David Renard
Centre de Mathématiques
Laurent Schwartz,
Ecole Polytechnique

GROUPES ET REPRÉSENTATIONS

David Renard, Centre de Mathématiques, Laurent Schwartz,,
Ecole Polytechnique

21 juillet 2009

GROUPES ET REPRÉSENTATIONS

David Renard
Centre de Mathématiques
Laurent Schwartz,
Ecole Polytechnique

TABLE DES MATIÈRES

CHAPITRE I

GROUPES ET ACTIONS DE GROUPES

“ *Un principe directeur des mathématiques modernes tient en cette leçon : lorsque vous avez affaire à une entité S munie d'une certaine structure, essayez de déterminer son groupe d'automorphismes, le groupe des transformations de ses éléments qui préservent les relations structurales. Vous pouvez espérer gagner une profonde compréhension de la constitution de S de cette manière.*” Hermann Weyl[(1)].

Le but de ce chapitre est de rappeler les définitions et les résultats de base de la théorie des groupes, supposées déjà plus ou moins connues du lecteur, en en profitant pour introduire la terminologie et les notations employées par la suite.

I.1. Un exemple fondamental et quelques définitions

Soit X un ensemble. Notons $\mathbf{Aut}(X)$ l'ensemble des bijections de X dans lui-même. Cet ensemble est muni de la loi de composition des applications :

$$\mu : \mathbf{Aut}(X) \times \mathbf{Aut}(X) \to \mathbf{Aut}(X), \quad (\phi, \psi) \mapsto \phi \circ \psi. \tag{I.1.1}$$

[(1)]Traduit librement d'une traduction de l'allemand en anglais... j'espère que le sens général se sera conservé.

La loi de composition est associative, c'est-à-dire que quels que soient ϕ_1, ϕ_2 et ϕ_3 dans $\mathbf{Aut}(X)$,

$$\mu(\mu(\phi_1, \phi_2), \phi_3) = \mu(\phi_1, \mu(\phi_2, \phi_3)), \tag{I.1.2}$$

ou plus simplement $(\phi_1 \circ \phi_2) \circ \phi_3 = \phi_1 \circ (\phi_2 \circ \phi_3)$.

D'autre part, cette loi admet un élément neutre, l'identité de X, notée Id_X :

$$(\forall \phi \in \mathbf{Aut}(X)), \qquad \mathrm{Id}_X \circ \phi = \phi \circ \mathrm{Id}_X = \phi. \tag{I.1.3}$$

Enfin, tout élément ϕ de $\mathbf{Aut}(X)$ admet un inverse, c'est-à-dire un élément de $\mathbf{Aut}(X)$, noté ϕ^{-1}, vérifiant

$$\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = \mathrm{Id}_X. \tag{I.1.4}$$

Le lecteur instruit reconnaît là le fait que $\mathbf{Aut}(X)$ est muni d'une structure de groupe. Pour les autres, nous rappelons la définition d'un groupe ci-dessous, qui consiste à prendre comme axiomes ces propriétés de $\mathbf{Aut}(X)$, de μ et de Id_X.

Remarquons que nous disposons aussi d'une application canonique

$$a : \mathbf{Aut}(X) \times X \longrightarrow X, \qquad (\phi, x) \mapsto \phi(x). \tag{I.1.5}$$

L'application a vérifie les propriétés suivantes : quels que soient ϕ_1, ϕ_2 dans $\mathbf{Aut}(X)$ et x dans X,

$$a(\mu(\phi_1, \phi_2), x) = a(\phi_1, a(\phi_2, x)), \tag{I.1.6}$$

et de plus

$$a(\mathrm{Id}_X, x) = x. \tag{I.1.7}$$

Autrement dit l'application a définit une action du groupe $\mathbf{Aut}(X)$ sur X. Donnons maintenant les définitions générales.

Définition I.1.1. — Un groupe est un ensemble G, muni d'une loi

$$\mu : G \times G \to G, \quad (g, h) \mapsto gh := \mu(g, h), \tag{I.1.8}$$

appelée produit du groupe, et vérifiant :

(i) (associativité) quels que soient g, h, k dans G,

$$\mu(\mu(g,h),k) = \mu(g,\mu(h,k)),$$

(ou encore, $(gh)k = g(hk)$),

(ii) (élément neutre) il existe un élément $e = e_G$ de G, appelé l'élément neutre, tel que pour tout $g \in G$, $\mu(g,e) = \mu(e,g) = g$ (ou encore $ge = eg = g$),

(iii) (inverse) quelque soit $g \in G$, il existe un élément de G, noté g^{-1}, tel que $\mu(g, g^{-1}) = \mu(g^{-1}, g) = e$ (ou encore $gg^{-1} = g^{-1}g = e$).

Remarque I.1.2. — On déduit facilement de ces axiomes l'unicité de l'élément neutre et de l'inverse d'un élément donné.

Soit G un groupe, et X un ensemble. Une action (à gauche) de G sur X est la donnée d'une application

$$a : G \times X \to X, \quad (g,x) \mapsto g \cdot x \tag{I.1.9}$$

vérifiant :

$$(\forall g, h \in G), (\forall x \in X), \quad a(\mu(g,h),x) = a(g, a(h,x)). \tag{I.1.10}$$

Lorsque l'action est notée par un “ $\cdot$ ”, ceci s'écrit $(gh) \cdot x = g \cdot (h \cdot x)$, et de plus,

$$(\forall x \in X), \quad a(e,x) = e \cdot x = x. \tag{I.1.11}$$

Remarque I.1.3. — On peut exprimer les propriétés des applications μ et a ci-dessus sans faire référence aux éléments de G et de X, et sans utiliser de quantificateurs universels, simplement par des diagrammes commutatifs :

$$\begin{tikzcd}
G \times G \times G \arrow[r, "\mu \times \mathrm{Id}_G"] \arrow[d, "\mathrm{Id}_G \times \mu"'] & G \times G \arrow[d, "\mu"] \\
G \times G \arrow[r, "\mu"'] & G
\end{tikzcd}$$

exprime l'associativité de la loi μ, et :

$$\begin{tikzcd} G \times G \times X \arrow[r, "\mu\times \mathrm{Id}_X"] \arrow[d, "\mathrm{Id}_G\times \mathbf{a}"'] & G \times X \arrow[d, "\mathbf{a}"] \\ G \times X \arrow[r, "\mathbf{a}"'] & X \end{tikzcd}$$

est une retraduction du fait que a est une action. Nous laissons en exercice au lecteur le soin de traduire en terme de diagrammes commutatifs les propriétés de l'élément neutre.

Définition I.1.4. — On appelle G-ensemble un ensemble X muni d'une action de G. Un G-morphisme du G ensemble X vers le G-ensemble Y est une application $f : X \to Y$ compatible avec les actions de G, c'est-à-dire

$$f(g \cdot x) = g \cdot f(x), \quad (x \in X), (g \in G).$$

On peut penser aux G-ensembles X, Y, comme à des ensembles munis de "symétries", et aux G-morphismes comme à des applications préservant ces symétries.

Un morphisme de groupes est une application d'un groupe vers un autre qui préserve la structure de groupe :

Définition I.1.5. — Soient G et H deux groupes. Une application de $f : G \to H$ est un morphisme de groupes si quels que soient g, h dans G,

$$f(gh) = f(g)f(h).$$

Dans ce cas, l'ensemble des $g \in G$ tels que $f(g) = e_H$ est appelé noyau du morphisme f. C'est un sous-groupe de G. On le note $\ker f$. L'image du morphisme f est un sous-groupe de H que l'on note $\operatorname{Im} f$.

Remarque I.1.6. — La donnée d'une action a d'un groupe G sur un ensemble X est équivalente à la donnée d'un morphisme de groupes

$$A : G \to \mathbf{Aut}(X).$$

On passe de a à A et réciproquement par

$$A(g)(x) = a(g, x), \quad (x \in X), (g \in G).$$

Définition I.1.7. — Un sous-ensemble H d'un groupe G est un sous-groupe s'il contient l'élément neutre e et est stable par produits et passage aux inverses.

On obtient de nombreux exemples de groupes et d'actions de groupes à partir de l'exemple fondamental $(X, \mathbf{Aut}(X))$ ci-dessus, et en supposant que l'ensemble X est muni d'une structure supplémentaire, clairement spécifiée par le contexte. On redéfinit alors $\mathbf{Aut}(X)$ comme l'ensemble des bijections de X dans lui-même qui préservent, ainsi que leurs inverses, la structure de X. Les applications μ et a définies comme en (I.1.1) et (I.1.5) vérifient encore (I.1.2), (I.1.3), (I.1.4), (I.1.6), (I.1.7). Lorsque X est muni d'une structure supplémentaire, on supposera, souvent de manière implicite, qu'une action d'un groupe G sur X préserve cette structure. Remarquons aussi que si l'on part d'un ensemble X muni d'une certaine structure et de son groupe d'automorphismes $\mathbf{Aut}(X)$, et que l'on rajoute une structure supplémentaire, l'ensemble des éléments de $\mathbf{Aut}(X)$ préservant de plus cette nouvelle structure est un sous-groupe de $\mathbf{Aut}(X)$. Ces considérations un peu abstraites seront illustrées par des exemples dans la section suivante.

Une autre manière d'obtenir des exemples de groupes à partir d'une action d'un groupe G sur un ensemble X est de considérer, pour toute partie Y de X

$$\mathbf{Fix}_G(Y) = \{g \in G \mid (\forall y \in Y),\ g \cdot y = y\},$$
$$\mathbf{Stab}_G(Y) = \{g \in G \mid (\forall y \in Y),\ g \cdot y \in Y\}.$$

On vérifie facilement que l'on obtient ainsi des sous-groupes du groupe G. Il est intéressant de remarquer que tout sous-groupe d'un groupe G peut s'obtenir ainsi.

Définition I.1.8. — Soit G un groupe agissant sur un ensemble X. On appelle orbite d'un point x de X sous l'action de G l'ensemble des points de la forme $g \cdot x$, g décrivant le groupe G. Notons $G \cdot x$ l'orbite d'un point x de X. On dit que l'action de G sur X est transitive s'il n'y a qu'une seule orbite, et qu'elle est fidèle si le morphisme

$$A : G \to \mathbf{Aut}(X)$$

défini par l'action est injectif. On dit que l'action est libre si tout élément différent de l'élément neutre agit sans point fixe. Une action libre est fidèle.

Proposition I.1.9. — *Soit G un groupe agissant sur un ensemble X. La relation binaire*

$$x \sim y \quad \textit{si} \quad G \cdot x = G \cdot y$$

est une relation d'équivalence sur X. Les orbites de l'action de G forment donc une partition de l'ensemble X.

Nous laissons la vérification de ce fait au lecteur.

On note X/G l'ensemble des orbites de l'action de G sur X. On appelle système de représentants des orbites de G dans X un ensemble $\{x_i\}$ d'éléments de X tel que

$$\{x_i\} \to X/G, \quad x_i \mapsto G \cdot x_i$$

soit une bijection.

Exemple I.1.10. — Soit G soit un groupe. Le groupe $\mathbf{Aut}(G)$ est l'ensemble des automorphismes de groupes de G dans lui-même. Le groupe G agit sur lui-même par

$$a : G \times G \to G, \quad (g, h) \mapsto ghg^{-1}.$$

On parle de l'action de G sur lui-même par conjugaison, ou d'action adjointe. Le morphisme de groupes $G \to \mathbf{Aut}(G)$ associé à a par la remarque I.1.6 est noté Ad :

$$\mathrm{Ad}(g) \in \mathbf{Aut}(G), \quad \mathrm{Ad}(g)(h) = ghg^{-1}.$$

Les orbites de G dans lui-même pour cette action s'appellent classes de conjugaison. Un groupe est abélien si et seulement si ses classes de conjugaison sont des singletons.

Exemple I.1.11. — Soit G soit un groupe et soit X l'ensemble de ses sous-groupes. Alors G agit sur X par conjugaison : si H est un sous-groupe de G,

$$g \cdot H = \{ghg^{-1} \,|\, h \in H\}.$$

Si $\mathbf{Fix}_G(\{H\}) = G$, ou de manière équivalente, si l'orbite de H sous G est réduite à $\{H\}$, alors on dit que le sous-groupe H est distingué, ou normal, dans G.

Exemple I.1.12. — Le groupe G agit sur lui-même par translation à gauche

$$l : G \times G \to G, \quad (g, h) \mapsto gh.$$

Cette action ne préserve pas la structure de groupe de G. Notons $\mathbf{Bij}(G)$, pour le distinguer de $\mathbf{Aut}(G)$, le groupe des bijections de l'ensemble G dans lui même. Le morphisme de groupes $G \to \mathbf{Bij}(G)$ associé à l par la remarque I.1.6 est noté L. On a $L(g)(h) = gh$.

On a aussi une action de G sur lui-même par translation à droite

$$r : G \times G \to G, \quad (g, h) \mapsto hg^{-1}.$$

Le morphisme associé est noté R. Remarquons le passage à l'inverse qui permet de replacer les éléments de G dans le bon ordre :

$$\begin{aligned} R(g_1g_2)(h) &= h(g_1g_2)^{-1} = (hg_2^{-1})g_1^{-1} = R(g_1)(R(g_2)(h)) \\ &= (R(g_1) \circ R(g_2))(h). \end{aligned}$$

Ces actions sont transitives.

Exemple I.1.13. — Soit H un sous-groupe de G. Alors H agit sur G par translation à gauche, par restriction de l'action de l'exemple précédent. Les orbites s'appellent les classes à droite. On note Hg l'orbite de $g \in G$ et $H\backslash G$ l'ensemble des classes à droite.

Bien sûr, H agit aussi sur G par translation à droite, les orbites s'appellent les classes à gauche, on note gH l'orbite de $g \in G$ et G/H l'ensemble des classes à gauche.

Proposition I.1.14. — *Soit G un groupe agissant sur un ensemble X. Alors, pour tout $x \in X$, si l'on note $G^x = \mathbf{Fix}_G(\{x\})$, l'application*

$$G/G^x \to G \cdot x, \quad gG^x \mapsto g \cdot x$$

est bijective.

Démonstration. Cette application est bien définie, car si $h \in G^x$, $(gh)\cdot x = g\cdot x$. Elle est surjective par définition de l'orbite, et injective par définition de G^x. □

***Corollaire I.1.15* (Formule des classes)**. — *Soit G un groupe fini agissant sur un ensemble X fini et soit $\{x_i\}$ un système de représentants des orbites de G dans X. Alors*

$$|X| = \sum_{\mathcal{O} \in X/G} |\mathcal{O}| = \sum_i \frac{|G|}{|G^{x_i}|}$$

Remarque I.1.16. — Soit G un groupe agissant sur un ensemble X, l'action étant fidèle et transitive (donc libre). Alors il découle facilement des définitions que tout choix d'un point de base $x \in X$ donne une bijection $X \simeq G$. On dit alors que X est un espace homogène principal sur G. Par exemple, si G est un espace vectoriel sur un corps k, un espace homogène principal sur G est un espace affine.

L'action d'un groupe G sur un ensemble X muni d'une certaine structure, est un moyen puissant d'obtenir des informations sur la structure du groupe G, ou sur celle de l'espace X, selon la nature du problème considéré.

I.2. Exemples de groupes et d'actions de groupes

Exemple I.2.1. — Le groupe des bijections (on dit aussi permutations dans ce contexte) de l'ensemble $\{1, \ldots, n\}$ est noté $\mathfrak{S}_n$.

Exemple I.2.2. — Soit V un espace vectoriel sur un corps k. L'ensemble des applications linéaires bijectives de V dans lui-même est souvent noté $\mathbf{GL}(V)$ plutôt que $\mathbf{Aut}(V)$. On appelle ce groupe le groupe général linéaire.

Une action d'un groupe G dans un espace vectoriel V qui préserve la structure d'espace vectoriel (on parle aussi d'action linéaire) est donc équivalent à la donnée d'un morphisme de groupes :

$$A : G \to \mathbf{GL}(V).$$

De telles actions apparaissent dans de nombreux contextes en mathématiques (leur étude est l'objet de ce cours), et l'importance de ce concept justifie une terminologie spécifique. On dit que l'espace vectoriel V, muni d'une action linéaire d'un groupe G, est une **représentation** du groupe G. Lorsque $V = k^n$, on utilise la notation $\mathbf{GL}_n(k)$ pour $\mathbf{GL}(V)$.

Exemple I.2.3. — Soit G un groupe agissant sur un ensemble X, et soit $\mathcal{F}(X)$ l'espace vectoriel des fonctions sur X à valeurs complexes. Alors $\mathcal{F}(X)$ est lui aussi muni d'une action linéaire de G, donnée par

$$(g \cdot f)(x) = f(g^{-1} \cdot x), \quad (g \in G), (f \in \mathcal{F}(X)), (x \in X).$$

Cette nouvelle action, d'une certaine manière, contient autant d'information que l'ancienne, mais présente l'avantage de pouvoir utiliser les techniques d'algèbre linéaire. C'est pourquoi ce cours s'attache plus particulièrement à l'étude des actions linéaires des groupes, c'est-à-dire, de leurs représentations.

Exemple I.2.4. — Soit V un espace vectoriel sur $\mathbb{C}$, muni d'une structure hilbertienne, c'est-à-dire d'un produit produit hermitien défini positif. Le sous-groupe de $\mathbf{GL}(V)$ préservant ce produit hermitien est noté $\mathbf{U}(V)$ et est appelé groupe unitaire. Lorsque $V = \mathbb{C}^n$, muni du produit hermitien canonique, on le note $\mathbf{U}(n)$. Une action d'un groupe G dans V préservant la structure hilbertienne est équivalente à la donnée d'un morphisme de groupes :

$$A : G \to \mathbf{U}(V).$$

On dit alors que la représentation de G dans V est unitaire.

Exemple I.2.5. — Soit V un espace vectoriel sur $\mathbb{R}$ muni d'un produit scalaire. Le sous-groupe de $\mathbf{GL}(V)$ préservant ce produit scalaire est noté $\mathbf{O}(V)$ et est appelé groupe orthogonal. Lorsque $V = \mathbb{R}^n$, muni du produit scalaire canonique, on le note $\mathbf{O}(n)$.

Si $p+q=n$, munissons $\mathbb{R}^n$ de la forme bilinéaire symétrique :

$$(x,y)_{p,q} = x_1y_1 + x_2y_2 + \cdots + x_py_p - x_{p+1}y_{p+1} - \cdots x_ny_n,$$

où $x = (x_1,\dots x_n)$, $y = (y_1,\dots,y_n)$ sont des vecteurs de $\mathbb{R}^n$. Cette forme est non dégénérée, de signature (p,q). Le sous-groupe de $\mathbf{GL}_n(\mathbb{R})$ préservant la forme $(.\,,.)_{p,q}$ est noté $\mathbf{O}(p,q)$. Si l'on note J_{pq} la matrice diagonale formée de 1 puis de -1 avec pour multiplicités respectives p et q, on a

$$\mathbf{O}(p,q) = \{A \in \mathbf{GL}_n(\mathbb{R}) \mid AJ_{pq}\,{}^tA = J_{pq}\}.$$

Le groupe $\mathbf{O}(3,1)$ joue un rôle important comme groupe de symétrie en electromagnétisme et en théorie de la relativité. Il s'appelle le groupe de Lorentz.

Exemple I.2.6. — Si V est un espace vectoriel de dimension finie sur le corps k, on note $\mathbf{SL}(V)$ le sous-groupe de $\mathbf{GL}(V)$ des éléments de déterminant 1. Ce groupe s'appelle le groupe spécial linéaire. Remarquons que

$$\det : \mathbf{GL}(V) \to k^*$$

est un morphisme de groupes, et donc $\mathbf{SL}(V)$ est son noyau. L'intersection d'un sous-groupe H de $\mathbf{GL}(V)$ avec $\mathbf{SL}(V)$ sera notée $\mathbf{S}H$. En reprenant les exemples ci-dessus, on obtient $\mathbf{SU}(V)$, $\mathbf{SO}(V)$, $\mathbf{SO}(p,q)$...

Exemple I.2.7. — Considérons l'action naturelle de $\mathbf{O}(2)$ dans $\mathbb{R}^2$, et soit $Y \subset \mathbb{R}^2$ un polygone régulier à n cotés ($n \leq 3$), centré en 0. Le sous-groupe de $\mathbf{O}(2)$ laissant invariant Y est le groupe dihédral D_n. Son ordre est $2n$. Son intersection avec $\mathbf{SO}(2)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple I.2.8. — Si k est un corps, et si K est une extension de k (c'est-à-dire un autre corps contenant k, alors le groupe des automorphismes du corps K fixant tout élément de k est noté $\mathbf{Aut}_k(K)$. Lorsque l'extension K/k possède certaines propriétés (plus explicitement, être séparable et normale) le groupe $\mathbf{Aut}_k(K)$ s'appelle le groupe de Galois de l'extension K/k. On le note aussi $\mathrm{Gal}(K/k)$. Si P est un polynôme à coefficients dans k, $\mathbf{Aut}_k(K)$ agit sur l'ensemble des racines de P dans K.

Exemple I.2.9. — Si X est un espace métrique, où plus généralement topologique, $\mathbf{Aut}(X)$ est l'ensemble des homéomorphismes de X dans lui-même. Si a est une action d'un groupe G sur X, on demande que les applications $a(g,.) : X \to X$ soient continues. Dans le cas où X est une variété différentiable, $\mathbf{Aut}(X)$ est l'ensemble des difféomorphismes de X dans lui-même. Les actions sur X sont alors supposées différentiables.

I.3. Le groupe symétrique

Nous rappelons rapidement dans cette section les notations et les principaux résultats concernant le groupe symétrique $\mathfrak{S}_n$, le groupe des permutations de l'ensemble $\{1,\ldots,n\}$.

Nous adoptons les notations usuelles pour les éléments de $\mathfrak{S}_n$. Ainsi, par exemple

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

est la bijection de l'ensemble $\{1,2,3,4,5\}$ envoyant 1 sur 4, 2 sur 2, 3 sur 5, 4 sur 1 et 5 sur 3.

Ceci permet d'effectuer facilement les calculs de produits, si l'on n'oublie pas que dans une composition de fonctions $f \circ g$, c'est la fonction g qui agit avant f :

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

On peut aussi noter les permutations selon leur décomposition en cycles, par exemple,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 6 & 9 & 2 & 5 & 8 & 1 & 3 \end{pmatrix},$$

est aussi notée

$$\sigma = (178)(249365).$$

Remarquons qu'il n'y a pas d'unicité d'une telle écriture :

$$\sigma = (178)(249365) = (817)(365249) \in \mathfrak{S}_9,$$

mais, en dehors de ces ambiguïtés évidentes, la décomposition en cycles est essentiellement déterminée.

On omet généralement les cycles de longueur 1 (les points fixes) d'une telle écriture :

$$\sigma = (178)(2)(4536)(9) = (178)(4536).$$

Remarquons que dans cette dernière écriture, il n'est plus apparent que σ soit un élément de $\mathfrak{S}_9$.

Soit $\sigma \in \mathfrak{S}_n$ et $k \in \{1, \ldots, n\}$. On appelle par abus de langage orbite de k sous σ l'orbite de k sous l'action du sous-groupe $\langle\sigma\rangle$ de $\mathfrak{S}_n$ ($\langle\sigma\rangle$ est le sous-groupe engendré par σ). La décomposition de $\{1, \ldots, n\}$ en orbites sous σ est apparente dans une écriture en cycles de σ.

Voyons maintenant certaines permutations particulières. Si i et j sont deux éléments différents de $\{1, \ldots, n\}$, on appelle **transposition** $\tau_{ij} = (i, j)$ de i et de j la permutation de $\mathfrak{S}_n$ qui échange i et j et laisse tous les autres éléments fixes.

On appelle **cycle** une permutation dont toutes les orbites sauf au plus une sont des singletons. On appelle longueur du cycle le cardinal de cette orbite particulière, la longueur de l'identité étant 1. Ainsi une transposition est un cycle de longueur 2.

On appelle **permutation circulaire** de $\mathfrak{S}_n$ une permutation n'ayant qu'une seule orbite. Les permutations circulaires sont donc les cycles de longueur n.

Théorème I.3.1. — *Les transpositions $\tau_{i,i+1}$, $i = 1, \ldots n-1$, engendrent $\mathfrak{S}_n$.*

Démonstration. (Esquisse). Par récurrence sur n, on montre que $\mathfrak{S}_n$ est engendré par les transpositions. On montre ensuite qu'une transposition quelconque est produit de transpositions de la forme $\tau_{i,i+1}$. □

Ecrivons une représentation σ comme produit de transpositions. Bien sûr, il n'y a pas unicité de cette écriture, ni même unicité du nombre de transpositions intervenant dans cette écriture. En revanche, la parité de ce nombre de transpositions est déterminée par σ, comme l'affirme le théorème suivant :

Théorème I.3.2. — *Soit $\sigma \in \mathfrak{S}_n$. Il y a égalité entre les nombres suivants :*

(i) $(-1)^T$ où T est le nombre de transpositions dans une écriture de σ comme produit de transpositions.

(ii) $(-1)^D$, $D = n - m$ où m est le nombre d'orbites de σ dans $\{1, \ldots, n\}$.

(iii) $(-1)^S$ où S est le cardinal de l'ensemble des couples $(i, j) \in \{1, \ldots, n\}^2$ tels que $i < j$ et $\sigma(i) > \sigma(j)$.

(iv) $\prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$.

On appelle ce nombre la **signature** *de σ et on le note* $\mathrm{sgn}(\sigma)$*. Si* $\mathrm{sgn}(\sigma) = 1$*, on dit que σ est* **paire***, et* **impaire** *si* $\mathrm{sgn}(\sigma) = -1$

Démonstration. l'égalité entre (iii) et (iv) est évidente car tous les facteurs $(i-j)$, au signe près, apparaissent une et une seule fois au numérateur et au dénominateur. La valeur absolue de (iv) est donc 1, et son signe est donné par le nombre de couples (i, j) tels que $i < j$ et $\sigma(i) > \sigma(j)$.

Montrons que $(i) = (ii)$, ce qui montre au passage que (i) est bien défini, c'est-à-dire ne dépend pas de l'écriture de σ en un produit de transpositions. Notons $\epsilon(\sigma)$ la quantité définie en (ii). On montre d'abord que si $\tau = \tau_{ij}$ est une transposition $\epsilon(\sigma\tau) = -\epsilon(\sigma)$, en distinguant deux cas :

- si i et j sont dans la même orbite sous σ, alors les orbites sous $\sigma\tau$ sont les mêmes que celle sous σ, sauf l'orbite contenant i et j qui se scinde en deux.

- si i et j ne sont pas sont dans la même orbite sous σ, alors les orbites sous $\sigma\tau$ sont les mêmes que celle sous σ, sauf celles contenant i et j qui n'en forment plus qu'une.

On raisonne alors par récurrence sur le nombre de transpositions dans une écriture de σ comme produit de celles-ci. Ceci montre au passage que la signature d'un cycle de longueur k est $(-1)^{k-1}$.

Montrons maintenant que $(i) = (iv)$. On a, quels que soient $\sigma\tau \in \mathfrak{S}_n$,

$$\prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{i-j} = \prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \quad \prod_{i<j} \frac{\tau(i) - \tau(j)}{i-j}$$

$$= \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i-j} \quad \prod_{i<j} \frac{\tau(i) - \tau(j)}{i-j}$$

par un changement de variables dans le premier produit. Si l'on note $\epsilon'(\sigma)$ la quantité définie en (iv), on a donc $\epsilon'(\sigma\tau) = \epsilon'(\sigma)\epsilon'(\tau)$. On conclut alors encore par récurrence sur le nombre de transpositions dans une écriture de σ comme produit de celles-ci, en remarquant que $\epsilon'(\tau) = -1$ si τ est une transposition. $\square$

Corollaire I.3.3. — *L'application*

$$\mathfrak{S}_n \to \{\pm 1\}, \quad \sigma \mapsto \mathrm{sgn}(\sigma)$$

est un morphisme de groupes.

Le noyau du morphisme sgn, c'est-à-dire l'ensemble des représentations paires, est appelé le **groupe alterné**, et noté $\mathfrak{A}_n$.

Exercice I.3.4. — Montrer que le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles. Montrer que si $n \geq 5$, tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Le but de l'exercice est maintenant de montrer que $\mathfrak{A}_n$, $n \geq 5$, est **simple**, c'est-à-dire qu'il n'admet pas de sous-groupes distingué autre que lui-même et le sous-groupe trivial.

Soit H un sous-groupe distingué de $\mathfrak{A}_n$, non trivial. La question précédente montre qu'il s'agit de voir que H contient un 3-cycle. Soit $\sigma \in H$, $\sigma \neq \mathrm{Id}$ tel que le nombre de points fixes de σ soit maximal. On distingue deux cas :

- σ contient un cycle de longueur au moins égale à 3. A conjugaison près, on peut supposer que $\sigma = (123...)...$. Si σ est un 3-cycle, c'est gagné, sinon, il existe $i, j \notin \{1, 2, 3\}$ tels que i et j ne soient pas fixés par σ. En effet, la seule autre possibilité, σ de la forme $(123j)$ est exclue car c'est une permutation impaire. Posons $\tau = (2ij)$ et formons $\gamma = \tau\sigma\tau^{-1}\sigma^{-1}$.

Montrer que γ est dans H, non trivial, et a plus de points fixes que σ. Conclure.

- σ est un produit de transpositions disjointes. A conjugaison près, $\sigma = (12)(34)$.... Posons $\tau = (345)$, et $\gamma = \tau\sigma\tau^{-1}\sigma^{-1}$. Conclure comme dans le cas précédent.

Nous allons décrire les classes de conjugaison dans le groupe symétrique $\mathfrak{S}_n$. Rappelons qu'une **partition** de l'entier n est un collection d'entiers ≥ 1 (avec répétitions) $\{n_1, \dots, n_k\}$ tel que

$$n = n_1 + \cdots + n_k.$$

On note souvent une partition en ordonnant les n_i dans l'ordre décroissant :

$$\lambda = (n_1, \dots, n_k)$$

avec $n_1 \geq n_2 \geq \cdots \geq n_k$, $n = n_1 + \cdots + n_k$. Une autre notation souvent utilisée pour une partition est d'indiquer, pour chaque entier $1, 2, \dots$ la multiplicité avec lequel celui-ci intervient dans la partition par un exposant (en omettant les entiers n'intervenant pas) . Par exemple, la notation

$$\lambda = (1^2, 2^2, 4^1)$$

désigne la partition

$$10 = 4 + 2 + 2 + 1 + 1.$$

A chaque élément $\sigma \in \mathfrak{S}_n$, on associe une partition de n donnée par les longueurs des cycles dans la décomposition en cycles de σ. Par exemple, $\sigma = (178)(2)(4536)(9)$ donne la partition $9 = 4 + 3 + 1 + 1$.

Théorème I.3.5. — *Deux permutations σ et τ de $\mathfrak{S}_n$ sont conjuguées si et seulement si les partitions de n données par leur décomposition en cycles sont les mêmes.*

La démonstration est laissée en exercice.

Exercice I.3.6. — Calculer le cardinal de la classe de conjugaison de $\mathfrak{S}_n$ correspondant à la partition $\lambda = (\lambda_1^{\alpha_1}, \dots, \lambda_r^{\alpha_r})$ de n.

I.4. Exercices

Exercice I.4.1. — **Produit semi-direct**

— 1. *Le point de vue interne.* Soient G un groupe et H et N deux sous-groupes de G vérifiant :

(a) N est distingué dans G,

(b) H et N engendrent G, $H \cap N = \{e\}$.

Montrer que tout élément $g \in G$ se décompose de manière unique sous la forme $g = nh$, $n \in N$, $h \in H$. En déduire que l'on a une bijection

$$N \times H \to G, \quad (n, h) \mapsto nh.$$

Montrer que la loi de groupe sur $N \times H$ induite de celle de G par transport de structure est

$$(n, h)(n', h') = (n(hn'h^{-1}), hh').$$

— 2. *Le point de vue externe.* Soient H et N deux groupes, et supposons que H agisse sur N par automorphismes de groupe, c'est-à-dire que l'on dispose d'un morphisme de groupes

$$\phi : H \to \mathbf{Aut}(N),$$

et l'on pose $h \cdot n = \phi(h)(n)$. On définit sur $N \times H$ le produit

$$(n, h)(n', h') = (n\,(h \cdot n'), hh').$$

Montrer que $N \times H$ muni de ce produit est un groupe, que l'on appelle le produit semi-direct de N et H, et que l'on note $N \rtimes H$. Vérifier que les parties $N \times \{e_H\}$ et $\{e_N\} \times H$ sont deux sous-groupes de $N \rtimes H$, respectivement isomorphes à N et H. On identifie ainsi N et H à deux sous-groupes de $N \rtimes H$. Montrer qu'ils vérifient les hypothèses du 1.

— 3. *Extensions.* Une suite exacte de groupes est une suite de groupes G_i, et de morphismes $\phi_i : G_i \to G_{i+1}$,

$$\cdots G_{i-1} \xrightarrow{\phi_{i-1}} G_i \xrightarrow{\phi_i} G_{i+1} \xrightarrow{\phi_{i+1}} G_{i+2} \xrightarrow{\phi_{i+2}} \cdots$$

telle que pour tout i, $\ker \phi_{i+1} = \operatorname{Im} \phi_i$. Une suite exacte courte est une suite exacte de la forme

$$\{e\} \to N \xrightarrow{\phi} G \xrightarrow{\psi} H \to \{e\}.$$

Le morphisme ϕ est injectif, et ψ est surjectif.

Supposons que soit donnée une suite exacte courte comme ci-dessus. Une section de cette suite exacte est un morphisme de groupes $s : H \to G$ tel que $\psi \circ s = \mathrm{Id}_H$.

Montrer que s est injective. Montrer que $\phi(N)$ et $s(H)$ sont deux sous-groupes vérifiant les hypothèses du 1. Faire le lien avec le point de vue externe.

— 4. *Exemples.* Montrer que le groupe dihédral D_n est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Déterminer les classes de conjugaison de D_n. Montrer que le groupe $E(2)$ des isométries affines du plan est le produit semi-direct $\mathbb{R}^2 \rtimes \mathbf{O}(2)$. Chercher dans la littérature ou sur internet la définition du groupe de Poincaré.

Exercice I.4.2. — Soit G un groupe fini, opérant sur un ensemble S. Alors G opère naturellement sur le produit cartésien $S^n = S \times \ldots \times S$ pour chaque entier n par

$$g \cdot (s_1, \ldots, s_n) = (g \cdot s_1, \ldots, g \cdot s_n).$$

Définissons $S^{(n)} \subset S^n$ comme l'ensemble des n-uplets d'élément distincts de S :

$$S^{(n)} = \{(s_1, \ldots s_n) \in S^n | i \neq j \Rightarrow s_i \neq s_j\}.$$

Alors G opère sur $S^{(n)}$. On dit que l'action de G sur S est n-transitive si l'action de G sur $S^{(n)}$ est transitive.

Montrer que l'action de $\mathfrak{A}_n$ sur $\{1, 2, \ldots, n\}$ est $n-2$-transitive.

Exercice I.4.3. — Soit G un groupe. Une **présentation** du groupe G est la donnée d'un ensemble $\mathcal{G} = \{g_i, i \in I\}$ d'éléments de G engendrant G, et d'un ensemble $\mathcal{R}$ de relations, une relation étant une égalité de la forme :

$$h_1 h_2 \ldots h_n = e, \quad h_j \in \mathcal{G} \cup \mathcal{G}^{-1}, \ j = 1, \ldots, n. \tag{I.4.1}$$

de telle sorte que la propriété universelle suivante soit vérifiée : pour tout groupe G' admettant un système de générateur $\mathcal{G}' = \{g'_i, i \in I\}$ (c'est le même I) vérifiant les relations

$$h'_1 h'_2 \dots h'_n = e, \quad h_j \in \mathcal{G} \cup \mathcal{G}^{-1},\ j = 1, \dots, n$$

dès que $h_1 h_2 \dots h_n = e$ est dans $\mathcal{R}$, avec $h'_j = g'_i$ si $h_j = g_i$ et $h'_j = (g'_i)^{-1}$ si $h_j = g_i^{-1}$, il existe un unique morphisme de groupes $\phi :\ G \to G'$ tel que $\phi(g_i) = g'_i$ pour tout $i \in I$.

— 1. Montrer que $\mathcal{G} = \{1\}$, $\mathcal{R} = \{m1 = 0\}$ est une présentation de $\mathbb{Z}/m\mathbb{Z}$ (notation additive de la loi de groupe).

— 2. On se donne un ensemble $\mathcal{G}$ et un ensemble de relations $\mathcal{R}$ de la forme (I.4.1) (l'ensemble $\mathcal{G}^{-1}$ est défini formellement comme l'ensemble des symboles g_i^{-1}, $i \in I$). Montrer qu'il n'existe à isomorphisme près qu'un seul groupe admettant $\mathcal{G}$ et $\mathcal{R}$ comme présentation.

— 3. Soit $\mathbb{F}$ un corps. Considérons les éléments suivants de $\mathbf{SL}_{\mathbb{F}}(2)$:

$$t(y) = \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix},\ y \in \mathbb{F}^{\times}, \quad n(z) = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix},\ z \in \mathbb{F}, \quad w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Posons

$$\mathcal{G} = \{t(y),\ y \in \mathbb{F}^{\times},\ n(z),\ z \in \mathbb{F}, w\},$$

et soit $\mathcal{R}$ l'ensemble des relations suivantes :

$$t(y_1)t(y_2) = t(y_1 y_2) \qquad n(z_1)n(z_2) = n(z_1 + z_2)$$
$$t(y)n(z)t(y)^{-1} = n(y^2 z) \qquad wt(y)w^{-1} = t(y^{-1})$$
$$n(z)wn(z^{-1})w^{-1}n(z) = t(z)w, \quad (z \neq 0).$$

Montrer que $(\mathcal{G}, \mathcal{R})$ est une présentation de $\mathbf{SL}_{\mathbb{F}}(2)$.

Indication. Constater que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = n(a/c)t(-c^{-1})wn(d/c) \quad \text{si } c \neq 0, \qquad \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = t(a)n(b/a).$$

CHAPITRE II

REPRÉSENTATIONS LINÉAIRES DES GROUPES FINIS

Dans ce chapitre, les espaces vectoriels sont définis sur le corps des nombres complexes.

