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.

Les résultats principaux de ces 2 cours sont:

• 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 $\mathbf{GL}_n(\mathbf{C})$ (i.e. l'existence d'une forme compacte d'un groupe réductif).

• le théorème de Cartan-Mostow sur la conjugaison des sous-groupes compacts maximaux d'un groupe réductif.

• le théorème de restriction de Chevalley concernant l'étude des fonctions invariantes par conjugaison sur l'algèbre de Lie d'un tel groupe.

• le théorème de finitude de Harish-Chandra.

Ces résultats fondamentaux sont délicats et nous en donnons des preuves complètes. Nous étudions ensuite les tores maximaux dans un groupe réductif et construisons le système de racines.

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

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 $\mathbf{GL}_n(\mathbf{C})$.

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.

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

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. □

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].

[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 ...

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

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

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.

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

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).

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 $g_i \in G$, $1 \leq i \leq d$. 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 $W = \mathrm{Vect}_{1 \leq i \leq m, g \in G}(g.f_i)$. 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). □

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.

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

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.

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 $f = f_1F_1 + ... + f_rF_r$, et on peut supposer que F_i est homogène, de degré $d - \deg(f_i) < d$. Alors

$$f = R_X(f) = R_X(f_1F_1 + ... + f_rF_r) = f_1R_X(F_1) + ... + f_rR_X(F_r).$$

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. □

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. □

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 $g_1H \neq g_2H$, puisque g_1H et g_2H 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_1H et qui vaut 1 sur g_2H, donc $\pi_G(g_1) \neq \pi_G(g_2)$. □

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:

[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.

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

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

*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.*

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

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. □

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 $g \in H_x \setminus G$, 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).

[11] Pour la topologie usuelle!

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

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

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! □

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 $k^T p k = p$ 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

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

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 $k^Tpk = p$,

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

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! □

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. □

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 $1 \leq i \leq k$.*

4 Sous-groupes d'un tore algébrique

Rappelons qu'un tore algébrique est un groupe algébrique isomorphe au groupe $D_n(\mathbf{C})$ des matrices diagonales dans $\mathbf{GL}_n(\mathbf{C})$. Si G est un groupe algébrique on note

$$X(G) = \mathrm{Hom}_{\mathrm{gr.alg}}(G, \mathbf{C}^*), \quad X_*(G) := \mathrm{Hom}_{\mathrm{gr.alg}}(\mathbf{C}^*, G)$$

le groupe des caractères (resp. co-caractères) algébriques de G.

Exercice 4.1. Soit T un tore.

a) Montrer que $X(T)$ est une $\mathbf{C}$-base de $\mathbf{C}[T]$ et un $\mathbf{Z}$-module libre de rang $\dim T$. De plus, si $\chi_1, ..., \chi_n$ est une base de $X(T)$, alors $T \simeq D_n(\mathbf{C})$ via $t \to \operatorname{diag}(\chi_1(t), ..., \chi_n(t))$.

b) $X_*(T)$ est un $\mathbf{Z}$-module libre de rang $\dim T$ et il s'identifie au $\mathbf{Z}$-dual de $X(T)$.

Le résultat suivant décrit explicitement les sous-groupes algébriques d'un tore.

Théorème 4.2. *Soit T un tore, $X = X(T)$, G un sous-groupe Zariski fermé de T.*

a) $A(G) := \{\chi \in X | \ \chi|G = 1\}$ est un sous-groupe de X et $G = \cap_{\chi \in A(G)} \ker(\chi)$.

b) $X(G) = X/A(G)$ et G est un tore si et seulement si $X(G)$ est sans torsion.

Proof. a) Il est clair que $A(G)$ est un sous-groupe de X. Pour montrer que $G = \cap_{\chi \in A(G)} \ker(\chi)$ on va montrer d'abord qu'il existe des $\chi_i \in X$ tels que $G = \cap_{i \in I} \ker(\chi_i)$. Il suffit de montrer que l'idéal I de G est engendré comme $\mathbf{C}$-espace vectoriel par des fonctions de la forme $\chi - \chi'$, avec $\chi, \chi' \in X$ (car alors G sera l'intersection des noyaux des $\chi' \cdot \chi^{-1}$ pour ces χ, χ'). Soit $f \in I \subset \mathbf{C}[T]$, écrivons $f = \sum_{i=1}^n a_i \chi_i$ avec $a_i \in \mathbf{C}$ et $\chi_i \in X$. On peut supposer que les a_i ne sont pas tous nuls. Alors $\sum a_i \mu_i = 0$, où $\mu_i = \chi_i | G \in X(G)$, et par indépendance linéaire des caractères deux des μ_i sont égaux, disons $\mu_1 = \mu_2$, donc $\chi_1 - \chi_2 \in I$. Alors $F := (a_1 + a_2)\chi_2 + a_3\chi_3 + ... + a_n\chi_n \in I$ et par récurrence sur n c'est une combinaison linéaire de $\chi - \chi'$, avec $\chi, \chi' \in X$. Donc $f = a_1(\chi_1 - \chi_2) + F$ est de la même forme, ce qui permet de conclure.

On a donc $G = \cap_{\chi \in A} \ker(\chi)$ pour un sous-groupe A de X (celui engendré par les χ_i ci-dessus). Il reste à voir que $A = A(G)$. Soit $\chi_1, ..., \chi_n$ une $\mathbf{Z}$-base de X et $d_1, ..., d_k \geq 1$ tels que $d_1\chi_1, ..., d_k\chi_k$ soit une base de A. L'isomorphisme $T \simeq (\mathbf{C}^*)^n, t \to (\chi_1(t), ..., \chi_n(t))$ identifie G à $H = \{(x_1, ..., x_n) \in (\mathbf{C}^*)^n | x_1^{d_1} = ... = x_k^{d_k} = 1\}$. Un caractère $\chi = \prod_{i=1}^n \chi_i^{k_i}$ est dans $A(G)$ si et seulement si $\prod_{i=1}^n x_i^{k_i} = 1$ pour tous $(x_1, ..., x_n) \in H$. Cela équivaut clairement à $k_i = 0$ pour $i > k$ et $d_i \mid k_i$ pour $i \leq k$, autrement dit à ce que $\chi \in A$. On a donc $A(G) = A$.

b) $A(G)$ est clairement le noyau de la restriction $X \to X(G)$. Il reste à voir que celle-ci est surjective. Soit $\chi \in X(G)$, alors $\chi \in \mathbf{C}[G]$, donc χ est la restriction à G d'un élément de $\mathbf{C}[T]$, qui est de la forme $\sum_{i=1}^n a_i \mu_i$, avec $\mu_i \in X$. Or si $\sum_{i=1}^n a_i \mu_i | T = \chi$, l'indépendance linéaire des caractères montre que $\chi = \mu | T$ pour un $\mu \in X$ et donc $X \to X(G)$ est surjective.

Si G est un tore il est clair que $X(G)$ est sans torsion. Dans l'autre sens, si $X(G) = X/A(G)$ est sans torsion, il existe une base $\chi_1, ..., \chi_n$ de X et $k \leq n$ tel que $\chi_1, ..., \chi_k$ soit une base de $A(G)$. En identifiant T et $(\mathbf{C}^*)^n$ via $t \to (\chi_1(t), ..., \chi_n(t))$, il est clair que G s'identifie à $(\mathbf{C}^*)^{n-k}$ et donc est un tore. □

Nous pouvons caractériser maintenant les tores: ce sont les groupes réductifs commutatifs et connexes, comme le montre le résultat important suivant:

Corollaire 4.1. *Soit G un groupe algébrique réductif. Alors $Z(G)^0$ est un tore. En particulier, si G est commutatif, alors G^0 est un tore.*

Proof. Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ et $V = \mathbf{C}^n$. Comme G est réductif, on peut écrire $V = \oplus_i V_i$, avec V_i des G-modules simples. Le groupe $H = Z(G)^0$ préserve chaque V_i et son action commute à celle de G, qui est irréductible. Par le lemme de Schur tout $h \in H$ agit par un scalaire sur chaque V_i. Donc les éléments de H forment une famille commutative d'endomorphismes diagonalisables de V, et donc ils sont simultanément diagonalisables. On en déduit que H est conjugué à un sous-groupe Zariski fermé de $D_n(\mathbf{C})$. On conclut via le th. 4.2. □

5 Le théorème de restriction de Chevalley et le théorème de finitude de Harish-Chandra

Le but principal de ce chapitre est de démontrer deux théorèmes fondamenraux: le théorème de finitude de Harish-Chandra et le théorème de restriction de Chevalley, le second concernant l'étude des fonctions polynomiales sur $\mathfrak{g}$ invariantes par conjugaison par G. Pour $G = \mathbf{GL}_n(\mathbf{C})$ c'est très simple (exercice!), mais le cas général est nettement plus délicat. Nous introduisons pour cela un certain nombre d'outils qui seront pleinement utilisés dans la construction du système de racines d'un groupe réductif.

