mathbf{C})$ est un sous-groupe algébrique auto-adjoint défini sur R et $G_0 = G(\mathbf{R}) = G \cap \mathbf{GL}_n(\mathbf{R})$ est le groupe des points réels de G. Notons que G_0 est un sous-groupe fermé de $\mathbf{GL}_n(\mathbf{R})$, qui n'est pas forcément connexe même si G l'est (penser à $G = \mathbf{GL}_n(\mathbf{C})$). Posons

$$\mathfrak{g} = \mathrm{Lie}(G),\ K = G \cap U(n),\ \mathfrak{k} = \mathrm{Lie}(K),\ \mathfrak{p} = i\mathfrak{k}$$

et leurs versions réelles

$$\mathfrak{g}_0 = \mathrm{Lie}(G_0) = \mathfrak{g} \cap M_n(\mathbf{R}),\ K_0 := G_0 \cap K = G \cap O(n),\ \mathfrak{k}_0 = \mathrm{Lie}(K_0),\ \mathfrak{p}_0 = \mathfrak{p} \cap M_n(\mathbf{R}).$$

La "décomposition de Cartan réelle" devient:

Proposition 3.1. *a) L'application naturelle $\mathfrak{g}_0 \otimes_{\mathbf{R}} \mathbf{C} \to \mathfrak{g}$ est bijective.*

b) L'application $K_0 \times \mathfrak{p}_0 \to G_0, (k, X) \to ke^X$ est un homéomorphisme.

c) K_0 est un sous-groupe compact maximal de G_0, rencontrant chaque composante connexe de G_0.

Proof. a) découle du corollaire 1.1. Pour b), il suffit (par le théorème 3.2) de montrer que si $ke^X \in G_0$ ($k \in K, X \in \mathfrak{p}$), alors $k \in K_0$ et $X \in \mathfrak{p}_0$. Comme $\theta(ke^X) = ke^{-X} \in G_0$, on a $e^{2X} \in G_0 \subset M_n(\mathbf{R})$. Or $X = UDU^{-1}$ pour une matrice $U \in U(n)$ et $D \in M_n(\mathbf{R})$ diagonale (car X est hermitienne), donc $Ue^{2D}U^{-1}$ est à coefficients réels et donc $A = \bar{U}^{-1}U$ commute à e^{2D}. On en déduit que A commute à D (immédiat) et donc $X = \bar{X}$ et enfin $X \in M_n(\mathbf{R}) \cap \mathfrak{p} = \mathfrak{p}_0$. Mais alors $ke^X \in G_0$ force $k \in G_0 \cap K = K_0$. Le premier point de c) se démontre comme dans le théorème 3.2. Le fait que K_0 rencontre toute composante connexe de G_0 vient du point b), qui montre que G_0/K_0 est connexe (et simplement connexe). □

Le théorème suivant est franchement difficile:

Théorème 3.7. *(Cartan) Si K_1 est un sous-groupe compact de G_0 (resp. G), il existe $X \in \mathfrak{p}_0$ (resp. $X \in \mathfrak{p}$) tel que $e^X K_1 e^{-X} \subset K_0$ (resp. $e^X K_1 e^{-X} \subset K$). Ainsi, les sous-groupes compacts maximaux de G_0 (resp. G) sont conjugués à K_0 (resp. K).*

Proof. Nous allons montrer uniquement l'assertion concernant G_0, l'argument est identique pour G. Soit $G_0^+ = e^{\mathfrak{p}_0}$. Par la décomposition de Cartan, G_0^+ est l'ensemble des matrices symétriques définies positives dans G_0. On veut trouver $h \in G_0^+$ tel que $h^{-1}K_1 h \subset K_0$, ce qui revient à dire que $h^{-1}kh$ est orthogonale pour $k \in K_1$, ou encore $kh^2k^T = h^2$. Autrement dit on veut trouver $X_0 \in G_0^+$ tel que $kX_0k^T = X_0$ pour $k \in K_1$. Nous le ferons en deux étapes:

Etape 1: construction de X_0. La matrice symétrique, définie positive $p = \int_{K_1} k^T \cdot k dk$ vérifie $k^T pk = p$ pour $k \in K_1$. Nous allons montrer que la fonction

$$F : G_0^+ \to \mathbf{R}, \quad F(X) = \mathrm{Tr}(pX + p^{-1}X^{-1})$$

possède un minimum > 0 sur G_0^+, et X_0 sera un point de G_0^+ où le minimum est atteint. Pour montrer cela nous avons besoin du:

Exercice 3.8. Si $A, B \in M_n(\mathbf{R})$ sont symétriques définies positives, alors $\mathrm{Tr}(AB) \geq \min(\mathrm{Sp}(A)) \cdot \mathrm{Tr}(B) > 0$, où $\mathrm{Sp}(A)$ est l'ensemble des valeurs propres de A.