Rappelons que si V est un espace vectoriel, $\mathbf{GL}(V)$ désigne le groupe des isomorphismes linéaires de V dans lui-même. Si V est de plus muni d'un produit hermitien $(.\,,.)_V$, $\mathbf{U}(V)$ désigne le sous-groupe de $\mathbf{GL}(V)$ des applications linéaires u préservant le produit hermitien, c'est-à-dire

$$(u(v), u(w))_V = (v, w)_V, \quad (v, w \in V).$$

II.1. Représentations

II.1.1. Représentations unitaires. —

Définition II.1.1. — Une représentation (ρ, V) du groupe G est la donnée d'un espace vectoriel V, appelé espace de la représentation, et d'un morphisme de groupes

$$\rho : G \to \mathbf{GL}(V).$$

Si V est un espace de Hilbert pour le produit hermitien $(.\,,.)_V$, la représentation (ρ, V) est dite **unitaire** si ρ est à valeurs dans $\mathbf{U}(V)$, c'est-à dire si pour tout $g \in G$, pour tous $v, w \in V$,

$$(\rho(g) \cdot v, \rho(g) \cdot w)_V = (v, w)_V.$$

La dimension de la représentation (ρ, V) est la dimension de V. On la note d_ρ.

La représentation triviale de G est celle où $V = \mathbb{C}$ et tout $g \in G$ agit comme l'identité de $\mathbb{C}$. On la note 1_G.

L'espace vectoriel $\{0\}$ est aussi un espace de représentation pour tout groupe G (de manière unique, puisque $\mathbf{GL}(\{0\})$ est le groupe à un élément). Nous l'appellerons **représentation nulle** de G.

Théorème II.1.2. — *Soit (ρ, V) une représentation de dimension finie de G d'un groupe fini. On peut munir V d'un produit hermitien $(.\,,.)_V$ qui rend la représentation (ρ, V) unitaire.*

Démonstration. Munissons V d'un produit hermitien $(.\,,.)_0$ quelconque. Définissons un nouveau produit hermitien $(.\,,.)_1$ par

$$(v, w)_1 = \frac{1}{|G|} \sum_{g \in G} (\rho(g) \cdot v, \rho(g) \cdot w)_0, \quad (v, w \in V).$$

Ce nouveau produit vérifie les propriétés de sesquilinéarité requises et est positif, comme on peut le voir immédiatement. Il est défini car si

$$(v, v)_1 = \frac{1}{|G|} \sum_{g \in G} (\rho(g) \cdot v, \rho(g) \cdot v)_0 = 0$$

alors tous les termes de la somme étant positifs, ils sont nuls. Pour $g = e$, ceci donne $(v, v)_0 = 0$, et donc $v = 0$.

Vérifions que ce nouveau produit hermitien est invariant par ρ. Pour tout $h \in H$:

$$\begin{aligned}(\rho(h) \cdot v, \rho(h) \cdot w)_1 &= \frac{1}{|G|} \sum_{g \in G} (\rho(g) \cdot \rho(h) \cdot v, \rho(g) \cdot \rho(h) \cdot w)_0 \\ &= \frac{1}{|G|} \sum_{g \in G} (\rho(gh) \cdot v, \rho(gh) \cdot w)_0 \\ &= \frac{1}{|G|} \sum_{g \in G} (\rho(g) \cdot v, \rho(g) \cdot w)_0 \\ &= (v, w)_1\end{aligned}$$

Le point crucial du calcul est donc juste un changement de variable dans la somme.

Remarquons que l'hypothèse de la dimension finie ne sert qu'à s'assurer que V est bien un espace de Hilbert. Si l'on suppose au départ que $(V, (.\,,.)_0)$ est un espace de Hilbert de dimension infinie, le même procédé de moyenne donne un nouveau produit hermitien $(.\,,.)$ invariant par G. Il est facile de voir que la topologie définie par ce nouveau produit hermitien est la même que l'ancienne (les normes induites sont équivalentes), et donc que V est encore un espace de Hilbert pour $(.\,,.)$. $\square$

Remarque II.1.3. — Lorsque nous étudierons des groupes plus généraux que les groupes finis, il nous faudra remplacer les arguments basés sur ce procédé de moyenne par quelque chose de plus général, à savoir l'existence de mesure de Haar sur les groupes. Nous ne définissons pas la notion de mesure de Haar pour l'instant, mais nous remarquons simplement que l'on peut munir l'ensemble fini G de sa **mesure de comptage normalisée** μ_G. Plus explicitement, pour toute fonction f sur G

$$\int_G f(g)\; d\mu(g) = \frac{1}{|G|}\sum_{g\in G} f(g).$$

La propriété fondamentale de cette mesure est que quels que soient x, y dans G,

$$\int_G (l(x)r(y)\cdot f)(g)\; d\mu(g) = \int_G f(g)\; d\mu(g),$$

c'est-à-dire que μ_G est invariante par translation à gauche et à droite.

II.1.2. Sous-représentations, représentations irréductibles. —

Soit (ρ, V) une représentation du groupe G. Un sous-espace W de V est dit invariant par ρ si pour tout $g \in G$, $\rho(g)\cdot W \subset W$. On peut alors parler de la restriction de ρ à W, que l'on note $(\rho_{|W}, W)$. Une telle représentation restreinte à un sous-espace invariant s'appelle une **sous-représentation** de G.

Définition II.1.4. — Une représentation (ρ, V) du groupe G est dite **irréductible** si elle est non nulle n'admet aucun sous-espace autre que $\{0\}$ et V invariant par ρ.

Proposition II.1.5. — *Une représentation irréductible d'un groupe fini est de dimension finie.*

Démonstration. Soit (ρ, V) une représentation irréductible du groupe fini G. Soit $v \in V$, non nul, et soit W le sous-espace engendré par les vecteurs de la forme $\rho(g) \cdot v$, $g \in G$. Ce sous-espace est donc de dimension finie, et il est immédiat de vérifier qu'il est invariant par ρ. On a donc $V = W$ et V est de dimension finie. □

Soit (ρ, V) une représentation du groupe G et supposons que l'espace V soit somme directe de sous-espaces W_i (non nuls), $i = 1, \dots, r$:

$$V = \bigoplus_{i=1,\dots,r} W_i$$

et que ces espaces W_i soient invariants par ρ. On dit alors que la représentation (ρ, V) se décompose en somme directe des représentations $(\rho_{|W_i}, W_i)$ et l'on écrit

$$(\rho, V) = \bigoplus_{i=1,\dots,r} (\rho_{|W_i}, W_i).$$

L'étude de la représentation (ρ, V) se ramène alors à celle des $(\rho_{|W_i}, W_i)$. Il parait raisonnable d'espérer pouvoir décomposer toute représentation en somme directe de représentations, jusqu'à ce que toutes celles-ci soient irréductibles. Ceci n'est pourtant pas totalement évident, le problème étant le suivant : si (ρ, V) est une représentation qui n'est pas irréductible, alors il existe un sous-espace W invariant par ρ. Pour pouvoir décomposer (ρ, V), il faudrait pouvoir exhiber un supplémentaire de W dans V qui soit lui aussi invariant par ρ. Le théorème ci-dessous affirme que pour les représentations d'un groupe fini, ceci est toujours possible. Pour des représentations plus générales, ce n'est pas le cas. Il est donc utile d'introduire la terminologie **représentation indécomposable** pour une représentation qui ne peut pas s'écrire comme somme directe non triviale. Une représentation irréductible est toujours indécomposable, l'inverse n'étant pas vrai en général (mais l'est pour les représentations des groupes finis).

Théorème II.1.6. — *Soient G un groupe fini et (ρ, V) une représentation de dimension finie de G. Soit W un sous-espace de V invariant* *par ρ. Alors W admet un supplémentaire invariant W', de sorte que l'on peut décomposer (ρ, V) en somme directe de $(\rho_{|W}, W)$ et $(\rho_{|W'}, W')$.*

Démonstration. D'après le théorème II.1.2, on peut munir V d'un produit hermitien invariant $(\,.\,,.\,)_V$. Il est alors immédiat de voir que l'orthogonal $W^\perp$ de W dans V pour ce produit hermitien est invariant par ρ. Ceci fournit une décomposition

$$V = W \oplus W^\perp$$

en somme directe de sous-espaces invariants. □

Corollaire II.1.7. — *Toute représentation de dimension finie (ρ, V) d'un groupe fini G se décompose en somme directe de représentations irréductibles.*

Démonstration. Ceci est facile à établir par récurrence sur la dimension de la représentation. Remarquons que le fait que le groupe soit fini permet de montrer l'existence d'un supplémentaire stable, et le fait que la représentation soit de dimension finie permet la récurrence. □

Une représentation est dite **complètement réductible**, ou **semisimple** si elle peut s'écrire comme somme directe de représentations irréductibles. Le corollaire affirme que toute représentation de dimension finie d'un groupe fini est complètement réductible. Ceci permet de réduire dans une certaine mesure l'étude des représentations de dimension finie du groupe G à celle des représentations irréductibles.

II.1.3. Opérateurs d'entrelacement. Lemme de Schur. —

Définition II.1.8. — Soient (ρ, V) et (τ, W) deux représentations du groupe G. Un opérateur d'entrelacement $T : V \to W$ est une application linéaire de V dans W vérifiant

$$T(\rho(g) \cdot v) = \tau(g) \cdot T(v), \quad (g \in G), (v \in V)$$

Autrement dit, un opérateur d'entrelacement est un G-morphisme linéaire (*cf.* Définition I.1.4).

On note $\mathrm{Hom}_G(V, W)$ ou parfois $\mathrm{Hom}_G(\rho, \tau)$ l'ensemble des opérateurs d'entrelacement entre (ρ, V) et (τ, W). Il est clair que c'est un sous-espace vectoriel de l'espace des applications linéaires de V vers W.

Il devient maintenant possible de définir la notion de **représentations équivalentes**, ou **isomorphes**.

Définition II.1.9. — Soient (ρ, V) et (τ, W) deux représentations du groupe G. Elles sont équivalentes (ou isomorphes) s'il existe un opérateur d'entrelacement inversible $T : V \to W$.

Si T est un tel opérateur d'entrelacement inversible, T^{-1} est bien sûr aussi un opérateur d'entrelacement et

$$\tau(g) = T \circ \rho(g) \circ T^{-1}, \quad (g \in G)$$

L'équivalence dans le sens défini ci-dessus est une relation d'équivalence sur l'ensemble des représentations du groupe G. Dans la pratique, comme souvent en mathématique, on a tendance à souvent confondre équivalence et égalité, c'est-à-dire à confondre une représentation et sa classe d'équivalence, ou dans le sens contraire, une classe d'équivalence et l'un de ses représentants. Il s'agit là d'abus de langage la plupart du temps inoffensifs.

Définition II.1.10. — Soit G un groupe fini. Le dual de G, noté $\hat{G}$, est l'ensemble des classes d'équivalence de représentations irréductibles de G.

Lemme II.1.11. — (*i*) *Soient* (ρ, V) *et* (τ, W) *deux représentations du groupe* G *et* $T : V \to W$ *un opérateur d'entrelacement. Alors le noyau* $\ker T$ *est un sous-espace de* V *invariant par* ρ*, et* $\mathrm{Im}\, T$ *est un sous-espace de* W *invariant par* τ*.*

(*ii*) *Soit* (ρ, V) *une représentation du groupe* G*, et* T *un opérateur d'entrelacement de* (ρ, V) *avec elle-même. Alors tout sous-espace propre de* T *est invariant par* ρ*.*

Démonstration. (i) Si $v \in \ker T$, alors, pour tout $g \in G$,

$$T(\rho(g) \cdot v) = \tau(g) \cdot T(v) = 0$$

donc $\rho(g) \cdot v \in \ker T$. Si $w \in \operatorname{Im} T$, il existe $v \in V$ tel que $T(v) = w$, et pour tout $g \in G$,

$$\tau(g) \cdot w = \tau(g) \cdot T(v) = T(\rho(g) \cdot v)$$

donc $\tau(g) \cdot w \in \operatorname{Im} T$. □

(ii) Soit λ une valeur propre de T, et V_λ le sous-espace propre correspondant. Alors pour tout $g \in G$, pour tout $v \in V_\lambda$,

$$T(\rho(g) \cdot v) = \rho(g) \cdot T(v) = \lambda\rho(g) \cdot v$$

et donc $\rho(g) \cdot v \in V_\lambda$. □

***Théorème II.1.12* (Lemme de Schur)**. — *Soit T un opérateur d'entrelacement entre deux représentations irréductibles (ρ_1, V_1) et (ρ_2, V_2) d'un groupe fini G. Alors*

- si (ρ_1, V_1) et (ρ_2, V_2) ne sont pas équivalentes, $T = 0$,

- si (ρ_1, V_1) et (ρ_2, V_2) sont équivalentes, $\operatorname{Hom}_G(V_1, V_2)$ est de dimension 1. De manière équivalente, $\operatorname{Hom}_G(V_1, V_1)$ est l'ensemble des multiples scalaires de l'identité de V_1.

Démonstration. Ceci découle facilement du lemme précédent. En effet, si (ρ_1, V_1) et (ρ_2, V_2) ne sont pas équivalentes, T n'est pas inversible. S'il n'est donc pas injectif, son noyau est non trivial. Mais (ρ_1, V_1) étant irréductible, ceci donne $\ker T = V_1$, et donc $T = 0$. De même, s'il n'est pas surjectif, son image $\operatorname{Im} T$ est un sous-espace invariant de V_2, et donc V_2 étant irréductible, $\operatorname{Im} T = \{0\}$, donc $T = 0$.

Pour le second point, soit $T \in \operatorname{Hom}_G(V_1, V_1)$, considérons une valeur propre λ de T, et soit V_λ le sous-espace de V_1 correspondant. Il est non nul par hypothèse, et donc par irréductibilité de (ρ_1, V_1), c'est V_1 tout entier. Ceci montre que $T = \lambda \mathrm{Id}_{V_1}$. L'équivalence entre les deux formulations du second point vient du fait que si $S : V_1 \to V_2$ est un opérateur d'entrelacement inversible réalisant l'équivalence entre (ρ_1, V_1) et (ρ_2, V_2), il est clair que

$$\begin{aligned}\mathrm{Hom}_G(V_1, V_1) &\to \mathrm{Hom}_G(V_1, V_2)\\ T &\mapsto S \circ T\end{aligned}$$

est un isomorphisme linéaire d'inverse donné par $T \mapsto S^{-1} \circ T$. □

II.2. Opérations sur les représentations : sommes (directes), produits (tensoriels) et représentations duales

II.2.1. Sommes directes. — Nous avons vu dans la section II.1.2 comment une représentation (ρ, V) d'un groupe G pouvait parfois se décomposer en somme directe de sous-représentations (point de vue interne). Voyons maintenant comment former la somme directe de deux représentations de G n'ayant a priori rien à voir l'une avec l'autre (point de vue externe). Soient donc (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G. L'espace vectoriel $V_1 \times V_2$, muni des deux projections canoniques

$$p_1 : V_1 \times V_2 \to V_1, \quad p_2 : V_1 \times V_2 \to V_2$$

est le **produit** des espaces vectoriels V_1 et V_2. La notion de somme directe est légèrement différente. La **somme directe** de V_1 et de V_2 est aussi le produit $V_1 \times V_2$, mais muni des deux injections canoniques :

$$i_1 : V_1 \to V_1 \times V_2, \quad i_2 : V_2 \to V_1 \times V_2$$

On peut ainsi identifier V_1 et V_2 à deux sous-espaces de $V_1 \times V_2$, noter $V_1 \oplus V_2$ plutôt que $V_1 \times V_2$ et écrire $v_1 + v_2$ l'élément (v_1, v_2) de $V_1 \times V_2$. On munit maintenant $V_1 \oplus V_2$ de la représentation $\rho_1 \oplus \rho_2$:

$$(\rho_1 \oplus \rho_2)(g) \cdot (v_1 + v_2) = \rho_1(v_1) + \rho_2(v_2), \quad (v_1 \in V_1), (v_2 \in V_2), (g \in G).$$

On peut généraliser cette construction à un nombre fini (et même infini) de représentations (ρ_i, V_i) de G.

II.2.2. Produits tensoriels. — Dans le paragraphe précédent, nous avons muni l'ensemble des représentations d'un groupe G d'une somme :

$$((\rho_1, V_1), (\rho_2, V_2)) \mapsto (\rho_1 \oplus \rho_2, V_1 \oplus V_2),$$

La terminologie et la notation "additive" se justifient par le fait que $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ est toujours isomorphe à $(\rho_2 \oplus \rho_1, V_2 \oplus V_1)$ et que

$$\dim(V_1 \oplus V_2) = \dim V_1 + \dim V_2,$$

lorsque V_1 et V_2 sont de dimension finie. La représentation de G dans l'espace nul $\{0\}$ est un "élément neutre" pour cette somme. Mais remarquons qu'une représentation (ρ, V) non nulle n'admet pas d'inverse.

Nous voudrions maintenant construire une opération analogue à un produit :

$$((\rho_1, V_1), (\rho_2, V_2)) \mapsto (\rho_1 \otimes \rho_2, V_1 \otimes V_2)$$

ayant de bonnes propriétés de distributivité par rapport à la somme définie précédemment, et vérifiant

$$\dim(V_1 \otimes V_2) = \dim V_1 \times \dim V_2, \tag{II.2.1}$$

lorsque V_1 et V_2 sont de dimension finie.

Définition II.2.1. — Soient V_1 et V_2 deux espaces vectoriels. Le **produit tensoriel** $V_1 \otimes V_2$ est un espace vectoriel muni d'une application

$$\iota : \; V_1 \times V_2 \to V_1 \otimes V_2, \quad (v_1, v_2) \mapsto v_1 \otimes v_2$$

vérifiant :

(i) ι est bilinéaire,

(ii) si $(e_i)_{i\in I}$ est une base de V_1 et si $(f_j)_{j\in J}$ est une base de V_2,

$$(e_i \otimes f_j)_{i\in I, j\in J}$$

est une base de $V_1 \otimes V_2$.

Remarques II.2.2. — Un tel espace existe et est déterminé à isomorphisme près. La propriété (ii) entraîne la formule (II.2.1). L'espace $V_1 \otimes V_2$ vérifie la propriété universelle suivante :

(ii') soit $\phi : V_1 \times V_2 \to W$ une application bilinéaire quelconque. Alors il existe une unique application linéaire

$$\tilde{\phi} : V_1 \otimes V_2 \to W$$

tel que $\tilde{\phi} \circ \iota = \phi$.

La propriété (ii') est équivalente à (ii).

Soient (ρ_1, V_1) une représentation d'un groupe G_1, et (ρ_2, V_2) une représentation d'un groupe G_2. On peut munir l'espace $V_1 \otimes V_2$ d'une représentation notée $\rho_1 \boxtimes \rho_2$ de $G_1 \times G_2$ définie par

$$(\rho_1 \boxtimes \rho_2)(g_1, g_2) \cdot (v_1 \otimes v_2) = \rho_1(g_1) \cdot v_1 \otimes \rho_2(g_2) \cdot v_2$$
$$(v_1 \in V_1),\ (v_2 \in V_2), (g_1 \in G_1), (g_2 \in G_2).$$

Lorsque $G_1 = G_2$ on obtient une représentation de G, notée $\rho_1 \otimes \rho_2$ définie par

$$(\rho_1 \otimes \rho_2)(g) \cdot (v_1 \otimes v_2) = \rho_1(g) \cdot v_1 \otimes \rho_2(g) \cdot v_2$$
$$(v_1 \in V_1),\ (v_2 \in V_2), (g \in G).$$

II.2.3. Représentation contragrédiente. — Si V est un espace vectoriel, notons V^* son dual, c'est-à-dire l'espace des formes linéaires sur V. Il est bien connu que

$$\mathbf{ev} : V \to (V^*)^*, \quad \mathbf{ev}(v) : \lambda \in V^* \mapsto \lambda(v)$$

est une application linéaire, injective. Si V est de dimension finie, par égalité des dimensions, cette application est un isomorphisme.

Si (π, V) est une représentation d'un groupe G, on définit une représentation $\tilde{\pi}$ de G dans V^*, appelée **représentation contragrédiente**, par la formule suivante :

$$(\tilde{\pi}(g) \cdot \lambda)(v) = \lambda(\pi(g)^{-1} \cdot v), \quad (\lambda \in V^*), (v \in V), (g \in g).$$

Il est clair que $(\tilde{\tilde{\pi}}, (V^*)^*) = (\pi, V)$ lorsque V est de dimension finie et que $(V^*)^*$ est identifié à V par la remarque ci-dessus.

Proposition II.2.3. — *Soit (π, V) une représentation d'un groupe fini G. Alors (π, V) est irréductible si et seulement si $(\tilde{\pi}, V^*)$ est irréductible.*

<u>*Démonstration*</u>. D'après la remarque que $(\tilde{\tilde{\pi}}, (V^*)^*) = (\pi, V)$ lorsque V est de dimension finie, il suffit de montrer une seule implication pour obtenir l'équivalence. Supposons (π, V) irréductible, et soit W un sous-espace invariant de V^*. Alors l'orthogonal dans V de W est aussi invariant, et donc ne peut-être que $\{0\}$ ou V. Ceci montre que $W = \{0\}$ ou V^*. □

II.3. Coefficients matriciels et relations de Schur

II.3.1. Une application du lemme de Schur. — Le résultat qui suit est une application du lemme de Schur qui nous servira par la suite.

Proposition II.3.1. — *Soient (ρ, V) et (τ, E) deux représentations irréductibles d'un groupe fini G et soit $A : V \to E$ une application linéaire. Alors*

$$A^\circ = \int_G \tau(g) A \rho(g)^{-1} d\mu_G(g)$$

est égal à 0 si τ n'est pas équivalente à ρ et égal à $\frac{\operatorname{Tr} A}{\dim V}\, \mathrm{Id}_V$ lorsque $(\tau, E) = (\rho, V)$.

<u>*Démonstration*</u>. Comme on voit facilement que A° est G-équivariant, d'après le lemme de Schur, $A^\circ = 0$ si τ n'est pas équivalent à ρ et $A^\circ = \alpha \mathrm{Id}_V$ lorsque $(\tau, E) = (\rho, V)$. Il reste à déterminer α. On a

$$\alpha \dim V = \operatorname{Tr} A^\circ = \int_G \operatorname{Tr}\left(\rho(g) A \rho(g^{-1})\right) d\mu_G(g) = \operatorname{Tr} A.$$

□

II.3.2. Coefficients matriciels. — Soit G un groupe fini. Soit $\mathcal{F}(G)$ l'espace des fonctions à valeurs complexes sur G. Nous allons introduire certains éléments de $\mathcal{F}(G)$, appelés coefficients matriciels des représentations.

Soit (π, V) une représentation du groupe G. On appelle **coefficient matriciel** de π une fonction de G, à valeurs complexes, de la forme

$$\phi^\pi_{v,\lambda} : g \mapsto \lambda(\pi(g) \cdot v),$$

où $\lambda \in V^*$ et $v \in V$. La terminologie vient du temps (révolu) où les mathématiciens aimaient choisir des bases de leur espaces vectoriels, et exprimer les applications linéaires sous forme de matrices. Si l'on fait ceci pour l'espace V, et que l'on exprime $\pi(g)$ comme une matrice $\pi(g)_{ij}$, $g \mapsto \pi(g)_{ij}$ est un coefficient matriciel.

Introduisons la notation suivante. Pour toute fonction ϕ sur G, notons $\check{\phi} : g \mapsto \phi(g^{-1})$.

Lemme II.3.2 **(Relations d'orthogonalité de Schur)**

(i) Soit (π, V) une représentation irréductible de G. Alors pour tous $v_1, v_2 \in V$, pour tous $\lambda_1, \lambda_2 \in V^*$, on a :

$$\int_G \phi^{\pi}_{v_1,\lambda_1}(g)\ \check{\phi}^{\pi}_{v_2,\lambda_2}(g)\ d\mu_G(g) = \frac{\lambda_1(v_2)\lambda_2(v_1)}{d_\pi}.$$

où $d_\pi = \dim V$.

(ii) Soient (π_1, V_1), (π_2, V_2) deux représentations irréductibles de G non équivalentes. Alors pour tous $v_1 \in V_1$, $v_2 \in V_2$, $\lambda_1 \in V_1^*$, $\lambda_2 \in V_2^*$,

$$\int_G \phi^{\pi_1}_{v_1,\lambda_1}(g)\ \check{\phi}^{\pi_2}_{v_2,\lambda_2}(g)\ d\mu_G(g) = 0.$$

Démonstration. Soient $\lambda_1 \in V_1^*$, $v_2 \in V_2$. Considérons l'application linéaire linéaire $A : V_1 \to V_2$ définie par :

$$A(v) = \lambda_1(v)v_2.$$

Soient maintenant aussi $\lambda_2 \in V_2^*$ et $v_1 \in V_1$. Alors, avec les notations de la proposition II.3.1,

$$\begin{aligned}
\lambda_2(A^\circ \cdot v_1) &= \lambda_2\left(\int_G \pi_2(g)A\pi_1(g)^{-1} \cdot v_1\ d\mu_G(g)\right) \\
&= \lambda_2\left(\int_G \pi_2(g) \cdot (\lambda_1(\pi_1(g)^{-1} \cdot v_1)v_2)\ d\mu_G(g)\right) \\
&= \lambda_2\left(\int_G \lambda_1(\pi_1(g)^{-1} \cdot v_1)\ \pi_2(g) \cdot v_2\ d\mu_G(g)\right) \\
&= \int_G \lambda_1(\pi_1(g)^{-1} \cdot v_1)\ \lambda_2(\pi_2(g) \cdot v_2)\ d\mu_G(g)
\end{aligned}$$

On effectue le changement de variable $g \mapsto g^{-1}$ dans l'intégrale (qui n'est qu'une somme...) pour retrouver le membre de gauche des égalités dans

(i) et (ii). On conclut alors grâce à la proposition II.3.1 et au fait que $\operatorname{Tr} A = \lambda_1(v_2)$ lorsque $\rho_1 = \rho_2$. □

Corollaire II.3.3. — *Soient (π_i, V_i), $i = 1, \ldots, r$, des représentations irréductibles de G, non équivalentes deux à deux. Pour chaque i, choisissons $v_i \in V_i$ et $\lambda_i \in V_i^*$ non nuls. Alors les coefficients matriciels $\phi^{\pi_i}_{v_i,\lambda_i}$ sont linéairement indépendants dans $\mathcal{F}(G)$.*

Démonstration. Supposons que $\sum_i c_i \phi^{\pi_i}_{v_i,\lambda_i} = 0$. Fixons j entre 1 et r, et choisissons $\lambda'_j \in V_j^*$ tel que $\lambda'_j(v_j) = 1$ et $v'_j \in V_j$ tel que $\lambda_j(v'_j) = 1$. Alors d'après le lemme, on a

$$\begin{aligned} 0 &= \int_G \left(\sum_i c_i \phi^{\pi_i}_{v_i,\lambda_i} \right) \check{\phi}^{\pi_j}_{v'_j,\lambda'_j} \, d\mu_G = c_j \int_G \phi^{\pi_j}_{v_j,\lambda_j} \check{\phi}^{\pi_j}_{v'_j,\lambda'_j} \, d\mu_G \\ &= c_j \, d_{\pi_j}^{-1}. \end{aligned}$$

Donc $c_j = 0$. □

Corollaire II.3.4. — *Le nombre de classes d'équivalences de représentations irréductibles d'un groupe fini G est fini.*

Démonstration. Les coefficients matriciels sont des éléments de l'espace $\mathcal{F}(G)$, qui est de dimension finie. L'assertion découle alors directement du corollaire précédent. □

II.4. L'algèbre de convolution $\mathcal{F}(G)$

Dans cette section, le groupe G est fini. L'algèbre de fonctions $\mathcal{F}(G)$ est muni d'un autre produit que celui de la multiplication usuelle des fonctions. Il s'agit du produit de convolution. Avant de le définir, faisons quelques remarques.

— Pour tout élément g de G, notons δ_g la fonction sur G valant $|G|$ en g et 0 en $h \neq g$. Il est clair que $(\delta_g)_{g \in G}$ est une base de $\mathcal{F}(G)$.

— Le groupe G agissant sur lui-même par translation à gauche, il agit sur $\mathcal{F}(G)$. Notons cette action L. Explicitement, quels que soient $g \in G$, $f \in \mathcal{F}(G)$, $x \in G$:

$$(L(g) \cdot f)(x) = f(g^{-1}x).$$

De même, le groupe G agit sur lui-même par translation à droite, et l'on en déduit une action, notée R, sur $\mathcal{F}(G)$:

$$(R(g) \cdot f)(x) = f(xg).$$

Ces deux actions commutent. Il s'ensuit que $\mathcal{F}(G)$ est muni d'une action de $G \times G$, la première copie de G agissant par L et la seconde par R. L'espace $\mathcal{F}(G)$ est donc un espace de représentation du groupe $G \times G$, la représentation étant appelée **représentation régulière** du groupe G. On la note $L \times R$. Explicitement, quels que soient $g_1, g_2 \in G$, $f \in \mathcal{F}(G)$, $x \in G$:

$$((L \times R)(g_1, g_2) \cdot f)(x) = f(g_1^{-1} x g_2).$$

— Comme G est fini, toutes les fonctions sur G sont de carré intégrable (pour la mesure de comptage normalisée μ_G), et l'on peut introduire sur $\mathcal{F}(G) = L^2(G, \mu_G)$ le produit hermitien habituel : pour toutes fonctions f_1 et f_2 sur G,

$$(f_1, f_2) = \int_G \overline{f_1(g)} f_2(g)\, d\mu_G = \frac{1}{|G|} \sum_{g \in G} \overline{f_1(g)} f_2(g). \tag{II.4.1}$$

Définition II.4.1. — Soient f_1 et f_2 deux fonctions dans $\mathcal{F}(G)$. Leur produit de convolution $f_1 * f_2$ est défini par

$$f_1 * f_2(g) = \int_G f_1(t) f_2(t^{-1}g)\, d\mu_G(t).$$

Donnons les propriétés usuelles de la convolution :

Proposition II.4.2. — *(i) Le produit de convolution sur $\mathcal{F}(G)$ est associatif, d'élément neutre δ_e.*

(ii) Quels que soient g, h dans G, $\delta_h * \delta_g = \delta_{hg}$.

(iii) Quels que soient $g_1, g_2 \in G$, $f \in \mathcal{F}(G)$,

$$((L \times R)(g_1, g_2) \cdot f) = \delta_{g_1} * f * \delta_{g_2^{-1}}.$$

<u>*Démonstration*</u>. Tout ceci se vérifie par des calculs ne présentant pas de difficultés. $\square$

Rappelons qu'une algèbre A sur un corps k est un k-espace vectoriel (donc muni d'une addition) muni d'un produit qui en fait aussi un anneau, les deux structures possédant les propriétés de compatibilité suivantes :

$$(\lambda a)b = a(\lambda b) = \lambda(ab), \quad (a, b \in A),\ (\lambda \in k)$$

L'espace vectoriel $\mathcal{F}(G)$, dont une base est donnée par les $(\delta_g)_{g \in G}$ est muni d'un produit (le produit de convolution) qui étend (par linéarité) le produit de G, et fait de $\mathcal{F}(G)$ une algèbre sur $\mathbb{C}$. Elle admet pour élément neutre δ_e, où e est l'élément neutre de G.

Dans la base $(\delta_g)_{g \in G}$ le produit de convolution est donné par la formule suivante

$$\left(\sum_{g \in G} \alpha_g \, \delta_g\right) * \left(\sum_{h \in G} \beta_h \, \delta_h\right) = \sum_{(g,h) \in G \times G} \alpha_g \beta_h \, \delta_{gh}.$$

Remarque II.4.3. — On peut définir de façon formelle *l'algèbre du groupe G* sur $\mathbb{C}$ comme étant un espace vectoriel sur $\mathbb{C}$ de base $(e_g)_{g \in G}$, et munie du produit

$$\left(\sum_{g \in G} \alpha_g \, e_g\right) * \left(\sum_{h \in G} \beta_h \, e_h\right) = \sum_{(g,h) \in G \times G} \alpha_g \beta_h \, e_{gh}.$$

Il est alors clair que l'application $\delta_g \mapsto e_g$ s'étend en un isomorphisme d'algèbres entre $\mathcal{F}(G)$ et $\mathbb{C}[G]$. Dans tout ce qui précède, et tout ce qui suit, nous aurions donc pu employer $\mathbb{C}[G]$ à la place de $\mathcal{F}(G)$.

Soit (π, V) une représentation de G. Nous allons étendre l'action de G sur V en une action de $\mathcal{F}(G)$ sur V, c'est-à-dire que nous allons définir un morphisme d'algèbres, encore noté π,

$$\pi : \mathcal{F}(G) \to \mathrm{End}(V)$$

grâce à la formule :

$$\text{(II.4.2)} \qquad \pi(f) \cdot v = \int_G f(g)\,\pi(g) \cdot v \; d\mu_G(g), \quad (v \in V),\ (f \in \mathcal{F}(G)).$$

Il est clair que $\pi(f)$ est linéaire. Il est aussi clair que π est linéaire.

Remarquons que $\mathrm{End}(V)$ est naturellement muni d'une action de $G \times G$, notée $\mathrm{End}\,\pi$ par

$$\text{(II.4.3)} \qquad ((\mathrm{End}\,\pi)(g_1, g_2) \cdot A)(v) = \pi(g_1) \cdot (A(\pi(g_2)^{-1} \cdot v)),$$

$(g_1, g_2 \in G),\ (v \in V),\ A \in \mathrm{End}(V)$.

Proposition II.4.4. — *L'application π est un morphisme d'algèbres de $\mathcal{F}(G)$ dans* $\mathrm{End}(V)$ *vérifiant*

$$\pi(\delta_g) = \pi(g)$$

pour tout $g \in G$. Le morphisme π entrelace la représentation régulière $L \times R$ de $G \times G$ sur $\mathcal{F}(G)$ et la représentation $\mathrm{End}\,\pi$ *(II.4.3) dans* $\mathrm{End}(V)$.

Démonstration. Il s'agit de montrer que si f_1, f_2 sont dans $\mathcal{F}(G)$,

$$\pi(f_1 * f_2) = \pi(f_1)\pi(f_2).$$

Dans le membre de droite, le produit est la composition des opérateurs dans $\mathrm{End}(V)$. Calculons

$$\begin{aligned}
\pi(f_1 * f_2) &= \int_G (f_1 * f_2)(g)\pi(g)\; d\mu_G(g) \\
&= \int_G \left(\int_G f_1(t) f_2(t^{-1}g)\; d\mu_G(t) \right) \pi(g)\; d\mu_G(g) \\
&= \int_G \int_G f_1(t) f_2(g) \pi(tg)\; d\mu_G(g)\; d\mu_G(t) \\
&= \int_G \left(\int_G f_1(t)\pi(t) d\mu_G(t) \right) f_2(g)\pi(g)\; d\mu_G(g) \\
&= \pi(f_1)\pi(f_2)
\end{aligned}$$

L'égalité $\pi(\delta_g) = \pi(g)$ est immédiate.

Montrons que π est un opérateur d'entrelacement. Soient $x, y \in G$, $f \in \mathcal{F}(G)$. Calculons :

$$\begin{aligned}
\pi((L \times R)(x,y) \cdot f) &= \int_G ((L \times R)(x,y) \cdot f)(g)\pi(g)\, d\mu_G(g) \\
&= \int_G f(x^{-1}gy)\pi(g)\, d\mu_G(g) \\
&= \int_G f(g)\pi(xgy^{-1})\, d\mu_G(g) \\
&= \pi(x)\left(\int_G f(g)\pi(g)\, d\mu_G(g)\right)\pi(y^{-1}) \\
&= \pi(x)\pi(f)\pi(y^{-1})
\end{aligned}$$

□

II.5. Transformée de Fourier

Notons $\widehat{G}$ l'ensemble des classes d'équivalences de représentations irréductibles du groupe G. Pour chaque $\delta \in \widehat{G}$, choisissons un représentant (π_δ, V_δ). Notons δ^* la classe d'équivalence de la représentation contragrédiente $(\tilde{\pi}_\delta, V_\delta^*)$ et d_δ la dimension de V_δ. On a bien sûr $d_{\delta^*} = d_\delta$. Soit $f \in \mathcal{F}(G)$. Sa **transformée de Fourier** est un élément du produit $\prod_{\delta \in \widehat{G}} \mathrm{End}(V_\delta)$ défini par :

$$\mathcal{F}f(\delta) = \pi_\delta(f) = \int_G f(g)\, \pi_\delta(g)\, d\mu_G(g).$$

Lemme II.5.1. — *La transformée de Fourier vérifie les propriétés suivantes : (i) quels que soient f_1, f_2 dans $\mathcal{F}(G)$,*

$$\mathcal{F}(f_1 * f_2) = \mathcal{F}(f_1)\mathcal{F}(f_2).$$

(ii) $\mathcal{F}$ est un $G \times G$-morphisme de $\mathcal{F}(G)$ dans $\prod_{\delta \in \widehat{G}} \mathrm{End}(V_\delta)$

Démonstration. Ceci découle directement de la proposition II.4.4. □

Définissons maintenant la **transformée de Fourier inverse**. Soit

$$(F(\delta))_{\delta \in \widehat{G}} \in \prod_{\delta \in \widehat{G}} \mathrm{End}(V_\delta).$$

Posons, pour tout $g \in G$,

$$\bar{\mathcal{F}}F(g) = \sum_{\delta \in \widehat{G}} d_\delta \operatorname{Tr}(\pi_\delta(g)\, {}^t F(\delta^*)) = \sum_{\delta \in \widehat{G}} d_\delta \operatorname{Tr}(\pi_{\delta^*}(g)\, {}^t F(\delta)).$$

On obtient une fonction sur G.