5.1 Sous-espaces de Cartan et tores maximaux

Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un groupe algébrique auto-adjoint et posons

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

de telle sorte que $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ et $G = Ke^{\mathfrak{p}}$. Posons

$$B(X, Y) = \mathrm{Tr}(XY), \langle X, Y\rangle = \mathrm{Tr}(XY^*).$$

L'accouplement $\langle\, ,\, \rangle$ est un produit hermitien sur $M_n(\mathbf{C})$, qui se restreint en un produit hermitien sur $\mathfrak{g}$ (qui est stable par $Y \to Y^*$) et donc B est non dégénérée sur $\mathfrak{g}$. Un objet central dans l'étude de la structure fine de G est:

Définition 5.1. Un **sous-espace de Cartan** de $\mathfrak{p}$ est un sous-espace $\mathfrak{a}$ de $\mathfrak{p}$ qui est abélien (i.e. les matrices dans $\mathfrak{a}$ commutent deux à deux) et maximal pour cette propriété.

Si $X \in \mathfrak{g}$ on écrit $\mathrm{ad}(X)$ pour l'endomorphisme $Y \to [X, Y] = XY - YX$ de $\mathfrak{g}$.

Proposition 5.1. *Soit $\mathfrak{a}$ un sous-espace de Cartan de $\mathfrak{p}$ et soit $\mathfrak{h} = \mathfrak{a} + i\mathfrak{a} \subset \mathfrak{g}$.*
a) Si $X \in \mathfrak{h}$, alors $X \in M_n(\mathbf{C})$ et $\mathrm{ad}(X) \in \mathrm{End}(\mathfrak{g})$ sont diagonalisables.
b) Si $X \in \mathfrak{g}$ commute à $\mathfrak{h}$, alors $X \in \mathfrak{h}$.
c) La restriction de B à $\mathfrak{h}$ est non dégénérée.

Proof. a) Les matrices dans $\mathfrak{a}$ sont hermitiennes, donc diagonalisables, et commutent deux à deux, donc les éléments de $\mathfrak{h}$ sont diagonalisables. Ensuite, $\mathrm{ad}(X)$ est auto-adjoint pour le produit scalaire $\langle ., .\rangle$ (calcul immédiat).

b) Si $X = Y + iZ$ avec $Y, Z \in \mathfrak{p}$ et $A \in \mathfrak{a}$, alors $YA + iZA = AY + iAZ$, i.e. $YA - AY = i(AZ - ZA)$. Comme A, Y, Z sont hermitiennes, cela force $YA = AY, AZ = ZA$. On a donc $Y, Z \in \mathfrak{a}$ par maximalité de $\mathfrak{a}$, et $X \in \mathfrak{h}$.

c) Si $X \in \mathfrak{h}$ alors $X^* \in \mathfrak{h}$, or $B(X, X^*) = 0$ force $X = 0$. □

Soient $\mathfrak{a}$ et $\mathfrak{h}$ comme ci-dessus. Les $\mathrm{ad}(H)$ pour $H \in \mathfrak{h}$ forment une famille commutative d'endomorphismes diagonalisables de $\mathfrak{g}$, d'où une décomposition en sous-espaces propres simultanés

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in \Phi(\mathfrak{g}, \mathfrak{h})} \mathfrak{g}_\alpha, \quad \mathfrak{g}_\alpha := \{X \in \mathfrak{g} |\, [H, X] = \alpha(H)X, \forall H \in \mathfrak{h}\},$$

$\Phi(\mathfrak{g}, \mathfrak{h})$ étant l'ensemble (fini) des $\alpha \in \mathfrak{h}^* = \mathrm{Hom}_{\mathbf{C}}(\mathfrak{h}, \mathbf{C})$ non nuls tels que $\mathfrak{g}_\alpha \neq 0$, appelés **racines de $\mathfrak{g}$ par rapport à $\mathfrak{h}$**. La proposition 5.1 montre que $\mathfrak{g}_0 = \mathfrak{h}$.

Un résultat fondamental et délicat est le suivant:

Théorème 5.1. *Soient* $\mathfrak{a}, \mathfrak{a}'$ *des sous-espaces de Cartan de* $\mathfrak{p}$.

a) Il existe $k \in K$ *tels que* $\mathfrak{a}' = k\mathfrak{a}k^{-1} = \mathrm{Ad}(k)(\mathfrak{a})$.

b) On a $\mathfrak{p} = \cup_{k \in K} \mathrm{Ad}(k)(\mathfrak{a})$ *et* $G = KAK$, *où* $A = e^{\mathfrak{a}}$.

Proof. a) Prenons $H \in \mathfrak{a}$ (resp. $H' \in \mathfrak{a}'$) tel que $\alpha(H) \neq 0$ (resp. $\alpha(H') \neq 0$) pour $\alpha \in \Phi(\mathfrak{g}, \mathfrak{h})$ (c'est possible car $\Phi(\mathfrak{g}, \mathfrak{h})$ est fini). Alors on voit tout de suite que $\mathfrak{a}$ (resp. $\mathfrak{a}'$) est le centralisateur de H (resp. H') dans $\mathfrak{p}$ (prendre X dans le centralisateur et écrire $X = A + \sum_\alpha X_\alpha$, avec $A \in \mathfrak{h}$ et $X_\alpha \in \mathfrak{g}_\alpha$). La fonction $f(k) = \mathrm{Re}(\langle \mathrm{Ad}(k)(H), H' \rangle)$ possède un minimum sur K, disons en $k_0 \in K$. Soit $Z = \mathrm{Ad}(k_0)(H) \in \mathfrak{p}$. Pour tout $X \in \mathfrak{k}$ on a

$$0 = \frac{d}{dt}|_{t=0} \mathrm{Re}\langle \mathrm{Ad}(e^{tX})Z, H' \rangle = \mathrm{Re}\langle \mathrm{ad}(X)(Z), H' \rangle =$$

$$-\mathrm{Re}\langle \mathrm{ad}(Z)(X), H' \rangle = -\mathrm{Re}\langle X, \mathrm{Ad}(Z)(H') \rangle,$$

la dernière égalité venant du fait que $\mathrm{Ad}(Z)$ est auto-adjoint par rapport à $\langle ., . \rangle$ (car $Z \in \mathfrak{p}$). La matrice $A = \mathrm{Ad}(Z)(H')$ est dans $\mathfrak{k}$, en particulier $\mathrm{Re}\langle A, A \rangle = 0$, ce qui force $A = 0$. Ainsi Z commute à H' et est dans $\mathfrak{p}$, donc $Z \in \mathfrak{a}'$ et $H \in \mathrm{Ad}(k_0^{-1})(\mathfrak{a}')$. Si $A \in \mathrm{Ad}(k_0^{-1})(\mathfrak{a}')$, alors A commute à H et donc $A \in \mathfrak{a}$. On en déduit que $\mathrm{Ad}(k_0^{-1})(\mathfrak{a}') \subset \mathfrak{a}$ et on a forcément égalité par maximalité.

b) Tout $X \in \mathfrak{p}$ est contenu dans un sous-espace de Cartan $\mathfrak{a}'$ de $\mathfrak{p}$. On applique alors a). Le dernier point découle de la décomposition de Cartan $G = Ke^{\mathfrak{p}}$. $\square$

Nous allons appliquer les résultats ci-dessus à l'étude des tores maximaux de G. Le théorème suivant utilise le difficile théorème de Cartan, Mostow sur la conjugaison des sous-groupes compacts maximaux dans un groupe auto-adjoint, ainsi que le théorème 5.1. Cela n'est pas très étonnant: le point c) est un des points les plus délicats de la théorie des groupes algébriques...

Théorème 5.2. *a) Soit* T *un tore (algébrique) maximal de* G, *stable par* $X \to X^*$. *Alors* $\mathrm{Lie}(T) = \mathfrak{a} + i\mathfrak{a}$ *pour un sous-espace de Cartan* $\mathfrak{a}$ *de* $\mathfrak{p}$.

b) Si T *est un tore de* G, *il existe* $g \in G$ *tel que* gTg^{-1} *soit stable par* $X \to X^*$.

c) Les tores maximaux de G *sont conjugués dans* G.