L'exercice montre qu'il existe $c > 0$ tel que pour $X \in G_0^+$

$$F(X) \geq c(\mathrm{Tr}(X) + \mathrm{Tr}(X^{-1})),$$

en particulier $F(X) \geq 2nc$ et $C = \inf_{X \in G_0^+} F(X) > 0$. La même inégalité montre que F est propre, i.e. pour tout $c > 0$ l'ensemble $\{X \in G_0^+ | F(X) \leq c\}$ est compact. Il existe donc $X_0 \in G_0^+$ tel que

$$F(X_0) = C = \min_{X \in G_0^+} F(X) > 0.$$

Etape 2: montrons que X_0 est solution du problème, i.e. que $kX_0k^T = X_0$ pour $k \in K_1$, ou encore $kX_0k^T = g^2$, avec $g = X_0^{1/2} \in G_0^+$.

Puisque $g^{-1}(kX_0k^T)g^{-1}$ est symétrique, définie positive et dans G, on peut écrire

$$kX_0k^T = ge^Z g, \quad Z \in \mathfrak{p}_0.$$

Pour la même raison, pour tout $t \in \mathbf{R}$ la matrice $ge^{tZ}g$ est dans G_0^+, en particulier

$$\mathrm{Tr}(p(ge^{tZ}g) + p^{-1}(ge^{tZ}g)^{-1}) \geq C.$$

En posant $A = gpg$, cela s'écrit

$$f(t) \geq C, \quad f(t) = \mathrm{Tr}(Ae^{tZ} + A^{-1}e^{-tZ}).$$

Puisque $g^2 = X_0$ et $k^T pk = p$,

$$\mathrm{Tr}(A) = \mathrm{Tr}(pX_0), \mathrm{Tr}(Ae^Z) = \mathrm{Tr}(gpge^Z) = \mathrm{Tr}(pge^Z g) = \mathrm{Tr}(pkX_0k^T) = \mathrm{Tr}(pX_0),$$

donc

$$f(0) = f(1) = C = F(X_0).$$

Ainsi $f(t) \geq f(0)$ pour tout t et donc $f'(0) = 0$. Enfin, si $Z \neq 0$ le lemme ci-dessus montre que pour tout t

$$f''(t) = \mathrm{Tr}(AZ^2e^{tZ} + A^{-1}Z^2e^{-tZ}) > 0,$$

donc f' est strictement croissante, s'annule en 0, et $f(0) = f(1)$. Cela est évidemment absurde, donc $Z = 0$ et $kX_0k^T = g^2 = X_0$. Ouf! $\square$

Exercice 3.9. Donner une preuve "facile" de ce théorème quand $G = \mathbf{GL}_n(\mathbf{C})$.

Combiné au théorème 3.3, cela fournit le résultat fondamental suivant:

Théorème 3.10. *(Cartan, Mostow) Si G est un groupe réductif, tous les sous-groupes compacts maximaux de G sont conjugués.*

Remarque 3.11. On peut résumer bon nombre de résultats ci-dessus comme suit: on dispose d'une correspondance (**dualité de Tannaka-Krein**) entre les groupes de Lie compacts (à isomorphisme près) et les groupes algébriques réductifs (à isomorphisme près). Si G est un groupe algébrique réductif, on lui associe un sous-groupe compact maximal de G, qui est bien défini à conjugaison près par le théorème ci-dessus. Dans l'autre sens, si K est un groupe de Lie compact, le théorème de Peter-Weyl entraîne facilement que K peut se réaliser comme un sous-groupe compact d'un $\mathbf{GL}_n(\mathbf{C})$ et alors l'adhérence Zariski de K dans G est un sous-groupe algébrique réductif de $\mathbf{GL}_n(\mathbf{C})$, qui a l'air de dépendre du choix du plongement de K dans $\mathbf{GL}_n(\mathbf{C})$ (et de n...). En fait, il n'en est rien (à isomorphisme près), car on montre que l'on peut caractériser l'algèbre A des fonctions régulières sur ce groupe algébrique de manière simple à partir de K: c'est l'algèbre des fonctions K-finies dans $C(K)$! Démontrer toutes ces assertions prend un peu de place, mais ce n'est pas difficile avec les outils que l'on a à notre disposition. Exercice!

Exercice 3.12. Soit G un groupe algébrique réductif et K un sous-groupe compact maximal de G. Soit $\mathrm{Rep}(G)$ la catégorie des représentations algébriques de dimension finie de G et $\mathrm{Rep}(K)$ la catégorie des représentations continues de dimension finie de K. On a un foncteur évident $F : \mathrm{Rep}(G) \to \mathrm{Rep}(K)$.

a) Montrer que F est pleinement fidèle.

b) Montrer que si $V \in \mathrm{Rep}(G)$ est irréductible, alors $F(V)$ l'est aussi.

c) Montrer que la restriction $\mathbf{C}[G] \to C(K)$ induit un isomorphisme

$$\mathbf{C}[G] \simeq C(K)_K = \{f \in C(K) |\, f \text{ est } K\text{-finie à droite (resp. gauche)}\}.$$

d) Montrer que F est une équivalence de catégories.