Théorème II.5.2. — *Les applications $\mathcal{F}$ et $\bar{\mathcal{F}}$ sont des isomorphismes d'algèbres, inverses l'un de l'autre, entre $\mathcal{F}(G)$ et $\prod_{\delta \in \hat{G}} \operatorname{End}(V_\delta)$. Ce sont aussi des opérateurs d'entrelacement entre la représentation régulière $L \times R$ de $G \times G$ sur $\mathcal{F}(G)$ et la représentation sur $\prod_{\delta \in \hat{G}} \operatorname{End}(V_\delta)$.*

Démonstration. La démonstration se fait en plusieurs étapes, en commençant par le résultat suivant :

Lemme II.5.3. — *Pour tout élément $(F(\delta))_{\delta \in \widehat{G}}$ dans $\prod_{\delta \in \widehat{G}} \operatorname{End}(V_\delta)$, on a*

$$\mathcal{F}\bar{\mathcal{F}}F = F.$$

Démonstration. Rappelons que si V est un espace vectoriel de dimension finie, la forme bilinéaire symétrique

$$(A, B) \mapsto \operatorname{Tr}(AB)$$

sur $\operatorname{End}(V)$ est non dégénérée. On a donc $\mathcal{F}\bar{\mathcal{F}}F = F$ si et seulement si pour tout $\delta \in \widehat{G}$ et pour tout $A \in \operatorname{End}(V_\delta)$, $\operatorname{Tr}((\mathcal{F}\bar{\mathcal{F}}F)(\delta)A) = \operatorname{Tr}(F(\delta)A))$.

$$\begin{aligned}
\operatorname{Tr}((\mathcal{F}\bar{\mathcal{F}}F)(\delta)A) &= \operatorname{Tr}\left(\left(\int_G (\bar{\mathcal{F}}F)(g)\, \pi_\delta(g)\, d\mu_G(g)\right) A\right) \\
&= \operatorname{Tr}\left(\left(\int_G \sum_{\nu \in \widehat{G}} d_\nu \operatorname{Tr}(\pi_{\nu^*}(g)\, {}^t F(\nu))\pi_\delta(g)\, d\mu_G(g)\right) A\right) \\
&= \sum_{\nu \in \widehat{G}} d_\nu \int_G \operatorname{Tr}(\pi_{\nu^*}(g)^t F(\nu)) \operatorname{Tr}(\pi_\delta(g)A)\, d\mu_G(g)
\end{aligned}$$

Or, si l'on fixe une base $(v_i)_i$ de V_ν de base duale $(v_i^*)_i$, on a

$$\mathrm{Tr}\,(\pi_{\nu^*}(g)^t F(\nu)) = \sum_i v_i(\pi_{\nu^*}(g)^t F(\nu) \cdot v_i^*)$$
$$= \sum_i (\pi_\nu(g)^{-1} \cdot v_i)({}^t F(\nu) \cdot v_i^*) = \sum_i (\pi_\nu(g)^{-1} \cdot v_i)(w_i^*)$$
$$= \sum_i w_i^*(\pi_\nu(g)^{-1} \cdot v_i) = \sum_i \check{\phi}^\nu_{v_i, w_i^*}(g),$$

où l'on a posé $w_i^* = {}^t F(\nu) \cdot v_i^*$.

De même, en fixant une base $(e_j)_j$ de V_δ de base duale $(e_j^*)_j$

$$\mathrm{Tr}\,(\pi_\delta(g)A)) = \sum_j e_j^*(\pi_\delta(g)A \cdot e_j) = \sum_j e_j^*(\pi_\delta(g) \cdot f_j) = \sum_j \phi^\delta_{f_j, e_j^*}(g)$$

où l'on a posé $f_j = A \cdot e_j$

En reportant dans le calcul précédent, ceci donne

$$\mathrm{Tr}\,((\mathcal{F}\bar{\mathcal{F}}F)(\delta)A) = \sum_{i,j} \sum_{\nu \in \hat{G}} d_\nu \int_G \phi^\delta_{f_j, e_j^*}(g)\, \check{\phi}^\nu_{v_i, w_i^*}(g)\, d\mu_G(g).$$

Les formules d'orthogonalité de Schur nous disent que les termes de cette somme sont nuls sauf si $\nu = \delta$, donc

$$\mathrm{Tr}\,((\mathcal{F}\bar{\mathcal{F}}F)(\delta)A) = \sum_{i,j} w_i^*(f_j)\, v_i^*(e_j)$$
$$= \sum_i ({}^t F(\delta) \cdot v_i^*)(A \cdot v_i) = \sum_i v_i^*(F(\delta)A \cdot v_i) = \mathrm{Tr}\,(F(\delta)A)$$

Ceci termine la démonstration du lemme. □

Lemme II.5.4. — *La transformation de Fourier $\mathcal{F}$ est injective.*

Démonstration. Soit $f \in \mathcal{F}(G)$ telle que $\mathcal{F}f = 0$, c'est-à-dire que pour tout $\delta \in \widehat{G}$, $\pi_\delta(f) = 0$. Considérons la représentation $(L, \mathcal{F}(G))$ de G : d'après le corollaire II.1.7, elle est complètement réductible. On peut donc écrire

$$(L, \mathcal{F}(G)) = \oplus_i(\rho_i, W_i),$$

où les (ρ_i, W_i) sont des représentations irréductibles de G. Par hypothèse, $\rho_i(f) = 0$ pour tout i, donc $L(f) = 0$. Or d'après la proposition II.4.2, on a

$$L(f) \cdot h = f * h \quad (h \in \mathcal{F}(G)).$$

Prenons $h = \delta_e$, l'élément neutre pour la convolution. On obtient

$$0 = L(f) \cdot \delta_e = f * \delta_e = f.$$

□

Remarques II.5.5. — Cette démonstration montre que la représentation régulière gauche est fidèle, c'est-à-dire que le morphisme

$$L : \ G \to \mathbf{GL}(\mathcal{F}(G))$$

est injectif.

— On voit aussi que les représentations irréductibles de G "séparent les points", c'est-à-dire que pour tout $g \in G$, $g \neq e$, il existe une représentation irréductible (π, V) de G telle que $\pi(g) \neq \mathrm{Id}_V$.

Le fin de la démonstration du théorème se déduit aisément de ces lemmes. □

***Corollaire II.5.6* (Formule de Burnside)**. — *On a*

$$\sum_{\delta \in \widehat{G}} \dim(V_\delta)^2 = \dim \mathcal{F}(G) = |G|.$$

Corollaire II.5.7. — *Soit $f \in \mathcal{F}(G)$. La formule d'inversion de Fourier $f = \bar{\mathcal{F}}\mathcal{F}f$ s'écrit explicitement*

$$f(g) = \sum_{\delta \in \widehat{G}} d_\delta \ \mathrm{Tr}\,(\pi_\delta(f)\pi_\delta(g)^{-1}) = \sum_{\delta \in \widehat{G}} d_\delta \ \mathrm{Tr}\,(\mathcal{F}f(\delta)\,\pi_\delta(g)^{-1}).$$

Pour $g = e$, on obtient

$$f(e) = \sum_{\delta \in \widehat{G}} d_\delta \,\mathrm{Tr}\,(\mathcal{F}f(\delta)).$$

Démonstration. Il s'agit juste d'un calcul, où nous allons, dans l'ordre, utiliser le fait que $\operatorname{Tr} X = \operatorname{Tr} {}^t X$ pour tout opérateur X, effectuer un changement de variable $\delta \mapsto \delta^*$, et enfin utiliser le fait que par définition de la représentation contragrédiente,

$$ {}^t(\pi_{\delta^*}(g)) = \pi_\delta(g)^{-1}. $$

$$\begin{aligned} f(g) = (\bar{\mathcal{F}}\mathcal{F}f)(g) &= \sum_{\delta \in \widehat{G}} d_\delta \operatorname{Tr}\left(\pi_\delta(g)\ {}^t(\mathcal{F}f(\delta^*))\right) \\ &= \sum_{\delta \in \widehat{G}} d_\delta \operatorname{Tr}\left(\mathcal{F}f(\delta^*)\ {}^t(\pi_\delta(g))\right) \\ &= \sum_{\delta \in \widehat{G}} d_\delta \operatorname{Tr}\left(\mathcal{F}f(\delta)\ {}^t(\pi_{\delta^*}(g))\right) \\ &= \sum_{\delta \in \widehat{G}} d_\delta \operatorname{Tr}\left(\mathcal{F}f(\delta)\ \pi_\delta(g)^{-1}\right) \\ &= \sum_{\delta \in \widehat{G}} d_\delta \operatorname{Tr}\left(\pi_\delta(f)\pi_\delta(g)^{-1}\right). \end{aligned}$$

□

***Corollaire II.5.8* (Formule de Plancherel).** — *Soient $f_1, f_2 \in \mathcal{F}(G)$. Alors*

$$\int_G f_1(g) f_2(g^{-1})\, d\mu_G(g) = \sum_{\delta \in \widehat{G}} d_\delta \operatorname{Tr}\left(\mathcal{F}f_1(\delta)\mathcal{F}f_2(\delta)\right)$$

Démonstration. Posons $f = f_1 * f_2$. On a $\mathcal{F}(f) = (\mathcal{F}f_1)(\mathcal{F}f_2)$ et $f(e) = \int_G f_1(g) f_2(g^{-1})\, d\mu_G(g)$. On utilise alors le corollaire précédent. □

Remarque II.5.9. — Interprétons le corollaire précédent, en remplaçant f_1 par $\bar{f_1}$ et f_2 par $\check{f_2}$ dans la formule. Le terme de gauche est alors le produit hermitien de f_1 et f_2 dans $\mathcal{F}(G)$ (*cf.* (II.4.1)). D'autre part, chaque $\operatorname{End}(V_\delta)$ est muni d'un produit hermitien

$$(X, Y)_\delta = d_\delta \operatorname{Tr}({}^t\bar{X} Y)$$

qui en fait un espace de Hilbert. L'espace $\prod_{\delta \in \widehat{G}} \operatorname{End}(V_\delta)$ est alors muni du produit hermitien $(\,.\,,\,.\,) = \sum_\delta (\,.\,,\,.\,)_\delta$. La formule de Plancherel s'interprète alors comme le fait que $\mathcal{F}$ soit une isométrie de $\mathcal{F}(G)$ dans $\prod_{\delta\in\widehat{G}}\mathrm{End}(V_\delta)$, c'est-à-dire que

$$(f_1, f_2) = (\mathcal{F}f_1, \mathcal{F}f_2).$$

Pour $\delta \in \widehat{G}$ fixé, l'espace $\mathrm{End}(V_\delta)$ se plonge canoniquement dans $\prod_{\nu\in\widehat{G}}\mathrm{End}(V_\nu)$. Nous identifions $\mathrm{End}(V_\delta)$ et son image dans $\prod_{\nu\in\widehat{G}}\mathrm{End}(V_\nu)$. Le théorème de Peter-Weyl pour les groupes finis identifie le sous-espace de $\mathcal{F}(G)$ qui lui correspond par transformée de Fourier.

***Théorème II.5.10* (Peter-Weyl).** — *Soit $\delta \in \widehat{G}$. Notons $\mathcal{F}(G)(\delta)$ le sous-espace de $\mathcal{F}(G)$ engendré par les coefficients matriciels $\check{\phi}^{\pi_\delta}_{v,\lambda}$, $v \in V_\delta$, $\lambda \in V_\delta^*$. Alors $\mathcal{F}$ réalise un isomorphisme entre $\mathcal{F}(G)(\delta)$ et* $\mathrm{End}(V_\delta)$. *Chaque sous-espace $\mathcal{F}(G)(\delta)$ est stable pour la représentation régulière de $G\times G$ sur $\mathcal{F}(G)$. Ceci fournit une décomposition*

$$\mathcal{F}(G) = \bigoplus_{\delta\in\widehat{G}} \mathcal{F}(G)(\delta)$$

de la représentation régulière $\mathcal{F}(G)$ en somme de sous-représentations.

<u>*Démonstration*</u>. Soient $v \in V_\delta$, $\lambda \in V_\delta^*$. Définissons $A \in \mathrm{End}(V_\delta)$ par

$$w \mapsto A(w) = \lambda(w)v.$$

L'endomorphisme A est de rang 1, et tous les endomorphismes de rang 1 sont obtenus ainsi. Soit $F \in \prod_{\nu\in\widehat{G}}\mathrm{End}(V_\nu)$ défini par

$$F(\nu) = 0 \text{ si } \nu \neq \delta, \quad F(\delta) = A.$$

On a alors

$$\begin{aligned}\bar{\mathcal{F}}F(g) &= \sum_{\nu\in\widehat{G}} d_\nu \mathrm{Tr}\left(\pi_{\nu^*}(g)\,{}^tF(\nu)\right)\\ &= d_\delta \mathrm{Tr}\left(\pi_{\delta^*}(g)\,{}^tA\right) = d_\delta \mathrm{Tr}\left(A\pi_\delta(g)^{-1}\right)\end{aligned}$$

On a utilisé le fait que $\mathrm{Tr}\,X = \mathrm{Tr}\,{}^tX$ et ${}^t(\pi_{\delta^*}(g)) = \pi_\delta(g)^{-1}$. Calculons maintenant

$$(A\pi_\delta(g)^{-1})(w) = \lambda(\pi_\delta(g)^{-1}\cdot w)v = (\pi_{\delta^*}(g)\cdot\lambda)(w)v.$$

La trace de cet endomorphisme est

$$(\pi_{\delta^*}(g)\cdot\lambda)(v) = \lambda(\pi_\delta(g)^{-1}\cdot v) = \phi^{\pi_\delta}_{v,\lambda}(g^{-1}) = \check{\phi}^{\pi_\delta}_{v,\lambda}(g).$$

Comme $\mathrm{End}(V_\delta)$ est engendré par les endomorphismes de rang un, on voit que l'image de $\mathrm{End}(V_\delta)$ par $\bar{\mathcal{F}}$ est $\mathcal{F}(G)(\delta)$. On a donc $\dim \mathcal{F}(G)(\delta) = d_\delta^2$. Les $\mathcal{F}(G)(\delta)$ sont en somme directe d'après les relations d'orthogonalité de Schur, et la formule de Burnside permet de conclure que

$$\mathcal{F}(G) = \bigoplus_{\delta\in\widehat{G}} \mathcal{F}(G)(\delta).$$

□

II.6. L'algèbre des fonctions centrales

Soit $\mathcal{F}(G)^G$ le centre de l'algèbre $\mathcal{F}(G)$, c'est-à-dire que $f \in \mathcal{F}(G)^G$ si et seulement si

$$(\forall k \in \mathcal{F}(G)), \quad f * k = k * f.$$

On appelle **fonctions centrales** les fonctions dans $\mathcal{F}(G)^G$. Le résultat qui suit donne une autre caractérisation des fonctions centrales.

Lemme II.6.1. — *Une fonction $f \in \mathcal{F}(G)$ est dans $\mathcal{F}(G)^G$ si et seulement si elle est constante sur les classes de conjugaison de G.*

Démonstration. Comme les δ_g, $g \in G$ forment une base de $\mathcal{F}(G)$, pour que f soit centrale, il faut et il suffit que f commute à tous les δ_g. Cette condition s'écrit

$$\delta_g * f = f * \delta_g,$$

ce qui peut se réécrire en utilisant la proposition II.4.2 (*iii*)

$$L(g)\cdot f = R(g^{-1})\cdot f$$

où encore

$$f(gx) = f(xg), \quad (x, g \in G)$$

□

Soit $\mathbf{Conj}(G)$ l'ensemble des classes de conjugaison de G. Pour toute classe de conjugaison C de G, notons $\mathbf{1}_C$ la fonction caractéristique de

C, c'est-à-dire $\mathbf{1}_C(g) = 1$ si $g \in C$ et 0 sinon. Il est clair grâce au lemme que les $\mathbf{1}_C$, $C \in \mathbf{Conj}(G)$ forment une base de $\mathcal{F}(G)^G$. En particulier, la dimension de $\mathcal{F}(G)^G$ est égale au nombre de classes de conjugaison dans G.

Un autre exemple fondamental de fonctions centrales est donné par les **caractères** des représentations de G. Soit (π, V) une représentation de dimension finie de G. Son caractère Θ_π est la fonction sur G définie par

$$\Theta_\pi(x) = \mathrm{Tr}\,(\pi(x)).$$

Comme

$$\mathrm{Tr}\,(\pi(xy)) = \mathrm{Tr}\,(\pi(x)\pi(y)) = \mathrm{Tr}\,(\pi(y)\pi(x)) = \mathrm{Tr}\,(\pi(yx)),$$

on voit que $\Theta_\pi(yxy^{-1}) = \Theta_\pi(x)$, et donc Θ_π est bien une fonction centrale.

Lemme II.6.2. — *Soient (π, V) une représentation de dimension finie de G et $x \in G$. On a alors*

$$\Theta_\pi(x^{-1}) = \overline{\Theta_\pi(x)} = \Theta_{\pi^*}(x), \quad \Theta_\pi(e) = \dim V.$$

Démonstration. $\Theta_\pi(x) = \mathrm{Tr}\,\pi(x)$ est la somme des valeurs propres, comptées avec leur multiplicité, de l'opérateur $\pi(x) \in \mathbf{GL}(V)$. Comme le groupe G est fini, il existe $n \in \mathbb{N}$ tel que $x^n = e$, et donc $\pi(x)^n = \mathrm{Id}_V$. Les valeurs propres de $\pi(x)$ sont donc des racines n-ième de l'unité, et donc leur inverse est égal à leur conjugué. D'autre part, λ est valeur propre de $\pi(x)$ si et seulement si λ^{-1} est valeur propre de $\pi(x)^{-1}$ avec même multiplicité (resp. λ^{-1} est valeur propre de $\tilde{\pi}(x)$ avec même multiplicité). Comme $\pi(e) = \mathrm{Id}_V$, $\Theta_\pi(e) = \dim V$. □

Une autre propriété importante des caractères est la manière dont ils se comportent par somme et produit :

Proposition II.6.3. — *Soient (π_1, V_1) et (π_2, V_2) deux représentations de dimension finie du groupe fini G. Alors, pour tout $x \in G$,*

$$\Theta_{\pi_1 \oplus \pi_2}(x) = \Theta_{\pi_1}(x) + \Theta_{\pi_2}(x), \quad \Theta_{\pi_1 \otimes \pi_2}(x) = \Theta_{\pi_1}(x)\Theta_{\pi_2}(x).$$

Démonstration. On exprime la trace en choisissant une base $(e_i)_i$ de V_1, de base duale $(e_i^*)_i$ et une base $(f_j)_j$ de V_2, de base duale $(f_j^*)_j$:

$$\operatorname{Tr}\pi_1(x) = \sum_i e_i^*(\pi(x)\cdot e_i), \quad \operatorname{Tr}\pi_2(x) = \sum_j f_j^*(\pi_2(x)\cdot f_j)$$

Une base de $V_1 \oplus V_2$ est obtenue en prenant la réunion des bases $(e_i)_i$ et $(f_j)_j$, la base duale étant la réunion des $(e_i^*)_i$ et des $(f_j^*)_j$, ce qui montre la première formule. Une base du produit tensoriel $V_1 \otimes V_2$ est $(e_i \otimes f_j)_{i,j}$, de base duale $(e_i^* \otimes f_j^*)_{i,j}$, donc

$$\begin{aligned}\Theta_{\pi_1\otimes\pi_2}(x) &= \sum_{i,j}(e_i^*\otimes f_j^*)((\pi_1\otimes\pi_2)(x)\cdot(e_i\otimes f_j))\\ &= \sum_{i,j}(e_i^*\otimes f_j^*)((\pi_1(x)\cdot e_i\otimes\pi_2(x)\cdot f_j)\\ &= \sum_i e_i^*(\pi(x)\cdot e_i)\sum_j f_j^*(\pi_2(x)\cdot f_j).\end{aligned}$$

□

Pour tout $\delta \in \widehat{G}$, choisissons une représentation irréductible (π_δ, V_δ) dans la classe δ. On note alors simplement Θ_δ le caractère de π_δ (il ne dépend pas du choix du représentant (π_δ, V_δ) car la trace est invariante par changement de base).

Nous pouvons aussi exploiter l'isomorphisme d'algèbres entre $\mathcal{F}(G)$ et $\prod_{\delta\in G}\operatorname{End}(V_\delta)$ pour étudier le centre $\mathcal{F}(G)^G$. En effet, le centre d'un produit d'algèbres est le produit des centres, et le centre de chaque $\operatorname{End}(V_\delta)$ consiste en l'ensemble des opérateurs scalaires de V_δ. Chaque facteur contribue donc d'un espace de dimension 1, ce qui montre que le centre est de dimension $|\widehat{G}|$. On en conclut, ce qui mérite d'être noté, que

$$|\widehat{G}| = |\mathbf{Conj}(G)|. \tag{II.6.1}$$

D'autre part, une fonction f est centrale si et seulement si sa transformée de Fourier est centrale dans $\prod_{\delta\in G}\operatorname{End}(V_\delta)$, c'est-à-dire si pour tout $\delta \in \widehat{G}$, il existe un scalaire c_δ tel que

$$\mathcal{F}f(\delta) = c_\delta\,\operatorname{Id}_{V_\delta}.$$

Notons E_ν l'élément de $\prod_{\delta\in G}\mathrm{End}(V_\delta)$ défini par $E_\nu(\delta)=0$ si $\delta\neq\nu$, $E_\nu(\nu)=\mathrm{Id}_{V_\nu}$. Les E_ν, $\nu\in\hat{G}$, forment une base du centre de l'algèbre $\prod_{\delta\in G}\mathrm{End}(V_\delta)$. Leurs transformées de Fourier inverses vont donc former une base de $\mathcal{F}(G)^G$. Posons

$$e_\nu=\bar{\mathcal{F}}E_\nu.$$

On calcule

$$\begin{aligned} e_\nu(g)=\bar{\mathcal{F}}E_\nu(g) &= \sum_{\delta\in\widehat{G}} d_\delta\,\mathrm{Tr}\,(\pi_\delta(g)\,{}^tE_\nu(\delta^*)) \\ &= d_\nu\,\mathrm{Tr}\,(\pi_{\nu^*}(g))=d_\nu\,\Theta_{\nu^*}(g). \end{aligned} \tag{II.6.2}$$

En prenant la transformée de Fourier de cette égalité, on obtient

$$\mathcal{F}\Theta_\nu=\frac{1}{d_\nu}E_{\nu^*}. \tag{II.6.3}$$

Remarque II.6.4. — Il est immédiat que les E_ν vérifient les relations suivantes

$$E_\delta E_\nu=0 \text{ si } \delta\neq\nu,\quad E_\delta^2=E_\delta,\quad \sum_{\delta\in\widehat{G}}E_\delta=\mathrm{Id}_{\prod_{\delta\in\widehat{G}}V_\delta}.$$

On en déduit que

$$e_\delta*e_\nu=0 \text{ si } \delta\neq\nu,\quad e_\delta*e_\delta=e_\delta,\quad \sum_{\delta\in\widehat{G}}e_\delta=\delta_e.$$

On dit que les e_δ forment un **système d'idempotents centraux** de l'algèbre $\mathcal{F}(G)$.

Rappelons que le produit hermitien sur $\mathcal{F}(G)$ est défini par

$$(f_1,f_2)=\int_G\overline{f_1(g)}f_2(g)\,d\mu_G(g)$$

Théorème II.6.5. — *(Orthogonalité des caractères) Soient δ,ν dans $\widehat{G}$. Si $\delta\neq\nu$,*

$$(\Theta_\delta,\Theta_\nu)=0$$

et $(\Theta_\delta,\Theta_\delta)=1$.

<u>*Démonstration*</u>. Par définition

$$\begin{aligned}(\Theta_\delta, \Theta_\nu) &= \int_G \overline{\Theta_\delta(g)}\Theta_\nu(g)\, d\mu_G(g)\\ &= \int_G \Theta_\delta(g^{-1})\Theta_\nu(g)\, d\mu_G(g)\end{aligned}$$

On utilise alors la formule de Plancherel (cor. II.5.8), puis le calcul des transformées de Fourier des caractères (II.6.3), et l'on obtient :

$$\begin{aligned}(\Theta_\delta, \Theta_\nu) &= \sum_{\mu\in\widehat{G}} d_\mu \operatorname{Tr}\left((\mathcal{F}\Theta_\delta)(\mu)(\mathcal{F}\Theta_\nu)(\mu)\right)\\ &= \sum_{\mu\in\widehat{G}} d_\mu \frac{1}{d_\delta}\frac{1}{d_\nu} \operatorname{Tr}\left(E_{\delta^*}(\mu)E_{\nu^*}(\mu)\right)\end{aligned}$$

Ceci est nul si $\delta \neq \nu$. Si $\delta = \nu$, on obtient

$$(\Theta_\delta, \Theta_\delta) = d_\delta \frac{1}{d_\delta^2} \operatorname{Tr}\left(E_{\delta^*}(\delta^*)E_{\delta^*}(\delta^*)\right) = \frac{1}{d_\delta} \operatorname{Tr}\left(\mathrm{Id}_{V_{\delta^*}}\right) = 1.$$

□

Corollaire II.6.6. — *La famille* $(\Theta_\delta)_{\delta\in\widehat{G}}$ *est une base orthonormale de* $\mathcal{F}(G)^G$.

<u>*Démonstration*</u>. On vient de démontrer que cette famille est orthonormale. Comme elle a le bon cardinal, c'est-à-dire $|\widehat{G}| = |\mathbf{Conj}(G)| = \dim \mathcal{F}(G)^G$, c'est une base. □

Toute fonction f de $\mathcal{F}(G)^G$ se décompose dans cette base :

$$f = \sum_{\delta\in\widehat{G}} (\Theta_\delta, f)\, \Theta_\delta.$$

Posons

$$\hat{f}(\delta) = (\Theta_\delta, f) = \int_G \overline{\Theta_\delta(g)} f(g)\, d\mu_G(g) = \int_G \Theta_{\delta^*}(g) f(g)\, d\mu_G(g).$$

On obtient la formule d'inversion de Fourier et la formule de Plancherel pour les fonctions centrales :

Théorème II.6.7. — *Pour toute fonction f dans $\mathcal{F}(G)^G$,*

$$f = \sum_{\delta \in \widehat{G}} \hat{f}(\delta)\Theta_\delta.$$

et pour toutes fonctions f_1, f_2 dans $\mathcal{F}(G)^G$

$$(f_1, f_2) = \sum_{\delta \in \widehat{G}} \overline{\hat{f}_1(\delta)}\hat{f}_2(\delta).$$

On a aussi les relations d'orthogonalité duales :

Théorème II.6.8. — *Soient C_1 et C_2 des classes de conjugaison de G. Alors si $C_1 \neq C_2$,*

$$\sum_{\delta \in \widehat{G}} \overline{\Theta_\delta(C_1)}\Theta_\delta(C_2) = 0$$

et si $C_1 = C_2$,

$$\sum_{\delta \in \widehat{G}} \overline{\Theta_\delta(C_1)}\Theta_\delta(C_1) = \frac{|G|}{|C_1|}$$

<u>*Démonstration*</u>. Calculons la transformée de Fourier de la fonction caractéristique de la classe de conjugaison C_1.

$$\begin{aligned}\widehat{\mathbf{1}_{C_1}}(\delta) &= \int_G \Theta_{\delta^*}(g)\mathbf{1}_{C_1}(g)\, d\mu_G \\ &= \frac{|C_1|}{|G|}\Theta_{\delta^*}(C_1).\end{aligned}$$

Idem pour C_2. On utilise maintenant le théorème précédent :

$$\begin{aligned}(\mathbf{1}_{C_1}, \mathbf{1}_{C_2}) &= \sum_{\delta \in \widehat{G}} \overline{\widehat{\mathbf{1}_{C_1}}(\delta^*)}\widehat{\mathbf{1}_{C_1}}(\delta) \\ &= \sum_{\delta \in \widehat{G}} \frac{|C_1|}{|G|}\Theta_\delta(C_1)\frac{|C_2|}{|G|}\Theta_{\delta^*}(C_2)\end{aligned}$$

Or $(\mathbf{1}_{C_1}, \mathbf{1}_{C_2}) = 0$ si $C_1 \neq C_2$ et $(\mathbf{1}_{C_1}, \mathbf{1}_{C_1}) = \frac{|C_1|}{|G|}$. On en déduit la formule du théorème. □

II.7. Application à la décomposition des représentations

Nous allons utiliser les résultats obtenus dans la section précédente pour l'étude des représentations de dimension finie d'un groupe fini G. Soit (ρ, V) une représentation de G de dimension finie. D'après le corollaire II.1.7, elle est complètement réductible, et peut donc s'écrire :

$$(\rho, V) = \bigoplus_{i=1}^{r} (\tau_i, W_i)$$

où les (τ_i, W_i) sont des représentations irréductibles. Il est important de remarquer que cette décomposition n'est pas unique en général. Dans cette section, nous allons étudier ce problème, en montrant que certains aspects d'une telle décomposition sont eux uniquement déterminés.

Commençons par le cas le plus simple. Soit (π, V) une représentation de dimension finie du groupe fini G. Notons V^G l'ensemble des vecteurs invariants sous l'action de G, c'est-à-dire

$$V^G = \{v \in V \mid (\forall v \in V),\ \pi(g) \cdot v = v\}.$$

Il est clair que V^G est une somme directe de représentations triviales de dimension 1 de G. D'autre part, on peut expliciter un opérateur de projection G-équivariant, $p \in \mathrm{Hom}_G(V, V^G)$ par :

$$p(v) = \int_G \pi(g) \cdot v \, d\mu_G(g). \tag{II.7.1}$$

Passons maintenant au cas général. Pour tout $\delta \in \widehat{G}$, notons $m_\delta(\rho)$ le nombre de (τ_i, W_i) apparaissant dans la décomposition ci-dessus qui sont dans la classe δ. On appelle $m_\delta(\rho)$ la multiplicité de δ dans ρ. On peut, par abus de notations[(1)], réécrire la décomposition de (ρ, V) sous la forme :

$$(\rho, V) = \bigoplus_{\delta \in \widehat{G}} m_\delta(\rho)(\pi_\delta, V_\delta),$$

ou plus simplement encore

$$\rho = \bigoplus_{\delta \in \widehat{G}} m_\delta(\rho)\delta.$$

[(1)] Comme souvent, l'abus consiste à confondre équivalence et égalité.

Théorème II.7.1. — *Soit (ρ, V) une représentation de dimension finie de G. Pour tout $\delta \in \widehat{G}$, soit $m_\delta(\rho)$ la multiplicité de δ dans ρ. Alors*

$$m_\delta(\rho) = (\Theta_\rho, \Theta_\delta)$$

et

$$(\Theta_\rho, \Theta_\rho) = \sum_{\delta \in \widehat{G}} m_\delta^2.$$

En particulier, ρ est irréductible si et seulement si $(\Theta_\rho, \Theta_\rho) = 1$.

Démonstration. Comme $\rho = \bigoplus_{\delta \in \widehat{G}} m_\delta(\rho)\delta$, on a :

$$\Theta_\rho = \sum_{\delta \in \widehat{G}} m_\delta(\rho)\Theta_\delta,$$

d'où, pour tout $\nu \in \widehat{G}$, d'après le théorème d'orthogonalité des caractères,

$$(\Theta_\rho, \Theta_\nu) = (\sum_{\delta \in \widehat{G}} m_\delta(\rho)\Theta_\delta, \Theta_\nu) = \sum_{\delta \in \widehat{G}} m_\delta(\rho)(\Theta_\delta, \Theta_\nu) = m_\nu(\rho).$$

La formule

$$(\Theta_\rho, \Theta_\rho) = \sum_{\delta \in \widehat{G}} m_\delta^2.$$

est elle aussi conséquence directe de l'orthogonalité des caractères, et la caractérisation des représentations irréductibles s'en déduit immédiatement. □

Corollaire II.7.2. — *Les multiplicités $m_\delta(\rho)$ ne dépendent pas de la décomposition de (ρ, V) donnée au départ.*

— Deux représentations (π_i, V_i), $i = 1, 2$ de G sont isomorphes si et seulement si leurs caractères sont égaux.

La décomposition de (ρ, V) en représentations irréductibles n'est pas unique, comme nous l'avons remarqué. On peut trouver une décomposition de (ρ, V) en somme directe moins fine qu'une décomposition en irréductibles, mais qui a l'avantage d'être canonique.

Théorème II.7.3. — *Soit $(\rho, V) = \bigoplus_{i=1}^r (\tau_i, W_i)$ une décomposition de (ρ, V) en irréductibles. Pour tout $\delta \in \widehat{G}$, notons $V(\delta)$ la somme directe de tous les (τ_i, W_i) appartenant à la classe δ. Alors $V(\delta)$ ne dépend pas de la* *décomposition de départ. On appelle $V(\delta)$* **la composante δ-isotypique** *de (ρ, V). On obtient donc la décomposition canonique :*

$$(\rho, V) = \bigoplus_{\delta \in \widehat{G}} V(\delta).$$

L'opérateur

$$P_\delta = \int_G d_\delta \, \Theta_{\delta^*}(g) \, \rho(g) \, d\mu_G(g) = \rho(e_\delta)$$

est la projection sur la composante δ-isotypique de ρ. C'est un opérateur G-équivariant (i.e. $P_\delta \in \mathrm{Hom}_G(V, V(\delta))$).

Démonstration. Il suffit de démontrer que P_δ est bien l'opérateur de projection voulu, car il ne dépend pas de la décomposition en irréductibles de départ. On a

$$P_\delta = \int_G d_\delta \Theta_{\delta^*}(g) \, \rho(g) \, d\mu_G(g) = d_\delta \rho(\Theta_{\delta^*}(g)) = \rho(e_\delta).$$

Or e_δ est un idempotent, donc P_δ vérifie aussi $P_\delta^2 = P_\delta$, et c'est donc une projection sur un sous-espace de V. Considérons la restriction de $\rho(e_\delta)$ au sous-espace W_i de V. Elle est égale à $\tau_i(e_\delta)$. Soit ν la classe de τ_i. Alors

$$\tau_i(e_\delta) = \pi_\nu(e_\delta) = \begin{cases} 0 \text{ si } \nu \neq \delta \\ \mathrm{Id}_{W_i} \text{ si } \nu = \delta \end{cases} .$$

Ceci vient du fait que $\mathcal{F}(e_\delta) = E_\delta$, et montre que P_δ est bien la projection sur la composante δ-isotypique. Comme $\delta_e = \sum_{\nu \in \widehat{G}} e_\nu$, on a :

$$\rho(\delta_e) = \mathrm{Id}_V = \sum_{\nu \in \widehat{G}} \rho(e_\nu) = \sum_{\nu \in \widehat{G}} P_\nu$$

L'espace V se décompose donc en somme directe de ses composantes isotypiques. $\square$

Exemple II.7.4. — Considérons la représentation $(L, \mathcal{F}(G))$ de G. La décomposition

$$\mathcal{F}(G) = \bigoplus_{\delta \in \widehat{G}} \mathcal{F}(G)(\delta)$$

du théorème de Peter-Weyl est la décomposition en composantes isotypiques (les notations sont donc cohérentes). Cette décomposition est aussi la décomposition en composantes isotypiques pour les représentations $(R, \mathcal{F}(G))$ de G et $(L \times R, \mathcal{F}(G))$ de $G \times G$.

II.8. Exercices

Exercice II.8.1. — Soit G un groupe fini abélien. Montrer que toutes les représentations irréductibles de G sont de dimension 1. Montrer que $\widehat{G}$ est muni d'une structure de groupe. Montrer que G est canoniquement isomorphe (comme groupe) à $\widehat{\widehat{G}}$.

Déterminer toutes les représentations irréductibles du groupe cyclique $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Déterminer $\widehat{\mathbb{Z}_n}$.

Exercice II.8.2. — Calculer le caractère de la représentation régulière $(L, \mathcal{F}(G))$ d'un groupe fini G.

Exercice II.8.3. — **Le groupe $\mathfrak{S}_3$.**

— 1. On note c la permutation circulaire (123) et t la transposition (23). Montrer que c et t engendrent $\mathfrak{S}_3$, et que $tc = c^2t$, $ct = tc^2$. Déterminer les classes de conjugaison de $\mathfrak{S}_3$.

— 2. Trouver les représentations de dimension 1 de $\mathfrak{S}_3$.

— 3. Soit (e_1, e_2, e_3) la base canonique de $\mathbb{C}^3$. Pour tout $g \in \mathfrak{S}_3$, posons $\rho(g) \cdot e_i = e_{g(i)}$. Montrer que ceci définit une représentation de $\mathfrak{S}_3$ dans $\mathbb{C}^3$. Montrer que

$$V = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \,|\, z_1 + z_2 + z_3 = 0\}$$

est invariant.

— 4. Montrer qu'il existe une base (u_1, u_2) de V telle que

$$\rho(t) \cdot u_1 = u_2,\ \rho(t) \cdot u_2 = u_1,\ \rho(c) \cdot u_1 = j^2 u_1,\ \rho(c) \cdot u_2 = j u_2,$$

où $j = e^{\frac{2i\pi}{3}}$. La représentation $\rho_{|V}$ est-elle irréductible ?

— 5. Etablir la table des caractères de $\mathfrak{S}_3$.

— 6. Quelle est l'interprétation géométrique de ρ comme groupe de symétries ? Quelle est l'interprétation géométrique de $\rho_{|V}$?

Exercice II.8.4. — **La représentation standard de $\mathfrak{S}_n$** La représentation (ρ, V) de l'exercice précédent admet un analogue pour tout n. En effet, soit $\mathcal{B}_n = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$, sur laquelle $\mathfrak{S}_n$ agit naturellement par permutation des indices. On en déduit une représentation ρ de $\mathfrak{S}_n$ dans $\mathbb{C}^n$.

— 1. Montrer que le caractère de ρ est donnée par :

$$\Theta_\rho(\tau) = \text{nombre de points fixes de } \tau, \qquad (\tau \in \mathfrak{S}_n)$$

— 2. Montrer que $\mathbb{C}^n$ est somme directe de deux sous-espaces stables U et V sous l'action de $\mathfrak{S}_n$, où

$$U = \{ze_1 + ze_2 + \ldots + ze_n,\ (z \in \mathbb{C})\}$$
$$V = \{z_1e_1 + z_2e_2 + \ldots + z_ne_n \mid \sum_i z_i = 0\}$$

Constater que (ρ_U, U) est la représentation triviale de $\mathfrak{S}_n$. En déduire le caractère de (ρ_V, V).

— 3. Nous allons maintenant montrer que (ρ_V, V) est irréductible. En fait, la restriction de (ρ_V, V) à $\mathfrak{A}_n$ est déjà irréductible pour $n \geq 4$. On rappelle que pour $n \geq 4$, l'action de $\mathfrak{A}_n$ sur $\{1, \ldots, n\}$ (ou sur $\mathcal{B}_n$) est doublement transitive (voir exercice I.4.2), c'est-à-dire $\mathcal{B}_n \times \mathcal{B}_n$ admet deux orbites sous $\mathfrak{A}_n$: la diagonale Δ et son complémentaire. Déterminons $\mathrm{Hom}_{\mathfrak{A}_n}(\rho, \rho)$. Soit T un opérateur d'entrelacement dans cet espace. Posons

$$T(e_i) = \sum_j K(e_i, e_j)\ e_j.$$

Montrer que la propriété d'entrelacement équivaut à

$$K(e_{\tau(i)}, e_{\tau(j)}) = K(e_i, e_j), \qquad (\tau \in \mathfrak{S}_n).$$

En déduire que

$$\dim \mathrm{Hom}_{\mathfrak{A}_n}(\rho, \rho) = 2.$$

Conclure.

— 4. Expliciter les opérateurs de projection sur U et V.