Proof. a) Soit $K_T = T \cap U(n) = T \cap K$, de telle sorte que $\mathrm{Lie}(T) = \mathrm{Lie}(K_T) \oplus i\mathrm{Lie}(K_T)$ et K_T est connexe, Zariski dense dans T (th. de Cartan-Chevalley). Comme $i\mathrm{Lie}(K_T)$ est un sous-espace abélien de $\mathfrak{p}$, il existe un sous-espace de Cartan $\mathfrak{a}$ de $\mathfrak{p}$ contenant $i\mathrm{Lie}(K_T)$. Alors $K_T \subset \overline{e^{i\mathfrak{a}}} \subset K$ (l'adhérence est pour la topologie usuelle). Notons aussi que K_T est connexe, donc engendré par les e^X avec $X \in \mathrm{Lie}(K_T)$, et $\mathrm{Lie}(K_T)$ est abélienne, donc $K_T = e^{\mathrm{Lie}(K_T)}$. Soit T_1 la composante neutre de l'adhérence de Zariski de $\overline{e^{i\mathfrak{a}}}$. C'est un groupe algébrique commutatif, connexe, réductif (adhérence Zariski d'un compact!), donc un tore algébrique (cor. 4.1), contenant l'adhérence Zariski de K_T, i.e. contenant T. Par maximalité de T on a donc $T_1 = T$. Mais $K_T \subset \overline{e^{i\mathfrak{a}}} \subset T_1 = T$ (la deuxième inclusion vient de la connexité de $\overline{e^{i\mathfrak{a}}}$ et du fait que les composantes neutres pour la topologie usuelle et celle de Zariski coïncident). Comme K_T est un sous-groupe compact maximal de T, on obtient enfin $K_T = \overline{e^{i\mathfrak{a}}}$, donc $\mathfrak{a} \subset i\mathrm{Lie}(K_T)$ et par maximalité $\mathfrak{a} = i\mathrm{Lie}(K_T)$, ensuite $\mathrm{Lie}(T) = \mathfrak{a} \oplus i\mathfrak{a}$.

b) Soit T_c un sous-groupe compact Zariski dense de T. Comme T_c est un sous-groupe compact de G, il est contenu dans un sous-groupe compact maximal de G, qui est conjugué (théorème de Cartan, Mostow) à K. Il existe donc $g \in G$ tel que $g^{-1}T_c g \subset K$. Alors $T_1 = g^{-1}Tg$ est auto-adjoint car $g^{-1}T_c g$ y est Zariski dense et contenu dans $U(n)$.

c) D'après b) n'importe quel tore maximal est conjugué dans G à un tore maximal auto-adjoint. D'après a) l'algèbre de Lie d'un tel tore est décrit par un sous-espace de Cartan. On conclut en utilisant le fait que les sous-espaces de Cartan de $\mathfrak{p}$ sont conjugués sous K (théorème 5.1). □

Remarque 5.3. En utilisant Peter-Weyl, on déduit du théorème ci-dessus que les tores compacts maximaux d'un groupe de Lie compact sont conjugués, un des théorèmes fondamentaux de la théorie des groupes de Lie compacts!

Exercice 5.4. Soit G un groupe réductif et T un tore dans G. Soit $Z(T)$ le centralisateur de T dans G. En utilisant le théorème ci-dessus, démontrer les résultats (fondamentaux!) suivants:

a) Montrer que $Z(T)$ est un groupe algébrique réductif (se ramener au cas où G et T sont auto-adjoints).

b) Supposons que G est connexe et prenons un sous-groupe compact maximal K de G. Rappelons que K est connexe.

i) Supposons de plus que T est auto-adjoint. Montrer que $T \cap K$ est la réunion des tores compacts maximaux de K (i.e. des sous-groupes compacts, abéliens, connexes maximaux de K) et donc que $T \cap K$ est connexe.

ii) En déduire que $Z(T)$ est connexe.

5.2 Etude préliminaire des fonctions invariantes sur G

Dans la suite de ce chapitre $G \subset \mathbf{GL}_n(\mathbf{C})$ est un groupe algébrique auto-adjoint[12], **connexe**, et on note $\mathfrak{g}, K, \mathfrak{p}, \ldots$ les objets usuels. On choisit un sous-espace de Cartan $\mathfrak{a} \subset \mathfrak{p}$ et on pose $\mathfrak{h} = \mathfrak{a} + i\mathfrak{a}$. Si G est défini sur $\mathbf{R}$, on pose $G_0 = G(\mathbf{R})$, $\mathfrak{g}_0 = \mathrm{Lie}(G_0)$, $K_0 = K \cap G_0$. Notons que G_0 est Zariski-dense dans G: si H est l'adhérence Zariski de G_0 dans G, H est un groupe algébrique donc $\mathrm{Lie}(H)$ est un sous-$\mathbf{C}$-espace vectoriel de G contenant $\mathfrak{g}_0$, donc égal à $\mathfrak{g} = \mathfrak{g}_0 \otimes_{\mathbf{R}} \mathbf{C}$, et comme G est connexe cela force $H = G$.

Quelques sorites avant de passer aux choses sérieuses. Si V est un $\mathbf{R}$-espace vectoriel de dimension finie, on note $P(V)$ la $\mathbf{R}$-algèbre des fonctions polynomiales réelles sur V, i.e. $\varphi : V \to \mathbf{R}$ telles que pour une/ toute base $v_1, \ldots, v_n$ de V la fonction $(t_1, \ldots, t_n) \to \varphi(t_1 v_1 + \ldots + t_n v_n)$ est polynomiale. Si V est un $\mathbf{C}$-espace de dimension finie, on note $P_h(V)$ la $\mathbf{C}$-algèbre des fonctions polynomiales complexes holomorphes sur V. Si $V = \mathbf{C}$, alors $P_h(V)$ s'identifie à $\mathbf{C}[Z]$, alors que $P(R(V))$ s'identifie à $\mathbf{R}[X, Y]$, où $R(V)$ est l'espace V vu comme $\mathbf{R}$-espace vectoriel. Bien sûr $P_h(V) \subset P(R(H)) \otimes \mathbf{C}$. Si W est de dimension finie sur $\mathbf{R}$, alors $P_h(W \otimes_{\mathbf{R}} \mathbf{C})$ s'identifie à $P(W) \otimes_{\mathbf{R}} \mathbf{C}$ et $P(W)$ s'identifie à $S(W^*)$, l'algèbre symétrique de l'espace $W^* = \mathrm{Hom}_{\mathbf{R}}(W, \mathbf{R})$. De même, si V est complexe, $P_h(V)$ s'identifie à $S(V^*)$, où l'on considère l'algèbre symétrique du $\mathbf{C}$-espace vectoriel V^*.

Puisque $\mathfrak{g} \simeq \mathfrak{p} \otimes_{\mathbf{R}} \mathbf{C}$, on obtient $P_h(\mathfrak{g}) \simeq P(\mathfrak{p}) \otimes_{\mathbf{R}} \mathbf{C}$. Le groupe G agit naturellement sur $\mathfrak{g}^*$, via l'action adjointe de G sur $\mathfrak{g}$ (i.e. $g.X = gXg^{-1}$ pour

[12] Rappelons que par le théorème de Cartan, Chevalley, Mostow tout groupe algébrique réductif est conjugué à un tel G, donc ce qui suit s'applique à tout groupe algébrique réductif.

$g \in G$ et $X \in \mathfrak{g}$), donc sur $S(\mathfrak{g}^*) \simeq P_h(\mathfrak{g})$, et c'est évidemment une représentation algébrique. Le théorème des invariants de Hilbert fournit alors:

Proposition 5.2. *$S(\mathfrak{g}^*)^G \simeq P_h(\mathfrak{g})^G$ est une $\mathbf{C}$-algèbre de type fini.*

Comme K est Zariski-dense et préserve $\mathfrak{p}$, la restriction à $\mathfrak{p}$ induit

$$P_h(\mathfrak{g})^G = P_h(\mathfrak{g})^K \simeq (P(\mathfrak{p}) \otimes_{\mathbf{R}} \mathbf{C})^K = P(\mathfrak{p})^K \otimes_{\mathbf{R}} \mathbf{C}.$$

De même, puisque $\mathfrak{h} \simeq \mathfrak{a} \otimes_{\mathbf{R}} \mathbf{C}$ on a $P_h(\mathfrak{h}) \simeq P(\mathfrak{a}) \otimes_{\mathbf{R}} \mathbf{C}$. La restriction $P_h(\mathfrak{g})^G \to P_h(\mathfrak{h})$ correspond à la restriction $P(\mathfrak{p})^K \to P(\mathfrak{a})$.