3.4 Les points réels d'un groupe réductif défini sur $\mathbf{R}$

Nous arrivons enfin à un point assez subtil: prenons $G \subset \mathbf{GL}_n(\mathbf{C})$ un groupe réductif **défini sur** $\mathbf{R}$, et soit $G_0 = G(\mathbf{R})$. D'après le théorème de Cartan, Chevalley, Mostow, G est conjugué à un sous-groupe auto-adjoint de $\mathbf{GL}_n(\mathbf{C})$. On voudrait en déduire que G_0 est conjugué à un sous-groupe auto-adjoint de $\mathbf{GL}_n(\mathbf{R})$. Le problème est que la matrice conjuguant G à un sous-groupe auto-adjoint n'est pas forcément réelle (pas à priori...), donc la déduction ci-dessus n'est pas formelle. En fait, l'argument (dû à Mostow, avec des simplifications apportées par Adams et Taïbi) est assez délicat et repose sur le théorème 3.10 ci-dessus.

Théorème 3.13. *(Mostow) Si $G \subset \mathbf{GL}_n(\mathbf{C})$ est un groupe réductif défini sur $\mathbf{R}$, il existe $A \in \mathbf{GL}_n(\mathbf{R})$ tel que AG_0A^{-1} soit auto-adjoint (i.e. stable par $g \to g^T$).*

Proof. Ce qui suit est un copié-collé d'un argument dans l'article d'Adams et Taïbi... Comme G est défini sur $\mathbf{R}$, il est stable par l'involution τ de $\mathbf{GL}_n(\mathbf{C})$ envoyant une matrice A sur son conjugué complexe $\bar{A}$. Il suffit (exercice) de montrer que G possède un sous-groupe compact maximal **stable par** τ. Soit K un sous-groupe compact maximal de G, d'où une décomposition de Cartan $G = Ke^{\mathfrak{p}}$. Alors $\tau(K)$ en est un aussi et donc (théorème 3.10) il existe $g \in e^{\mathfrak{p}}$ tel que $\tau K = gKg^{-1}$. Alors $K = \tau(g)\tau(K)\tau(g)^{-1} = xKx^{-1}$, où $x = \tau(g)g$. Ecrivons $x = e^X k$ avec $k \in K, X \in \mathfrak{p}$. Alors $e^X K e^{-X} = K$, donc si $k_1 \in K$ on peut écrire $e^X k_1 e^{-X} = k'$ pour un $k' \in K$, et donc $k_1 e^{-X} = k' e^{-\mathrm{Ad}(k')^{-1}(X)}$. L'unicité de la décomposition de Cartan fournit $k_1 = k'$, donc e^X commute à k_1, donc à K, donc à G (car K est Zariski dense dans G). Ainsi $e^X \in Z(G)$.

Ensuite, comme $g^{-1}\tau(K)g = K$ et $\mathfrak{p} = i\mathrm{Lie}(K)$, on obtient sans mal $g^{-1}\tau(e^{\mathfrak{p}})g = e^{\mathfrak{p}}$ et comme $g \in e^{\mathfrak{p}}$, il s'ensuit que $g^{-1}x \in e^{\mathfrak{p}}$. Mais $g^{-1}x = g^{-1}e^X k$ et $g^{-1}e^X \in e^{\mathfrak{p}}$ (puisque e^X est central dans G), donc par l'unicité dans la décomposition de Cartan $k = 1$ et $x = e^X \in Z(G)$. En particulier $\tau(x) = \tau(\tau(g)g) = g\tau(g) = gxg^{-1} = x$. En remplaçant g par $gx^{-1/2}$ (avec $x^{-1/2} = e^{-X/2}$), on peut supposer que $\tau(g) = g^{-1}$, ce qui force $\tau(g^{1/2}) = g^{-1/2}$. En posant $K_1 = g^{1/2}Kg^{-1/2}$ on obtient sans mal que $\tau(K_1) = K_1$, et K_1 est un compact maximal de G. $\square$

En fait on dispose du résultat plus général suivant:

Théorème 3.14. *(Mostow) Si $G_1 \subset ... \subset G_k$ sont des groupes algébriques réductifs définis sur $\mathbf{R}$, il existe $A \in \mathbf{GL}_n(\mathbf{R})$ tel que AG_iA^{-1} soit stable par $g \to g^T$ pour tout $1 \leq i \leq k$.*