Exercice II.8.5. — **Le groupe $\mathfrak{S}_4$.** Déterminer les classes de conjugaison de $\mathfrak{S}_4$ et sa table de caractères. Déterminer la table de caractères du groupe alterné $\mathfrak{A}_4$. Quelles représentations irréductibles de $\mathfrak{A}_4$ sont les restrictions de représentations irréductibles de $\mathfrak{S}_4$? Quelles représentations irréductibles de $\mathfrak{S}_4$ ont une restriction réductible à $\mathfrak{A}_4$?

Exercice II.8.6. — **Produits tensoriels.**

— 1. Soit E un espace vectoriel de dimension finie de base $(e_1, \dots, e_n)$. On note $\bigwedge^2 E$ (resp. $S^2(E)$ le sous-espace de $E \otimes E$ engendré par les vecteurs de la forme $e_i \otimes e_j - e_j \otimes e_i$ (resp. $e_i \otimes e_j + e_j \otimes e_i$). Montrer que ceci ne dépend pas de la base choisie. Montrer que si (ρ, E) est une représentation du groupe fini G,

$$E \otimes E = \bigwedge^2 E \oplus S^2(E),$$

comme représentation de G. On note $\bigwedge^2 \rho$ et $S^2\rho$ ces deux représentations de G. Calculer le caractère de $\bigwedge^2 \rho$ et de $S^2\rho$ en fonction de celui de ρ. Si ρ est la représentation irréductible de dimension 2 de $\mathfrak{S}_3$, déterminer ces deux caractères. Décomposer $\rho \otimes \rho$ en somme directe de représentations irréductibles.

— 2. Soit V un espace vectoriel de dimension finie. Montrer que

$$\mathrm{End}(V) \simeq V \otimes V^*.$$

Si (ρ, V) est une représentation du groupe G, alors $G \times G$ agit sur $V \otimes V^*$ par $\rho \otimes \tilde{\rho}$. Quelle est la représentation dans $\mathrm{End}(V)$ obtenue par transport de structure ?

Exercice II.8.7. — Soit n un entier ≥ 2. On pose $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

— 1. Soit $\chi_1(k) = e^{\frac{2ik\pi}{n}}$, $k \in \mathbb{Z}_n$. Montrer que les caractères irréductibles de $\mathbb{Z}_n$ sont les fonctions $k \mapsto \chi_q(k) = e^{\frac{2ik\pi q}{n}}$, pour $q = 0, 1, \dots, n-1$, autrement dit, que l'on a une identification $\hat{\mathbb{Z}}_n \simeq \mathbb{Z}_n$.

— 2. Pour toute $f \in \mathbb{C}[\mathbb{Z}_n]$, on pose

$$\hat{f}(q) = \frac{1}{n} \sum_{k=0}^{n-1} f(k) \chi_{-q}(k).$$

Montrer que

$$f(k) = \sum_{q=0}^{n-1} \hat{f}(q)\chi_q(k).$$

et que

$$\frac{1}{n}\sum_{k=0}^{n-1} |f(k)|^2 = \sum_{q=0}^{n-1} |\hat{f}(q)|^2.$$

Exercice II.8.8. — **Sommes de Gauss**

Soit ψ un caractère de $\mathbb{Z}_N^\times$. On le prolonge en une fonction sur $\mathbb{Z}_N$ en posant $\psi(k) = 0$ lorsque $(k, N) \neq 1$. Si N_1 divise N, un caractère de $\mathbb{Z}_{N_1}$ donne par composition avec la surjection canonique $\mathbb{Z}_N^\times \to \mathbb{Z}_{N_1}^\times$ un caractère de $\mathbb{Z}_N^\times$. Lorsque ψ n'est pas obtenu de la sorte, on dit que ψ est un caractère primitif (modulo N).

Le but de l'exercice est le calcul de la (valeur absolue de la) somme de Gauss

$$\tau(\psi) = \sum_{q \bmod N} \psi(q) e^{\frac{2i\pi q}{N}}$$

lorsque ψ est un caractère primitif (modulo N).

— 1. Exprimer $\tau(\psi)$ en fonction de $\hat{\psi}(-1)$.

— 2. Montrer que $\hat{\psi}(-q) = \overline{\psi(q)}\tau(\psi)$.

— 3. En déduire grâce à la formule de Plancherel que $|\tau(\psi)|^2 = N$.

Exercice II.8.9. — Soit $\mathbb{F}_q$ le corps fini à q éléments, $q = p^e$, p premier. Il contient le corps fini $\mathbb{F}_p = \mathbb{Z}_p$. Nous avons vu que les caractères irréductibles de $\mathbb{Z}_p$ sont les fonctions $k \mapsto \chi_q(k)$, pour $q = 0, 1, \ldots, p-1$, et l'on a une identification $\hat{\mathbb{Z}}_p \simeq \mathbb{Z}_p$.

Pour tout $a \in \mathbb{F}_q$, soit $l_a : \mathbb{F}_q \to \mathbb{F}_q$, $l_a(x) = ax$ la multiplication par l'élément a dans $\mathbb{F}_q$. Montrer que la trace de l'endomorphisme l_a est dans $\mathbb{F}_p$. Posons

$$\Psi_1(a) = \chi_1(\mathrm{Tr}\,(l_a)).$$

On dit que le caractère χ de F_q est non trivial s'il existe $x \in \mathbb{F}_q$ tel que $\chi(x) \neq 1$. Soit u un élément non nul de $\mathbb{F}_q$ et définissons

$$\eta_u(x) = \Psi_1(ux), \quad (x \in \mathbb{F}_q).$$

— 1. Montrer que $\eta_u(x)$ est un caractère non trivial de $\mathbb{F}_q$.

— 2. Montrer que si η est un caractère de $\mathbb{F}_q$, alors il existe un unique $u \in \mathbb{F}_q$ tel que $\eta = \eta_u$.

— 3. Exprimer les formules d'inversion de Fourier et de Plancherel pour le groupe $(\mathbb{F}_q, +)$.

Exercice II.8.10. — **Caractères et caractères...**

Une représentation de dimension 1 est souvent appelée un caractère. Cette terminologie entre en conflit avec celle de caractère d'une représentation (qui est une fonction à valeurs complexe sur le groupe). En quel sens une représentation de dimension 1 s'identifie-t-elle à son caractère ?

Soit A une algèbre sur $\mathbb{C}$. Un caractère de l'algèbre A est un morphisme d'algèbres

$$\chi \ : A \to \mathbb{C}.$$

Soit G un groupe fini. Montrer que si $\delta \in \widehat{G}$,

$$\chi_\delta : \ f \mapsto d_\delta^{-1} \hat{f}(\delta)$$

définit un caractère de l'algèbre $\mathcal{F}(G)^G$. Réciproquement, montrer que tout caractère de $\mathcal{F}(G)^G$ provient, à un scalaire près, d'une représentation irréductible de G.

Exercice II.8.11. — **Une application du lemme de Schur** Soit (π, V) une représentation irréductible d'un groupe fini G. Montrer que si $\langle .\,, . \rangle_1$ et $\langle .\,, . \rangle_2$ sont deux produits hermitiens invariants sur E, ils sont égaux à une constante multiplicative près.

Exercice II.8.12. — **Décomposition canonique d'une représentation.**

Soit (ρ, V) une représentation de dimension finie du groupe fini G. Pour tout élément $\delta \in \widehat{G}$, posons

$$H_\delta = \mathrm{Hom}_G(\pi_\delta, \rho).$$

Montrer que le morphisme

$$\Phi_\delta : H_\delta \otimes V_\delta \to V, \quad \phi \otimes v \mapsto \phi(v)$$

réalise un isomorphisme G équivariant entre $H_\delta \otimes V_\delta$ et la composante δ-isotypique de V (l'action de G sur $H_\delta \otimes V_\delta$ est le produit tensoriel de l'action triviale de G sur H_δ et de l'action π_δ sur V_δ). En déduire que la multiplicité de δ dans ρ est égale à la dimension de H_δ.

Exercice II.8.13. — Soient (ρ, V) et (τ, E) deux représentations de dimension finie d'un groupe fini G. Exprimer $\dim \mathrm{Hom}_G(V, E)$ en fonction des multiplicités $m_\delta(\rho)$ et $m_\tau(\rho)$, $\delta \in \widehat{G}$.

Exercice II.8.14. — Soit (ρ, V) une représentation de dimension finie du groupe fini G, que l'on suppose fidèle, c'est-à-dire $\rho(g) \neq \mathrm{Id}_V$ si $g \neq e$.

— 1. Montrer que $\Theta_V(g) \neq \dim V$ si $g \neq e$.

— 2. Soit W une représentation irréductible de G. Montrer que la série formelle

$$\sum_{n=0}^{\infty} \langle \Theta_W, \Theta_V^n \rangle X^n$$

est une fraction rationnelle que l'on explicitera, mais n'est pas un polynôme.

— 3. En déduire que W apparaît dans une infinité de $V^{\otimes n}$.

Exercice II.8.15. — **Le théorème du bicommutant et le théorème de Burnside.**

Soit (ρ, V) une représentation d'un groupe G dans un espace vectoriel V de dimension finie n. On ne suppose pas G fini, mais l'on suppose que

(ρ, V) est semi-simple. Si A est une sous-algèbre de $\mathrm{End}(V)$, notons A' son commutant, c'est-à-dire

$$A' = \{b \in \mathrm{End}(V) \mid \forall a \in A,\, ba = ab\},$$

et A'' son bicommutant, c'est-à-dire le commutant de A' (il est clair que A' est une sous-algèbre de $\mathrm{End}(V)$).

Le théorème du bicommutant affirme que si A est la sous-algèbre de $\mathrm{End}(V)$ engendrée par les opérateurs $\rho(g)$, $g \in G$, alors $A'' = A$.

— 1. Montrer que $A \subset A''$ et que $A' = \mathrm{End}_G(V) = \mathrm{Hom}_G(V, V)$.

— 2. Soit $v \in V$ et soit W le sous-espace de V engendré par les vecteurs de la forme $\rho(g) \cdot v$, $g \in G$ (de sorte que $W = A \cdot v$). Montrer qu'il existe un projecteur p de V sur W entrelaçant l'action de G (c'est-à-dire $p \in \mathrm{End}_G(V) = A'$). En déduire que si $u \in A''$, on a $u(W) \subset W$, puis qu'il existe $a \in A$ tel que $a(v) = u(v)$.

— 3. Soit $V^n = V \oplus \ldots \oplus V$ (n facteurs), muni de la représentation $\rho^n = \rho \oplus \ldots \oplus \rho$ de G. Cette représentation est semi-simple. Notons B la sous-algèbre de $\mathrm{End}(V^n)$ engendrée par les opérateurs $\rho^n(g)$, $g \in G$, B' son commutant et B'' son bicommutant. Choisissons une base $(e_1, \ldots, e_n)$ de V et identifions $B \subset \mathrm{End}(V^n)$ à des matrices diagonales par blocs, chaque bloc étant égal à un même endomorphisme dans A. A quoi s'identifie B' ? Soit $u \in A''$ et $t = u \oplus \ldots \oplus u$. Vérifier que $t \in B''$ et en déduire qu'il existe $b \in B$ tel que $b(e_1, \ldots e_n) = t(e_1, \ldots e_n)$. Conclure.

Passons maintenant au théorème de Burnside. Il affirme que si G est un groupe et (ρ, V) est une représentation irréductible de G dans un espace vectoriel de dimension finie, alors la sous-algèbre A de $\mathrm{End}(V)$ engendrée par les opérateurs $\rho(g)$, $g \in G$ est égale à $\mathrm{End}(V)$ toute entière.

— 4. Déduire le théorème de Burnside du théorème du bicommutant et du théorème de Schur.

Nous allons maintenant donner une application des résultats démontrés ci-dessus. Soient G et H deux groupes, et (ρ, V), (σ, W) des représentations irréductibles de G et H respectivement dans des espaces vectoriels de dimension finie. Alors

$$(\rho \boxtimes \sigma, V \otimes W)$$

est une représentation irréductible de $G \times H$ et toute représentation irréductible de $G \times H$ est de cette forme.

— 5. Montrons d'abord le sens direct. Quelle est la sous-algèbre de $\mathrm{End}(V \otimes W)$ engendrée par les opérateurs $\rho \boxtimes \sigma(g, h)$, $g \in G$, $h \in H$? En déduire que $V \otimes W$ est irréductible.

— 6. Soit (τ, U) une représentation irréductible de $G \times H$. Notons

$$\tau_1 : G \to \mathbf{GL}(U), \quad \tau_1(g) = \tau(g, e_H)$$
$$\tau_2 : H \to \mathbf{GL}(U), \quad \tau_2(h) = \tau(e_G, h).$$

Soit V un sous-espace de U invariant et irréductible pour la représentation τ_1 de G et posons $\rho = \tau_{1|V}$. Montrer que pour tout $h \in H$, $\tau_2(h)(V)$ est aussi invariant et irréductible pour la représentation τ_1 de G et que la restriction de τ_1 à $\tau_2(h)(V)$ est équivalente à (ρ, V). Montrer que si V' est un sous-espace de U invariant par τ_1 alors, pour tout $h \in H$, ou bien $\tau_2(h)(V) \cap V' = \{0\}$, ou bien $\tau_2(h)(V) \cap V' = \tau_2(h)(V)$.

— 7. Soient A l'algèbre engendrée par les opérateurs $\tau(g, h)$, $g \in G$, $h \in H$ et B l'algèbre engendrée par les opérateurs $\tau_2(h)$, $h \in H$, Montrer que

$$U = B(V).$$

En déduire qu'il existe $h_1, \dots h_d$ dans H tels que

$$U = \bigoplus_{j=1}^{d} \tau_2(h_j)(V),$$

puis qu'il existe un espace vectoriel W de dimension d et un isomorphisme de représentations $\phi\ :\ (\tau_1, U) \to (\rho \otimes \mathrm{Id}_W, V \otimes W)$.

— 8. Montrer que les opérateurs $\phi \circ \tau_2(h) \circ \phi^{-1}$, $h \in H$ commutent avec tous les opérateurs de la forme $T \otimes \mathrm{Id}_W$ dans $\mathrm{End}(V \otimes W)$.

— 9. Soit $S \in \mathrm{End}(V \otimes W)$ commutant à tous les opérateurs de la forme $T \otimes \mathrm{Id}_W$. Montrer qu'il existe $Y \in \mathrm{End}(W)$ tel que $S = \mathrm{Id}_V \otimes Y$.

— 10. Déduire de ce qui précède que $\tau_2 \simeq \mathrm{Id}_V \otimes \sigma$ pour une certaine représentation σ de H dans W. Montrer que σ est irréductible.

CHAPITRE III

REPRÉSENTATIONS INDUITES

III.1. Construction des représentations induites

Soient G un groupe et H un sous-groupe. Une représentation (π, V) de G donne par restriction, une représentation de H. Notons $r_H^G(\pi, V)$ cette représentation de H. Si ϕ est un opérateur d'entrelacement entre deux représentations (π_1, V_1) et (π_2, V_2) de G, il est trivial de constater que ϕ est encore un opérateur d'entrelacement entre $r_H^G(\pi_1, V_1)$ et $r_H^G(\pi_2, V_2)$. On le note $r_H^G(\phi)$ si on le considère ainsi.

Notre but est maintenant de décrire une opération naturelle permettant de passer d'une représentation de H à une représentation de G, et d'un opérateur d'entrelacement entre deux représentations de H, à un opérateur d'entrelacement entre les deux représentations de G obtenues.

Définition III.1.1. — Soient G un groupe et H un sous-groupe et (ρ, W) une représentation de H. Notons $I_H^G(W)$ l'espace des fonctions $f : G \to W$ vérifiant

$$f(hg) = \rho(h) \cdot f(g). \tag{III.1.1}$$

Le groupe G agit par translation à droite sur l'espace $I_H^G(W)$. Notons $I_H^G(\rho)$ cette action :

$$(I_H^G(\rho)(k) \cdot f)(g) = f(gk) \quad (k, g \in G).$$

On appelle $(I_H^G(\rho), I_H^G(W))$ la **représentation induite** de H à G de (ρ, W).

Soit ϕ un opérateur d'entrelacement entre les représentations (τ_1, W_1) et (τ_2, W_2) de H. L'opérateur

$$I_H^G(\phi) : \ I_H^G(W_1) \to I_H^G(W_2), \quad f \mapsto \phi \circ f$$

est un opérateur d'entrelacement entre $I_H^G(\rho_1, W_1)$ et $I_H^G(\rho_2, W_2)$.

Cette construction admet l'interprétation géométrique suivante. La donnée de G, H et (ρ, W) permet de construire un espace, noté $G \times_H W$: le produit cartésien $G \times W$ est muni d'une action de H,

$$h \cdot (g, w) = (hg, \rho(h) \cdot w), \quad (g \in G, \, w \in W, \, h \in H)$$

et $G \times_H W$ est l'ensemble des orbites. Comme $G \times W$ est aussi muni d'une action de G :

$$k \cdot (g, w) = (gk^{-1}, w), \quad (g, k \in G, \, v \in W)$$

qui commute avec celle de H, $G \times_H W$ hérite d'une action de G. De plus, on dispose d'une projection naturelle $p : \ G \times_H W \to H\backslash G$, dont la fibre au-dessus de chaque point est isomorphe à W : c'est clair au dessus du point $He \in H\backslash G$ et comme la projection p est un G-morphisme et que l'action de G sur $H\backslash G$ est transitive, le résultat s'en déduit par translation. L'espace $I_H^G(W)$ s'identifie alors aux sections de p, c'est-à-dire aux fonctions s de $H\backslash G$ dans $G \times_H W$ telles que $p \circ s = \mathrm{Id}_{H\backslash G}$ et l'action $I_H^G(\rho)$ est donnée par l'action par translation à droite sur l'espace de ces sections.

Lorsque G est fini, on voit que $I_H^G(W)$ contient de manière canonique un sous-espace isomorphe à W : c'est l'espace des sections s comme ci-dessus dont le support est le point He de $H\backslash G$. Par abus de notation, identifions W et cet espace. L'espace $I_H^G(\rho)(g)(W)$ est alors l'espace des sections de support Hg dans $H\backslash G$. L'espace $I_H^G(W)$ est la somme de tous ces espaces lorsque g décrit un système de représentants des classes à droite de H dans G :

$$\text{(III.1.2)} \qquad I_H^G(W) = \bigoplus_{\bar{g} \in H\backslash G} I_H^G(\rho)(g)(W)$$

Exemple III.1.2. — Prenons $H = \{e\}$, et induisons la représentation triviale de H. Il est clair que $I_H^G(1_H)$ est la représentation régulière droite de G.

III.2. Réciprocité de Frobénius

Les opérations de restriction et d'induction sont reliées par la formule suivante, dite **réciprocité de Frobénius** :

Théorème III.2.1. — *Soient G un groupe et H un sous-groupe, (π, V) une représentation de G et (ρ, W) une représentation de H. Alors il existe un isomorphisme naturel :*

$$\mathrm{Hom}_G(\pi, I_H^G(\rho)) \simeq \mathrm{Hom}_H(r_H^G(\pi), \rho).$$

Démonstration. Soit $\phi \in \mathrm{Hom}_G(\pi, I_H^G(\rho))$. Définissons

$$\psi_\phi \in \mathrm{Hom}_H(r_H^G(\pi), \rho)$$

de la manière suivante :

$$\psi_\phi(v) = \phi(v)(e), \quad (v \in V).$$

Vérifions que ψ_ϕ est bien un opérateur d'entrelacement : pour tout $h \in H$, pour tout $v \in V$,

$$\begin{aligned}
\psi_\phi(\pi(h) \cdot v) &= \phi(\pi(h) \cdot v)(e) \\
&= (I_H^G(\rho)(h) \cdot \phi(v))(e) \\
&= \phi(v)(eh) = \phi(v)(he) \\
&= \rho(h) \cdot (\phi(v)(e)) = \rho(h) \cdot \psi_\phi(v).
\end{aligned}$$

Il est clair que $\phi \mapsto \psi_\phi$ est linéaire. Soit $\psi \in \mathrm{Hom}_H(r_H^G(\pi), \rho)$. Définissons $\phi_\psi \in \mathrm{Hom}_G(\pi, I_H^G(\rho))$ par la formule

$$\phi_\psi(v)(g) = \psi(\pi(g) \cdot v),$$

pour tout $v \in V$, et tout $g \in G$. Vérifions simultanément que ϕ_ψ est un opérateur d'entrelacement et que $\phi_\psi(v) \in I_H^G(W)$ pour tout $v \in V$. On a, pour tout $g, k \in G$, $h \in H$,

$$\begin{aligned}\phi_\psi(v)(hgk) &= \psi(\pi(hgk) \cdot v) \\ &= \rho(h) \cdot \psi(\pi(g)\pi(k) \cdot v) \\ &= \rho(h) \cdot \phi_\psi(\pi(k) \cdot v)(g).\end{aligned}$$

Enfin, vérifions que $\phi_{\psi_\phi} = \phi$ et $\psi_{\phi_\psi} = \psi$:

$$\phi_{\psi_\phi}(v)(g) = \psi_\phi(\pi(g) \cdot v) = \phi(\pi(g) \cdot v)(e) = (I_H^G(\rho)(g) \cdot \phi(v))(e) = \phi(v)(g),$$
$$\psi_{\phi_\psi}(v) = \phi_\psi(v)(e) = \psi(\pi(e) \cdot v) = \psi(v).$$

Disons quelques mots de la “naturalité” de cet isomorphisme. On peut donner un sens précis, technique, à ce mot, mais cela nécessite d'introduire des concepts qui dépassent le cadre de ce cours (théorie des catégories). Disons simplement que les isomorphismes donnés par le théorème, lorsque (π, V) et (ρ, W) varient, se comportent convenablement par rapport aux opérateurs d'entrelacement. Plus précisément, supposons que (π_1, V_1), (π_2, V_2) soient deux représentations de G, que (ρ_1, W_1), (ρ_2, W_2) soient deux représentations de H, et que $\phi \in \mathrm{Hom}_G(\pi_2, \pi_1)$, $\psi \in \mathrm{Hom}_H(\rho_1, \rho_2)$ soient deux opérateurs d'entrelacement. On en déduit des morphismes :

$$\begin{aligned}\mathrm{Hom}_G(\pi_1, I_H^G(\rho_1)) &\to \mathrm{Hom}_G(\pi_2, I_H^G(\rho_2)), \\ f &\mapsto I_H^G(\psi) \circ f \circ \phi,\end{aligned}$$

$$\begin{aligned}\mathrm{Hom}_H(r_H^G(\pi_1), \rho_1) &\to \mathrm{Hom}_H(r_H^G(\pi_2), \rho_2), \\ f &\mapsto \psi \circ f \circ r_H^G(\phi).\end{aligned}$$

Le diagramme suivant, où les flèches horizontales sont les isomorphismes de réciprocité de Frobénius, et les flèches verticales les morphismes que nous venons de définir, est alors commutatif :

$$\begin{tikzcd}\mathrm{Hom}_G(\pi_1, I_H^G(\rho_1)) \arrow[r] \arrow[d] & \mathrm{Hom}_H(r_H^G(\pi_1), \rho_1) \arrow[d] \\ \mathrm{Hom}_G(\pi_2, I_H^G(\rho_2)) \arrow[r] & \mathrm{Hom}_H(r_H^G(\pi_2), \rho_2)\end{tikzcd}$$

□

Dans le même ordre d'idée, le résultat suivant affirme que l'induction est transitive "à isomorphisme près".

Proposition III.2.2. — *Soient H et K deux sous-groupes de G, $K \subset H$ et soit (ρ, W) une représentation de K. Alors*

$$I_H^G(I_K^H(\rho, W)) \simeq I_K^G(\rho, W)$$

Nous laissons au lecteur le soin de d'expliciter l'isomorphisme et de montrer qu'il est "naturel". Une manière plus conceptuelle de démontrer ce résultat est de constater que la restriction est trivialement transitive :

$$r_K^H \circ r_H^G = r_K^G.$$

Il s'agit ici d'une vrai égalité, et non simplement d'un isomorphisme, mais peu importe. Ensuite, il s'agit de voir que $I_H^G(\rho, W)$ est caractérisé à isomorphisme près par le théorème de réciprocité de Frobénius. Nous laissons encore une fois la vérification des détails au lecteur. □

III.3. Caractères des représentations induites

Nous supposons que les groupes sont finis. Soient G un groupe, H un sous-groupe de G, (π, V) une représentation de G et (ρ, W) une représentation de H. Le résultat suivant est un corollaire de la réciprocité de Frobénius :

Corollaire III.3.1. — *On a*

$$(\Theta_\pi, \Theta_{I_H^G(\rho)}) = (\Theta_{r_H^G(\pi)}, \Theta_\rho).$$

Par linéarité, il suffit de montrer ceci lorsque π et ρ sont irréductibles. On sait alors $(\Theta_\pi, \Theta_{I_H^G(\rho)})$ est la multiplicité de π dans $I_H^G(\rho)$, qui est aussi la dimension de $\mathrm{Hom}_G(\pi, I_H^G(\rho))$. De même $(\Theta_{r_H^G(\pi)}, \Theta_\rho)$ est la multiplicité de ρ dans $r_H^G(\pi)$, et est égal à la dimension de $\mathrm{Hom}_H(r_H^G(\pi), \rho)$. □

Nous voulons maintenant calculer le caractère de $I_H^G(\rho)$ en fonction de celui de ρ. Soit $g \in G$, nous voulons donc calculer la trace de l'opérateur $I_H^G(\rho)(g)$. Ceci est facile en utilisant (III.1.2) ; en effet g permute les classes dans $H \backslash G$, et les seules contributions à cette trace proviennent donc des classes $\bar{s} \in H\backslash G$ telles que $g \cdot \bar{s} = \overline{sg^{-1}} = \bar{s}$, c'est-à-dire $sg^{-1}s^{-1} \in H$, où encore $sgs^{-1} \in H$. On a alors

$$\Theta_{I_H^G(\rho)}(g) = \sum_{\bar{s} \in H\backslash G, sgs^{-1} \in H} \Theta_\rho(sgs^{-1}). \tag{III.3.1}$$

III.4. Exercices

Exercice III.4.1. — Soient G un groupe fini, H un sous-groupe de G et (ρ, W) une représentation de H. Soit C une classe de conjugaison dans G, et écrivons

$$C \cap H = \coprod_i D_i$$

où les D_i sont des classes de conjugaison dans H. Montrer que (III.3.1) peut se réécrire

$$\Theta_{I_H^G(\rho)}(C) = \frac{|G|}{|H|} \sum_i \frac{|D_i|}{|C|} \Theta_\rho(D_i).$$

Que cela donne-t-il lorsque ρ est la représentation triviale de H ?

Exercice III.4.2. — Considérons $\mathfrak{S}_2$ comme sous-groupe de $\mathfrak{S}_3$. Déterminer la décomposition en représentations irréductibles de $I_{\mathfrak{S}_2}^{\mathfrak{S}_3}(\mathrm{sgn})$.

Exercice III.4.3. — Considérons $\mathfrak{S}_3$ comme sous-groupe de $\mathfrak{S}_4$. Soit V la représentation standard de $\mathfrak{S}_3$ (c'est la représentation de dimension 2 introduite dans l'exercice II.8.3). Calculer la décomposition en représentations irréductibles de $I_{\mathfrak{S}_3}^{\mathfrak{S}_4}(V)$.

Exercice III.4.4. — Soient H et K deux sous-groupes de G, et (ρ, W) une représentation de H. Nous allons calculer

$$r_K^G(I_H^G(\rho, W)).$$

Rappelons que $I_H^G(W)$ est l'espace des fonctions $f : G \to W$ vérifiant

$$f(hg) = \rho(h) \cdot f(g)$$

Soit $g \in G$. Montrer que le sous-espace des fonctions $f \in I_H^G(\rho)$ à support dans la double classe HgK est stable sous l'action de K. Notons V_g cet espace. Fixons un système de représentants $\{g_i\}$ des doubles classes dans $H\backslash G/K$. En déduire que

$$I_H^G(W) = \bigoplus_i V_{g_i}$$

est une décomposition de $I_H^G(W)$ en somme directe de représentations de K.

— Si (τ, E) est une représentation d'un sous-groupe Γ de G, on note, pour tout $g \in G$, (τ^g, E) la représentation de $g\Gamma g^{-1}$ dans E donnée par

$$\tau^g(g\gamma g^{-1}) = \tau(\gamma).$$

Montrer que pour tout $g \in G$, $H(gK) \simeq (K \cap g^{-1}Hg)\backslash K$. (1)

En déduire que V_g est isomorphe en tant que représentation de K à :

$$I^K_{K\cap g^{-1}Hg}(r^H_{gKg^{-1}\cap H}(\rho)^{g^{-1}}),$$

Puis que

$$r_K^G(I_H^G(\rho, W)) = \bigoplus_i I^K_{K\cap g_i^{-1}Hg_i}(r^H_{g_iKg_i^{-1}\cap H}(\rho)^{g_i^{-1}}).$$

(1) $H(gK)$ est l'orbite sous l'action de H dans G/K du point gK

CHAPITRE IV

COMPLÉMENTS D'ALGÈBRE

On suppose connues les notions d'anneau, de module, d'idéal (à gauche, à droite, bilatère), d'algèbre sur un corps k. Les algèbres sont toujours supposées munies d'une unité, notée 1.

Une **algèbre à division** sur k est une k-algèbre avec unité dont tout élément non nul est inversible. Si elle est commutative, c'est un corps (et donc une extension de k).

IV.1. Forme trace et radical d'une algèbre

Nous avons vu dans le chapitre II que la donnée d'une représentation (π, V) d'un groupe fini G est équivalente à la donnée d'un morphisme d'algèbres

$$\mathcal{F}(G) \to \operatorname{End}(V), \quad f \mapsto \pi(f).$$

On appelle représentation d'une algèbre A (sur un corps k) dans un k-espace vectoriel V, la donnée d'un morphisme d'algèbres

$$\pi : A \to \operatorname{End}(V).$$

Se donner une représentation (π, V) de A est équivalent à se donner une structure de A-module sur V.

Nous allons retrouver les résultats du chapitre II d'une autre manière, en étudiant plus précisément la structure des algèbres de dimension finie et leurs représentations.

On travaille sur un corps k de caractéristique nulle quelconque. Le lecteur impressionné par tant de généralité pourra considérer que $k = \mathbb{C}$. Soit A une k-algèbre de dimension finie avec unité. Pour tout $a \in A$, notons

$$m_a : A \to A, \quad b \mapsto ab$$

l'endomorphisme de A donnée par la multiplication à gauche par a. Il est clair que $a \mapsto m_a$ définit un morphisme linéaire injectif de A dans $\mathrm{End}_k(A)$. On peut alors munir A d'une forme bilinéaire symétrique non dégénérée, la forme trace, définie par

$$(a, b) = \mathrm{Tr}\,(m_a m_b) = \mathrm{Tr}\,(m_{ab}).$$

Cette forme bilinéaire symétrique vérifie de manière évidente

$$(ax, b) = (a, xb), \quad (a, b, x \in A). \tag{IV.1.1}$$

Définition IV.1.1. — On dit que l'algèbre A est **semi-simple** lorsque la forme trace sur A est non dégénérée.

Exercice IV.1.2. — Soit $\mathcal{B} = (e_i)_{i=1,\dots,n}$ une base de A. Montrer que A est semi-simple si et seulement si le discriminant

$$\Delta_{\mathcal{B}}(A) = \det((e_i, e_j)_{i,j})$$

est non nul.

En général, le **radical** $J = J(A)$ de la forme trace, défini par

$$J(A) = \{x \in A \mid \forall y \in A,\ (x, y) = 0\}$$

est un idéal bilatère (grâce à l'équation (IV.1.1)). Si $a \in J(A)$, alors $\mathrm{Tr}\,(m_a^n) = 0$ pour tout $n \in \mathbb{N}^*$, ce qui implique par des arguments bien connus d'algèbre linéaire que m_a est un endomorphisme nilpotent. L'injectivité de $a \mapsto m_a$ nous dit alors que a lui-même est nilpotent dans A. Réciproquement, tout idéal à gauche I de A constitué d'éléments nilpotents est dans le radical $J(A)$, puisque pour tout $x \in A$, pour tout $a \in I$, comme $xa \in I$, xa est nilpotent, et donc aussi m_{xa}, ce qui montre que

$$(a, x) = (x, a) = \mathrm{Tr}\,(m_x m_a) = \mathrm{Tr}\,(m_{xa}) = 0.$$

On en déduit que $J(A)$ est le plus grand idéal à gauche constitué d'éléments nilpotents. On a ainsi $J(A/J(A)) = \{0\}$.

Soit M un A-module simple (c'est-à-dire que M est non nul et n'admet pas de sous-module propre), et soit m un élément non nul de M. Alors $M = A \cdot m$, et

$$A \to M, \quad a \mapsto a \cdot m$$

est un morphisme de A-modules surjectif, dont le noyau, noté I_m, est un idéal à gauche maximal de A. On a alors $J(A) \subset I_m$ car sinon, comme I_m est maximal, $I_m + J(A) = A$, ce qui fait que l'on peut écrire $1 = x + y$, $x \in I_m$, $y \in J(A)$. Alors $x = 1 - y$ est inversible puisque y est nilpotent (exercice), ce qui constitue une contradiction.

Résumons les résultats obtenus :

Théorème IV.1.3. — *Le radical $J(A)$ de la forme trace est le plus grand idéal à gauche constitué d'éléments nilpotents. Il annule tous les A-modules irréductibles. L'algèbre $A/J(A)$ est semi-simple.*

Rappelons qu'un anneau A est dit **simple** s'il n'admet aucun idéal bilatère propre. Il s'ensuit qu'une algèbre A simple est semi-simple, ce qui montre que la terminologie a été longuement pensée.

IV.2. Algèbres semi-simples

Supposons A semi-simple. Soit I un idéal bilatère non nul minimal dans A, et posons

$$I^{\perp} = \{x \in a | \forall a \in I,\ (a, x) = 0\}.$$

Alors (IV.1.1) implique que $I^{\perp}$ est aussi un idéal bilatère de A. Par minimalité de I, on a soit $I \subset I^{\perp}$, soit $I \cap I^{\perp} = \{0\}$. Dans le premier cas, on obtient $\operatorname{Tr} m_x^2 = 0$ pour tout $x \in I$, et ainsi $I \subset J(A)$, ce qui est en contradiction avec l'hypothèse que A est semi-simple. On a donc $I \cap I^{\perp} = \{0\}$. Par de l'algèbre bilinéaire élémentaire, on obtient

$$A = I \oplus I^{\perp}, \quad II^{\perp} = I^{\perp}I = \{0\}.$$

En écrivant

$$1 = e + e', \quad e \in I, e' \in I^{\perp}$$

on voit immédiatement que e et e' sont des idempotents centraux de A, qui agissent par multiplication respectivement sur I et $I^{\perp}$ comme l'identité. Ainsi $A = I \oplus I^{\perp}$ est une somme directe d'algèbres semi-simples. La minimalité de I entraîne que I est une algèbre simple. En effet, si $J \subset I$ est un idéal bilatère de I, on a $J = eJ = Je$, d'où

$$AJ = A(eJ) = (Ae)J = IJ = J, \quad JA = (Je)A = J(eA) = JI = J.$$

et donc J est un idéal bilatère de A contenu dans I, ce qui permet de conclure. Une récurrence montre alors que A est somme directe d'algèbres simples.

Un idempotent central e dans A est dit **décomposable** s'il existe deux idempotents centraux e_1 et e_2 tels que $e = e_1 + e_2$, $e_1e_2 = e_2e_1 = 0$ et **indécomposable** s'il n'est pas décomposable. D'après ce qui précède, on voit que si $\{e_1, \dots e_s\}$ est l'ensemble des idempotents centraux indécomposables de A, alors $\{Ae_1, \dots Ae_s\}$ est l'ensemble des idéaux bilatères minimaux de A, $1 = e_1 + \dots + e_s$ et $A = \bigoplus_{i=1,\dots,s} Ae_i$.

Posons, avec les notations ci-dessus, $I_i = Ae_i$. Soit M un A-module où 1 agit comme l'identité. Alors on a une décomposition de A-modules

$$M = \bigoplus_{i=1,\dots,s} e_i \cdot M. \tag{IV.2.1}$$

Si M est simple, ceci prouve que $M = e_i \cdot M$ pour un indice i et que $e_j \cdot M = \{0\}$ si $j \neq i$. En particulier, $M = e_i \cdot M$ est un I_i-module simple, et comme I_i est simple, l'annulateur dans I_i de M est nul, c'est-à-dire que

$$\{x \in I_i \,|\, x \cdot M = 0\} = \{0\}.$$

Soit J un idéal à gauche minimal de I_i. Alors $J \cdot M$ est un sous-module non nul de M. Soit $m \in M$ tel que $J \cdot m \neq \{0\}$. On a alors $J \cdot m = M$ et

$$x \mapsto x \cdot m$$

est un morphisme non nul de I_i-modules entre les modules simples J et M, et c'est donc un isomorphisme. En particulier, la structure de I_i-module de J ne dépend pas du choix de celui-ci, et I_i (donc toute algèbre simple) n'admet à isomorphisme près qu'un seul module simple. On a donc obtenu le

Théorème IV.2.1. — *Soit A une algèbre semi-simple et soit $\{e_1, \dots e_s\}$ l'ensemble des idempotents centraux indécomposables de A. Alors*

$$\{Ae_1, \dots Ae_s\}$$

est l'ensemble des idéaux bilatères minimaux de A, chaque $I_i = Ae_i$ est une algèbre simple d'élément unité e_i, et A est la somme directe d'algèbres

$$A = \bigoplus_{i=1,\dots,s} Ae_i.$$

D'autre part, si pour chaque i, on fixe un idéal à gauche minimal J_i de I_i, alors les J_i forment un système de représentants des classes d'isomorphismes de A-modules simples.

On peut en dire plus à propos des algèbres simples.

Théorème IV.2.2. — *Soient B une algèbre simple, I un idéal à gauche et $D = \mathrm{End}_B(I)$. Alors l'application naturelle*

$$B \to \mathrm{End}_D(I), \quad b \mapsto [m_b : x \mapsto bx] \tag{IV.2.2}$$

est un isomorphisme.

Précisons que $D = \mathrm{End}_B(I)$ est l'espace des endomorphismes de I commutant avec l'action de B et que $\mathrm{End}_D(I)$ est l'espace des endomorphismes de I commutant avec ceux de D.