Théorème 5.5. *Le morphisme de restriction $P(\mathfrak{p})^K \to P(\mathfrak{a})$ est injectif et entier, et l'extension $\mathrm{Frac}(P(\mathfrak{a}))/\mathrm{Frac}(P(\mathfrak{p})^K)$ est finie galoisienne.*

Proof. L'injectivité suit de l'égalité $\mathfrak{p} = \cup_{k \in K} \mathrm{Ad}(k)(\mathfrak{a})$ (th. 5.1). Les matrices dans $\mathfrak{a}$ sont simultanément diagonalisables dans $M_n(\mathbf{C})$, à valeurs propres réelles (car hermitiennes), d'où une décomposition $\mathbf{C}^n = \oplus_{i=1}^d V_i$ et des formes linéaires $l_i \in \mathfrak{a}^*$ telles que $Xv = l_i(X)v$ pour $X \in \mathfrak{a}$ et $v \in V_i$. Alors l_i engendrent $\mathfrak{a}^*$, donc $P(\mathfrak{a})$ est engendrée en tant que $\mathbf{R}$-algèbre par les l_i. Le polynôme

$$F(T) = \det(T \cdot \mathrm{id} - X) = T^n + \sum_{i=0}^{n-1} f_i(X) T^i$$

est à coefficients dans $P(\mathfrak{p})^K$ (les f_i sont des fonctions polynomiales en X, prenant des valeurs réelles pour $X \in \mathfrak{p}$ car X est alors hermitienne). Mais si $X \in \mathfrak{a}$ on a aussi

$$F(T) = \prod_{i=1}^d (T - l_i(X))^{\dim V_i},$$

donc les l_i sont les racines de F. Ainsi les l_i sont entiers sur $P(\mathfrak{p})^K$ et $\mathrm{Frac}(P(\mathfrak{a}))$ est le corps de décomposition de F sur $\mathrm{Frac}(P(\mathfrak{p})^K)$, ce qui permet de conclure.[13] $\square$

Nous avons aussi une version "réelle" des résultats précédents: supposons que G est défini sur $\mathbf{R}$. Un sous-espace de Cartan de $\mathfrak{p}_0$ est un sous-espace abélien maximal $\mathfrak{a}_0$ de $\mathfrak{p}_0$. On montre comme ci-dessus que les sous-espaces de Cartan sont conjugués sous K_0, que $\mathfrak{p}_0 = \cup_{k \in K_0} \mathrm{Ad}(k)(\mathfrak{a}_0)$ pour tout sous-espace de Cartan $\mathfrak{a}_0$, donc la restriction $P(\mathfrak{p}_0)^K \to P(\mathfrak{a}_0)$ est injective. Le même argument que ci-dessus montre que la restriction $P(\mathfrak{g}_0)^{G_0} \to P(\mathfrak{a}_0)$ est un morphisme entier, donc fini (car $P(\mathfrak{a}_0)$ est de type fini sur $\mathbf{R}$). Le résultat suivant est au coeur du théorème de finitude d'Harish-Chandra (à venir):

Théorème 5.6. *Le morphisme de restriction $P(\mathfrak{g}_0)^{G_0} \to P(\mathfrak{p}_0)^{K_0}$ est fini.*

Proof. Posons $A = P(\mathfrak{g}_0)^{G_0}$, $B = P(\mathfrak{p}_0)^{K_0}$ et $C = P(\mathfrak{a}_0)$. On a des morphismes de restriction $f : A \to B$, $g : B \to C$, g étant injectif et $g \circ f : A \to C$ étant fini (cf. discussion ci-dessus). Il faut voir que f est fini. Montrons d'abord que A est noethérien. Il suffit de voir que $A \otimes_{\mathbf{R}} \mathbf{C}$ l'est, or puisque $\mathfrak{g}_0 \otimes_{\mathbf{R}} \mathbf{C} = \mathfrak{g}$

$$A \otimes_{\mathbf{R}} \mathbf{C} = (P(\mathfrak{g}_0) \otimes_{\mathbf{R}} \mathbf{C})^{G_0} = P_h(\mathfrak{g})^{G_0} = P_h(\mathfrak{g})^G,$$

[13] Noter que le morphisme $P(\mathfrak{p})^K \to P(\mathfrak{a})$ est entier et que $P(\mathfrak{a})$ est de type fini, donc ce morphisme est fini et induit une extension finie au niveau des corps des fractions.

la dernière égalité ayant lieu car G_0 est Zariski dense dans G. Comme $P_h(\mathfrak{g})^G$ est une $\mathbf{C}$-algèbre de type fini (prop 5.2), $A \otimes_{\mathbf{R}} \mathbf{C}$ est noethérien.

On voit B et C comme des A-modules via f et $g \circ f$, alors $g(B) \subset C$ est un sous A-module de C et C est de type fini comme A-module, donc $g(B)$ est un A-module de type fini, disons engendré par $g(b_1), ..., g(b_k)$. Alors

$$g(B) = \sum_{i=1}^{k} A.g(b_i) = \sum_{i=1}^{k} g(f(A)b_i) = g(\sum_{i=1}^{k} f(A)b_i),$$

et l'injectivité de g montre que $B = \sum_{i=1}^{k} f(A)b_i$, ce qui finit la preuve. $\square$

5.3 Application 1: le théorème de finitude d'Harish-Chandra

On suppose dans ce paragraphe que G est défini sur $\mathbf{R}$ et on note $U = U(\mathfrak{g})$ l'algèbre enveloppante de $\mathfrak{g} = \mathfrak{g}_0 \otimes_{\mathbf{R}} \mathbf{C}$. L'action adjointe de G sur $\mathfrak{g}$ s'étend en une action de G sur U. Nous avons besoin de quelques sorites concernant cette action sur U avant de nous lancer dans la bataille.

La connexité de G entraîne (exercice) l'égalité $\mathfrak{Z}(\mathfrak{g}) = U^G$, où $\mathfrak{Z}(\mathfrak{g})$ est le centre de U. De plus, U possède une filtration $0 = U_{-1} \subset U_0 \subset ...$ définie en prenant pour U_n l'espace (de dimension finie) engendré par les $X_1...X_k$, avec $k \leq n$ et $X_i \in \mathfrak{g}$. On vérifie sans mal que $xy - yx \in U_{n+m-1}$ si $x \in U_n, y \in U_m$ (exercice), donc

$$\mathrm{gr}(U) = \bigoplus_{n \geq 0} U_n/U_{n-1}$$

est une $\mathbf{C}$-algèbre commutative, ainsi l'application naturelle $\mathfrak{g} \to U \to \mathrm{gr}(U)$ s'étend en un morphisme de $\mathbf{C}$-algèbres commutatives $S(\mathfrak{g}) \to \mathrm{gr}(U)$, qui est un isomorphisme, comme on le voit facilement à partir du théorème de Poincaré-Birkhoff-Witt.

Noter aussi que U est une représentation algébrique de G, chaque U_n étant G-stable, de dimension finie et une représentation algébrique de G. Comme $V \to V^G$ est exact sur les représentations algébriques de G, on obtient un isomorphisme

$$\mathrm{gr}(\mathfrak{Z}(\mathfrak{g})) \simeq \mathrm{gr}(U^G) \simeq (\mathrm{gr}(U))^G \simeq S(\mathfrak{g})^G,$$

en munissant $\mathfrak{Z}(\mathfrak{g})$ de la filtration induite par U. Nous sommes enfin capables de nous attaquer au théorème de finitude:

Théorème 5.7. *(Harish-Chandra) Si M est un $(\mathfrak{g}, K_0)$-module de type fini en tant que $U(\mathfrak{g})$-module, alors $M(\tau)$ est un $\mathfrak{Z}(\mathfrak{g})$-module de type fini pour tout $\tau \in \hat{K}_0$.*

Proof. On va découper la preuve en morceaux:

Etape 1: on commence par filtrer M. Prenons $M_0 \subset M$ de dimension finie, stable par K_0 et tel que $M = UM_0$ (prendre des générateurs $v_1, ..., v_k$ de M sur $U(\mathfrak{g})$ et $M_0 = \sum_{i=1}^{k} K.v_i$). Les espaces $M_n = U_n M_0$ sont de dimension finie et stables sous K_0, avec $U_m M_n \subset M_{n+m}$. On en déduit que

$$\mathrm{gr}(M) = \oplus_{n \geq 0} M_n/M_{n-1}$$

est un K_0-module et aussi un $\mathrm{gr}(U) \simeq S(\mathfrak{g})$-module engendré par M_0. Si $X \in \mathfrak{k}_0 \otimes \mathbf{C}$, on a $X.M_n \subset M_n$ car M_n est stable sous K_0, et d'autre part l'action de X sur la classe de $m \in M_n$ est la classe de $Xm \in M_{n+1}$ modulo M_n, donc elle est nulle, autrement dit $\mathfrak{k}_0 \otimes \mathbf{C}$ agit par 0 sur $\mathrm{gr}(M)$, qui devient ainsi un $S(\mathfrak{g}_0 \otimes \mathbf{C}/(\mathfrak{k}_0 \otimes \mathbf{C})) \simeq S(\mathfrak{p}_0 \otimes \mathbf{C})$-module engendré par M_0.