Démonstration. Comme B est simple, $B = IB$. Il est clair que $m_b \in \mathrm{End}_D(I)$. Pour tout $x \in I$, notons $d_x : I \to I$ la multiplication à droite par x. Alors $d_x \in D = \mathrm{End}_B(I)$ car

$$(by)x = b(yx), \quad (b \in B), (x, y \in I).$$

Ainsi, pour tout $\phi \in \mathrm{End}_D(I)$, on a, pour tous $x, y \in I$, $\phi(yx) = \phi(y)x$, et donc, pour tout $b \in b$,

$$\phi(ybx) = \phi(y(bx)) = \phi(y)(bx).$$

On fixe alors b, y, ϕ comme ci-dessus et l'on obtient

$$\phi \circ m_{yb} = m_{\phi(y)b}.$$

Ceci montre que l'image de $B = IB$ par (IV.2.2) est un idéal à gauche de $\mathrm{End}_D(I)$, mais cette image contient l'identité, et c'est donc $\mathrm{End}_D(I)$ tout entier. Comme B est simple, le noyau de (IV.2.2) est trivial, ce qui finit la démonstration du théorème. □

Remarque IV.2.3. — Si I est un idéal à gauche minimal de B, alors D est une algèbre à division (c'est-à-dire que tout élément non nul est inversible). En effet, si $\phi \in D$ est non nul, $\ker\phi$ et $\mathrm{Im}\,\phi$ sont des idéaux à gauche de B, inclus dans I, et donc [1] $\ker\phi = 0$, $\mathrm{Im}\,\phi = I$.

Comme une algèbre de dimension finie admet des idéaux minimaux, on obtient :

Corollaire IV.2.4. — *Soient B une k-algèbre simple de dimension finie, I un idéal à gauche minimal de B et $D = \mathrm{End}_B(I)$. Alors D est une algèbre à division de dimension finie sur k, et B est isomorphe à l'algèbre des matrices $n \times n$ à coefficients dans D, où $n = \dim_D(I)$.*

Nous allons maintenant montrer le résultat suivant :

Théorème IV.2.5. — *Soient A une k-algèbre semi-simple de dimension finie. Alors tout A-module est complètement réductible (c'est-à-dire qu'il peut s'écrire comme somme directe de modules simples).*

Démonstration. D'après (IV.2.1), il suffit de démontrer le résultat pour une k-algèbre B simple, et d'après le corollaire précédent, on peut supposer que $B = M_n(D)$, où D est une k-algèbre à division. Commençons par montrer que B, vu comme module à gauche sur lui-même, est complètement réductible. Notons E_i la matrice de $M_n(D)$ ayant pour coefficients 1 en (i,i) et 0 partout ailleurs. Alors Be_i est l'idéal à gauche des matrices dont seule la i-ième colonne est non nulle. On a $\dim_D(Be_i) = n = \dim_D(I)$, ce qui montre que Be_i est un idéal à gauche minimal de B. De plus, on a clairement

$$B = M_n(D) = \bigoplus_i Be_i,$$

[1] Cette observation est l'une des nombreuses versions du lemme de Schur

qui est une décomposition de B en B-modules simples.

Le théorème découle alors des lemmes suivants :

Lemme IV.2.6. — *Tout module sur un anneau A est quotient d'un module libre.*

<u>*Démonstration*</u>. Rappelons qu'un A-module libre est isomorphe à une somme directe $\bigoplus_i A_i$, où chaque A_i est isomorphe à A en tant que A-module.

Pour chaque $m \in M$, m est dans l'image du morphisme

$$A \to M, \quad a \mapsto a \cdot m$$

puisque $1 \cdot m = m$. Il s'ensuit que l'on peut construire un morphisme surjectif

$$\bigoplus_{m \in M} A \to M.$$

□

Lemme IV.2.7. — *Soit A un anneau et E un A-module. Les conditions suivantes sont équivalentes :*

(i) E est isomorphe à une somme directe de modules simples (E est complètement réductible).

(ii) E est engendré par ses sous-modules simples.

(iii) Pour tout sous-module E' de E, il existe un sous-module E'' de E tel que $E = E' \oplus E''$.

<u>*Démonstration*</u>. Il est clair que (i) implique (ii). Supposons (ii), et soit E' un sous-module de E. On peut, d'après l'hypothèse, écrire E comme une somme (mais pas directe),

$$E = \sum_{i \in I} E_i$$

pour un certain ensemble d'indices I (on peut prendre $I = E$ en choisissant pour chaque $v \in E$ un module simple qui le contient). Prenons dans I un sous-ensemble maximal pour l'inclusion (dont l'existence est assurée par le lemme de Zorn) tel que la somme $F = E' + \sum_{j \in J} E_j$ soit directe.

Alors cette somme est égale à E. En effet, il suffit de voir que chaque E_i, $i \in I$, est dans $E' \oplus (\bigoplus_{j\in J} E_j)$. Comme l'intersection de F avec E_i est un sous-module de E_i, cette intersection est E_i ou 0 puisque E_i et simple. Si cette intersection était nulle, on pourrait adjoindre i à J ce qui contredit la maximalité de J. Donc $E_i \subset F$. Montrons maintenant que (iii) implique (i). Commençons par voir que E admet alors un sous-module simple. Soit $v \in E$, $v \neq 0$. Le noyau du morphisme canonique

$$A \mapsto Av$$

est un idéal (à gauche) L de A, qui par le lemme de Zorn, est contenu dans un idéal (à gauche) maximal M. Alors M/L est un sous-module maximal propre de A/L, et donc Mv est un sous-module maximal propre de Av, correspondant à M/L par l'isomorphisme $A/L \simeq Av$. On peut écrire $E = Mv \oplus F$, pour un certain sous-module F, grâce à l'hypothèse. On a alors

$$Av = Mv \oplus (Av \cap F).$$

Comme Mv est maximal dans Av, $Av \cap F$ est simple. Ceci montre que E admet un sous-module simple. Soit maintenant E_0 la somme de tous les sous-modules simples de E. Si $E \neq E_0$, on écrit $E = E_0 \oplus F$. On applique maintenant la remarque précédente à F : il existe un sous-module simple de F. Ceci contredit la définition de E_0. $\square$

Lemme IV.2.8. — *Tout sous-quotient d'un module complètement réductible est réductible.*

Démonstration. Soit M un module complètement réductible. Ecrivons

$$M = \bigoplus_{s\in S} M_s,$$

où les modules M_s sont simples. Soit N un sous-module et p la projection naturelle de M sur M/N. Pour tout $s \in S$, l'image $\bar{M}_s$ de M_s dans M/N est soit nulle, soit c'est un sous-module simple de M/N, isomorphe à M_s. Soit $U \subset S$ l'ensemble des $s \in S$ tels que $\bar{M}_s \simeq M_s$. Il est alors clair que :

$$M/N = \sum_{u\in U} \bar{M}_u,$$

et comme dans la démonstration du lemme précédent, on peut extraire $T \subset U$ tel que

$$M/N = \bigoplus_{t \in T} \bar{M}_t \simeq \bigoplus_{t \in T} M_t.$$

Ceci montre que le quotient M/N est complètement réductible. On en déduit facilement que

$$M = N \oplus M_T$$

où $M_T = \bigoplus_{t \in T} M_t$. De plus $N \simeq M/M_T$, et comme l'on vient de montrer qu'un tel quotient est complètement réductible, ceci montre que N l'est.

□

IV.3. Application à la théorie des représentations

Nous avons montré dans le chapitre II que les représentations d'un groupe fini G sont complètement réductibles en utilisant l'existence d'un produit hermitien invariant. Nous voyons maintenant qu'il existe aussi une démonstration purement algébrique de ce fait, qui consiste à montrer que l'algèbre du groupe $\mathcal{F}(G)$ est semi-simple. Pour voir ceci, calculons la matrice de la forme trace dans la base des éléments du groupe. La trace de la multiplication à gauche dans $\mathcal{F}(G)$ par un élément $g \in G$ est

$$\operatorname{tr}(m_g) = 0 \ \text{ si } g \neq e, \quad \operatorname{tr}(m_e) = |G|.$$

On voit que la matrice de la forme trace est égale à $|G|P$ où P est la matrice de la permutation $g \mapsto g^{-1}$. Elle est de déterminant non nul, ce qui montre que la forme trace est non dégénérée.

La théorie développée dans la section précédente montre qu'alors, si $\{e_1, \ldots, e_s\}$ sont les idempotents minimaux de $\mathcal{F}(G)$, les $B_i = \mathcal{F}(G)e_i$ sont les idéaux bilatères minimaux de $\mathcal{F}(G)$, et si $I_i \subset B_i$ est un idéal minimal à gauche de B_i, les I_i forment un système de représentants des représentations irréductibles de $\mathcal{F}(G)$ (donc de G). Notons Θ_i le caractère de I_i. Comme le corps des complexes est algébriquement clos, $D_i = \operatorname{End}_{B_i}(I_i) = \mathbb{C}$, et l'on obtient un isomorphisme d'algèbres

$$B_i = \operatorname{End}(I_i) \simeq M_{n_i}(\mathbb{C}),$$

où $n_i = \Theta_i(e)$ est la dimension de I_i.

Soit L la représentation régulière de $M_n(\mathbb{C})$, agissant sur elle-même par multiplication à gauche. Un calcul dans la base canonique de $M_n(\mathbb{C})$ montre facilement que

$$\mathrm{tr}(L(X)) = n\ \mathrm{tr}(X), \quad (X \in M_n(\mathbb{C})).$$

Notons aussi L la représentation régulière gauche de $\mathcal{F}(G)$ et définissons pour tout $\alpha \in \mathcal{F}(G)$,

$$\chi_i(\alpha) = \mathrm{tr}(L(\alpha * e_i)).$$

Remarquons que $\chi_i(\alpha)$ est la trace de la multiplication à gauche par $\alpha * e_i$ dans $B_i \simeq M_{n_i}(\mathbb{C})$. On obtient donc que :

$$\chi_i(\delta_g) = \mathrm{tr}(L(\delta_g * e_i)) = n_i\ \Theta_i(g), \quad (g \in G). \tag{IV.3.1}$$

Utilisons ceci pour exprimer les idempotents e_i en fonction des caractères Θ_i : Ecrivons la décomposition de e_i dans la base $\{\delta_x\}_{x\in G}$ de $\mathcal{F}(G)$:

$$e_i = \sum_{x\in G} \epsilon_i(x)\ \delta_x$$

dans $\mathcal{F}(G)$. Multiplions par δ_g, pour obtenir

$$\delta_g * e_i = \sum_{x\in G} \epsilon_i(x)\ \delta_g * \delta_x = \sum_{x\in G} \epsilon_i(x)\ \delta_{gx} = \sum_{x\in G} \epsilon_i(g^{-1}x)\delta_x \tag{IV.3.2}$$

En prenant $\mathrm{tr}(L)$, et en utilisant (IV.3.1), on obtient

$$\mathrm{tr}(L(\delta_g * e_i)) = n_i\ \Theta_i(g) = \sum_{x\in G} \epsilon_i(g^{-1}x)\mathrm{tr}(L(\delta_x)) = |G|\epsilon_i(g^{-1}).$$

On obtient ainsi la formule donnant l'idempotent e_i :

$$e_i = \frac{n_i}{|G|} \sum_{g\in G} \Theta_i(g^{-1})\ \delta_g = n_i\ \overline{\Theta_i}. \tag{IV.3.3}$$

CHAPITRE V

GROUPES COMPACTS

Dans ce chapitre, nous allons généraliser des groupes finis aux groupes compacts certains des résultats obtenus. Il nous faut commencer par définir les groupes topologiques, et une bonne notion de représentation pour de tels groupes.

V.1. Groupes topologiques

Un **groupe topologique** est à la fois un groupe et un espace topologique séparé, où l'on exige que ces deux structures soient compatibles, c'est-à-dire que les applications

$$m : G \times G \to G, \quad (g, h) \mapsto gh$$

et

$$\iota : G \to G, \quad g \mapsto g^{-1}$$

soient continues.

Il convient d'adapter le vocabulaire des représentations lorsque l'on a affaire à des groupes topologiques :

Une **représentation** (π, V) d'un groupe topologique dans un espace vectoriel topologique V est la donnée d'un morphisme

$$\pi : G \to \mathbf{GL}(V)$$

tel que l'application

$$G \times V \to V, \quad (g, v) \mapsto \pi(g) \cdot v$$

soit **continue**.

Si V est un espace de Hilbert, muni d'un produit scalaire invariant, on dit que (π, V) est unitaire.

Lorsque l'espace de représentation V est de dimension finie, on le suppose toujours muni de la topologie transcendante.

Une **sous-représentation** de (π, V) est un sous-espace **fermé** de V invariant sous l'action de G.

Une représentation (π, V) est **irréductible** si elle n'admet aucune autre sous-représentation qu'elle-même et $\{0\}$.

Soient (π_1, V_1) et (π_2, V_2) deux représentations d'un groupe topologique G. Un **opérateur d'entrelacement** T entre ces représentations est un G-morphisme linéaire **continu** $T: V_1 \to V_2$. Ceci permet de définir la notion de représentations isomorphes ou équivalentes.

Dans ce contexte, nous avons l'analogue du théorème II.1.6 :

Théorème V.1.1. — *Soit (π, V) une représentation unitaire du groupe topologique G dans un espace de Hilbert V. Soit W un sous-espace invariant fermé de V. Alors $W^{\perp}$ est stable sous l'action de G et la représentation V se décompose en somme directe*

$$V = W \oplus W^{\perp}$$

Démonstration. La démonstration est la même que pour le théorème II.1.6, en remarquant de plus que si W est fermé, alors $W^{\perp}$ aussi et qu'on a alors $V = W \oplus W^{\perp}$. $\square$

Il n'est pas possible d'en dire plus à ce niveau de généralité. En particulier, il n'est pas vrai :

- qu'une représentation irréductible soit toujours de dimension finie.

- qu'une représentation (même de dimension finie) soit toujours unitaire.

- qu'une représentation de dimension finie soit toujours complètement réductible.

Un espace topologique est dit **localement compact** si tout point admet une base de voisinages compacts. Un groupe topologique est dit localement compact (resp. compact) s'il est localement compact en tant qu'espace topologique (resp. compact).

V.2. Mesure de Haar

Dans le chapitre sur les représentations des groupes finis, nous avons fait un usage immédiat (théorème II.1.2) de la mesure de comptage normalisée sur un groupe fini, et de ses propriétés d'invariance par translation à gauche ou à droite (voir la remarque II.1.3). Définissons l'analogue pour un groupe topologique localement compact quelconque.

Rappelons qu'une mesure de Radon λ sur un espace topologique localement compact X est une forme linéaire continue sur $\mathcal{C}_c(X, \mathbb{R})$, positive (c'est-à-dire que si $f \geq 0$, $\lambda(f) \geq 0$). Un théorème d'analyse nous dit qu'une telle forme linéaire est donnée par intégration par rapport à une mesure borélienne μ

$$\lambda(f) = \int_X f \, d\mu$$

possédant certaine propriétés (elle est localement finie et régulière intérieurement).

Définition V.2.1. — Soit G un groupe topologique localement compact. Une mesure de Radon μ_G sur G sera dite mesure de Haar à gauche (resp. à droite) sur G, si pour toute fonction intégrable f de G à valeurs dans $\mathbb{C}$, et pour tout $t \in G$,

$$\int_G (L(t) \cdot f)(g) d\mu_G(g) = \int_G f(g) d\mu_G(g)$$

(resp.

$$\int_G (R(t) \cdot f)(g) d\mu_G(g) = \int_G f(g) d\mu_G(g).$$

Nous admettrons le théorème suivant.

Théorème V.2.2. — *Soit G un groupe localement compact. Alors il existe une mesure de Haar à gauche μ_G sur G. Une telle mesure est unique à un facteur scalaire réel positif près.*

On peut lire la démonstration dans Bourbaki, Intégration, chapitre VII. Dans le cas des groupes compacts, on peut trouver dans [**3**] une démonstration de ce résultat basée sur le théorème d'Ascoli et le théorème de point fixe de Kakutani.

Remarque V.2.3. — Dans l'énoncé du théorème précédent, on peut remplacer "mesure de Haar à gauche" par "mesure de Haar à droite", mais les deux notions sont distinctes, une mesure de Haar à gauche n'est pas nécessairement une mesure de Haar à droite.

Cette remarque nous permet d'introduire la notion de **fonction modulaire** sur un groupe topologique G admettant une mesure de Haar. En effet, si μ_G est une mesure de Haar à gauche sur G, et si $h \in G$, on peut définir la mesure $R(h) \cdot \mu_G$ par

$$\int_G f(g)\, d(R(h) \cdot \mu_G)(g) = \int_G (R(h)^{-1} \cdot f)(g)\, d\mu_G(g),$$

pour toute fonction intégrable f. Alors $R(h) \cdot \mu_G$ est encore une mesure de Haar à gauche sur G. En effet, pour tout $t \in G$

$$\begin{aligned}
&\int_G (L(t) \cdot f)(g)\, d(R(h) \cdot \mu_G)(g) = \int_G (R(h)^{-1} \cdot (L(t) \cdot f))(g)\, d\mu_G(g) \\
&= \int_G (L(t) \cdot (R(h)^{-1} \cdot f))(g)\, d\mu_G(g) = \int_G (R(h)^{-1} \cdot f)(g)\, d\mu_G(g) \\
&= \int_G f(g)\, d(R(h) \cdot \mu_G)(g)
\end{aligned}$$

Le point crucial de ce calcul est que les actions L et R commutent. Il découle de ceci par unicité de la mesure de Haar que

$$R(h) \cdot \mu_G = \Delta(h)\mu_G$$

pour un certain réel strictement positif $\Delta(h)$. Ceci définit la fonction modulaire Δ sur G. Un calcul simple montre que

$$\Delta(h_1 h_2) = \Delta(h_1)\Delta(h_2), \quad (h_1, h_2 \in G).$$

La fonction modulaire Δ est donc un caractère de G dans $\mathbb{R}_+^*$. Il est assez facile de montrer qu'il est continu, en prenant pour fonction f dans l'identité ci-dessous la fonction caractéristique d'un voisinage compact de e, et en utilisant les propriété de régularité de la mesure μ_G. On a, pour toute fonction intégrable f sur G, et tout $h \in G$,

$$\int_G f(gh)\, d\mu_G(g) = \Delta(h) \int_G f(g)\, d\mu_G(g). \tag{V.2.1}$$

Théorème V.2.4. — *Soit G un groupe compact. Toute mesure de Haar à gauche est aussi une mesure de Haar à droite. On peut normaliser la mesure de Haar μ_G de sorte que $\mu_G(G) = 1$.*

Démonstration. Puisque G est compact, on peut intégrer la fonction constante égale à 1 sur G. Reportant dans (V.2.1), on obtient, pour tout $h \in G$,

$$\mu_G(G) = \Delta(h)\mu_G(G).$$

La fonction modulaire est donc identiquement égale à 1 sur G, et ceci signifie que μ_G est aussi une mesure de Haar à droite. La deuxième assertion du théorème est évidente. □

Exemples V.2.5. — si G est un groupe fini, il est compact pour la topologie discrète, et la mesure de comptage normalisée est une mesure de Haar.

— Dans un groupe topologique abélien, toute mesure de Haar à gauche est aussi une mesure de Haar à droite.

— Une mesure de Haar sur $(\mathbb{R}, +)$ est un multiple scalaire de la mesure de Lebesgue.

— Si $G = U(1) = \{z \in \mathbb{C} |\ |z| = 1\}$, une mesure de Haar est un multiple scalaire de $\frac{dz}{2i\pi z}$. Si l'on identifie $U(1)$ et $\mathbb{R}/2\pi\mathbb{Z}$ par $\theta \mapsto e^{i\theta}$, cette mesure est donnée par $\frac{d\theta}{2\pi}$.

V.3. Représentations des groupes compacts

Nous allons commencer par un résultat intéressant, mais qui ne servira pas vraiment dans la suite, et dont nous omettons la démonstration.

Théorème V.3.1. — *Toute représentation irréductible d'un groupe compact dans un espace de Banach est de dimension finie.*

Voir par exemple [**3**], corollaire 5.8.

Nous pouvons ensuite généraliser le théorème II.1.2 aux groupes compact.

Théorème V.3.2. — *Toute représentation d'un groupe compact G de dimension finie peut être munie d'un produit hermitien invariant, qui rend la représentation unitaire.*

Démonstration. La démonstration est la même que pour les groupes fini, grâce à l'existence de la mesure de Haar sur G. □

Corollaire V.3.3. — *Toute représentation d'un groupe compact G de dimension finie est complètement réductible.*

Démonstration. Ceci découle du théorème précédent et du théorème V.1.1 de la même façon que pour les groupes finis. □

Tout espace vectoriel complexe de dimension finie peut être muni d'un produit hermitien qui en fait un espace de Hilbert. Le théorème V.3.2 ci-dessus montre que l'on peut, par un argument de moyenne, rendre ce produit hermitien invariant sous l'action du groupe G. Que se passe-t-il si l'on part d'une représentation (non nécessairement unitaire) de G dans un espace de Hilbert ? Peut-on la rendre unitaire ? L'argument de moyenne marche encore, et l'on obtient un produit hermitien invariant. Le problème est de vérifier que la nouvelle topologie définie par ce produit hermitien invariant coïncide avec l'ancienne, en particulier, que l'espace reste complet. La réponse à cette question est positive :

Proposition V.3.4. — *Toute représentation d'un groupe compact dans un espace de Hilbert H peut être munie d'un produit hermitien invariant,* *qui rend la représentation unitaire et définit la même structure topologique sur H.*

Voir [**3**], proposition 2.7. La démonstration nécessite bien sûr un peu d'analyse, en particulier le théorème de Banach-Steinhaus.

Soit G un groupe compact. Notons $\widehat{G}$ l'ensemble des classes d'équivalences des représentations de dimension finie irréductibles de G. Les notations afférentes sont les mêmes que pour les groupes finis. Les notions de somme directe, de produit tensoriel et de représentation contragrédiente s'étendent sans difficultés aux groupes compacts. Le lemme de Schur est encore valide (si l'on ne souhaite pas utiliser le théorème V.3.1, il faut rajouter que les représentations sont de dimension finie dans les hypothèses). Les coefficients matriciels sont définis de la même manière que pour les groupes finis. Ce sont des éléments de l'espace $\mathcal{C}(G)$ des fonctions continues sur G. Cet espace, muni de la norme sup, est un espace de Banach. Les relations de Schur (lemme II.3.2) sont encore valides, ainsi que le corollaire II.3.3 d'indépendance linéaire des coefficients matriciels dans $\mathcal{C}(G)$. Comme $\mathcal{C}(G)$ n'est pas de dimension finie, on ne peut en déduire que $\widehat{G}$ est fini (il ne l'est pas en général).

Soit $L^2(G)$ l'espace de Hilbert des fonctions (à valeurs complexes, mesurables, modulo l'égalité presque partout) de carré intégrable par rapport à la mesure de Haar μ_G (le produit hermitien étant défini de la manière habituelle). L'espace $\mathcal{C}(G)$ est un sous-espace dense de $L^2(G)$.

Définissons maintenant le produit de convolution sur $\mathcal{C}(G)$ et $L^2(G)$. Soient f_1 et f_2 deux fonctions dans $\mathcal{C}(G)$. Leur produit de convolution $f_1 * f_2$ est défini par

$$f_1 * f_2(g) = \int_G f_1(t) f_2(t^{-1}g)\, d\mu_G(t).$$

Il est clair que $f_1 * f_2$ est dans $\mathcal{C}(G)$. L'inégalité de Cauchy-Schwarz donne

$$|f_1 * f_2(g)| \leq ||f_1||_2\, ||f_2||_2$$

ce qui montre que le produit de convolution peut être étendu par continuité à $L^2(G)$:

$$* \;:\; L^2(G) \times L^2(G) \to \mathcal{C}(G) \subset L^2(G).$$

L'espace $L^2(G)$ muni du produit de convolution est une algèbre associative. D'autre part, $L^2(G)$ est muni de la représentation régulière $L\times R$ de $G\times G$ (cette représentation est unitaire). Dans le cas des groupes finis, $\mathcal{F}(G) = L^2(G)$. Pour les groupes compacts généraux, c'est l'espace $L^2(G)$ muni de toutes ces structures (espace de Hilbert, représentation unitaire de $G \times G$, algèbre de convolution) qui joue le premier rôle, comme nous allons le voir ci-dessous. Remarquons que $L^2(G)$ n'admet pas d'élément neutre, si G n'est pas fini.

Lorsque (π, V) est une représentation de dimension finie d'un groupe compact G, on peut encore, comme en II.4.4, définir un morphisme d'algèbres

$$\pi :\ L^2(G) \to \mathrm{End}(V), \quad f \mapsto \pi(f) = \int_G f(g)\pi(g)\, d\mu_G(g).$$

entrelaçant la représentation régulière $L\times R$ de $G\times G$ et la représentation $\mathrm{End}(\pi)$ de $\mathrm{End}(V)$. Remarquons que l'intégrale ci-dessus est bien définie car, comme G est compact, $L^2(G) \subset L^1(G)$.

Ceci permet de définir la **transformée de Fourier** d'une fonction $f \in L^2(G)$ comme pour les groupes finis, mais il faut remarquer que cette transformée de Fourier est à valeurs dans le produit **infini** $\prod_{\delta\in\widehat{G}} \mathrm{End}(V_\delta)$. Ceci pose un problème pour définir la transformée de Fourier inverse, puisque celle-ci est définie par une somme sur $\widehat{G}$, qui pourrait ne pas converger. Pour éviter cela, nous allons restreindre le domaine de la transformée de Fourier inverse à $\bigoplus_{\delta\in\widehat{G}} \mathrm{End}(V_\delta)$. La somme directe

$$\bigoplus_{\delta\in\widehat{G}} \mathrm{End}(V_\delta)$$

est le sous-espace de $\prod_{\delta\in\widehat{G}} \mathrm{End}(V_\delta)$ constitué des familles $F(\delta)_{\delta\in\widehat{G}}$ telle que $F(\delta) = 0$ sauf pour un nombre **fini** de δ. Ceci nous assure que la transformée de Fourier inverse est bien définie sur ce sous-espace, puisque seul un nombre fini de termes sont non nuls dans la somme définissant la transformée de Fourier inverse. La relation

$$\mathcal{F}\bar{\mathcal{F}}F = F$$

est encore valide pour tout $F \in \bigoplus_{\delta\in\widehat{G}} \mathrm{End}(V_\delta)$. Le problème est maintenant de déterminer l'image de $\bar{\mathcal{F}}$ dans $L^2(G)$. Mais pour cela, il nous suffit de remarquer que le calcul de la démonstration du théorème II.5.10 est toujours valide, à condition d'introduire une nouvelle notation : pour tout $\delta \in \widehat{G}$, on définit $\mathcal{R}(\delta)$ comme le sous-espace de $\mathcal{C}(G)$ engendré par les coefficients matriciels de la représentation δ. On pose aussi

$$\mathcal{R}(G) = \bigoplus_{\delta \in \widehat{G}} \mathcal{R}(\delta).$$

Il est alors clair que $\bar{\mathcal{F}}$ réalise un isomorphisme entre $\bigoplus_{\delta \in \widehat{G}} \mathrm{End}(V_\delta)$ et $\mathcal{R}(G)$, plus précisément, $\bar{\mathcal{F}}$ réalise un isomorphisme entre chaque $\mathrm{End}(V_\delta)$ et $\mathcal{R}(\delta)$.

Le théorème de Peter-Weyl pour les groupes compacts peut s'énoncer ainsi :

Théorème V.3.5. — *Le sous-espace $\mathcal{R}(G)$ est dense dans $\mathcal{C}(G)$ et dans $L^2(G)$.*

Dans le cas des groupes finis, nous avons montré que $\mathcal{F}$ et $\bar{\mathcal{F}}$ sont des isomorphismes inverses l'un de l'autre en montrant que $\mathcal{F}\bar{\mathcal{F}}$ est l'identité, puis en montrant l'injectivité de $\mathcal{F}$. La surjectivité de $\bar{\mathcal{F}}$ s'en déduit alors. Le résultat ci-dessus remplace la surjectivité de $\bar{\mathcal{F}}$. On le démontre en commençant par établir un résultat qui est l'analogue de l'injectivité de $\mathcal{F}$ (*cf.* remarques II.5.5) :

Théorème V.3.6. — *Pour tout $g \in G$, $g \neq e$, il existe une représentation irréductible de dimension finie (π, V) de G telle que $\pi(g) \neq \mathrm{Id}_V$.*

La démonstration de ce théorème utilise le théorème spectral pour les opérateurs auto-adjoints compacts. Nous renvoyons le lecteur à [**3**], chapitre 4.

Choisissons, dans chaque $\mathcal{R}(\delta)$, une base orthonormale. Alors le théorème ci-dessus affirme que la réunion de toutes ces bases forme une base **au sens hilbertien** de l'espace de Hilbert $L^2(G)$. Nous écrivons ceci :

$$L^2(G) = \widehat{\bigoplus}_{\delta \in \widehat{G}} \mathcal{R}(\delta).$$

Nous pouvons maintenant identifier l'image de $L^2(G)$ par la transformation de Fourier $\mathcal{F}$. Il s'agit de l'espace de Hilbert

$$\widehat{\bigoplus}_{\delta\in\widehat{G}}\mathrm{End}(V_\delta).$$

Concrètement, cet espace est obtenu de la manière suivante : chaque $\mathrm{End}(V_\delta)$ est une représentation de dimension finie du groupe compact $G\times G$, il est donc muni d'un produit hermitien invariant. On choisit une base orthonormale de chacun des $\mathrm{End}(V_\delta)$, et l'on forme un espace de Hilbert en décrétant que la réunion de toutes ces bases est une base orthonormale (au sens hilbertien). La transformée de Fourier inverse est définie sur ce sous-espace (par une série convergente). Une autre version du théorème de Peter-Weyl est donc

Théorème V.3.7. — *La transformée de Fourier $\mathcal{F}$ réalise un isomorphisme*

$$L^2(G)\simeq\widehat{\bigoplus}_{\delta\in\widehat{G}}\mathrm{End}(V_\delta).$$

La formule d'inversion de Fourier et la formule de Plancherel (corollaires II.5.7 et II.5.8) sont donc valable pour les groupes compacts. Comme les fonctions dans $L^2(G)$ ne sont définies que modulo l'égalité presque partout, l'inversion de Fourier doit être comprise comme telle. En particulier la formule pour $g=e$ n'a pas de sens dans ce contexte.

Exemple V.3.8. — Soit $G=U(1)$. C'est un groupe abélien dont les représentations irréductibles continues (de dimension 1) sont

$$\chi_n : e^{i\theta}\mapsto e^{in\theta},$$

où $n\in\mathbb{Z}$. Le dual $\widehat{G}$ s'identifie donc à $\mathbb{Z}$. L'inversion de Fourier dans ce cas est bien la décomposition en série de Fourier des fonctions dans $L^2(U(1))$ (que l'on peut voir comme fonctions sur $\mathbb{R}$, 2π-périodiques). Il est bien connu que pour une fonction continue, il n'y a pas convergence ponctuelle de sa série de Fourier.

Passons maintenant à la théorie des caractères pour les groupes compacts. Pour les représentations de dimension finie, la définition de ceux-ci et leurs propriétés (lemme II.6.2 et proposition II.6.3) restent valables.

Pour le lemme II.6.2, il faut adapter l'argument : les valeurs propres de $\pi(x)$ ne sont plus nécessairement des racines de l'unité, mais restent des nombres complexes de module 1, grâce à la compacité de G (les valeurs propres de $\pi(x)^n$ restent bornées). Les relations d'orthogonalité (théorème II.6.5) s'obtiennent sans difficulté ainsi que le corollaire II.6.6 (on obtient une base orthonormale au sens Hilbertien de $L^2(G)^G$), le théorème II.6.7, le théorème II.7.1, le corollaire II.7.2 et le théorème II.7.3. En revanche, les calculs fondés sur les fonctions caractéristiques des classes de conjugaison ne se généralisent pas (théorème II.6.8).

V.4. Exercices

Exercice V.4.1. — Montrer qu'un groupe compact G est abélien si et seulement si toutes ses représentations irréductibles de dimension finie sont de dimension 1.

Exercice V.4.2. — Soit G le groupe des matrices complexes de la forme

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \quad |a| = 1$$

muni de la topologie usuelle.

a) Ce groupe est-il compact ?

b) Montrer que la représentation standard de G sur $\mathbb{C}^2$ est réductible, mais pas complètement réductible.

c) Déterminer les opérateurs d'auto-entrelacement de cette représentation standard.

Exercice V.4.3. — Déterminer la mesure de Haar et le caractère modulaire du groupe $\begin{pmatrix} \mathbb{R}^\times & \mathbb{R} \\ 0 & 1 \end{pmatrix}$.

Exercice V.4.4. — Soient (π_1, V_1) et (π_2, V_2) deux représentations unitaires équivalentes d'un groupe topologique G. Montrer qu'elles sont unitairement équivalentes (c'est-à-dire qu'il existe un opérateur d'entrelacement unitaire réalisant l'isomorphisme entre V_1 et V_2).

Exercice V.4.5. — Soient (π_1, V_1) et (π_2, V_2) deux représentations irréductibles de dimension finie respectivement des groupes compacts G_1 et G_2. Montrer que la représentation $\pi_1 \boxtimes \pi_2$ de $G_1 \times G_2$ est irréductible. Montrer que toute représentation irréductible de dimension finie de $G_1 \times G_2$ est de cette forme.

CHAPITRE VI

GROUPES ET ALGÈBRES DE LIE

VI.1. Le groupe $\mathbf{GL}(n,\mathbb{K})$ et son algèbre de Lie $\mathfrak{gl}(n,\mathbb{K})$

La notation $\mathbb{K}$ désigne un corps pouvant être soit le corps des nombres réels $\mathbb{R}$, soit le corps des nombres complexes $\mathbb{C}$.

Soit $M_n(\mathbb{K})$ l'algèbre sur $\mathbb{K}$ des matrices carrés $n \times n$ à coefficients dans $\mathbb{K}$. C'est un espace de dimension n^2, et toutes les normes sur cet espace sont donc équivalentes. On suppose $\mathbb{K}^n$ muni de la norme usuelle provenant du produit scalaire canonique sur $\mathbb{R}^n$ ou du produit hermitien canonique sur $\mathbb{C}^n$. Munissons $M_n(\mathbb{K})$ de la norme d'opérateur

$$||X|| = \sup_{x\in\mathbb{K}^n\setminus\{0\}} \frac{||X(x)||}{||x||}.$$

Cette norme vérifie

$$\text{(VI.1.1)} \qquad ||XY|| \leq ||X||\,||Y||, \quad (X, Y \in M_n(\mathbb{K})).$$

L'algèbre $M_n(\mathbb{K})$ est donc munie d'une norme qui en fait un espace vectoriel normé complet (un espace de Banach).

Rappelons maintenant quelques propriétés du groupe des matrices inversibles $\mathbf{GL}(n,\mathbb{K})$. On note Id_n la matrice identité de $M_n(\mathbb{K})$.

Proposition VI.1.1. — *Le groupe des matrices inversibles* $\mathbf{GL}(n,\mathbb{K})$ *est un groupe topologique pour la topologie induite de celle de* $M_n(\mathbb{K})$. *De plus,* $\mathbf{GL}(n,\mathbb{K})$ *est un ouvert dense de* $M_n(\mathbb{K})$.

Démonstration. Considérons l'application det : $M_n(\mathbb{K}) \to \mathbb{K}$. C'est une application polynomiale, donc continue, et le groupe $\mathbf{GL}(n, \mathbb{K})$ est l'image réciproque de $\mathbb{K}^*$. Ceci montre que $\mathbf{GL}(n, \mathbb{K})$ est un ouvert de $M_n(\mathbb{K})$. Le produit de matrices est continu, d'après (VI.1.1). D'autre part, l'inverse est donné par $X^{-1} = \det(X)^{-1}({}^t\tilde{X})$, où $\tilde{X}$ désigne la comatrice de X. Les coefficients de la comatrice sont des fonctions polynomiales des coefficients de X. Ceci montre que le passage à l'inverse est une application continue. Le groupe $\mathbf{GL}(n, \mathbb{K})$ est ainsi muni d'une structure de groupe topologique. Soit X dans $M_n(\mathbb{K})$ non nulle, et soit λ_0 le plus petit module non nul d'une valeur propre de X. Alors la matrice $X - \lambda \mathrm{Id}_n$ à toutes ses valeurs propres non nulles si $0 < |\lambda| < \lambda_0$ et est donc inversible. Ceci montre que $\mathbf{GL}(n, \mathbb{K})$ est dense dans $M_n(\mathbb{K})$. □

Exercice VI.1.2. — Montrer que le centre de $\mathbf{GL}(n, \mathbb{K})$ est l'ensemble des homothéties.

Comme $\mathbf{GL}(n, \mathbb{K})$ est un ouvert de $M_n(\mathbb{K})$, l'espace tangent à $\mathbf{GL}(n, \mathbb{K})$ en l'identité s'identifie à $M_n(\mathbb{K})$. Le produit dans $\mathbf{GL}(n, \mathbb{K})$ donne par différentiation un "crochet de Lie" sur $M_n(\mathbb{K})$. Nous verrons cela de manière plus générale dans la suite. Pour le moment, munissons $M_n(\mathbb{K})$ de l'opération suivante :

$$(X, Y) \mapsto [X, Y] = XY - YX, \quad (X, Y \in M_n(\mathbb{K})).$$

Il est clair que c'est une application bilinéaire antisymétrique de $M_n(\mathbb{K}) \times M_n(\mathbb{K})$ dans $M_n(\mathbb{K})$. Elle vérifie d'autre part **l'identité de Jacobi** :

$$[X, [Y, Z]] + [Z, [X, Y]] + [Y, [Z, X]] = 0. \tag{VI.1.2}$$

Définition VI.1.3. — Une algèbre de Lie L sur $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel muni d'une application (appelée "crochet") :

$$[.\,,.] \ : L \times L \to L$$

bilinéaire antisymétrique vérifiant l'identité de Jacobi (VI.1.2).

Une sous-algèbre de Lie de L est un sous-espace vectoriel de L stable par crochets.

Un idéal de l'algèbre de Lie L est un sous-espace vectoriel I de L tel que quels que soient $X \in I$ et $Y \in L$, $[X, Y] \in I$.

Exemples VI.1.4. — Nous avons vu que $M_n(\mathbb{K})$ est une algèbre de Lie. On la note $\mathfrak{gl}(n, \mathbb{K})$. Plus généralement, si V est un espace vectoriel sur $\mathbb{K}$, $\mathrm{End}(V)$ est une algèbre de Lie, notée $\mathfrak{gl}(V)$.

— $\mathfrak{sl}(n, \mathbb{K})$ est la sous-algèbre de Lie de $\mathfrak{gl}(n, \mathbb{K})$ des matrices de trace nulle.

— $\mathfrak{b}(n, \mathbb{K})$ est la sous-algèbre de Lie de $\mathfrak{gl}(n, \mathbb{K})$ des matrices triangulaires supérieures.

— $\mathfrak{n}(n, \mathbb{K})$ est la sous-algèbre de Lie de $\mathfrak{gl}(n, \mathbb{K})$ des matrices triangulaires supérieures strictes. C'est un idéal de la précédente.

— $\mathfrak{so}(n)$ est la sous-algèbre de Lie de $\mathfrak{gl}(n, \mathbb{R})$ des matrices antisymétriques.

— $\mathfrak{su}(n)$ est la sous-algèbre de Lie de $\mathfrak{gl}(n, \mathbb{C})$ des matrices antihermitiennes.

— Soit M une variété différentiable et $\mathcal{X}(M)$ l'espace des champs de vecteurs sur M. Alors $\mathcal{X}(M)$, muni du crochet de Lie des champs de vecteurs, est une algèbre de Lie sur $\mathbb{R}$.

Définition VI.1.5. — Un morphisme d'algèbres de Lie est une application linéaire entre algèbres de Lie respectant le crochet. Un morphisme d'algèbres de Lie d'une algèbre de Lie L dans $\mathfrak{gl}(V)$ est appelée représentation de L dans l'espace vectoriel V.

VI.2. L'application exponentielle

Définition VI.2.1. — Soit X un élément de $M_n(\mathbb{K})$. l'exponentielle de X, notée $\exp X$, désigne la somme de la série (normalement convergente dans l'espace de Banach $M_n(\mathbb{K})$)

$$\sum_{n=0}^{+\infty} \frac{X^n}{n!}.$$

Donnons quelques propriétés de l'exponentielle.

Proposition VI.2.2. — *Quels que soient X et Y dans $M_n(\mathbb{K})$:*

(i) *Si X et Y commutent* $\exp X \exp Y = \exp(X+Y)$.

(ii) *L'exponentielle est à valeurs dans $\mathbf{GL}(n,\mathbb{K})$ et*

$$(\exp X)^{-1} = \exp(-X).$$

(iii) *Quels que soient t, s dans $\mathbb{K}$,*

$$\exp(sX)\exp(tX) = \exp((s+t)X)$$

(iv) *L'application $\mathbb{K} \to \mathbf{GL}(n,\mathbb{K})$, $t \mapsto \exp(tX)$ est l'unique solution différentiable de l'équation différentielle du premier ordre*

$$a'(t) = X\,a(t)$$

avec la condition initiale $a(0) = \mathrm{Id}_n$.

(v) *L'application $\mathbb{K} \to \mathbf{GL}(n,\mathbb{K})$, $t \mapsto \exp(tX)$ est l'unique solution différentiable de l'équation fonctionelle*

$$a(s)a(t) = a(s+t), \quad a(0) = \mathrm{Id}_n, \quad a'(0) = X.$$

(vi) *Pour tout $g \in \mathbf{GL}(n,\mathbb{K})$, $g \exp X\, g^{-1} = \exp(gXg^{-1})$.*

<u>*Démonstration*</u>. Démontrons (i).

$$\exp X \exp Y = \left(\sum_{n=0}^{+\infty} \frac{X^n}{n!}\right)\left(\sum_{n=0}^{+\infty} \frac{Y^n}{n!}\right) = \sum_{j,k=1}^{+\infty} \frac{X^jY^k}{j!k!}.$$

et si X et Y commutent :

$$\exp(X+Y) = \sum_{n=0}^{+\infty} \frac{(X+Y)^n}{n!} = \sum_{n=0}^{+\infty} \frac{1}{n!} \sum_{j+k=n} \frac{n!}{j!k!} X^jY^k = \sum_{j,k=1}^{+\infty} \frac{X^jY^k}{j!k!}.$$

On en déduit immédiatement (ii) et (iii).

La série définissant l'exponentielle étant à convergence normale, on peut dériver terme à terme. On obtient

$$\frac{d}{dt}(\exp tX) = \frac{d}{dt}\sum_{n=0}^{+\infty} \frac{t^nX^n}{n!} = \sum_{n=0}^{+\infty} \frac{t^nX^{n+1}}{n!} = X\exp tX = \exp tX\; X$$

Comme $\exp 0 = \mathrm{Id}$, on voit que $t \mapsto \exp tX$ est solution de l'équation différentielle du (iv).

Supposons que $a(t)$ soit une autre solution. On a

$$\frac{d}{dt}((\exp -tX)a(t)) = (\exp -tX)(-X)a(t) + (\exp -tX)a'(t) = 0$$

et l'on en déduit que $a(t) = \exp tX$.

Montrons (v). Soit $a(t)$ une solution de l'équation fonctionnelle. On a

$$\frac{d}{dt}a(t) = \lim_{s\to 0}\frac{a(t+s)-a(t)}{s} = a(t)\lim_{s\to 0}\frac{a(s)-\mathrm{Id}}{s} = a(t)a'(0) = a(t)X.$$

L'assertion découle alors de (iv).

(vi) est évident. □

Exercice VI.2.3. — Montrer que X et Y commutent si et seulement si $\exp(tX+sY) = \exp(tX)\exp(sY)$ quels que soient t, s dans $\mathbb{R}$.

Remarque VI.2.4. — On peut reformuler (iii) en disant que

$$t \mapsto \exp tX$$

est un morphisme de groupes (continu) de $\mathbb{R}$ dans $\mathbf{GL}(n,\mathbb{K})$. On appelle un tel morphisme un **sous-groupe à un paramètre** de $\mathbf{GL}(n,\mathbb{K})$.

Exercice VI.2.5. — Montrer qu'un morphisme de groupe continu $\phi : \mathbb{R} \to \mathbf{GL}(n,\mathbb{K})$ est différentiable. En déduire que tout sous-groupe à un paramètre de $\mathbf{GL}(n,\mathbb{K})$ est de la forme $t \mapsto \exp tX$ pour un certain X dans $M_n(\mathbb{K})$.

Proposition VI.2.6. — *L'application exponentielle*

$$\exp : M_n(\mathbb{K}) \longrightarrow \mathbf{GL}(n,\mathbb{K})$$

est de classe $\mathcal{C}^\infty$; sa différentielle à l'origine est l'application identique de $M_n(\mathbb{K})$.

<u>*Démonstration*</u>. L'exponentielle étant définie par une série normalement convergente, elle est $\mathcal{C}^\infty$. On a

$$|| \exp X - \exp 0 - X|| = ||X \sum_{p=1}^{\infty} \frac{X^p}{p+1!}||.$$

Posons $\epsilon(X) = \sum_{p=1}^{\infty} \frac{X^p}{p+1!}$. C'est une fonction définie par une intégrale normalement convergente, donc continue, et $\epsilon(0) = 0$. Ceci montre que la différentielle de l'exponentielle à l'origine est l'application identique de $M_n(\mathbb{K})$. □

Le calcul de la différentielle en un point quelconque est l'objet de l'exercice VI.4.4.

Corollaire VI.2.7. — *Il existe un voisinage $\mathcal{U}$ ouvert de* 0 *dans* $M_n(\mathbb{K})$ *et un voisinage ouvert $\mathcal{V}$ de l'identité dans* $\mathbf{GL}(n, \mathbb{K})$ *tels que l'application exponentielle réalise un difféomorphisme de $\mathcal{U}$ sur $\mathcal{V}$.*

<u>*Démonstration*</u>. C'est une conséquence immédiate du théorème d'inversion locale. □

Exercice VI.2.8. — Montrer que quitte à restreindre les ouverts $\mathcal{U}$ et $\mathcal{V}$ dans le corollaire, l'inverse de l'exponentielle est donné par une série. On note log : $\mathcal{V} \to \mathcal{U}$ cet inverse. Montrer que quels que soient $X, Y \in \mathfrak{gl}(n, \mathbb{K})$, quelque soit $t \in \mathbb{R}$ suffisamment petit

$$\log(\exp tX \ \exp tY) = tX + tY + \frac{t^2}{2}[X, Y] + 0(t^3).$$

Calculer le terme suivant dans ce développement.

Remarque VI.2.9. — La formule de Baker-Campbell-Hausdorff calcule le développement à tout ordre en t de l'exercice précédent. L'essence de la formule est que le terme en t^n peut s'exprimer à partir de crochets successifs de X et de Y.

VI.3. Groupes linéaires

Définition VI.3.1. — On appelle groupe linéaire un sous-groupe d'un groupe général linéaire $\mathbf{GL}(n, \mathbb{R})$.

Remarques VI.3.2. — Tout sous-groupe d'un groupe linéaire est linéaire. Le groupe $\mathbf{GL}(n, \mathbb{C})$ est linéaire, puisqu'on peut le plonger naturellement dans $\mathbf{GL}(2n, \mathbb{R})$.

Exemples VI.3.3. — Le groupe $\mathbf{SL}(n, \mathbb{K})$ des matrices de déterminant 1.

— Le groupe $\mathrm{B}(n, \mathbb{K})$ des matrices triangulaires supérieures inversibles.

— Le groupe $\mathrm{N}(n, \mathbb{K})$ des matrices des matrices triangulaires supérieures avec des 1 sur la diagonale.

— Le groupe $\mathbf{SO}(n)$ des matrices orthogonales (réelles) de déterminant 1.

— Le groupe $\mathbf{SU}(n)$ des matrices unitaires (complexes) de déterminant 1.

Exercice VI.3.4. — Montrer que tout groupe fini est linéaire.

Définition VI.3.5. — Soit G un groupe linéaire, disons $G \subset \mathbf{GL}(n, \mathbb{R})$. L'espace tangent $\mathfrak{g}$ à G en Id_n est l'espace des matrices $X \in \mathfrak{gl}(n, \mathbb{R})$ telles qu'il existe une courbe $a(t)$, définie sur un intervalle ouvert autour de 0 dans $\mathbb{R}$, de classe $\mathcal{C}^1$, à valeurs dans G, et vérifiant $a(0) = \mathrm{Id}_n$ et $a'(0) = X$.

Exercice VI.3.6. — Montrer que l'algèbre de Lie d'un groupe linéaire fini est $\{0\}$.

Donnons la propriété fondamentale de cet espace tangent.

Proposition VI.3.7. — *L'espace tangent $\mathfrak{g}$ est une sous-algèbre de Lie de $\mathfrak{gl}(n, \mathbb{R})$.*

Démonstration. Soient $X, Y \in \mathfrak{g}$ et $\alpha, \beta \in \mathbb{R}$. Soient $a(t)$ et $b(t)$ des courbes de classe $\mathcal{C}^1$ dans G vérifiant $a(0) = b(0) = \mathrm{Id}_n$, $a'(0) = X$, $b'(0) = Y$. Posons $c(t) = a(\alpha t)b(\beta t)$. On a bien $c(0) = \mathrm{Id}_n$ et $c'(0) = \alpha X + \beta Y$. Ceci montre que $\mathfrak{g}$ est un sous-espace vectoriel de $\mathfrak{gl}(n, \mathbb{R})$. Montrons maintenant que $[X, Y]$ est dans $\mathfrak{g}$. Posons, pour s suffisamment proche de 0,

$$c_s(t) = a(s)b(t)a(s)^{-1}.$$

C'est une courbe dans G vérifiant $c_s(0) = \mathrm{Id}_n$ et $c_s'(0) = a(s)Ya(s)^{-1}$. Ceci montre que $a(s)Ya(s)^{-1} \in \mathfrak{g}$ pour tout s suffisamment proche de 0. Maintenant, $s \mapsto a(s)Ya(s)^{-1}$ est une courbe dans $\mathfrak{g}$, et son vecteur tangent en 0 est dans $\mathfrak{g}$, donc

$$\frac{d}{ds}(a(s)Ya(s)^{-1})_{|s=0} = XY - YX = [X, Y] \in \mathfrak{g}.$$

□

On appelle $\mathfrak{g}$ l'algèbre de Lie du groupe linéaire G. Un résultat crucial dans la théorie des groupes linéaires est que l'application exponentielle renvoie l'algèbre de Lie $\mathfrak{g}$ dans le groupe G.

Théorème VI.3.8. — *Soit G un groupe linéaire et soit $\mathfrak{g}$ son algèbre de Lie. Alors l'application* exp *envoie $\mathfrak{g}$ dans G.*

Démonstration. L'idée est la suivante. On a $\exp 0 = \mathrm{Id}_n$ et si $X \in \mathfrak{g}$, alors $\left(\frac{d}{dt} \exp tX\right)_{|t=0} = X$, donc la courbe $c(t) = \exp tX$ passe par $\mathrm{Id} \in G$ en 0 et est tangente à G en ce point. L'espace tangent à G en un point g quelconque de G peut s'identifier à $g\mathfrak{g}$. La courbe $t \mapsto gc(t)$ à valeur dans G est donc tangente à G en $t = 0$, c'est-à-dire au point g. Il est donc raisonnable de croire que la courbe $c(t)$, qui est tangente en chaque point à G, reste dans G. Démontrons-le rigoureusement.

L'algèbre de Lie $\mathfrak{g}$ est par définition une sous-algèbre de Lie de $\mathfrak{gl}(n, \mathbb{R})$ pour un certain n. En particulier $k = \dim \mathfrak{g} \leq n^2$. Choisissons une base $X_1, \ldots, X_k$ de $\mathfrak{g}$, et soit $\mathfrak{s}$ un supplémentaire de $\mathfrak{g}$ dans $\mathfrak{gl}(n, \mathbb{R})$. Pour tout $i = 1, \ldots, k$, soit $a_i(t)$ une courbe dans G passant par Id_n en 0 et dont la dérivée en ce point est le vecteur X_i. Les courbes a_i sont définies dans un voisinage de 0.

Posons, pour tout $X = t_1X_1 + \ldots + t_kX_k \in \mathfrak{g}$, avec les t_i suffisamment petits,

$$\phi(X) = a(t_1)a(t_2)\ldots a(t_k),$$

pour tout $Y \in \mathfrak{s}$,

$$\psi(Y) = \mathrm{Id}_n + Y,$$

et pour tout élément $X + Y$ de $\mathfrak{gl}(n,\mathbb{R})$, $X \in \mathfrak{g}$, $Y \in \mathfrak{s}$

$$k(X + Y) = \phi(X)\psi(Y).$$

Calculons la différentielle de k en 0. Il est clair que

$$d\phi_0(X) = X, \quad d\psi_0(Y) = Y$$

d'où $dk_0(X+Y) = X+Y$, dk_0 est l'identité de $\mathfrak{gl}(n,\mathbb{R})$. Cette différentielle en zéro étant inversible, il en résulte par le théorème d'inversion locale qu'il existe un voisinage U de 0 dans $\mathfrak{g}$ et un voisinage V de 0 dans $\mathfrak{s}$ tels que k soit un difféomorphisme de $U \times V$ vers un voisinage ouvert W de l'identité dans $\mathbf{GL}(n,\mathbb{R})$.

Pour tout $a \in W$, posons $k^{-1}(a) = F(a) + G(a)$, avec $F(a) \in U$ et $G(a) \in V$. Si $G(a) = 0$, alors $a = \phi(F(a))\psi(0) = \phi(F(a))$ est dans G.

Soit $(X,Y) \in U \times V$ et posons $a = k(X + Y)$. Alors pour tout $Z \in \mathfrak{g}$ et pour tout τ dans un voisinage de 0 suffisamment petit, on a

$$G(\phi(X + \tau Z)\psi(Y)) = Y.$$

En différenciant en $\tau = 0$, on obtient

$$0 = dG_a(d\phi_X(Z)\psi(Y)) = dG_a(d\phi_X(Z)\phi(X)^{-1}a). \tag{VI.3.1}$$

La courbe

$$\tau \mapsto \phi(X + \tau Z)\phi(X)^{-1}$$

est une courbe différentiable dans G, valant Id en 0, dont la dérivée en 0 est

$$\frac{d}{d\tau}\left(\phi(X + \tau Z)\phi(X)^{-1}\right)_{|\tau=0} = d\phi_X(Z)\phi(X)^{-1}.$$

Ceci montre que $d\phi_X(Z)\phi(X)^{-1} \in \mathfrak{g}$.

Définissons $A_X : \mathfrak{g} \to \mathfrak{g}$, $A_X(Z) = d\phi_X(Z)\phi(X)^{-1}$. C'est une application linéaire qui dépend continûment de X. En $X = 0$, A_X est l'identité de $\mathfrak{g}$, car $\phi(0) = \mathrm{Id}_n$ et $d\phi_0(Z) = Z$. En particulier, $\det A_0 \neq 0$. Par continuité, $\det A_X \neq 0$ pour X dans un voisinage de 0 dans $\mathfrak{g}$. Quitte à réduire U, on peut supposer que tel est le cas pour tous les X dans U.

L'équation (VI.3.1) donne alors

$$0 = dG_a(A_X(Z)a)$$

pour tout X et tout Z suffisamment proches de 0 dans $\mathfrak{g}$. L'application linéaire A_X étant inversible pour X dans U, ceci peut se réécrire

$$0 = dG_a(Za) \tag{VI.3.2}$$

pour tout Z suffisamment proche de 0 dans $\mathfrak{g}$.

Montrons maintenant que exp envoie $\mathfrak{g}$ dans G. Soit $Z \in \mathfrak{g}$ et posons $b(\tau) = \exp \tau Z$. Pour τ suffisamment proche de 0, $b(\tau)$ est dans W, et donc (VI.3.2) en $b(\tau)$ donne

$$0 = dG_{b(\tau)}(Zb(\tau)) = \frac{d}{d\tau} G(b(\tau))_{|\tau=0}.$$

La fonction $\tau \mapsto G(b(\tau))$ est constante dans un voisinage de 0. Comme en $\tau = 0$ on a $G(b(0)) = 0$, cette constante est nulle. Ceci montre que $b(\tau) \in G$. Il reste à étendre cette relation à tout $\tau \in \mathbb{R}$. Mais comme pour tout entier k

$$\exp tX = \left(\exp(\frac{t}{k}X)\right)^k,$$

ceci est facilement établi. □

Corollaire VI.3.9. — *L'algèbre de Lie $\mathfrak{g}$ d'un groupe linéaire G dans $\mathbf{GL}(n, \mathbb{R})$ est l'ensemble des éléments X dans $M_n(\mathbb{R})$ tels que $\exp tX \in G$ pour tout $t \in \mathbb{R}$.*

Démonstration. Une inclusion provient du théorème, et l'autre de la définition de $\mathfrak{g}$ en considérant les courbes $t \mapsto \exp tX$. □

Corollaire VI.3.10. — *Il existe un ouvert $\mathcal{U}$ contenant l'identité dans $\mathbf{GL}(n, \mathbb{R})$ tel que tout élément g dans $\mathcal{U}$ qui appartient à G pouvant être relié dans G à l'identité par un chemin différentiable restant dans $\mathcal{U}$ est de la forme $g = \exp X$ pour un certain $X \in \mathfrak{g}$.*

Démonstration. Soit $a(t)$, $t \in [0,1]$ le chemin mentionné. Alors $a'(t)a(t)^{-1}$ est dans $\mathfrak{g}$, car c'est le vecteur tangent en l'identité à la courbe

$$s \mapsto a(t+s)a(t)^{-1}.$$

Il s'ensuit que $a'(t) \in \mathfrak{g}a(t)$ pour tout t. En reprenant l'argument de la démonstration du théorème, on voit que ceci entraîne que $G(a(t))$ est identiquement nul. On peut aussi, dans l'argument de cette démonstration, prendre $\phi :\ Y \mapsto \exp Y$. On obtient

$$a(t) = \phi(\exp X(t))\psi(0) = \exp X(t)$$

où $X(t) = F(a(t))$. □

Remarque VI.3.11. — Cette propriété de l'exponentielle est subtile. Il se trouve des groupes linéaires dans $\mathbf{GL}(n,\mathbb{R})$ tel que tout voisinage de l'identité contienne des éléments de G qui ne sont pas dans l'image de l'exponentielle (exemple : $\mathbb{Q}^\times$ dans $\mathbb{R}^\times$). Il existe aussi des groupes linéaires dont l'application exponentielle est surjective, et malgré cela, possédant des éléments arbitrairement proche de l'identité ne pouvant être relié à celle-ci par un chemin différentiable dans G restant proche de l'identité (voir l'exemple suivant).

Exemple VI.3.12. — **La droite dans le tore.** L'algèbre de Lie du groupe $\mathbf{U}(1) = \{z \in \mathbb{C}, |z| = 1\}$ est $i\mathbb{R}$. L'application exponentielle $\exp : i\mathbb{R} \to U(1)$ est dans ce cas un morphisme de groupes, de noyau $2\pi\mathbb{Z}$. Le tore $\mathbb{T} = \mathbb{T}^2$ est la sous-variété $U(1) \times U(1)$ de $\mathbb{C} \times \mathbb{C}$, que l'on voit comme groupe linéaire par $(z_1, z_2) \mapsto \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} \in \mathbf{GL}(2,\mathbb{C})$. Son algèbre de Lie est $\mathfrak{t} \simeq i\mathbb{R} \times i\mathbb{R}$. Soit $X = \begin{pmatrix} i\alpha & 0 \\ 0 & i\beta \end{pmatrix} \in \mathfrak{t}$. Cet élément définit un sous-groupe à un paramètre L de $\mathbb{T}$:

$$t \mapsto \exp tX = \begin{pmatrix} e^{2\pi i\alpha} & 0 \\ 0 & e^{2\pi i\beta} \end{pmatrix}.$$

La nature du sous-groupe à un paramètre L ainsi défini dépend du rapport α/β. Pour simplifier, nous supposons $\alpha > 0$, $\beta > 0$.

Si α/β est rationnel, disons $\alpha/\beta = p/q$ avec p et q premier entre eux, alors L est une courbe fermée dans $\mathbb{T}$, dont la première composante décrit p rotations, tandis que la seconde en décrit q. On a $L \simeq \mathbb{R}/\frac{p}{\alpha}\mathbb{Z}$. Le groupe L est un sous-groupe fermé de $\mathbf{GL}(2,\mathbb{C})$. La topologie induite sur L par celle de $\mathbf{GL}(2,\mathbb{C})$ coïncide la topologie quotient de $\mathbb{R}/\frac{p}{\alpha}\mathbb{Z}$.

Si α/β est irrationnel, alors $t \mapsto \exp tX$ est injective et L est dense dans $\mathbb{T}$. La topologie induite par celle de $\mathbf{GL}(2,\mathbb{C})$ ne coïncide pas avec celle, intrinsèque donnée par l'isomorphisme $L \simeq \mathbb{R}$. En effet, un élément de L peut être très proche de Id pour la topologie induite, mais un chemin dans L le reliant à Id peut devoir faire plusieurs tours du tore.

Remarque VI.3.13. — Une conséquence du théorème VI.3.8, tenant compte de la remarque VI.2.9, est que le produit dans un groupe linéaire, au voisinage de l'identité, est déterminé par la structure de son algèbre de Lie.

La définition d'un groupe linéaire G comme sous-groupe de $\mathbf{GL}(n,\mathbb{R})$ pour un certain n munit G d'une topologie, la **topologie induite** qui en fait un groupe topologique. D'autre part, nous avons montré que l'exponentielle envoie $\mathfrak{g}$ dans G. Comme $\mathfrak{g}$ est naturellement en tant qu'espace vectoriel complexe de dimension finie un espace topologique (un espace de Banach de dimension finie), on peut se servir de l'exponentielle pour munir G d'une autre topologie, la **topologie intrinsèque**. Une base de voisinages de Id est obtenue en prenant des voisinages de la forme $\exp U$, où U est un voisinage de 0 suffisamment petit dans $\mathfrak{g}$ (dans le domaine où l'exponentielle est injective). Par translation, nous obtenons une base de voisinages en chaque point de G, qui fait encore de G un groupe topologique. Dans cette topologie, au voisinage de chaque point, G “ressemble” à l'espace vectoriel $\mathfrak{g}$. En termes technique, G est muni d'une **structure de variété différentiable**. Ceci permet de définir sur G la notion de fonction différentiable, par exemple. Le produit et le passage à l'inverse sont alors différentiables (et même $\mathcal{C}^\infty$), on dit alors que G est un **groupe de Lie**.

La question évidente qui se pose alors est celle de la comparaison de ces deux topologies. Prenons un premier exemple, celui de l'inclusion de $\mathbb{Q}^\times$ dans $\mathbb{R}^\times = \mathbf{GL}(1, \mathbb{R})$, qui fait de $\mathbb{Q}^\times$ un groupe linéaire. Comme $\mathbb{Q}^\times$ est d'intérieur vide dans $\mathbb{R}^\times$, on voit que son algèbre de Lie est réduite à $\{0\}$. La topologie intrinsèque de $\mathbb{Q}^\times$ est donc discrète, et ne coïncide pas avec la topologie induite, qui est moins fine.

Un deuxième exemple est celui de la droite dans le tore VI.3.12. La topologie intrinsèque ne coïncide pas avec la topologie induite, qui là encore est moins fine.

C'est une conséquence directe des définitions que la topologie intrinsèque est toujours plus fine que la topologie induite, puisque l'exponentielle est continue. Le résultat suivant donne un critère simple pour les deux topologies coïncident.

Théorème VI.3.14. — *Soit G un groupe linéaire, muni de sa topologie intrinsèque. Soit H un sous-groupe fermé de G. Soit $\mathfrak{s}$ un supplémentaire de $\mathfrak{h}$ dans $\mathfrak{g}$. Alors il existe un voisinage U de 0 dans $\mathfrak{s}$ tel que l'application*

$$\Psi : H \times U \to G, \quad (h, X) \mapsto h \exp X$$

réalise un difféomorphisme de $H \times U$ dans un voisinage de H dans G.

<u>Démonstration</u>. Dans cet énoncé, H est bien entendu muni de sa topologie intrinsèque qui en fait un groupe de Lie, sinon, on ne pourrait pas parler de difféomorphisme. Montrons tout d'abord que la différentielle de Ψ est inversible en chaque point (h, X) avec X dans un voisinage de 0 dans $\mathfrak{s}$. Par translation à gauche par h^{-1}, il suffit de le montrer aux points (Id, X), et par continuité, il suffit de le démontrer pour le point $(\mathrm{Id}, 0)$. Mais en ce point, la différentielle est simplement :

$$\mathfrak{h} \times \mathfrak{s} \to \mathfrak{g}, \quad (X, Y) \mapsto X + Y$$

qui est inversible puisque $\mathfrak{h} \oplus \mathfrak{s} = \mathfrak{g}$. Il découle du théorème d'inversion locale que l'application

$$H \times U \to G, \quad (h, X) \mapsto h \exp X$$

est un difféomorphisme *local* sur un voisinage de H dans G, c'est-à-dire que pour tout point (h, Y) dans $H \times U$, il existe un voisinage ouvert $\mathcal{V}_{h,Y}$

de (h, Y) dans $H \times U$ tel que Ψ réalise un difféomorphisme de $\mathcal{V}_{h,Y}$ sur son image.

Il suffit de montrer qu'en prenant U plus petit, on peut faire en sorte que l'application ci-dessus devienne injective, et réalise ainsi un difféomorphisme sur son image. Supposons que tel ne soit pas le cas, c'est à dire que pour tout voisinage V de 0 dans $\mathfrak{s}$, on puisse trouver h_1, h_2 dans H et X_1, X_2 dans V avec $X_1 \neq X_2$ tels que

$$h_1 \exp X_1 = h_2 \exp X_2.$$

Alors $\exp X_1 \exp(-X_2) \in H$. Comme

$$\psi : \mathfrak{h} \times \mathfrak{s} \to G, \quad (X, Y) \mapsto \exp X \exp Y$$

est de différentielle inversible en $(0, 0)$, ψ réalise un difféomorphisme d'un voisinage W de $(0, 0)$ sur son image $\psi(W)$, qui est un ouvert contenant l'identité dans G. On voit que pour V assez petit, $\exp X_1 \exp -X_2 \in \psi(W)$ s'écrit de manière unique

$$\exp X_1 \exp -X_2 = \exp X \exp Y$$

avec $(X, Y) \in V$. On en déduit que l'on a $\exp Y \in H$. D'autre part, $Y \neq 0$, sinon l'égalité $\exp X_1 \exp -X_2 = \exp X$ donnerait

$$\exp X \exp X_2 = \exp X_1$$

et par unicité de l'écriture, $X_1 = X_2$. On voit donc ainsi que l'on peut trouver des $Y \neq 0$ dans $\mathfrak{s}$ aussi proche de 0 que l'on veut vérifiant $\exp Y \in H$. Soit une suite Y_k d'éléments non nuls vérifiant ces hypothèses et tendant vers 0. La suite $\frac{Y_k}{||Y_k||}$ est bornée dans $\mathfrak{s}$ (on a choisi une norme quelconque sur $\mathfrak{s}$), et quitte à extraire une sous-suite, on peut supposer qu'elle converge. La limite est un élément Y de $\mathfrak{s}$ et de norme 1, donc non nul.

Fixons $t \in \mathbb{R}$. Prenons des entiers $n_k \in \mathbb{R}$ tels que $n_k ||Y_k|| \to t$ (il suffit de prendre n_k tel que $n_k ||Y_k|| \leq t < (n_k + 1)||Y_k||$). On a alors :

$$(\exp Y_k)^{n_k} = \exp n_k Y_k = \exp n_k ||Y_k|| \frac{Y_k}{||Y_k||} \to \exp tY$$

Ceci montre, comme H est fermé, que $\exp tY \in H$ pour tout $t \in \mathbb{R}$. En conséquence, $Y \in \mathfrak{h}$, et comme $\mathfrak{s} \cap \mathfrak{h} = \{0\}$, $Y = 0$: contradiction. $\square$

Corollaire VI.3.15. — *Soit G un groupe linéaire et soit H un sous-groupe fermé de G. Alors les topologies intrinsèque et induite de H coïncident, c'est-à-dire que tout ouvert de H est l'intersection d'un ouvert de G avec H.*

Démonstration. Soit $h \in H$. Une base de voisinages de h dans G est donnée par des ouverts de la forme $h \exp V$, où V est un voisinage de 0 suffisamment petit dans $\mathfrak{g}$. Le théorème montre que pour V suffisamment petit, l'intersection de ce voisinage avec H est de la forme $h \exp U$, où $U = \mathfrak{h} \cap V$ est un voisinage de 0 dans $\mathfrak{h}$. $\square$

VI.4. Ad, ad

Soit G un groupe linéaire. G agit sur lui-même par conjugaison, et nous notons Ad cette action :

$$\mathrm{Ad}(x) \cdot y = xyx^{-1}, (x, y \in G).$$

Différentions cette action en l'identité : pour tout $Y \in \mathfrak{g}$

$$d\mathrm{Ad}(x)_{\mathrm{Id}}(Y) = \frac{d}{dt}\left(x(\exp tY)x^{-1}\right)_{t=0} = \frac{d}{dt}\left(\exp(t\, xYx^{-1})\right)_{t=0} = xYx^{-1}$$

Ceci définit une application linéaire, encore notée $\mathrm{Ad}(x)$

$$\mathrm{Ad}(x) : \mathfrak{g} \to \mathfrak{g}, \quad Y \mapsto xYx^{-1}.$$

Cette application linéaire est un morphisme d'algèbres de Lie. En effet

$$\begin{aligned} \mathrm{Ad}(x)([Y, Z]) &= x(YZ - ZY)x^{-1} \\ &= (xYx^{-1})(xZx^{-1}) - (xZx^{-1})(xYx^{-1}) \\ &= [\mathrm{Ad}(x)(Y), \mathrm{Ad}(x)(Z)]. \end{aligned}$$

D'autre part, $\mathrm{Ad}(x)$ est inversible, d'inverse $\mathrm{Ad}(x^{-1})$. Ceci montre que

$$\mathrm{Ad} : G \to \mathbf{Aut}(\mathfrak{g}) \subset \mathbf{GL}(\mathfrak{g}).$$

est une application de G dans le groupe des automorphismes d'algèbres de Lie de $\mathfrak{g}$. Il est facile de voir que c'est un morphisme de groupes. En particulier, Ad est une représentation de G dans l'espace $\mathfrak{g}$. On l'appelle représentation adjointe.

On peut différencier Ad en l'identité. Pour tout $X \in \mathfrak{g}$:

$$dAd_{\mathrm{Id}} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$$
$$X \mapsto \left[Y \mapsto \frac{d}{dt} \left(\mathrm{Ad}(\exp tX).Y\right)_{t=0} \right] = XY - YX = [X, Y]$$

On note $\mathrm{ad} = d\mathrm{Ad}_{\mathrm{Id}}$. Ainsi $\mathrm{ad}(X)(Y) = [X, Y]$. L'identité de Jacobi entraîne que quels que soient $X, Y, Z \in \mathfrak{g}$

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

ce qui montre que ad est un morphisme d'algèbre de Lie de $\mathfrak{g}$ dans $\mathfrak{gl}(\mathfrak{g})$.

D'autre part, toujours par l'identité de Jacobi, quels que soient X, Y, Z dans $\mathfrak{g}$

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

Définition VI.4.1. — Une application linéaire $A : \mathfrak{g} \to \mathfrak{g}$ vérifiant

$$A([Y, Z]) = [A(Y), Z] + [Y, A(Z)].$$

est appelée dérivation de l'algèbre de Lie $\mathfrak{g}$.

Exercice VI.4.2. — Montrer que l'algèbre de Lie du groupe $\mathbf{Aut}(\mathfrak{g})$ est l'algèbre de Lie $\mathbf{Der}(\mathfrak{g})$ des dérivations de $\mathfrak{g}$.

Exercice VI.4.3. — Montrer que pour tout $X \in \mathfrak{g}$,

$$\mathrm{Ad}(\exp X) = \exp(\mathrm{ad}(X)).$$

Exercice VI.4.4. — **Calcul de la différentielle de** $\exp$**.**

Posons, pour $X, Y \in \mathfrak{g}$ et $s, t \in \mathbb{R}$,

$$A_{s,t}(X, Y) = \exp(-sX) \frac{\partial}{\partial t}(\exp(s(X + tY))).$$

Calculer $\frac{\partial}{\partial s} A_{s,t}(X, Y)$. En déduire que

$$\frac{\partial}{\partial s} A_{s,0}(X, Y) = \exp(-s\,\mathrm{ad}(X)) \cdot Y,$$

puis que

$$A_{1,0}(X,Y) = \int_0^1 \exp(-s\,\mathrm{ad}(X)) \cdot Y\ ds = \left(\frac{1-\exp(-\mathrm{ad}(X))}{\mathrm{ad}(X)}\right) \cdot Y.$$

Conclure que $(d\exp)_X = \exp(X)\frac{1-\exp(-\mathrm{ad}(X))}{\mathrm{ad}(X)}$.

VI.5. Connexité et correspondance de Lie

Comme nous l'avons vu dans l'exercice VI.3.4, les groupes finis sont linéaires. Or, il est clair d'après la définition que l'algèbre de Lie d'un groupe fini est l'espace vectoriel nul $\{0\}$. En fait, et on le comprend bien en regardant la définition, l'algèbre de Lie d'un groupe linéaire ne dépend que de la composante connexe du groupe contenant l'identité (pour un groupe fini, cette composante connexe est $\{\mathrm{Id}\}$). Il existe plusieurs notions de connexité en topologie (connexité, connexité par arcs...). Pour les groupes linéaires, elles coïncident toutes, comme le montre le résultat suivant

Proposition VI.5.1. — *Soit G un groupe linéaire, muni de sa topologie intrinsèque. Les conditions suivantes sont équivalentes :*

(i) *Deux éléments quelconques de G peuvent être reliés par un chemin continu.*

(ii) *G n'est pas l'union de deux ouverts disjoints non vides.*

(iii) *G est engendré par un voisinage quelconque de* Id.

(iv) *G est engendré par* $\exp U$*, pour tout voisinage U de* 0 *dans* $\mathfrak{g}$.

Si ces conditions sont vérifiées, on dit que G est connexe.

Démonstration. (i) $\Rightarrow$ (ii) Supposons (i) et soient U et V deux ouverts disjoints non vides dont la réunion est G. Alors un chemin continu reliant un élément de U à un élément de V donnerait une partition de l'intervalle de définition du chemin en deux ouverts non vides disjoints, contradiction.

(ii) $\Rightarrow$ (iii) Supposons (ii) et soit G_0 le sous-groupe de G engendré par un voisinage de Id dans G. Alors G_0 est ouvert dans G, car il contient un voisinage de chacun de ses points (c'est clair pour Id, et pour tout autre point par translation). De même, chaque partie de la forme gG_0, $g \in G$, est ouverte dans G. Comme G peut être décomposé en une union disjointe de telles classes à gauche, l'hypothèse entraîne que $G = G_0$.

$(iii) \Rightarrow (iv)$ est clair car $\exp U$ est un voisinage de Id, d'après la définition de la topologie intrinsèque.

$(iv) \Rightarrow (i)$ Si l'on suppose (iv), alors tout élément g de G peut se mettre sous la forme

$$g = \exp X_1 \exp X_2 \ldots \exp X_k,$$

les X_i étant dans U. En particulier, étant donnés deux éléments a_0 et a_1 dans G, on peut écrire

$$a_1 = a_0 \exp X_1 \exp X_2 \ldots \exp X_k.$$

On prend alors $a(t) = a_0 \exp tX_1 \exp tX_2 \ldots \exp tX_k$. C'est un chemin continu dans G vérifiant $a(0) = a_0$, $a(1) = a_1$. □

Corollaire VI.5.2. — *Soit G un groupe linéaire, d'algèbre de Lie $\mathfrak{g}$. Alors la composante neutre G_0 de G (c'est-à-dire la composante connexe de G contenant* Id*) est le sous-groupe de G engendré par* $\exp \mathfrak{g}$*. C'est un sous-groupe ouvert, fermé, distingué de G et c'est le seul sous-groupe ouvert connexe de G. La composante connexe d'un élément g de G est la classe à droite gG_0.*

<u>Démonstration</u>. La première assertion est claire d'après la démonstration de la proposition. Le reste se vérifie facilement.

Définition VI.5.3. — Le groupe quotient G/G_0 est appelé groupe des composantes connexes de G.

Exercice VI.5.4. — **Composantes connexes de $\mathbf{O}(2,1)$**
Le groupe $\mathbf{O}(2,1)$ est-il connexe ?

Rappelons que $\mathbf{O}(2,1)$ est le sous-groupe de $\mathbf{GL}(3,\mathbb{R})$ préservant la forme bilinéaire symétrique non-dégénérée de $\mathbb{R}^3$

$$(x,y) = x_1y_1 + x_2y_2 - x_3y_3.$$

Soit $\mathcal{C}$ le cône $\{x \in \mathbb{R}^3 |\, (x,x) = 0\}$. Montrer que $\mathbb{R}^3$ est l'union disjointe de

- $\mathcal{C}$
- $A = \{x \in \mathbb{R}^3 |\, (x,x) > 0\}$
- $B^+ = \{x \in \mathbb{R}^3 |\, (x,x) < 0, (x,e_3) > 0\}$
- $B^-\{x \in \mathbb{R}^3 |\, (x,x) < 0, (x,e_3) < 0\}$

Soit $a \in \mathbf{SO}(2,1)$. Montrer que les conditions suivantes sont équivalentes :

(i) a stabilise chacun des ensembles A, B^+, B^-.