Etape 2: Notons que $\mathrm{gr}(M)(\tau)$ est naturellement un module sur $\mathrm{gr}(U)^{K_0}$ et donc sur $\mathrm{gr}(U)^G \simeq S(\mathfrak{g})^G$. La partie difficile de la preuve est alors le

Lemme 5.1. $\mathrm{gr}(M)(\tau)$ *est un* $S(\mathfrak{g})^G$*-module de type fini.*

Proof. La forme bilinéaire G-invariante $B(X,Y) = \mathrm{Tr}(XY)$ étant non dégénérée sur $\mathfrak{g}$ et $\mathfrak{p}_0$, elle permet d'identifier (de façon compatible avec l'action de G) $\mathfrak{g}$ et $\mathfrak{g}^*$, pareil avec $\mathfrak{p}_0$ et son dual. En particulier elle permet d'identifier $S(\mathfrak{g})^G$ et $S(\mathfrak{g}^*)^G \simeq P_h(\mathfrak{g})^G \simeq P(\mathfrak{g}_0)^{G_0} \otimes_{\mathbf{R}} \mathbf{C}$, et de même on peut identifier $S(\mathfrak{p}_0 \otimes \mathbf{C})^{K_0}$ et $P(\mathfrak{p}_0)^{K_0} \otimes_{\mathbf{R}} \mathbf{C}$. Le morphisme $S(\mathfrak{g})^G \to S(\mathfrak{p}_0 \otimes \mathbf{C})^{K_0}$ correspondant à la restriction $P(\mathfrak{g}_0)^{G_0} \to P(\mathfrak{p}_0)^{K_0}$ est alors induit par la projection $\mathfrak{g} = \mathfrak{g}_0 \otimes \mathbf{C} \to \mathfrak{p}_0 \otimes \mathbf{C}$ et il est fini par le théorème 5.6. Il suffit donc de montrer que $\mathrm{gr}(M)(\tau)$ est un $S(\mathfrak{p}_0 \otimes \mathbf{C})^{K_0}$-module de type fini.

Posons $W = \tau^* \otimes_{\mathbf{C}} \mathrm{gr}(M) \simeq \mathrm{Hom}_{\mathbf{C}}(\tau, \mathrm{gr}(M))$, on a alors une surjection $\tau \otimes_{\mathbf{C}} W^{K_0} \to \mathrm{gr}(M)(\tau)$. De plus W est muni d'une structure de $S(\mathfrak{p}_0 \otimes \mathbf{C})^{K_0}$-module de type fini, engendré par M_0, à travers la structure de $S(\mathfrak{p}_0 \otimes \mathbf{C})^{K_0}$-module de $\mathrm{gr}(M)$, ainsi que d'une action de K_0, via l'action de K_0 sur $W = \mathrm{Hom}_{\mathbf{C}}(\tau, \mathrm{gr}(M))$ par $(k\varphi)(x) = k(\varphi(k^{-1}x))$. Comme $S(\mathfrak{p}_0 \otimes \mathbf{C})$ est noethérien, il existe un nombre fini de $\varphi_i \in W^{K_0} = \mathrm{Hom}_{K_0}(\tau, \mathrm{gr}(M))$ tels que $S(\mathfrak{p}_0 \otimes \mathbf{C}) W^{K_0} = \sum_j S(\mathfrak{p}_0 \otimes \mathbf{C})\varphi_j$. Nous allons voir que $W^{K_0} = \sum_j S(\mathfrak{p}_0 \otimes \mathbf{C})^K \varphi_j$, ce qui permettra de conclure. En effet, si $\varphi = \sum_j p_j \varphi_j \in W^{K_0}$, avec $p_j \in S(\mathfrak{p}_0 \otimes \mathbf{C})$, on a pour tout $k \in K_0$ une égalité

$$\varphi = k\varphi = \sum_j (\mathrm{Ad}(k)p_j)\varphi_j,$$

donc aussi (en intégrant sur K_0)

$$\varphi = \sum_j q_j \varphi_j, q_j := \int_{K_0} \mathrm{Ad}(k) p_j dk \in S(\mathfrak{p}_0 \otimes \mathbf{C})^{K_0},$$

ce qui montre que $\varphi \in \sum_j S(\mathfrak{p}_0 \otimes \mathbf{C})^{K_0} \varphi_j$. □

Etape 3 La fin de la preuve est un argument classique. On vient de voir que $\mathrm{gr}(M)(\tau)$ est un $S(\mathfrak{g})^G$-module de type fini, donc un $\mathrm{gr}(\mathfrak{Z}(\mathfrak{g}))$-module de type fini (cf. discussion précédant le théorème). On peut donc trouver un nombre fini de k_j et $w_j \in (M_{k_j}/M_{k_j-1})(\tau)$ tels que

$$\mathrm{gr}(M)(\tau) = \sum_j \mathrm{gr}(\mathfrak{Z}(\mathfrak{g})) w_j.$$

On relève w_j en $v_j \in M_{k_j}(\tau)$, ce que l'on peut faire car les K_0-représentations de dimension finie sont semi-simples. Si $v \in M_n(\tau)$, son image dans $\mathrm{gr}(M)$ est dans $\mathrm{gr}(M)(\tau)$, et d'après ce qui précède il existe $\lambda_j \in \mathfrak{Z}(\mathfrak{g})$ tels que l'image de v soit la même que l'image de $\sum \lambda_j v_j$, autrement dit $v_1 := v - \sum \lambda_j v_j \in M_{n-1}$. On a bien sûr $v_1 \in M_{n-1}(\tau)$. On recommence avec v_1, et on s'arrête au bout de n (ou $n+1$...) étapes. □

5.4 Application 2: le théorème de restriction de Chevalley

Nous allons décrire maintenant l'image de $P(\mathfrak{g})^G \to P(\mathfrak{a})$. Introduisons le **groupe de Weyl de** G

$$W = N_K(\mathfrak{a})/Z_K(\mathfrak{a}) = N_G(\mathfrak{a})/Z_G(\mathfrak{a}),$$

l'égalité étant une conséquence de la Zariski densité de K dans G. Noter que W ne dépend pas (à isomorphisme près) du choix de $\mathfrak{a}$, par le théorème 5.1.

Proposition 5.3. *W est un groupe fini.*

Proof. W est un groupe de Lie compact, il suffit donc de voir que $\mathrm{Lie}(W) = 0$, i.e. $\mathrm{Lie}(N_K(\mathfrak{a})) = \mathrm{Lie}(Z_K(\mathfrak{a}))$, ou encore $N_{\mathfrak{k}}(\mathfrak{a}) = Z_{\mathfrak{k}}(\mathfrak{a})$. On veut donc montrer que si $X \in \mathfrak{g}$ vérifie $[X, \mathfrak{a}] \subset \mathfrak{a}$, alors $[X, \mathfrak{a}] = 0$. Si $H \in \mathfrak{a}$, l'endomorphisme $T = \mathrm{ad}(H)$ est diagonalisable (prop. 5.1) et $T^2(X) = [H, T(X)] = 0$, car $T(X) = -[X, H] \in \mathfrak{a}$ et $[\mathfrak{a}, \mathfrak{a}] = 0$. On a donc $T(X) = 0$, ce qui permet de conclure. □

Le résultat suivant est d'une beauté rare, égalée uniquement par son importance:

Théorème 5.8. *(Chevalley) Le morphisme de restriction $P_h(\mathfrak{g})^G \to P_h(\mathfrak{h})^W$ est un isomorphisme.*

Proof. Il suffit de vérifier que la restriction $P(\mathfrak{p})^K \to P(\mathfrak{a})^W$ est un isomorphisme. Il est clair que l'image de la restriction $P(\mathfrak{p})^K \to P(\mathfrak{a})$ est contenue dans $P(\mathfrak{a})^W$. La surjectivité du morphisme $P(\mathfrak{p})^K \to P(\mathfrak{a})^W$ est bien plus délicate.

Etape 1 Il suffit de vérifier que $\mathrm{Frac}(P(\mathfrak{p})^K) \to \mathrm{Frac}(P(\mathfrak{a})^W)$ est un isomorphisme. En effet, admettons cela et prenons $f \in P(\mathfrak{a})^W$. Le morphisme $P(\mathfrak{p})^K \to P(\mathfrak{a})$ étant fini (théorème 5.5), il existe d et $F_i \in P(\mathfrak{p})^K$ tels que

$$f^d + \sum_{i=0}^{d-1} F_i|_{\mathfrak{a}} f^i = 0.$$

Comme $\mathrm{Frac}(P(\mathfrak{p})^K) \simeq \mathrm{Frac}(P(\mathfrak{a})^W)$, il existe $U, V \in P(\mathfrak{p})^K$ tels que $f = (U/V)|_{\mathfrak{a}}$. Alors $U^d + F_{d-1}U^{d-1}V + ... + F_0V^d$ est dans $P(\mathfrak{p})^K$ et sa restriction à $\mathfrak{a}$ est nulle, donc cette fonction est nulle. Ainsi $U/V \in \mathrm{Frac}(P(\mathfrak{p}))$ est entier sur $P(\mathfrak{p})$, et comme $P(\mathfrak{p})$ est intégralement clos dans son corps des fractions, on a $U/V \in P(\mathfrak{p})$ et $U/V \in P(\mathfrak{p})^K$. Ainsi $P(\mathfrak{p})^K \to P(\mathfrak{a})^W$ est surjective.

Etape 2 Montrons que $\mathrm{Frac}(P(\mathfrak{p})^K) \to \mathrm{Frac}(P(\mathfrak{a})^W)$ est un isomorphisme. D'après le théorème 5.5, l'extension $L = \mathrm{Frac}(P(\mathfrak{a}))$ est finie galoisienne sur $M = \mathrm{Frac}(P(\mathfrak{p})^K)$. Il suffit donc de vérifier que tout $\sigma \in \mathrm{Aut}(L/M)$ fixe $P(\mathfrak{a})^W$. Comme $P(\mathfrak{p})^K \to P(\mathfrak{a})$ est entier et $P(\mathfrak{a})$ est intégralement clos dans son corps des fractions, on a $\sigma(P(\mathfrak{a})) \subset P(\mathfrak{a})$. Fixons $X \in \mathfrak{a}$. Comme $P(\mathfrak{a})$ est une algèbre de polynômes, le morphisme $P \to \sigma(P)(X)$ de $P(\mathfrak{a})$ dans $\mathbf{R}$ est donné par $P \to P(A)$ pour un $A \in \mathfrak{a}$. Comme σ fixe $P(\mathfrak{p})^K$, on obtient $P(X) = P(A)$ pour tout $P \in P(\mathfrak{p})^K$.

Etape 3 Nous allons montrer que $\mathrm{Ad}(K).X = \mathrm{Ad}(K).A$. Sinon il existe $F \in C^0(\mathfrak{p})$ nulle sur $\mathrm{Ad}(K).X$ et égale à 1 sur $\mathrm{Ad}(K).A$. La fonction $F_1(X) = \int_K F(\mathrm{Ad}(k)(X))dk$ est dans $(C^0(\mathfrak{p}))^K$ et $F_1(X) = 0$, $F_1(A) = 1$. Par Stone-Weierstrass il existe $F_2 \in P(\mathfrak{p})$ telle que $|F_2 - F_1| < 1/2$ sur le compact $C = \mathrm{Ad}(K).X \cup \mathrm{Ad}(K).A$. Alors

$$P(x) = \int_K F_2(\mathrm{Ad}(k)x)dk$$

est dans $P(\mathfrak{p})^K$ et $P(A) \neq P(X)$, une contradiction.

Etape 4 Montrons enfin que $W.X = W.A$, ce qui montrera que $\sigma(P)(X) = P(A) = P(X)$ pour $P \in P(\mathfrak{a})^W$ et donc σ fixe $\mathrm{Frac}(P(\mathfrak{a})^W)$. Prenons $k \in K$ tel que $\mathrm{Ad}(k)X = A$ (il existe d'après l'étape 3). Tout $U \in \mathfrak{a}$ commute à $A = kXk^{-1}$, donc $k^{-1}Uk$ commute à X et donc $k^{-1}\mathfrak{a}k \subset Z_{\mathfrak{p}}(X)$. Soit $H = Z_G(X)$, un sous-groupe Zariski fermé de G, auto-adjoint (car $X \in \mathfrak{a}$, donc $X = X^*$) et $\mathrm{Lie}(H) = Z_{\mathfrak{g}}(X)$. Le sous-espace $\mathfrak{p}$ correspondant à H est $Z_{\mathfrak{p}}(X)$, et $k^{-1}\mathfrak{a}k$, $\mathfrak{a}$ sont des sous-espaces de Cartan de $Z_{\mathfrak{p}}(X)$. Par la conjugaison des sous-espaces de Cartan (th. 5.1) appliquée à H on obtient l'existence d'un $u \in H \cap U(n) = Z_K(X)$ tel que $u^{-1}(k^{-1}\mathfrak{a}k)u = \mathfrak{a}$. Ainsi $ku \in W = N_K(\mathfrak{a})$ et $kuX(ku)^{-1} = A$, ce qui permet de conclure. Ouf! $\square$

Exercice 5.9. Démontrer directement le théorème de Chevalley pour $G = \mathbf{GL}_n(\mathbf{C})$.

Remarque 5.10. Si on combine les résultats précédents, on obtient un isomorphisme

$$\mathrm{gr}(\mathfrak{Z}(\mathfrak{g})) \simeq S(\mathfrak{g})^G \simeq S(\mathfrak{h})^W.$$

Un théorème délicat de Harish-Chandra (dont un des ingrédients principaux de la preuve est le théorème de restriction de Chevalley) fournit un isomorphisme canonique

$$\mathfrak{Z}(\mathfrak{g}) \simeq U(\mathfrak{h})^W \simeq S(\mathfrak{h})^W.$$

6 Le système de racines d'un groupe réductif

Soit G un groupe auto-adjoint et $\mathfrak{a}$ un sous-espace de Cartan de $\mathfrak{p}$, $\mathfrak{h} = \mathfrak{a} + i\mathfrak{a}$ et $\Phi = \Phi(\mathfrak{g}, \mathfrak{h}) \subset \mathfrak{h}^* \setminus \{0\}$ l'ensemble des racines de $\mathfrak{h}$ dans $\mathfrak{g}$, comme avant. On a donc

$$\mathfrak{g} = \mathfrak{h} \oplus \oplus_{\alpha\in\Phi}\mathfrak{g}_\alpha, \quad \mathfrak{g}_\alpha := \cap_{H\in\mathfrak{h}} \ker(\mathrm{ad}(H) - \alpha(H)) \qquad (*).$$

L'étude de cette décomposition est fondamentale pour comprendre G.

6.1 Le système de racines absolu d'un groupe réductif

Commençons par un peu de vocabulaire... Si V est un $\mathbf{R}$-espace vectoriel de dimension finie, une **réflexion de vecteur** $v \in V$ est un automorphisme s de V tel que $s(v) = -v$ et $\ker(s - 1)$ soit un hyperplan. Cela équivaut à l'existence de $l \in V^*$ telle que $s(w) = w - l(w)v$ pour tout $w \in V$ et $l(v) = 2$.

Définition 6.1. i) Un ensemble fini $R \subset V$ est un **système de racines** dans V si:

a) R engendre V et $0 \notin R$.

b) Pour tout $\alpha \in R$ il existe une symétrie s_α de vecteur α qui laisse invariant R (s_α est alors unique). En particulier on a $-R = R$ (car $s_\alpha(\alpha) = -\alpha$).

c) On a $s_\alpha(\beta) - \beta \in \mathbf{Z}\alpha$ pour $\alpha, \beta \in R$.

On dit que R est **réduit** si $-\alpha$ et α sont les seules racines proportionnelles à α pour $\alpha \in R$ (cela revient à demander que $\alpha/2 \notin R$ pour $\alpha \in R$).

On définit de la même manière la notion de système de racines dans un espace vectoriel sur $\mathbf{Q}$ ou $\mathbf{C}$. Un des théorèmes fondamentaux (et délicats!) de la théorie des groupes réductifs est alors:

Théorème 6.1. *Pour $G, \mathfrak{h}$ comme ci-dessus $\Phi = \Phi(\mathfrak{g}, \mathfrak{h})$ est un système de racines réduit dans l'orthogonal V de $\mathfrak{h} \cap \mathfrak{z}$ dans $\mathfrak{h}^*$, où $\mathfrak{z}$ est le centre de $\mathfrak{g}$ (donc $V = \mathfrak{h}^*$ si G est de centre fini). De plus* $\dim \mathfrak{g}_\alpha = 1$ *pour $\alpha \in \Phi$.*

Exercice 6.2. Démontrer ce théorème quand $G = \mathbf{GL}_n(\mathbf{C})$.

Nous allons expliquer les (nombreuses...) étapes de la preuve de ce théorème. Si $\alpha \in \mathfrak{h}^*$ il existe un unique $H_\alpha \in \mathfrak{h}$ tel que $B(H, H_\alpha) = \alpha(H)$ pour $H \in \mathfrak{h}$, car $B|_{\mathfrak{h}\times\mathfrak{h}}$ est non dégénérée. Posons pour $\alpha, \beta \in \mathfrak{h}^*$ $B(\alpha, \beta) = B(H_\alpha, H_\beta)$. Soit

$$V = \mathrm{Vect}_{\alpha\in\Phi}\alpha \subset \mathfrak{h}^*.$$

Alors en identifiant $\mathfrak{h}$ et $(\mathfrak{h}^*)^*$ on a

$$V^\perp = \{H \in \mathfrak{h} |\, \alpha(H) = 0, \alpha \in \Phi\} = \{H \in \mathfrak{h} |\, [\mathfrak{g}_\alpha, H] = 0, \alpha \in \Phi\} = \mathfrak{h} \cap \mathfrak{z},$$

la dernière égalité découlant de la commutativité de $\mathfrak{h}$ et de la décomposition (*). Donc V est bien l'orthogonal de $\mathfrak{h} \cap \mathfrak{z}$.

Il nous faut définir des réflexions s_α pour $\alpha \in \Phi$. Un premier point délicat consiste à montrer que $B(\alpha, \alpha) \neq 0$, car si cela est acquis on pourra poser

$$s_\alpha(H) = H - 2\frac{\alpha(H)}{B(\alpha, \alpha)} H_\alpha, H \in \mathfrak{h},$$

que l'on voit aussi comme symétrie de $\mathfrak{h}^*$, i.e. on écrit encore s_α pour s_α^T. Concrètement, cela signifie

$$s_\alpha(l) = l - \frac{2l(H_\alpha)}{B(\alpha,\ \alpha)}\alpha,\ l \in \mathfrak{h}^*$$

et il faudra montrer que $s_\alpha(\beta) \in \Phi$ pour $\alpha, \beta \in \Phi$ et que $2\frac{B(\alpha,\beta)}{B(\alpha,\alpha)} \in \mathbf{Z}$ (noter que $\beta(H_\alpha) = B(\alpha, \beta)$). Il faut bien se fatiguer pour démontrer tout ceci...