(ii) a stabilise B^+.

(iii) $(ae_3, e_3) < 0$.

Le groupe $\mathbf{SO}(2,1)$ est-il connexe ?

Soit $\mathbf{SO}_0(2,1)$ le sous-groupe des éléments de $\mathbf{SO}(2,1)$ vérifiant ces conditions équivalentes. On veut maintenant montrer que $\mathbf{SO}_0(2,1)$ est la composante neutre de $\mathbf{SO}(2,1)$ et de $\mathbf{O}(2,1)$. Pour cela, introduisons les transformations linéaires suivantes de $\mathbb{R}^3$:

- les *rotations euclidiennes*. On fixe deux vecteurs u et v de $\mathbb{R}^3$ vérifiant

$$(u,u) = 1, \quad (v,v) = 1, \quad (u,v) = 0$$

et $\alpha \in \mathbb{R}$. On pose

$$\begin{aligned} a(u) &= \cos\alpha\, u - \sin\alpha\, v \\ a(v) &= \sin\alpha\, u + \cos\alpha\, v \\ a(x) &= x \text{ si } (x,u) = 0, (x,v) = 0 \end{aligned}$$

- les *rotations hyperboliques*. On fixe deux vecteurs u et v de $\mathbb{R}^3$ vérifiant

$$(u,u) = 1, \quad (v,v) = -1, \quad (u,v) = 0$$

et $\alpha \in \mathbb{R}$. On pose

$$\begin{aligned} a(u) &= \cosh \alpha\, u + \sinh \alpha\, v \\ a(v) &= \sinh \alpha\, u + \cosh \alpha\, v \\ a(x) &= x \text{ si } (x, u) = 0, (x, v) = 0 \end{aligned}$$

Montrer que les rotations euclidiennes et hyperboliques sont dans le groupe $\mathbf{SO}_e(2,1)$, puis que tout élément de $\mathbf{SO}_e(2,1)$ s'écrit $a = kh$ où k est une rotation euclidienne d'axe e_3 et h une rotation hyperbolique dans un plan contenant e_3.

Théorème VI.5.5. — *(***Correspondance de Lie***) Il existe une bijection entre les sous-groupes connexes de* $\mathbf{GL}(n, \mathbb{R})$ *et les sous-algèbres de Lie de* $\mathfrak{gl}(n, \mathbb{R})$ *donnée par*

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

dont l'inverse est $\mathfrak{g} \mapsto \Gamma(\mathfrak{g})$*, où* $\Gamma(\mathfrak{g})$ *est le sous-groupe de* $\mathbf{GL}(n, \mathbb{R})$ *engendré par* $\exp \mathfrak{g}$*.*

Démonstration. Nous avons déjà démontré que si G est connexe, $\Gamma(\mathfrak{g}) = G$. Il reste à voir que $\mathfrak{g} = \mathrm{Lie}(\Gamma(\mathfrak{g}))$ pour toute sous-algèbre de Lie $\mathfrak{g}$ de $\mathfrak{gl}(n, \mathbb{R})$. Il est clair que $\mathfrak{g} \subset \mathrm{Lie}(\Gamma(\mathfrak{g}))$ car $\exp tX \in \Gamma(\mathfrak{g})$ pour tout $t \in \mathbb{R}$ et tout $X \in \mathfrak{g}$.

Plaçons nous dans un voisinage U_1 de 0 dans $\mathfrak{g}$ où l'exponentielle réalise un homéomorphisme sur une partie V_1 contenant l'identité dans $\Gamma(\mathfrak{g})$, l'inverse étant donné par le log (voir Exercice VI.2.8)

Prenons un ouvert $U \subset U_1$, tel que la fonction

$$C : \bar{U} \times \bar{U} \to \mathfrak{g}, \quad (X, Y) \mapsto \log(\exp X \exp Y)$$

est bien définie ($C(X, Y)$ est donnée par la série de Baker-Campbell-Hausdorff). De plus, on peut prendre pour U une boule ouverte de centre 0, de sorte que $\bar{U}$ est une boule fermée, donc compacte. Enfin, on suppose que $\exp U \exp U \subset V_1$. Posons $W = C(U, U)$, de sorte que $\exp W = \exp U \exp U$. Comme $C(0, Y) = Y$, la fonction $Y \mapsto C(0, Y)$ à une différentielle de rang $\dim \mathfrak{g}$ en $Y = 0$, et par continuité, la fonction $Y \mapsto C(X, Y)$ à la même propriété pour X suffisamment proche de 0. Le théorème d'inversion locale implique alors que $Y \mapsto C(X,Y)$ est inversible dans un voisinage de 0 et donc $C(X,U)$ est un voisinage de X dans $\mathfrak{g}$ si X est suffisamment petit. Quitte à restreindre encore U, on peut supposer que tel est le cas pour tout X dans U. Soit $\mathcal{O}(X,U)$ un ouvert contenant X et contenu dans $C(X,U)$. L'ensemble $\bar{W} := C(\bar{U},\bar{U}) = \exp \bar{U} \exp \bar{U}$ est recouvert par les $\mathcal{O}(X,U)$, $X \in \bar{W}$. Comme $\bar{W}$ est l'image d'un compact par une application continue, c'est un compact, et nous pouvons donc extraire un nombre fini d'ouverts $\mathcal{O}(X_i,U)$, $i = 1,\dots,k$ recouvrant $\bar{W}$. Ecrivons $\exp X_i = a_i a_i'$ avec $a_i, a_i' \in \exp \bar{U}$ pour chaque i et prenons l'image par exp de l'inclusion

$$\bar{W} \subset \bigcup_{i=1,\dots k} \mathcal{O}(X_i,U) \subset \bigcup_{i=1,\dots k} C(X_i,U),$$

pour obtenir

$$\exp \bar{U} \exp \bar{U} \subset \bigcup_{i=1,\dots k} a_i a_i' \exp U.$$

L'ensemble des produits finis d'éléments parmi les a_i, a_i', avec répétitions, est dénombrable. Notons-le $\{b_j\}_{j\in\mathbb{N}}$. On obtient facilement par récurrence que

$$(\exp \bar{U})^k \subset \bigcup_{j\in\mathbb{N}} b_j \exp \bar{U},$$

où $(\exp \bar{U})^k$ est l'ensemble des produits de k éléments de $\exp \bar{U}$. Ceci montre que

$$\Gamma(\mathfrak{g}) = \bigcup_{j\in\mathbb{N}} b_j \exp \bar{U} \tag{VI.5.1}$$

où $b_j \in \Gamma(\mathfrak{g})$.

Nous allons utiliser maintenant un résultat de topologie générale :

Lemme VI.5.6. — (**Lemme de recouvrement de Baire**) *Soit G un groupe linéaire et soit $(A_i)_i$ une famille dénombrable de sous-ensembles de G telle que $G = \bigcup_j A_j$. Alors l'adhérence de l'un des A_j contient un ouvert de G.*

Nous démontrerons ce résultat par la suite. Finissons tout d'abord la démonstration du théorème en appliquant le lemme à $\Gamma(\mathfrak{g})$. L'application du lemme de recouvrement de Baire montre que l'une des parties $b_j \exp \bar{U}$

est voisinage de l'un de ses points, disons a_0. Prenons un ouvert $U' \subset U$ de Lie($\Gamma(\mathfrak{g})$) suffisamment petit de sorte que $\exp U'$ soit ouvert dans $\Gamma(\mathfrak{g})$ et que $a_0 \exp U' \subset b_j \exp \bar{U}$. Réécrivons ceci :

$$\exp U' \subset c \exp \bar{U}$$

où $c = a_0^{-1} b_j$. Pour tout $X' \in U'$, il existe $X \in \bar{U}$ tel que $\exp X' = c \exp X$. Comme X est suffisamment proche de 0, il est donné par

$$X = \log(c^{-1} \exp X').$$

En remplaçant X' par tX', $t \in [0, 1]$, on écrit

$$\exp tX' = c \exp X(t),$$

avec $X(t) \in \bar{U}$ qui dépend différentiablement de t. En $t = 0$, on trouve $c = \exp -X(0)$ et donc

$$\exp tX' = \exp -X(0) \exp X(t).$$

En différenciant en $t = 0$, on obtient (voir exercice VI.4.4)

$$X' = \frac{\mathrm{Id} - \exp(-\mathrm{ad}(X(0)))}{\mathrm{ad}(X(0))} X'(0)$$

qui est dans $\mathfrak{g}$ car $X(0)$, $X'(0)$ sont dans $\mathfrak{g}$ et $\mathfrak{g}$ est une algèbre de Lie. Donc le voisinage U' de 0 dans Lie($\Gamma(\mathfrak{g})$) est dans $\mathfrak{g}$, et donc Lie($\Gamma(\mathfrak{g}) \subset \mathfrak{g}$.

Ceci termine la démonstration du théorème. □

Nous passons maintenant à la démonstration du lemme. Posons $\mathfrak{g} =$ Lie(G). Remarquons tout d'abord que nous pouvons supposer les A_j fermés. Nous raisonnons par l'absurde. Si aucun A_j ne contient un ouvert de G, le complémentaire de A_1 est non vide, et donc, étant ouvert, il contient une partie de la forme $a_1 \exp B_1$ où B boule fermée de centre 0 dans $\mathfrak{g}$, de rayon suffisamment petit de sorte que l'exponentielle réalise un difféomorphisme de B_1 sur son image. Pour la même raison, le complémentaire de A_2 dans $a \exp B_1$ est un ouvert de G contenu dans $a \exp B_1$, et contient donc une partie de la forme $a \exp B_2$, où B_2 est une boule fermée de $\mathfrak{g}$ contenue dans B_1 (mais non nécessairement centrée en 0)... On construit ainsi une suite

$$\ldots B_n \subset B_{n-1} \ldots \subset B_1.$$

L'intersection des B_i est non vide, mais n'intersecte aucun des A_j : contradiction. $\square$

La correspondance de Lie fournit un dictionnaire entre les groupes linéaires connexes et les algèbres Lie de matrices. Nous allons donner quelques exemples :

Corollaire VI.5.7. — *Soit G un groupe linéaire connexe d'algèbre de Lie $\mathfrak{g}$. Alors G est abélien si et seulement si $\mathfrak{g}$ est abélienne (c'est-à-dire que le crochet de Lie est toujours nul).*

Démonstration. C'est clair d'après l'exercice VI.2.3. $\square$

Proposition VI.5.8. — *Tout groupe linéaire connexe abélien est isomorphe à $\mathbb{R}^m \times \mathbb{T}^k$ pour un certain $m \in \mathbb{N}$ et un certain $k \in \mathbb{N}$.*

Démonstration. Soit A un tel groupe, et soit $\mathfrak{a}$ son algèbre de Lie. Comme $\mathfrak{a}$ est abélienne, l'exponentielle est un morphisme de groupes, et donc $\exp \mathfrak{a}$ est un sous-groupe de A. Comme A est connexe, $A = \exp \mathfrak{a}$. Soit $L = \ker \exp$. C'est un sous-groupe discret de $\mathfrak{a}$, puisque l'exponentielle est un difféomorphisme au voisinage de 0. Le lemme qui suit donne la forme d'un tel sous-groupe discret, ce qui permet de terminer aisément la démonstration. $\square$

Lemme VI.5.9. — *Soit V un espace vectoriel réel de dimension finie n et L un sous-groupe discret de V. Alors il existe une base $u_1, u_2, \dots u_n$ de V et un entier $k \leq n$ tels que*

$$L = \mathbb{Z}u_1 + \dots \mathbb{Z}u_k.$$

Démonstration. La démonstration se fait par récurrence. On considère un sous-espace W de V tel que $L \cap W = \mathbb{Z}u_1 + \dots \mathbb{Z}u_m$ pour un certain entier $m \leq n$, où $(u_1, \dots, u_m)$ est une famille libre. Ceci existe car on peut commencer avec $W = \{0\}$ et $m = 0$. Supposons que L ne soit pas inclus dans W et soit $u \in L$, $u \notin W$. Considérons l'ensemble des points de V de la forme

$$\alpha_1 u_1 + \dots \alpha_m u_m + \alpha u, \quad 0 \leq \alpha_i \leq 1,\ 0 \leq \alpha \leq 1$$

C'est un ensemble fermé borné de V qui intersecte L. Il ne contient qu'un nombre fini d'éléments du groupe discret L. Parmi ces éléments, choisissons-en un tel que le coefficient α soit minimal, non nul (de tels éléments existent, par exemple u), et appelons-le u_{m+1}. Alors tout élément de L dans $W \oplus \mathbb{R}u = W \oplus \mathbb{R}u_{m+1}$ a pour composante sur $\mathbb{R}u_{m+1}$ un multiple entier de u_{m+1}. En effet, supposons le contraire : soit

$$l = \beta_1 u_1 + \dots \beta_m u_m + \beta u_{m+1} \in L$$

avec $\beta = k + \nu$, $k \in \mathbb{Z}$, $0 < \nu < 1$. On peut réécrire ceci sous la forme

$$l = \gamma_1 u_1 + \dots \gamma_m u_m + (k + \nu)\alpha u$$

et en ajoutant un élément bien choisi de L, on trouve $l' \in L$ de la forme

$$l' = \gamma'_1 u_1 + \dots \gamma'_m u_m + \nu\alpha u$$

avec $0 \leq \gamma'_i \leq 1$. Comme $0 < \nu\alpha < \alpha$, ceci contredit la minimalité de α. Tout ceci montre que

$$L \cap (W \oplus \mathbb{R}u) = (L \cap W) \oplus \mathbb{Z}u_{m+1}.$$

On répète l'argument jusqu'à obtenir $u_1, \dots, u_k$ comme dans le lemme.

□

En exercice, nous allons maintenant voir d'autres exemples de la correspondance de Lie.

Exercice VI.5.10. — Soit G un groupe linéaire connexe d'algèbre de Lie $\mathfrak{g}$. Montrer qu'un sous-groupe connexe H de G est distingué dans G si et seulement si son algèbre de Lie $\mathfrak{h}$ est un idéal de $\mathfrak{g}$.

Exercice VI.5.11. — Soit G un groupe linéaire connexe d'algèbre de Lie $\mathfrak{g}$. Le sous-groupe dérivé de G, noté (G, G) est le sous-groupe de G engendré par les éléments de la forme $aba^{-1}b^{-1}$, $a, b \in G$. L'algèbre dérivée de $\mathfrak{g}$, notée $[\mathfrak{g}, \mathfrak{g}]$ est la sous-algèbre de Lie de $\mathfrak{g}$ engendré par les éléments de la forme $[X, Y]$, $X, Y \in \mathfrak{g}$. Montrer que (G, G) est connexe et que $[\mathfrak{g}, \mathfrak{g}]$ est son algèbre de Lie.

Exercice VI.5.12. — Soit G un groupe linéaire connexe d'algèbre de Lie $\mathfrak{g}$. Si A une est une partie de G et $\mathcal{A}$ une partie de $\mathfrak{g}$, posons

$$Z_G(A) = \{g \in G |\, \mathrm{Ad}(g) \cdot a = a, (\forall a \in A)\}$$

$$Z_{\mathfrak{g}}(A) = \{X \in \mathfrak{g} |\, \mathrm{Ad}(a) \cdot X = X, (\forall a \in A)\}$$

$$Z_G(\mathcal{A}) = \{g \in G |\, \mathrm{Ad}(g) \cdot X = X, (\forall X \in \mathcal{A})\}$$

$$Z_{\mathfrak{g}}(\mathcal{A}) = \{X \in \mathfrak{g} |\, \mathrm{ad}(X) \cdot Y = Y, (\forall Y \in \mathcal{A})\}.$$

Montrer que $Z_G(A)$ est un groupe d'algèbre de Lie $Z_{\mathfrak{g}}(A)$ et que $Z_G(\mathcal{A})$ est un groupe d'algèbre de Lie $Z_{\mathfrak{g}}(\mathcal{A})$.

VI.6. Homomorphismes de groupes linéaires. Revêtements

La correspondance de lie $G \to \mathrm{Lie}(G)$ est fonctorielle, c'est-à-dire qu'elle se prolonge aux morphismes. Les morphismes entre groupes linéaires sont toujours supposés différentiables (pour la structure de variété différentiable donnée par la topologie intrinsèque). Plus précisément :

Théorème VI.6.1. — *Soit $f : G \to H$ un morphisme (différentiable) entre groupes linéaires. Soit $\phi = df_{Id}$ la différentielle de f en* Id. *Alors*

$$\phi : \mathfrak{g} \to \mathfrak{h}$$

est un morphisme d'algèbres de Lie et

$$f(\exp X) = \exp(\phi(X)), \quad (\forall X \in \mathfrak{g})$$

<u>*Démonstration*</u>. C'est encore et toujours la même méthode. Montrons que $f(\exp X) = \exp(\phi(X))$. Posons $a(s) = f(\exp sX)$. On a

$$\begin{aligned}\frac{d}{ds}a(s) &= \frac{d}{dt}f(\exp((s+t)X))_{|t=0} = \frac{d}{dt}f(\exp sX \exp tX)_{|t=0}\\ &= f(\exp sX)\frac{d}{dt}f(\exp tX)_{|t=0} = a(s)\phi(X)\end{aligned}$$

Ceci montre que $a(s)$ vérifie l'équation différentielle $a'(s) = a(s)\phi(X)$, avec condition initiale $a(0) = \mathrm{Id}$. Ceci montre que $a(s) = \exp(s\phi(X))$, et en particulier $f(\exp X) = \exp(\phi(X))$.

Montrons que ϕ est un morphisme d'algèbres de Lie, c'est-à-dire que quels que soient X, Y dans $\mathfrak{g}$,

$$\phi([X,Y]) = [\phi(X), \phi(Y)].$$

On part de l'équation

$$f(\exp tX \exp sY \exp -tX) = \exp t\phi(X)\, \exp s\phi(Y)\, \exp -t\phi(X)$$

que l'on dérive par rapport à s et que l'on évalue en $s = 0$:

$$\phi(\exp tX\, Y\, \exp -tX) = \exp t\phi(X)\, \phi(Y)\, \exp -t\phi(X).$$

On dérive par rapport à t et l'on évalue en $t = 0$:

$$\phi([X,Y]) = [\phi(X), \phi(Y)].$$

□

Corollaire VI.6.2. — *Soit $f : G \to H$ un morphisme différentiable entre groupes linéaires. Soit $\phi = df_{Id}$ la différentielle de f en* Id. *Alors*

(i) $\ker(\phi) = \mathrm{Lie}(\ker f)$,

(ii) *si G n'a qu'un nombre au plus dénombrable de composantes connexes,* $\mathrm{Im}\,(\phi) = \mathrm{Lie}(\mathrm{Im}\, f)$.

Démonstration. (i) $X \in \mathrm{Lie}(\ker f)$ si et seulement si $f(\exp tX) = \mathrm{Id}$ pour tout $t \in \mathbb{R}$. Or $f(\exp tX) = \exp(t\phi(X))$, donc $X \in \mathrm{Lie}(\ker f)$ si et seulement si $\exp(t\phi(X)) = \mathrm{Id}$ pour tout $t \in \mathbb{R}$, c'est-à-dire $\phi(X) = 0$.

(ii) Comme $f(\exp tX) = \exp(t\phi(X))$, on a $\mathrm{Im}\,\phi \subset \mathrm{Lie}(\mathrm{Im}\, f)$. Pour l'inclusion dans l'autre sens, il suffit de voir que $\Gamma(\mathrm{Im}\,\phi)$ contient un ouvert de $\mathrm{Im}\, f$. Ecrivons $G_0 = \bigcup_j A_j$ comme dans l'équation VI.5.1. Comme G n'a qu'un nombre dénombrable de composantes connexes, on peut écrire $G = \bigcup g_k \cdot \bigcup_j A_j = \bigcup_{k,j} g_k A_j$. Ainsi

$$f(G) = \bigcup_{k,j} f(g_k A_j).$$

Comme les parties A_j sont compactes, chaque $f(g_k A_j)$ est compact, donc fermé, et d'après le lemme de recouvrement de Baire, l'un d'eux contient un ouvert de $\mathrm{Im}\,(f)$. □

Soit $f : X \to Y$ une application continue entre deux espaces topologiques. On dit que f est localement surjective (resp. bijective), si pour tout $x \in X$, il existe un voisinage U de x dans X, et un voisinage V de $f(x)$ dans Y tels que la restriction de f à U soit une surjection (resp. bijection) de U dans V.

Corollaire VI.6.3. — *Soit $f : G \to H$ un morphisme différentiable entre groupes linéaires. Soit $\phi = df_{Id}$ la différentielle de f en* Id. *Alors*

(i) f est localement injective (en tout point $g \in G$, il existe un voisinage U de g dans G tel que $f_{|U}$ soit injective) si et seulement si ϕ est injective.

(ii) si G n'a qu'un nombre au plus dénombrable de composantes connexes, et si H est connexe, f est surjective si et seulement si ϕ est surjective.

(iii) f est localement bijective si et seulement si ϕ est bijective. Dans ce cas, $\ker f$ *est un sous-groupe discret de G.*

Démonstration. Les deux premiers points sont clairs d'après le corollaire précédent. En fait, l'assertion de (ii) peut être remplacée par l'assertion que f est localement surjective si et seulement si ϕ est surjective. Ceci montre (iii). □

Un morphisme différentiable localement bijectif $p : \tilde{G} \to G$ entre groupes linéaires connexes est appelé un **revêtement** (1) de G. Le noyau d'un tel morphisme est discret dans $\tilde{G}$ et f est surjectif. Réciproquement, un morphisme différentiable surjectif à noyau discret entre deux groupes connexes est localement bijectif. Le noyau de p est nécessairement contenu dans le centre de $\tilde{G}$. En effet tout élément g de $\tilde{G}$ peut être relié à Id par un chemin continu $a(t)$. Pour tout $z \in \ker p$, on a $a(t)za(t)^{-1} \in \ker p$ et en $t = 0$, $a(0)za(0)^{-1} = z$. La fonction $t \mapsto a(t)za(t)^{-1}$ est continue, à valeurs dans un sous-groupe discret de $\tilde{G}$, donc constante, ce qui prouve l'assertion. Réciproquement, pour tout sous-groupe central discret Z de $\tilde{G}$, la suite exacte

$$1 \to Z \to \tilde{G} \to \tilde{G}/Z \to 1.$$

(1) C'est alors un revêtement au sens de la topologie.

fait apparaître $\tilde{G}$ comme revêtement de $\tilde{G}/Z$. (Il faut munir $\tilde{G}/Z$ de la topologie quotient et montrer que c'est bien un groupe linéaire).

Soient G et H deux groupes linéaires, G étant connexe, respectivement d'algèbres de Lie $\mathfrak{g}$ et $\mathfrak{h}$, et supposons donné un morphisme d'algèbre de Lie

$$\phi : \mathfrak{g} \to \mathfrak{h}.$$

Pouvons nous relever ϕ en un morphisme de groupes linéaires

$$f : G \to H$$

de telle sorte que $df_{\mathrm{Id}} = \phi$?

L'exemple de $G = \mathbb{C}^\times$, $H = \mathbb{C}$, $\mathfrak{g} = \mathfrak{h} = \mathbb{C}$ et $\phi = \mathrm{Id}_{\mathbb{C}}$ montre que tel n'est pas le cas. En effet, supposons que f existe. Alors $f(e^z) = \exp(\phi(z)) = \exp z$ pour tout $z \in \mathbb{C}$. Mais il faut prendre garde au fait que dans le membre de droite de cette équation, l'exponentielle n'est pas l'exponentielle usuelle des nombres complexes. Pour bien comprendre ceci, il faut revenir aux définitions, qui demandent de réaliser $(\mathbb{C}^\times, \times)$ et $(\mathbb{C}, +)$ comme des groupes linéaires. Or, si $(\mathbb{C}^\times, \times) = \mathbf{GL}(1, \mathbb{C})$ est trivialement linéaire, il faut être plus subtil pour $(\mathbb{C}, +)$. Ce groupe se plonge dans $\mathbf{GL}(2, \mathbb{C})$ par

$$z \mapsto \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix},$$

et donc son algèbre de Lie $\mathbb{C}$ s'identifie à une sous-algèbre de Lie de $\mathfrak{gl}(2, \mathbb{R})$

$$x \mapsto \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix},$$

On a alors

$$\exp \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Donc, il faut interpréter la formule ci-dessus comme

$$f(e^z) = \exp z = z.$$

Or il est bien connu que la fonction $z \mapsto e^z$ n'admet pas d'inverse global sur $\mathbb{C}^\times$. Si G et H sont donnés comme ci-dessus, un morphisme d'algèbres de Lie $\phi : \mathfrak{g} \to \mathfrak{h}$ ne se relève donc pas forcément en un morphisme de groupes linéaires. Mais il existe toujours un revêtement de G qui va permettre ce relèvement :

Théorème VI.6.4. — *Soit G et H deux groupes linéaires connexes et $\phi : \mathfrak{g} \to \mathfrak{h}$ un morphisme d'algèbres de Lie. Alors il existe un revêtement $p : \tilde{G} \to G$ tel que ϕ se relève en un morphisme de groupes*

$$f : \tilde{G} \to H.$$

Démonstration. Dans l'énoncé ci-dessus, il faut comprendre que les algèbres de Lie de G et $\tilde{G}$ sont identifiée par l'isomorphisme dp_{Id}. Posons :

$$\tilde{\mathfrak{g}} = \{(X, Y) \in \mathfrak{g} \times \mathfrak{h} | Y = \phi(X)\}.$$

C'est le graphe de ϕ, et c'est une algèbre de Lie linéaire. Soit $\tilde{G}$ le groupe lui correspondant par la correspondance de Lie : c'est un sous-groupe de $G \times H$. Soit $p : \tilde{G} \to G$ la restriction à $\tilde{G}$ de la projection de $G \times H$ sur G et $f : \tilde{G} \to H$ la restriction à $\tilde{G}$ de la projection de $G \times H$ sur H. On a

$$dp_{\mathrm{Id}} : \tilde{\mathfrak{g}} \to \mathfrak{g}, \quad (X, \phi(X)) \mapsto X$$

qui est un isomorphisme, ce qui montre que $p : \tilde{G} \to G$ est un revêtement. D'autre part

$$df_{\mathrm{Id}} : \tilde{\mathfrak{g}} \to \mathfrak{h}, \quad (X, \phi(X)) \mapsto \phi(X),$$

ce qui montre que f est un relèvement de ϕ. □

Exemple VI.6.5. — Dans la discussion précédente avec $G = \mathbb{C}^\times$, $H = \mathbb{C}$ le morphisme d'algèbres de Lie

$$\phi : \mathbb{C} \to \mathbb{C}, \quad z \mapsto z$$

se relève en un morphisme de $\tilde{G} \to \mathbb{C}$, où

$$\tilde{G} = \{M(z) = \begin{pmatrix} e^z & 0 & 0 \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}, (z \in \mathbb{C})\}.$$

En effet $p : \tilde{G} \to \mathbb{C}^\times$, $M(z) \mapsto e^z$ est un isomorphisme local et $f : \tilde{G} \to \mathbb{C}$, $M(z) \mapsto z$ relève ϕ.

On dit qu'un groupe linéaire connexe G est **simplement connexe** lorsqu'il vérifie la condition suivante. Tout morphisme d'algèbres de Lie entre son algèbre de Lie $\mathfrak{g}$ et une algèbre de Lie linéaire $\mathfrak{h}$ se relève en un morphisme de groupes linéaires entre G et le groupe linéaire H donné par la correspondance de Lie. Un groupe est simplement connexe en ce sens s'il l'est au sens de la topologie (admis).

Exemples VI.6.6. — Les groupes $\mathbf{SL}(n, \mathbb{C})$ sont simplement connexes, ainsi que les groupes compacts $\mathbf{SU}(n)$. Les groupes $\mathbf{SO}(n, \mathbb{C})$ ne le sont pas, ni les groupes compacts $\mathbf{SO}(n)$. Il existe un revêtement d'ordre 2 de $\mathbf{SO}(n)$ simplement connexe que l'on note $\mathbf{Spin}(n)$. Lorsque $n = 3$, $\mathbf{Spin}(3) \simeq \mathbf{SU}(2)$. Cet exemple sera détaillé dans le chapitre suivant.

Une question naturelle est de savoir si tout groupe linéaire connexe G admet un revêtement simplement connexe $\tilde{G}$. En topologie, tout espace connexe " raisonnable" (une variété différentiable par exemple), admet un revêtement simplement connexe (appelé revêtement universel). Un **groupe de Lie** est une variété différentiable, munie d'une structure de groupe telle que le produit et le passage un l'inverse soient $\mathcal{C}^\infty$. Le revêtement universel d'un groupe de Lie connexe peut être muni d'une structure de groupe de Lie. Un groupe linéaire connexe est un groupe de Lie, mais son revêtement universel n'est pas nécessairement linéaire. Ainsi, par exemple, le groupe $\mathbf{SL}(2, \mathbb{R})$ admet un revêtement universel $\widetilde{\mathbf{SL}}(2, \mathbb{R})$ qui est un groupe de Lie non linéaire. Le noyau de $p : \widetilde{\mathbf{SL}}(2, \mathbb{R}) \to \mathbf{SL}(2, \mathbb{R})$ est isomorphe à $\mathbb{Z}$.

VI.7. Représentations de dimension finie des groupes linéaires connexes

Soit G un groupe linéaire connexe. Une représentation de dimension finie (π, V) de G est donnée par un morphisme de groupes linéaires :

$$\pi : G \to \mathbf{GL}(V).$$

La différentielle de ce morphisme est un morphisme d'algèbre de Lie :

$$d\pi_{\mathrm{Id}} : \ \mathfrak{g} \to \mathfrak{gl}(V).$$

Le résultat suivant est immédiat, et montre que l'étude des représentations de G se ramène dans une large mesure à l'étude des représentations de son algèbre de Lie $\mathfrak{g}$.

Proposition VI.7.1. — *Un sous-espace W de V est stable sous l'action de G si et seulement s'il est stable sous l'action de $\mathfrak{g}$.*

Démonstration. Dans un sens, on différencie, de l'autre, on utilise le fait que G étant connexe, il est engendré par l'image de l'exponentielle. □

Ainsi une représentation irréductible de G donne une représentation irréductible de $\mathfrak{g}$. Si l'on cherche par exemple à déterminer toutes les représentations irréductibles de dimension finie de G, on commencera par le problème, en pratique plus simple, de déterminer toutes les représentations irréductibles de dimension finie de $\mathfrak{g}$. Bien sûr, si G n'est pas simplement connexe, une représentation de $\mathfrak{g}$ ne se remonte pas forcément en une représentation de G. La stratégie sera alors la suivante. On essaie d'identifier le revêtement universel $\tilde{G}$ de G. Toute représentation de $\mathfrak{g}$ se remonte en une représentation de $\tilde{G}$. Une telle représentation définit aussi une représentation de G si et seulement si elle est triviale sur le noyau de $p : \ \tilde{G} \to G$.

Dans le chapitre suivant, nous allons utiliser cette stratégie pour étudier les représentations du groupe compact $\mathbf{SO}(3)$.

Une représentation de dimension finie de l'algèbre de Lie $\mathfrak{g}$ est un morphisme d'algèbres de Lie :

$$\phi : \mathfrak{g} \to \mathfrak{gl}(V)$$

où V est un espace vectoriel **complexe** de dimension finie. Or $\mathfrak{g}$ est un espace vectoriel **réel** et ϕ est $\mathbb{R}$-linéaire. Il est avantageux, comme nous le verrons dans l'exemple du chapitre suivant, de remplacer $\mathfrak{g}$ par sa **complexification**.

Définition VI.7.2. — Soit E un espace vectoriel réel. La complexification de E, notée $E_{\mathbb{C}}$, est l'espace vectoriel complexe

$$E_{\mathbb{C}} = E \otimes_{\mathbb{R}} \mathbb{C}.$$

La multiplication par un scalaire $\lambda \in \mathbb{C}$ d' un élément $v \otimes z$ est donnée par

$$\lambda \cdot (v \otimes z) = v \otimes \lambda z.$$

En pratique, il suffit de comprendre que si $(e_i)_{i\in I}$ est un base de E (sur $\mathbb{R}$), alors c'est aussi une base de $E_{\mathbb{C}}$ (sur $\mathbb{C}$). Si $\dim_{\mathbb{R}} E = n$, alors $\dim_{\mathbb{C}} E_{\mathbb{C}} = n$. Remarquons que tout espace vectoriel sur $\mathbb{C}$ est naturellement un espace vectoriel sur $\mathbb{R}$, mais que la complexification n'est pas l'inverse de cette opération. Ainsi, la complexification de $\mathbb{R}$ est $\mathbb{C}$, et $\mathbb{C} \simeq \mathbb{R}^2$ en tant qu'espace vectoriel réel.

Proposition VI.7.3. — *Toute application $\mathbb{R}$-linéaire*

$$\phi : E \to V$$

où V est un espace vectoriel complexe se prolonge naturellement en une application $\mathbb{C}$-linéaire (encore notée ϕ pour ne pas alourdir)

$$\phi : E_{\mathbb{C}} \to V.$$

Réciproquement, toute application $\mathbb{C}$-linéaire $\phi : E_{\mathbb{C}} \to V$ est entièrement déterminée par sa restriction à $E \simeq E \otimes \mathbb{R} \subset E \otimes_{\mathbb{R}} \mathbb{C} = E_{\mathbb{C}}$ qui est $\mathbb{R}$-linéaire.

Démonstration. C'est tautologique, les définitions sont faites pour. □

En résumé, il est équivalent d'étudier les représentations $\mathbb{R}$-linéaires de $\mathfrak{g}$ dans des espaces vectoriels complexes ou les représentations $\mathbb{C}$-linéaires de sa complexification $\mathfrak{g}_{\mathbb{C}}$.

CHAPITRE VII

REPRÉSENTATIONS DE $\mathfrak{sl}(2,\mathbb{C})$, $\mathbf{SU}(2)$, ET $\mathbf{SO}(3)$

Notre but est d'étudier les représentations du groupe compact $\mathbf{SO}(3)$ selon les principes dégagés dans la dernière section du chapitre précédent. Nous commençons par identifier le revêtement universel de $\mathbf{SO}(3)$.

VII.1. Le revêtement $\mathbf{SU}(2) \to \mathbf{SO}(3)$

Rappelons que $\mathbf{SU}(2)$ est le groupe de matrices :

$$\mathbf{SU}(2) = \{a \in \mathbf{GL}(2,\mathbb{C}) |\, {}^t\bar{a}a = \mathrm{Id}, \det a = 1\},$$

et que son algèbre de Lie est :

$$\mathfrak{su}(2) = \{X \in \mathfrak{gl}(2,\mathbb{C}) |\, {}^t\bar{X} + X = 0, \mathrm{Tr}\, X = 0\}.$$

Plus explicitement, on a donc :

$$\mathbf{SU}(2) = \{\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix},\ \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\},$$

$$\mathfrak{su}(2) = \{\begin{pmatrix} iz & -y+ix \\ y+ix & -iz \end{pmatrix}, x, y, z \in \mathbb{R}\}.$$

On voit donc que, topologiquement, $\mathbf{SU}(2)$ est la sphère unité dans $\mathbb{C}^2 \simeq \mathbb{R}^4$. En particulier :

Proposition VII.1.1. — $\mathbf{SU}(2)$ *est un groupe connexe, simplement connexe.*

Passons maintenant à $\mathbf{SO}(3)$. C'est le groupe de matrices :

$$\mathbf{SO}(3) = \{a \in \mathbf{GL}(3,\mathbb{R}) |\, {}^t aa = \mathrm{Id}, \det a = 1\},$$

dont l'algèbre de Lie est

$$\begin{aligned} \mathfrak{so}(3) &= \{X \in \mathfrak{gl}(3,\mathbb{R}) |\, {}^t X + X = 0\} \\ &= \{ \begin{pmatrix} 0 & -z & y \\ z & 0 & x \\ -y & -x & 0 \end{pmatrix}, x, y, z \in \mathbb{R}\} \end{aligned}$$

Une base de $\mathfrak{su}(2)$ est donnée par :

$$I = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

et l'on a les relations de commutation suivantes :

$$[I,J] = 2K, \quad [J,K] = 2I, \quad [K,I] = 2J.$$

Munissons $\mathfrak{su}(2)$ de la forme bilinéaire κ symétrique définie par

$$\kappa(X,Y) = \mathrm{Tr}\,(\mathrm{ad}(X)\mathrm{ad}(Y)), \quad (X, Y \in \mathfrak{su}(2)).$$

Les relations de commutation ci-dessus donnent les matrices de $\mathrm{ad}(I)$, $\mathrm{ad}(J)$, $\mathrm{ad}(K)$ dans la base I, J, K : On calcule alors facilement que

$$\kappa(I,I) = \kappa(J,J) = \kappa(K,K) = -8, \quad \kappa(I,J) = \kappa(J,K) = \kappa(K,I) = 0.$$

La base $\{I, J, K\}$ de $\mathfrak{su}(2)$ est donc orthogonale, et l'on constate que la forme κ est définie négative. Si l'on préfère travailler avec un produit scalaire (défini positif) et une base orthonormale, on peut remplacer κ par $\frac{-1}{8}\kappa$. L'espace euclidien $(\mathfrak{su}(2), \frac{-1}{8}\kappa)$ est alors, par le choix de la base $\{I, J, K\}$, isomorphe à $\mathbb{R}^3$ muni de son produit scalaire canonique.