Proposition 6.1. *a) On a $[\mathfrak{g}_\lambda, \mathfrak{g}_\mu] \subset \mathfrak{g}_{\lambda+\mu}$ pour $\lambda, \mu \in \mathfrak{h}^*$ et $B(\mathfrak{g}_\lambda, \mathfrak{g}_\mu) = 0$ si $\lambda + \mu \neq 0$.*

b) Pour $X \in \mathfrak{g}_\alpha, Y \in \mathfrak{g}_{-\alpha}$ on a $[X, Y] = B(X, Y)H_\alpha$. De plus $[\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}] = \mathbf{C}H_\alpha$.

c) On a $B(\alpha, \alpha) \neq 0$.

Proof. a) Si $X \in \mathfrak{g}_\lambda$ et $Y \in \mathfrak{g}_\mu$, $H \in \mathfrak{h}$

$$HXY - XYH = (HX - XH)Y + X(HY - YH) = (\lambda + \mu)(H)XY$$

et de même $HYX - YXH = (\lambda + \mu)(H)YX$, donc $[X, Y] = XY - YX \in \mathfrak{g}_{\lambda+\mu}$. Si $\lambda(H) + \mu(H) \neq 0$, la relation $(\lambda + \mu)(H)XY = HXY - XYH$ montre que $\mathrm{Tr}(XY) = 0$, d'où le point a).

b) On a $[X, Y] \in \mathfrak{g}_0 = \mathfrak{h}$ d'après a). Ensuite, pour tout $H \in \mathfrak{h}$ on a

$$B(H[X,Y]) = \mathrm{Tr}(HXY - HYX) = B([H,X],Y) = \alpha(H)B(X,Y) = B(H \cdot B(X,Y)H_\alpha)$$

et donc $[X, Y] = B(X, Y)H_\alpha$, car $B|_{\mathfrak{h}}$ est non dégénérée. Si $[\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}] = 0$, on obtient $B(\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}) = 0$, ensuite $B(\mathfrak{g}_\alpha, \mathfrak{g}) = 0$ grâce à a), donc $\mathfrak{g}_\alpha = 0$, une contradiction.

c) Supposons que $B(\alpha, \alpha) = 0$, i.e. $\alpha(H) = 0$, où $H = H_\alpha$. D'après b) il existe $X \in \mathfrak{g}_\alpha$ et $Y \in \mathfrak{g}_{-\alpha}$ non nuls tels que $[X, Y] = H$. Comme $\alpha(H) = 0$ on obtient $[H, X] = 0$ et $[H, Y] = 0$. Si $k \geq 1$ on a (puisque $[H, Y] = 0$)

$$\mathrm{Tr}(H^k) = \mathrm{Tr}(H^{k-1}(XY - YX)) = \mathrm{Tr}(H^{k-1}XY - YH^{k-1}X) = 0,$$

donc $\mathrm{Tr}(H^k) = 0$ pour $k \geq 1$ et donc (argument standard) H est nilpotente. Mais $H \in \mathfrak{h}$, donc H est diagonalisable et $H = 0$, une contradiction. $\square$

Proposition 6.2. *Soit $\alpha \in \Phi$ et $h_\alpha = \frac{2}{B(\alpha,\alpha)} H_\alpha$. Il existe $e_\alpha \in \mathfrak{g}_\alpha$ et $f_\alpha \in \mathfrak{g}_{-\alpha}$ non nuls tels que*

$$[e_\alpha, f_\alpha] = h_\alpha,\ [h_\alpha, e_\alpha] = 2e_\alpha,\ [h_\alpha, f_\alpha] = -2f_\alpha.$$

Proof. Prenons $e_\alpha \in \mathfrak{g}_\alpha$ et $f_\alpha \in \mathfrak{g}_{-\alpha}$ non nuls tels que $h_\alpha = [e_\alpha, f_\alpha]$, ce qui est possible (prop 6.1). On a alors

$$[h_\alpha, e_\alpha] = \frac{2}{B(\alpha,\alpha)}[H_\alpha, e_\alpha] = \frac{2}{B(\alpha,\alpha)} \cdot \alpha(H_\alpha) e_\alpha = 2e_\alpha$$

et de même $[h_\alpha, f_\alpha] = -2\alpha$. □

Gardons les choix précédents. Alors $\mathfrak{sl}_2(\alpha) := \mathbf{C}e_\alpha + \mathbf{C}f_\alpha + \mathbf{C}h_\alpha$ est une sous-algèbre de Lie de $\mathfrak{g}$ isomorphe à $\mathfrak{sl}_2(\mathbf{C})$. En particulier $\mathfrak{g}$ devient un $\mathfrak{sl}_2(\mathbf{C})$-module de dimension finie. De plus

$$s_\alpha(H) = H - \alpha(H)h_\alpha,\ s_\alpha(l) = l - l(h_\alpha)\alpha,\ l \in \mathfrak{h}^*.$$

Fixons α, β et posons $k = \beta(h_\alpha)$, donc $s_\alpha(\beta) = \beta - k\alpha$. Prenons $X \in \mathfrak{g}_\beta$ non nul, alors pour tout $j \geq 0$ on a (prop 6.1)

$$\mathrm{ad}^j(e_\alpha)(X) \in \mathfrak{g}_{\beta+j\alpha},\ \mathrm{ad}^j(f_\alpha)(X) \in \mathfrak{g}_{\beta-j\alpha},$$

et on a aussi $\mathrm{ad}(h_\alpha)(X) = kX$. Pour conclure que Φ est un système de racines, il reste donc à démontrer la:

Proposition 6.3. *Soit M un $\mathfrak{sl}_2(\mathbf{C})$-module de dimension finie et soit $v \in M$ non nul et $k \in \mathbf{C}$ tel que $h.v = kv$. Alors $k \in \mathbf{Z}$. De plus, si $k \geq 0$ alors $f^k v \neq 0$, sinon $e^{-k}v \neq 0$.*

Proof. Exercice! □

Proposition 6.4. *Le système de racines Φ est réduit et* $\dim \mathfrak{g}_\alpha = 1$ *pour $\alpha \in \Phi$.*

Proof. Puisque $[\mathfrak{g}_\mu, \mathfrak{g}_\lambda] \subset \mathfrak{g}_{\mu+\lambda}$ et $[\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}] = \mathbf{C}H_\alpha = \mathbf{C}h_\alpha$, l'espace

$$W = \mathbf{C}f_\alpha + \mathbf{C}h_\alpha + \sum_{k\geq 1} \mathfrak{g}_{k\alpha} = \mathbf{C}f_\alpha \oplus \mathbf{C}h_\alpha \oplus \oplus_{k\geq 1}\mathfrak{g}_{k\alpha}$$

est stable par l'action adjointe de e_α, f_α et h_α. Ainsi h_α induit un endomorphisme de trace nulle sur W (car commutateur de ceux induits par e_α et f_α). Mais h_α agit par les scalaires $-\alpha(h_\alpha), 0, k\alpha(h_\alpha)$ sur $\mathbf{C}f_\alpha$, $\mathbf{C}h_\alpha$ et $\mathfrak{g}_{k\alpha}$. En posant $n_k = \dim \mathfrak{g}_{k\alpha}$ on obtient $\alpha(h_\alpha)(-1 + n_1 + n_2 + ...) = 0$ et comme $\alpha(h_\alpha) \neq 0$ (car $B(\alpha,\alpha) \neq 0$) on a $n_1 + n_2 + ... = 1$. Comme $n_1 \geq 1$, cela montre que $n_1 = 1$ et que $n_2 = 0$, donc R est réduit et $\dim \mathfrak{g}_\alpha = 1$. □

Le **groupe de Weyl** d'un système de racines R dans V est le sous-groupe $W = W(R)$ de $\mathbf{GL}(V)$ engendré par les s_α, pour $\alpha \in R$. C'est un sous-groupe du groupe des permutations de R (car R engendre V), donc fini. On admet le théorème profond suivant:

Théorème 6.3. *Le groupe de Weyl de Φ s'identifie au sous-groupe $W(G, \mathfrak{h}) = N_G(\mathfrak{h})/Z_G(\mathfrak{h})$ de $\mathbf{GL}(V)$.*

Exercice 6.4. Démontrer ce théorème pour $G = \mathbf{GL}_n(\mathbf{C})$.

Introduisons encore deux notions très importantes concernant les systèmes de racines. Soit R un système de racines dans V.

Définition 6.2. On dit que $\Delta \subset R$ est une **base de** R **ou systèmes de racines simples dans** R si Δ est une base de V et si toute racine $\alpha \in R$ s'écrit $\alpha = \sum_{\beta\in\Delta} n_\beta \beta$, avec n_β des entiers, tous du même signe.

Théorème 6.5. *Soit $R^+ \subset R$. Les assertions suivantes sont équivalentes:*

a) Il existe une base Δ de R telle que $R^+ = R \cap (\sum_{\alpha\in\Delta} \mathbf{Z}_{\geq 0}\alpha)$.

*b) $R = R^+ \coprod(-R^+)$ et R^+ est **fermé**, i.e. si $\alpha, \beta \in R$ et $\alpha+\beta \in R$, alors $\alpha+\beta \in R^+$.*

Dans ce cas, la base Δ dans a) est unique.

Un tel sous-ensemble R^+ de R est appelé un **système de racines positives**. On peut en construire comme suit, en supposant que V est un $\mathbf{R}$-espace vectoriel (si V vit sur $\mathbf{C}$, appliquer ce qui suit au $\mathbf{R}$-espace engendré par R). On prend $l \in V^*$ tel que $l(\alpha) \neq 0$ pour $\alpha \in R$. Alors $R^+ = \{\alpha \in R | l(\alpha) > 0\}$ est un système de racines positives dans R. L'ensemble Δ des éléments de R^+ qui ne sont pas la somme de deux éléments de R^+ est une base de R et $R^+ = R \cap (\sum_{\alpha\in\Delta} \mathbf{Z}_{\geq 0}\alpha)$. Toute base de R est ainsi obtenue. Bien sûr, tout ceci n'est pas évident (mais ce n'est pas très difficile non plus). Un résultat plus délicat est:

Théorème 6.6. *Soit R un système de racines **réduit**, de groupe de Weyl W.*

a) W agit simplement transitivement sur l'ensemble des bases de R

b) Soit Δ une base de R et R^+ le système de racines positives associé. Alors W est engendré par les s_α, $\alpha \in \Delta$, $R = \cup_{w\in W} w(\Delta)$, s_α permute $R^+ \setminus \{\alpha\}$ et $s_\alpha(\rho_{R^+}) = \rho_{R^+} - \alpha$ pour $\alpha \in \Delta$, où $\rho_{R^+} = \frac{1}{2}\sum_{\beta\in R^+} \beta$.

Nous pouvons dire maintenant un peu plus sur l'isomorphisme de Harish-Chandra (remarque 5.10). Prenons un système de racines positives R^+ dans le système de racines $R = \Phi$ d'un groupe réductif G et posons

$$\mathfrak{n}^+ = \oplus_{\alpha\in R^+} \mathfrak{g}_\alpha, \quad \mathfrak{n}^- = \oplus_{\alpha\in R^-} \mathfrak{g}_\alpha.$$

La décomposition usuelle de $\mathfrak{g}$ induit une **décomposition triangulaire** (d'espaces vectoriels!)

$$\mathfrak{g} = \mathfrak{n}^+ \oplus \mathfrak{h} \oplus \mathfrak{n},$$

avec $\mathfrak{n}^+$ et $\mathfrak{n}$ des sous-algèbres de Lie de $\mathfrak{g}$. Cela induit (théorème de Poincaré-Birkhoff-Witt) une décomposition d'espaces vectoriels

$$U(\mathfrak{g}) = U(\mathfrak{h}) \oplus (U(\mathfrak{g})\mathfrak{n}^+ + \mathfrak{n}^- U(\mathfrak{g})),$$

d'où une projection $p : U(\mathfrak{g}) \to U(\mathfrak{h})$, qui n'est **pas** un morphisme d'algèbres. Cependant, un peu miraculeusement il se trouve que sa restriction au centre de $U(\mathfrak{g})$ (et même au centralisateur de $\mathfrak{h}$ dans $U(\mathfrak{g})$) est effectivement un morphisme d'algèbres $\beta : \mathfrak{Z}(\mathfrak{g}) \to U(\mathfrak{h})$, uniquement caractérisé par le fait que $x - \beta(x) \in U(\mathfrak{g})\mathfrak{n}^+$ pour tout $x \in \mathfrak{Z}(\mathfrak{g})$. Puisque $\mathfrak{h}$ est commutative (i.e. $[\mathfrak{h}, \mathfrak{h}] = 0$) on peut identifier $U(\mathfrak{h})$, $S(\mathfrak{h})$ et l'algèbre des fonctions polynomiales holomorphes complexes sur $\mathfrak{h}^*$.

En posant $\rho = \frac{1}{2}\sum_{\alpha\in R^+}\alpha$, on définit pour $z \in \mathfrak{Z}(\mathfrak{g})$ un élément $\gamma(z) \in U(\mathfrak{h})$, vu comme fonction polynomiale sur $\mathfrak{h}^*$

$$\gamma(z)(\lambda) = \beta(z)(\lambda - \rho).$$

Le théorème fondamental de Harish-Chandra s'énonce alors:

Théorème 6.7. *(Harish-Chandra) L'application* $\gamma : \mathfrak{Z}(\mathfrak{g}) \to U(\mathfrak{h})$ *induit un isomorphisme de* $\mathbf{C}$*-algèbres* $\mathfrak{Z}(\mathfrak{g}) \simeq U(\mathfrak{h})^W$*, indépendant des choix faits ci-dessus.*

La preuve de ce théorème est franchement technique et sera admise. Un point pénible de la preuve est le fait que γ est bien à valeurs dans $U(\mathfrak{h})^W$, qui utilise tous les résultats précédents sur le groupe de Weyl, ainsi que les rudiments de la théorie des modules de Verma, que nous n'avons pas discutée. Une fois ce résultat établi, pour voir que γ est un isomorphisme on filtre les deux algèbres $\mathfrak{Z}(\mathfrak{g})$ (via la filtration induite par $U(\mathfrak{g})$) et $U(\mathfrak{h})^W$ (en identifiant $U(\mathfrak{h})$ à $S(\mathfrak{h})$ et en utilisant la filtration évidente de celle-ci) et on vérifie que l'application induite par γ au niveau des algèbres graduées n'est rien d'autre que l'application de restriction $S(\mathfrak{g})^G \to S(\mathfrak{h})^W$, qui est un isomorphisme par le théorème de restriction de Chevalley.

6.2 Le système de racines relatif

Les questions de rationalité sont très délicates et nous les admettrons. Soit k un sous-corps de $\mathbf{C}$, G un k-groupe réductif connexe. Un k-tore S est dit **déployé sur** k si tout caractère $\chi : S \to \mathbf{C}^*$ est défini sur k. On vérifie (exercice) que cela équivaut à l'existence d'un isomorphisme de k-groupes algébriques $S \simeq (\mathbf{C}^*)^d$ pour un certain d.

Soit S un k-tore déployé sur k maximal de G, i.e. un élément maximal de l'ensemble des k-tores déployés sur k de G (à ne pas confondre avec un tore maximal de G déployé sur k, qui n'existe pas forcément!). Un théorème hautement nontrivial de Borel et Tits montre que tous les choix de S sont conjugués sous $G(k)$, donc ce qui suit ne dépend pas vraiment de S.

Une **k-racine (ou racine relative)** de G par rapport à S est un élément non nul $\alpha \in X(S) = \mathrm{Hom}_{\mathrm{gr.alg}}(S, \mathbf{C}^*)$ tel que

$$\mathfrak{g}_\alpha^k := \{X \in \mathfrak{g} | \,\mathrm{Ad}(s)(X) = \alpha(s)X,\ \forall s \in S\} \neq 0.$$

Le **système de racines relatif** est l'ensemble fini $\Phi_k = \Phi_k(G, S)$ des k-racines. On a donc une décomposition

$$\mathfrak{g} = \mathrm{Lie}(Z_G(S)) \oplus \bigoplus_{\alpha\in\Phi_k} \mathfrak{g}_\alpha^k,$$

et $\Phi_k = \emptyset$ si et seulement si S est central dans G. Le **groupe de Weyl relatif** $W_k(G) = N_G(S)/Z_G(S)$ est fini et agit sur $X(S)$ par $(w\chi)(s) = \chi(x^{-1}sx)$ pour tout relèvement x de w dans $N_G(S)$. Il préserve Φ_k. Le théorème suivant est difficile:

Théorème 6.8. *(Borel, Tits)* Φ_k *est un système de racines (pas forcément réduit) dans* $\mathrm{Vect}(\Phi_k) \subset X(S) \otimes_{\mathbf{Z}} \mathbf{Q}$*, de groupe de Weyl isomorphe à* $W_k(G)$*. Si le centre de* G *est fini on a* $\mathrm{Vect}(\Phi_k) = X(S) \otimes_{\mathbf{Z}} \mathbf{Q}$*. Enfin, tout* $w \in W_k(G)$ *est l'image d'un élément de* $N_{G(k)}(S(k))$*.*

Si T est un k-tore maximal contenant S, la surjection (restriction) $X(T) \to X(S)$ envoie Φ dans $\Phi_k \cup \{0\}$. Ainsi toute k-racine est la restriction d'une racine "absolue".