Montrons que la forme κ est invariante par l'action adjointe de $\mathbf{SU}(2)$ sur $\mathfrak{su}(2)$. Il nous faut montrer que $(\forall X, Y \in \mathfrak{su}(2))$, $(\forall g \in \mathbf{SU}(2))$,

$$\kappa(\mathrm{Ad}(g)\cdot X, \mathrm{Ad}(g)\cdot Y) = \kappa(X,Y),$$

c'est-à-dire

(VII.1.1) $$\mathrm{Tr}\,(\mathrm{ad}(gXg^{-1})\mathrm{ad}(gYg^{-1})) = \mathrm{Tr}\,(\mathrm{ad}(X)\mathrm{ad}(Y)).$$

Or, pour tout $Z \in \mathfrak{su}(2)$,

$$\begin{aligned}
&\mathrm{ad}(gXg^{-1})\mathrm{ad}(gYg^{-1}) \cdot Z = [gXg^{-1}, [gYg^{-1}, Z]] \\
&= (gXg^{-1})(gYg^{-1})Z - (gXg^{-1})Z(gYg^{-1}) \\
&\qquad\qquad - (gYg^{-1})Z(gXg^{-1}) + Z(gYg^{-1})(gXg^{-1}) \\
&= gXY(g^{-1}Zg)g^{-1} - gX(g^{-1}Zg)Yg^{-1} - gY(g^{-1}Zg)Xg^{-1} + g((g^{-1}Zg)YXg^{-1} \\
&= \mathrm{Ad}(g) \cdot (XY(g^{-1}Zg) - (g^{-1}Zg)Y - Y(g^{-1}Zg)X + (g^{-1}Zg)YX) \\
&= \mathrm{Ad}(g) \cdot (X[Y, \mathrm{ad}(g^{-1}) \cdot Z] - [Y, \mathrm{ad}(g^{-1}) \cdot Z)X]) \\
&= \mathrm{Ad}(g) \circ \mathrm{ad}(X) \circ \mathrm{ad}(Y) \circ \mathrm{Ad}(g)^{-1}(Z)
\end{aligned}$$

D'où

$$\mathrm{ad}(gXg^{-1}) \circ \mathrm{ad}(gYg^{-1}) = \mathrm{Ad}(g) \circ \mathrm{ad}(X) \circ \mathrm{ad}(Y) \circ \mathrm{Ad}(g)$$

et

$$\mathrm{Tr}\,(\mathrm{ad}(gXg^{-1})\mathrm{ad}(gYg^{-1})) = \mathrm{Tr}\,(\mathrm{ad}(X) \circ \mathrm{ad}(Y)).$$

On a donc bien obtenu (VII.1.1).

Ainsi Ad est un morphisme du groupe $\mathbf{SU}(2)$ dans le groupe orthogonal $\mathbf{O}(\mathfrak{su}(2), \kappa) \simeq \mathbf{O}(3)$, et de plus, comme $\mathbf{SU}(2)$ est connexe, le déterminant de $\mathrm{Ad}(g)$, $g \in G$ est toujours 1. Donc en fait, l'on obtient un morphisme :

$$\mathrm{Ad} : \ \mathbf{SU}(2) \longrightarrow \mathbf{SO}(\mathfrak{su}(2), \kappa) \simeq \mathbf{SO}(3).$$

La différentielle de ce morphisme est le morphisme d'algèbre de Lie

$$\mathrm{ad} : \ \mathfrak{su}(2) \longrightarrow \mathfrak{so}(\mathfrak{su}(2), \kappa) \simeq \mathfrak{so}(3).$$

Un calcul explicite dans la base $\{I, J, K\}$ montre que

$$\mathrm{ad} \begin{pmatrix} iz & -y+ix \\ y+ix & -iz \end{pmatrix} = \begin{pmatrix} 0 & -2z & 2y \\ 2z & 0 & -2x \\ -2y & 2x & 0 \end{pmatrix}$$

et donc ad réalise un isomorphisme entre $\mathfrak{su}(2)$ et $\mathfrak{so}(3)$. Ainsi, Ad est un isomorphisme local entre $\mathbf{SU}(2)$ et $\mathbf{SO}(3)$. Comme $\mathbf{SO}(3)$ est connexe, il est surjectif. Calculons maintenant son noyau. On cherche les $g \in \mathbf{SU}(2)$ tels que

$$\mathrm{Ad}(g) \cdot I = I, \quad \mathrm{Ad}(g) \cdot J = J, \quad \mathrm{Ad}(g) \cdot K = K.$$

Un calcul explicite montre g est une matrice scalaire. La condition $\det g = 1$ impose alors $g = \pm\mathrm{Id}$. Résumons :

Proposition VII.1.2. — *La suite courte suivante est exacte :*

$$1 \longrightarrow \{\pm \mathrm{Id}\} \longrightarrow \mathbf{SU}(2) \longrightarrow \mathbf{SO}(3) \longrightarrow 1.$$

Le groupe $\mathbf{SU}(2)$ *est un revêtement de* $\mathbf{SO}(3)$ *(d'ordre* 2*).*

VII.2. Représentations de $\mathfrak{sl}(2,\mathbb{C})$

Comme nous l'avons expliqué en VI.7, nous allons étudier les représentations de dimension finie de $\mathbf{SO}(3)$ et $\mathbf{SU}(2)$ en étudiant celle de leur algèbre de Lie $\mathfrak{so}(3) \simeq \mathfrak{su}(2)$. Commençons par identifier la complexification de $\mathfrak{su}(2)$:

$$\mathfrak{su}(2)_{\mathbb{C}} = \mathfrak{su}(2) \otimes_{\mathbb{R}} \mathbb{C}.$$

Comme $\{I, J, K\}$ est une base de $\mathfrak{su}(2)$ sur $\mathbb{R}$, on obtient

$$\begin{aligned}
\mathfrak{su}(2)_{\mathbb{C}} &= \mathbb{C}I \oplus \mathbb{C}J \oplus \mathbb{C}K \\
&= \{\begin{pmatrix} iz & -y+ix \\ y+ix & -iz \end{pmatrix}, x, y, z \in \mathbb{C}\} \\
&= \{\begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}, \alpha, \beta, \gamma \in \mathbb{C}\} \\
&= \mathfrak{sl}(2,\mathbb{C})
\end{aligned}$$

Il est donc équivalent d'étudier les représentations $\mathbb{R}$-linéaires de $\mathfrak{su}(2)$ dans des espaces vectoriels complexes ou les représentations $\mathbb{C}$-linéaires de $\mathfrak{sl}(2,\mathbb{C})$.

Une base (sur $\mathbb{C}$) de $\mathfrak{sl}(2,\mathbb{C})$ est

$$h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

et l'on a les relations de commutation suivantes :

$$[h, e] = 2e, \quad [h, f] = -2f, \quad [e, f] = h.$$

Soit $\phi : \mathfrak{sl}(2,\mathbb{C}) \to \mathfrak{gl}(V)$ une représentation $\mathbb{C}$-linéaire de dimension finie. Pour tout $\lambda \in \mathbb{C}$, soit V_λ le sous-espace propre (éventuellement nul) de $\phi(h)$ pour la valeur propre λ. Comme $\mathbb{C}$ est algébriquement clos, si V n'est pas nul, il existe un V_λ non nul.

Lemme VII.2.1. —

$$\phi(e)(V_\lambda) \subset V_{\lambda+2}, \quad \phi(f)(V_\lambda) \subset V_{\lambda-2}.$$

Démonstration. Soit $v \in V_\lambda$. On a :

$$\begin{aligned}
\phi(h)(\phi(e)(v)) &= \phi(e)(\phi(h)(v)) + [\phi(h), \phi(e)](v) \\
&= \lambda\phi(e)(v) + \phi([h,e])(v) \\
&= \lambda\phi(e)(v) + 2\phi(e)(v) = (\lambda+2)\phi(e)(v)
\end{aligned}$$

ce qui montre la première inclusion. Le deuxième s'obtient de la même manière. □

Comme V est de dimension finie, il n'y a qu'un nombre fini de V_λ non nuls. Si V est non nul, il existe donc $\lambda_0 \in \mathbb{C}$ tel que $V_{\lambda_0} \neq \{0\}$ et $V_{\lambda_0+2} = \{0\}$. Soit $0 \neq v_0 \in V_{\lambda_0}$. Posons, pour tout $k \in \mathbb{N}$,

$$v_k = \phi(f)^k(v_0).$$

Alors v_k est dans V_{λ_0-2k}.

On a par exemple $v_1 = \phi(f)(v_0)$ et

$$\begin{aligned}
\phi(e)(v_1) &= \phi(e)(\phi(f)(v_0)) \\
&= \phi(f)(\phi(e)(v_0)) + [\phi(e), \phi(f)](v_0) \\
&= 0 + \phi([e,f])(v_0) = \phi(h)(v_0) \\
&= \lambda_0(v_0)
\end{aligned}$$

De même :

$$\begin{aligned}
\phi(e)(v_2) &= \phi(e)(\phi(f)(v_1)) \\
&= \phi(f)(\phi(e)(v_1)) + [\phi(e), \phi(f)](v_1) \\
&= \lambda_0\phi(f)(v_0) + \phi(h)(v_1) \\
&= \lambda_0 v_1 + (\lambda_0 - 2)v_1 = (2\lambda_0 - 2)v_1
\end{aligned}$$

Tentons d'avancer une hypothèse de récurrence :

$$(H) \quad \phi(e)(v_k) = k(\lambda_0 - k + 1)v_{k-1}.$$

Nous avons vu qu'elle est satisfaite pour $k = 1, 2$ et

En utilisant l'hypothèse de récurrence, on obtient, pour $k \geq 2$:

$$\begin{aligned}\phi(e)(v_{k+1}) &= \phi(e)(\phi(f)(v_k)) \\ &= \phi(f)(\phi(e)(v_k)) + [\phi(e), \phi(f)](v_k) \\ &= k(\lambda_0 - k + 1)\phi(f)(v_{k-1}) + \phi(h)(v_k) \\ &= k(\lambda_0 - k + 1)v_k + (\lambda_0 - 2k)v_k \\ &= (k+1)(\lambda_0 - k)v_k\end{aligned}$$

Ceci prouve l'hypothèse (H).

Tant que les vecteurs $v_0, v_1, \ldots, v_j$ sont tous non nuls, ils sont linéairement indépendants, et donc, comme la dimension de V est finie, il existe un plus petit entier n non nul tel que v_{n+1} est nul. En particulier $v_n \neq 0$. On a alors

$$0 = \phi(e)(v_{n+1}) = (n+1)(\lambda_0 - n)v_n,$$

d'où $\lambda_0 = n$.

D'autre part, $v_0, v_1, \ldots, v_n$ engendrent un sous-espace de V stable sous l'action de $\mathfrak{sl}(2,\mathbb{C})$. Si l'on suppose (ϕ, V) irréductible, on voit alors que $(v_0, v_1, \ldots, v_n)$ est une base de V. En particulier $\dim_{\mathbb{C}} V = n + 1$.

Réciproquement, si $n \in \mathbb{N}$, et si l'on fixe une base $(v_0, v_1, \ldots, v_n)$ de $\mathbb{C}^{n+1}$, alors on définit une représentation ϕ de $\mathfrak{sl}(2,\mathbb{C})$ par

$$\phi(h)(v_k) = (n - 2k)v_k, \quad \phi(e)(v_k) = k(n - k + 1)v_{k-1}, \quad \phi(f)(v_k) = v_{k+1},$$

pour tout $k = 0, \ldots n$, avec les conventions $v_{-1} = v_{n+1} = 0$. On voit facilement qu'elle est irréductible : tout sous-espace stable W contient un vecteur propre non nul pour $\phi(h)$, et est donc, à un scalaire non nul près, l'un des v_i.

Ceci donne la classification des représentations irréductibles $\mathbb{C}$-linéaires de $\mathfrak{sl}(2,\mathbb{C})$: notons $(\phi_n, \mathbb{C}^{n+1})$ la représentation irréductible de dimension $n+1$ de $\mathfrak{sl}(2,\mathbb{C})$ définie ci-dessus. Toute représentation irréductible $\mathbb{C}$-linéaire de $\mathfrak{sl}(2,\mathbb{C})$ de dimension $n+1$ est isomorphe à $(\phi_n, \mathbb{C}^{n+1})$.

Exercice VII.2.2. — Exprimer I, J, K dans la base (h, e, f). En déduire l'action de de I, J, K dans $(\phi_n, \mathbb{C}^{n+1})$.

Nous allons maintenant montrer que les représentations $(\phi_n, \mathbb{C}^{n+1})$ se remontent en des représentations du groupe $\mathbf{SU}(2)$. Pour cela, nous allons commencer par trouver une autre réalisation de ces représentations.

Soit $\mathbb{C}[z_1, z_2]$ l'espace vectoriel des polynômes à coefficients complexes à deux variables. Posons $\partial_i = \frac{\partial}{\partial z_i}$, $i = 1, 2$, et

$$D_e = -z_2\partial_1, \quad D_f = -z_1\partial_2, \quad D_h = z_2\partial_2 - z_1\partial_1. \tag{VII.2.1}$$

Alors D_e, D_f et D_h sont des opérateurs différentiels (linéaires à coefficients constants) qui agissent sur $\mathbb{C}[z_1, z_2]$. On vérifie par le calcul qu'ils satisfont les relations de commutation :

$$[D_h, D_e] = 2D_e, \quad [D_h, D_f] = -2D_f, \quad [D_e, D_f] = D_h.$$

Ainsi

$$e \mapsto D_e, \quad f \mapsto D_f, \quad h \mapsto D_h,$$

définit une représentation D de $\mathfrak{sl}(2,\mathbb{C})$ dans $\mathbb{C}[z_1, z_2]$.

Une base de $\mathbb{C}[z_1, z_2]$ est donnée par les monômes $z_1^k z_2^{n-k}$, avec k, n entiers, $k \leq n$. On calcule

$$D_h(z_1^k z_2^{n-k}) = (n-2k) z_1^k z_2^{n-k} \quad D_f(z_1^k z_2^{n-k}) = -(n-k) z_1^{k+1} z_2^{n-k-1},$$

$$D_e(z_1^k z_2^{n-k}) = -k z_1^{k-1} z_2^{n-k+1},$$

avec la convention $z_i^{-1} = 0$.

Ceci montre que l'espace $\mathbb{C}[z_1, z_2]_n$ des polynômes homogènes de degré n fixé (qui est de dimension $n+1$), est stable sous l'action de $\mathfrak{sl}(2,\mathbb{C})$. La représentation $(D, \mathbb{C}[z_1, z_2]_n)$ est isomorphe à $(\phi_n, \mathbb{C}^{n+1})$ comme on le voit en normalisant convenablement la base des $z_1^k z_2^{n-k}$, (n fixé), en posant

$$v_k = (-1)^k \frac{z_1^k z_2^{n-k}}{(n-k)!}.$$

Exercice VII.2.3. — En utilisant l'exercice précédent, écrire les formules donnant D_I,D_J, D_K et l'action de de I, J, K sur les monômes $z_1^k z_2^{n-k}$.

Nous allons maintenant montrer que l'action de $\mathfrak{sl}(2,\mathbb{C})$ sur $\mathbb{C}[z_1,z_2]_n$ est la différentielle d'une représentation de $\mathbf{SL}(2,\mathbb{C})$ dans ce même espace. En effet, $\mathbf{SL}(2,\mathbb{C})$ agit naturellement sur $\mathbb{C}^2$, et donc sur $\mathbb{C}[z_1,z_2]$ par

$$(\rho(g)\cdot P)(z_1,z_2) = P(g^{-1}\cdot(z_1,z_2)).$$

De manière explicite, si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $ad-bc=1$ est un élément de $\mathbf{SL}(2,\mathbb{C})$, son inverse est $g^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, et donc

$$g^{-1}\cdot(z_1,z_2) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = (dz_1 - bz_2, -cz_1 + az_2).$$

Ainsi

$$(\rho(g)\cdot P)(z_1,z_2) = P(dz_1 - bz_2, -cz_1 + az_2).$$

Nous espérons que le lecteur n'est pas gêné par le passage de l'écriture en colonnes des vecteurs de $\mathbb{C}^2$ à l'écriture en ligne des variables. Il est clair que cette action préserve les polynômes homogènes de degré n. On en déduit donc une représentation $(\rho,\mathbb{C}[z_1,z_2]_n)$. Nous allons maintenant calculer sa différentielle.

Soit $X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ dans $\mathfrak{sl}(2,\mathbb{C})$ (donc $\delta=-\alpha$) et posons

$$c(t) = \exp tX = \begin{pmatrix} a(t) & b(t) \\ c(t) & d(t) \end{pmatrix} \in \mathbf{SL}(2,\mathbb{C}), \quad (t\in\mathbb{R})$$

On a $c(0)=\mathrm{Id}$ et $c'(0)=X$, soit $a'(0)=\alpha$, $b'(0)=\beta$... On peut alors calculer la différentielle de ρ :

$$\begin{aligned}
&(d\rho(X)\cdot P)(z_1,z_2) = \frac{d}{dt}_{|t=0}(\rho(c(t))\cdot P)(z_1,z_2)\\
&= \frac{d}{dt}_{|t=0}P((d(t)z_1 - b(t)z_2, -c(t)z_1 + a(t)z_2)\\
&= (\delta z_1 - \beta z_2)(\partial_1 P)(z_1,z_2) + (-\gamma z_1 + \alpha z_2)(\partial_2 P)(z_1,z_2)
\end{aligned}$$

En particulier, on trouve :

$$d\rho(h) = -z_1\partial_1 + z_2\partial_2, \quad d\rho(e) = -z_2\partial_1, \quad d\rho(f) = -z_1\partial_2.$$

Nous retrouvons (VII.2.1).

On peut maintenant restreindre les représentations $(\rho, \mathbb{C}[z_1, z_2])_n$ à $\mathbf{SU}(2) \subset \mathbf{SL}(2,\mathbb{C})$. Notons (π_n, V_n) ces représentations. Nous avons montré que toute représentation irréductible de dimension $n+1$ de $\mathbf{SU}(2)$ est isomorphe à (π_n, V_n).

Les représentations irréductibles de dimension de $\mathbf{SO}(3)$ sont celles obtenues à partir de celles de $\mathbf{SU}(2)$ triviales en $-\mathrm{Id} \in \mathbf{SU}(2)$. Or $-\mathrm{Id}$ agit sur un polynôme P par

$$(\rho(-\mathrm{Id}) \cdot P)(z_1, z_2) = P(-z_1, -z_2).$$

Ainsi les représentations de $\mathbf{SU}(2)$ triviales en $-\mathrm{Id}$ sont les (π_n, V_n), n pair.

Exercice VII.2.4. — Montrer que tout élément de $\mathbf{SU}(2)$ est conjugué à un élément de la forme $g_\theta = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$. Calculer le caractère Θ_n de la représentation irréductible (π_n, V_n) en g_θ. En déduire que $\pi_n \otimes \pi_m \simeq \sum_{l=0}^{m} \pi_{n-2l}$ (Formule de Clebsch-Gordan).

VII.3. Représentations de dimension finie de $\mathbf{SL}(2,\mathbb{R})$

Le travail fait dans la paragraphe précédent permet aussi d'obtenir les représentations irréductibles de dimension finie de $\mathbf{SL}(2,\mathbb{R})$. Remarquons tout d'abord que ce groupe est non compact. Néanmoins, il est connexe, et ses représentations de dimension finie donnent par différentiation des représentations de l'algèbre de Lie $\mathfrak{sl}(2,\mathbb{R})$. Celles-ci correspondent à leur tour à des représentations $\mathbb{C}$-linéaires de $\mathfrak{sl}(2,\mathbb{C})$. On sait que l'irréductibilité est préservée par ces correspondances. Les représentations irréductibles $\mathbb{C}$-linéaires de $\mathfrak{sl}(2,\mathbb{C})$ ont été déterminée ci-dessus, il reste à voir si elle se remontent en des représentations de $\mathbf{SL}(2,\mathbb{R})$. La même méthode que celle utilisée pour $\mathbf{SU}(2)$ marche, car on a vu qu'elles se remontent en des représentations de $\mathbf{SL}(2,\mathbb{C})$, que l'on peut ensuite restreindre à $\mathbf{SL}(2,\mathbb{R})$. On voit donc que les représentations irréductibles de dimension finie de $\mathbf{SL}(2,\mathbb{R})$ sont en bijection avec les représentations irréductibles de dimension finie de $\mathbf{SU}(2)$ et qu'elles sont dans les deux cas obtenues par restriction des représentations irréductibles de dimension finie de $\mathbf{SL}(2,\mathbb{C})$ dont la différentielle est $\mathbb{C}$-linéaire. Lorsqu'un sous-$\mathbb{R}$-espace vectoriel E d'un espace vectoriel complexe V est tel que $E_{\mathbb{C}} \simeq V$, on dit que E est une forme réelle de V. Ce qui se passe ici est que $\mathfrak{sl}(2,\mathbb{R})$ et $\mathfrak{su}(2)$ sont deux formes réelles de $\mathfrak{sl}(2,\mathbb{C})$. De même, en développant un peu le formalisme des groupes algébriques (*cf.* [**1**] par exemple), on pourrait donner un sens à l'assertion que $\mathbf{SL}(2,\mathbb{R})$ et $\mathbf{SU}(2)$ sont des formes réelles de $\mathbf{SL}(2,\mathbb{C})$. Une autre conséquence de ceci est que les représentations de dimension finie de $\mathbf{SL}(2,\mathbb{R})$ sont complètement réductibles. Ceci n'était pas évident de prime abord, car $\mathbf{SL}(2,\mathbb{R})$ est non compact, et il n'existe pas de produit scalaire invariant sur une représentation de dimension finie de $\mathbf{SL}(2,\mathbb{R})$, sauf si elle est triviale. L'astuce qui consiste à relier la théorie des représentations de dimension finie d'un groupe linéaire connexe G à celle d'un autre groupe K compact, ces deux groupes étant deux formes réelles d'un même groupe complexe $\mathbb{G}$ est due à H. Weyl, et est connue sous le terme anglais de "unitarian trick". Par exemple, $\mathbf{SL}(n,\mathbb{R})$ et $\mathbf{SU}(n)$ sont des formes réelles de $\mathbf{SL}(n,\mathbb{C})$, $\mathbf{SO}(p,q)$ et $\mathbf{SO}(p+q)$ sont des formes réelles de $\mathbf{SO}(p+q,\mathbb{C})$...

Exercice VII.3.1. — Montrer que tout élément de $\mathbf{SL}(2,\mathbb{R})$ est conjugué à l'un des éléments suivants :

$$g_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \quad g_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

$\theta \in \mathbb{R}$, $a \in \mathbb{R}^\times$. Calculer le caractère Θ_n de la représentation irréductible $(\rho', \mathbb{C}[z_1,z_2])_n$ en ces éléments.

CHAPITRE VIII

ET APRÈS ?

La théorie des représentations des groupes (groupes de Lie, groupes algébriques...) et des algèbres de Lie s'est énormément développée au cours du XX-ième siècle. Elle joue un rôle majeur dans de nombreux domaines des mathématiques, en particulier la physique mathématique et la théorie des nombres. Nous souhaitons simplement indiquer ici quelques ouvrages accessibles après ce cours pour le lecteur désireux d'aller plus loin. Commençons par le très classique [**4**], qui étudie les représentations des groupes finis dans des espaces vectoriels sur un corps quelconque. Pour ceux intéressés par les applications à la physique, une excellente référence est [**5**]. Les applications à la théorie des nombres sont en général d'un niveau plus avancé. Il est bon de ce familiariser d'abord un petit peu avec le théorie des groupes algébriques ([**1**]). Le livre [**2**] explique le passage de la théorie des nombres "classique" de la fin XIX-ième début XX-ième (formes modulaires, opérateurs de Hecke...) à la vision moderne (représentations automorphes, conjectures de Langlands...).

CHAPITRE IX

PROBLÈMES CORRIGÉS

Le module MAT553 de l'Ecole Polytechnique, intitulé "Groupes et représentations" dont ce texte est le support pédagogique, consiste en 9 séances de trois heures trente, cours et séances d'exercices confondus. Les sujets d'examens et leurs corrigés sont donnés ci-dessous. Ils consistent en général en un problème sur les groupes finis, et un problème sur les groupes linéaires. On y trouvera :

— concernant les groupes finis :

une démonstration du théorème de structure des groupes abéliens finis, utilisant un peu de théorie des représentations, (2006)

un problème sur les fonctions sphériques dans les paires de Gelfand, (2007)

un problème sur la théorie des représentations du groupe dihédral, (2008)

— concernant les groupes linéaires :

un problème les représentations du groupe de Heisenberg réel de dimension 3, (2006)

un problème sur la paire de Gelfand $(\mathbf{SO}(3), \mathbf{SO}(2))$, autrement dit, les polynômes harmoniques, (2007)

un problème cherchant à démontrer que l'algèbre de Lie du sous-groupe d'un groupe G engendré par les commutateurs est l'algèbre dérivée $[\mathfrak{g}, \mathfrak{g}]$. La démonstration n'est complète que pour G compact. (2008)

Examen du 11 décembre 2006

Exercice 1.

a) Montrer qu'un groupe fini G est abélien si et seulement si toutes ses représentations irréductibles sont de dimension 1 et qu'alors $|\widehat{G}| = |G|$.

b) Dans la suite G est abélien fini. Montrer que si $g \in G$, $g \neq e$, il existe $\chi \in \widehat{G}$ tel que $\chi(g) \neq 1$. (On pourra utiliser les relations d'orthogonalité duales.)

c) En déduire que le morphisme canonique d'évaluation $G \to \widehat{\widehat{G}}$ est injectif, puis qu'il est bijectif.

d) Dans la suite, G est un groupe abélien fini d'ordre p^α, où p est un nombre premier, et α un entier naturel. Quelles sont les valeurs possibles des caractères de G ?

e) Soit x_0 un élément de G d'ordre maximal, disons p^β, avec $\beta \leq \alpha$. En utilisant *b*) montrer qu'il existe un caractère $\chi : G \to \mathbb{C}^*$ réalisant un isomorphisme entre le sous-groupe H de G engendré par x_0 et le groupe $\mu(p^\beta)$ des racines p^β-ième de l'unité. (On pourra remarquer que $x_1 = x_0^{p^{\beta-1}} \neq e$.)

f) Montrer que H et $\ker \chi$ engendrent G. En déduire que G est le produit direct de H et de $\ker \chi$.

g) Montrer que G est un produit direct de groupes cycliques.

h) On suppose maintenant que G est d'ordre mn, où m et n sont premiers entre eux. Soit H l'ensemble des éléments de G dont l'ordre divise n et K l'ensemble des éléments de G dont l'ordre divise m. Montrer que H et K sont des sous-groupes de G, que $H \cap K = \{e\}$ et que $HK = G$. En déduire que G est le produit direct de H et K.

i) Montrer que tout groupe abélien fini G est produit direct de groupes cycliques.

Exercice 2

Première Partie : Représentations de dimension finie du groupe de Heisenberg.

Soit $\mathfrak{h} = \{\begin{pmatrix} 0 & x & z \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix} \; ; \; x, y, z \in \mathbb{R}\}$.

Posons $X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ et $Z = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

— 1. Montrer que $[X, Y] = Z$, $[X, Z] = [Y, Z] = 0$. En déduire que $\mathfrak{h}$ est une sous-algèbre de Lie de $\mathfrak{gl}(3, \mathbb{R})$.

— 2. Calculer $\exp tX$, $\exp tY$ et $\exp tZ$ pour tout $t \in \mathbb{R}$.

— 3. Calculer $g_{a,b,c} = \exp cZ \exp bY \exp aX$. Exprimer $\exp aX \exp bY$ comme un élément $g_{a,b,c}$. Montrer que $g_{a,b,c}$ est dans l'image de l'exponentielle.

— 4. Quel est le sous-groupe connexe de $\mathbf{GL}(3, \mathbb{R})$ d'algèbre de Lie $\mathfrak{h}$? On le note H. Montrer que $\exp : \mathfrak{h} \to H$ est bijective.

— 5. Quelles sont les sous-algèbres de Lie de $\mathfrak{h}$?

— 6. Soit (ϕ, V) une représentation de dimension finie de $\mathfrak{h}$. Soit λ une valeur propre de l'opérateur $\phi(Z)$. Montrer que le sous-espace propre V_λ associé à cette valeur propre est stable par ϕ.

— 7. On suppose maintenant que (ϕ, V) est irréductible. Que vaut $\phi(Z)$? En déduire que la valeur propre λ est nulle.

— 8. Montrer qu'alors $\dim V = 1$. On pose $\phi(X) = \alpha$, $\phi(Y) = \beta$.

— 9. Montrer que les classes d'équivalence de représentations irréductibles de dimension finie de $\mathfrak{h}$ forment une famille à deux paramètres $\phi_{\alpha,\beta}$, $\alpha, \beta \in \mathbb{C}$. Ces représentations sont-elles les différentielles en Id de représentations de H. Les expliciter le cas échéant. Quelles sont les représentations unitaires de dimension finie de H ?

Deuxième partie : Représentations unitaires irréductibles de H

Soit $\mathcal{S}(\mathbb{R})$ l'espace de Schwartz sur $\mathbb{R}$. Rappelons que $\mathcal{S}(\mathbb{R})$ est l'espace des fonctions $\mathcal{C}^\infty$ sur $\mathbb{R}$, à valeurs complexes, qui sont, ainsi que toutes leurs dérivées, à "décroissance rapide" lorsque $t \to \pm\infty$. Ceci assure que les intégrales qui apparaissent ci-dessous convergent, et nous ne nous préoccuperons plus de ce problème. On munit $\mathcal{S}(\mathbb{R})$ du produit hermitien (défini positif) :

$$(f_1, f_2) = \int_{\mathbb{R}} f_1(t)\overline{f_2(t)}\, dt$$

La norme associée sera notée $||\cdot||_2$.

Considérons sur $\mathcal{S}(\mathbb{R})$ l'opérateur

$$a = \frac{1}{\sqrt{2}}(t + \frac{d}{dt}),$$

C'est-à-dire que $a(f)(t) = \frac{1}{\sqrt{2}}(tf(t) + f'(t))$. En général, si $g \in \mathcal{C}^\infty(\mathbb{R})$, on confond dans les notations la fonction g et l'opérateur $f \mapsto gf$ sur $\mathcal{S}(\mathbb{R})$.

— 1. Montrer que son adjoint pour le produit hermitien est

$$a^* = \frac{1}{\sqrt{2}}(t - \frac{d}{dt}).$$

— 2. Vérifier que $[a, a^*] = \mathrm{Id}_{\mathcal{S}(\mathbb{R})}$. En déduire que

$$\phi : \ X \mapsto a, \quad Y \mapsto a^*, \quad Z \mapsto \mathrm{Id}_{\mathcal{S}(\mathbb{R})}$$

définit une représentation de $\mathfrak{h}$ dans $\mathcal{S}(\mathbb{R})$.

— 3. On pose $E = aa^* + a^*a$ et $N = a^*a$. Montrer que $[E, a] = -2a$, $[E, a^*] = 2a^*$ et que $[N, a] = -a$, $[N, a^*] = a^*$.

— 4. Résoudre $Nf = 0$ dans $\mathcal{S}(\mathbb{R})$ (on pourra chercher une solution de la forme $t \mapsto e^{\alpha t^2}$). Montrer qu'il existe une unique solution v_0 de $Nf = 0$ dans $\mathcal{S}(\mathbb{R})$ vérifiant $(v_0, v_0) = 1$.

— 5. Montrer que si v est vecteur propre de N dans $\mathcal{S}(\mathbb{R})$ pour la valeur propre λ, alors $a \cdot v$ est dans le sous-espace propre de N pour la valeur propre $\lambda - 1$ et $a^* \cdot v$ est dans le sous-espace propre pour la valeur propre $\lambda + 1$.

— 6. On définit par récurrence $v_{k+1} = \frac{a^* \cdot v_k}{\sqrt{k+1}}$. Montrer que les $(v_k)_{k\in\mathbb{N}}$ forment une famille orthonormale de $\mathcal{S}(\mathbb{R})$. Montrer que les v_k sont des fonctions de la forme

$$v_k(t) = \frac{H_k(t)}{\sqrt{k+1}} e^{-\frac{t^2}{2}},$$

où les H_k sont des polynômes (polynômes d'Hermite)

— 7. On pose $p = \frac{a-a^*}{\sqrt{2}i} = -i\frac{d}{dt}$ et $q = \frac{a+a^*}{\sqrt{2}} = t$. Justifiez que si l'on pose $u(s) = e^{isq}$ et $v(s) = e^{isp}$ pour tout $s \in \mathbb{R}$, alors pour tout $f \in \mathcal{S}(\mathbb{R})$

$$(u(s)\cdot f)(t) = e^{ist} f(t), \quad (v(s)\cdot f)(t) = f(t+s).$$

(On demande simplement une justification et non une démonstration, car la démonstration complète est hors de portée du fait que $\mathcal{S}(\mathbb{R})$ est de dimension infinie : on pourra admettre que les propriétés de l'exponentielle d'un opérateur sont les mêmes qu'en dimension finie, par exemple le développement en série où l'équation différentielle vérifiée par l'exponentielle).

— 8. Pour tout $\lambda \in \mathbb{R}$, on pose

$$\pi_\lambda(g_{a,b,c}) = e^{2i\pi\lambda c} u(\lambda b) v(a).$$

Montrer que π_λ définit une représentation de H et qu'elle est continue et unitaire.

L'espace $\mathcal{S}(\mathbb{R})$ n'est pas complet pour la norme $||\cdot||_2$. Son complété est l'espace $L^2(\mathbb{R})$. On prolonge π_λ à $L^2(\mathbb{R})$ par continuité. On obtient ainsi une représentation unitaire de H dans l'espace de Hilbert $L^2(\mathbb{R})$.

— 9. Soit A un opérateur sur $L^2(\mathbb{R})$ qui commute avec les translations et la multiplication par t. On admet qu'alors A est un multiple scalaire de l'identité. Déduire des questions précédentes que $(\pi_\lambda, L^2(\mathbb{R}))$ est irréductible.

Corrigé de l'examen du 11 décembre 2006

Exercice 1

a) On sait d'après le cours que $|\widehat{G}|$ est le nombre de classes de conjugaisons de G et que d'autre part $|G| = \sum_{\delta\in\widehat{G}} \dim V_\delta^2$. Un groupe est abélien si et seulement si les classes de conjugaison dans G sont des singletons. Donc si G est abélien

$$|G| = |\widehat{G}| = \sum_{\delta\in\widehat{G}} \dim V_\delta^2.$$

Comme pour tout $\delta \in \widehat{G}$, $\dim V_\delta^2 \geq 1$, on voit que nécessairement $\dim V_\delta = 1$.

Réciproquement, si pour tout $\delta \in \widehat{G}$, $\dim V_\delta^2 = 1$, on obtient $|G| = |\widehat{G}|$, ce qui montre que chaque classe de conjugaison est un singleton.

b) Les relations d'orthogonalité duales affirment que

$$\sum_{\delta\in\widehat{G}} \overline{\Theta_\delta(C_1)}\Theta_\delta(C_2) = 0$$

où Θ_δ est le caractère de δ et C_1, C_2 sont des classes de conjugaison distinctes dans G. Dans le cas où G est abélien, toutes les représentations sont de dimension 1 et coïncident avec leur caractères, de sorte que l'on obtient, en prenant $C_1 = \{e\}$ et $C_2 = \{g\}$, pour tout $g \in G$, $g \neq e$,

$$0 = \sum_{\chi\in\widehat{G}} \overline{\chi(e)}\chi(g) = \sum_{\chi\in\widehat{G}} \chi(g).$$

Ceci montre qu'il existe χ tel que $\chi(g) \neq 1$.

c) Remarquons tout d'abord que puisque l'on a égalité des cardinaux

$$|G| = |\widehat{G}| = |\hat{\widehat{G}}|$$

il suffit de montrer l'injectivité de

$$\mathbf{ev} : G \to \hat{\widehat{G}}$$

pour montrer sa surjectivité.

Le morphisme d'évaluation **ev** est un morphisme de groupes, donc pour montrer l'injectivité, il suffit de voir que son noyau est trivial. Soit $g \in \ker \mathbf{ev}$. On a alors

$$\forall \chi \in \widehat{G}, \quad \chi(g) = 1$$

et d'après *b*), $g = e$.

d) Tout élément $g \in G$ vérifie $g^{p^\alpha} = e$, d'où pour tout $\chi \in \widehat{G}$

$$1 = \chi(e) = \chi(g^{p^\alpha}) = \chi(g)^{p^\alpha}$$

ce qui montre que χ prend ses valeurs dans les racines p^α-ième de l'unité.

e) D'après *c*), comme $x_1 \neq e$, il existe un caractère χ de G tel que $\chi(x_1) \neq 1$. On en déduit que $\chi(x_0)$ est une racine primitive p^β-ième de l'unité. On a donc deux groupes cycliques de même ordre p^β : le sous-groupe H engendré par x_0 dans G et le groupe des racines p^β-ième de l'unité, et un morphisme, χ qui envoie un générateur du premier de ces groupes sur un générateur du second : c'est un isomorphisme.

f) Soit $y \in G$. Il est d'ordre p^γ, avec $\gamma \leq \beta$. Donc $\chi(y)$ est une racine p^γ-ième de l'unité, donc en particulier aussi une racine p^β-ième. On peut donc trouver $h \in H$ tel que $\chi(h) = \chi(y)$. Ceci montre que $\chi(h^{-1}y) = 1$ et donc $h^{-1}y \in \ker \chi$. On peut donc écrire $y = hk$ avec $h \in H$ et $k \in \ker \chi$. Comme *e*) montre que $\ker \chi \cap H = \{e\}$, on en déduit que G est le produit direct de H et K.

g) On recommence avec K ce qu'on a fait avec G. En effet, K est un sous-groupe de G, il est d'ordre $p^{\alpha'}$ avec $\alpha' < \alpha$. On réitère le procédé jusqu'à obtenir G comme produit de groupes cycliques.

h) Soient $x, y \in H$, d'ordre respectifs k et l. Comme G est abélien, l'ordre de xy est $r = \mathrm{ppcm}(k, l)$. Comme k et l divisent n, r aussi, et donc H est un sous-groupe de G. Idem pour K. Un élément dans $H \cap K$ est d'ordre divisant à la fois n et m, donc divisant $\mathrm{pgcd}(m, n) = 1$, donc d'ordre 1. Donc $H \cap K = \{e\}$. Ceci montre que

$$H \times K \to G, \quad (h, k) \mapsto hk$$

est un morphisme de groupes injectif.

Pour la surjectivité, on utilise le théorème de Bézout : puisque m et n sont premiers entre eux, il existe des entiers u et v tels que $um + vn = 1$

et donc tout élément $g \in G$ s'écrit

$$g = g^{um+vn} = g^{um} g^{vn}$$

avec $(g^{um})^n = (g^u)^{mn} = e$, donc $g^{um} \in H$ et de même $g^{vn} \in K$.

i) On décompose $|G|$ en produit de puissances de nombres premiers distincts et on applique les résultats précédents.

Exercice 2

Première partie.

— 1. On fait le calcul. Tout élément de $\mathfrak{h}$ est une combinaison linéaire de X, Y et Z. Le commutateur de deux éléments de $\mathfrak{h}$ est encore une telle combinaison linéaire, donc $\mathfrak{h}$ est une sous-algèbre de Lie de $\mathfrak{gl}(3, \mathbb{R})$.

— 2. On constate que $X^2 = Y^2 = Z^2 = 0$, donc

$$\exp tX = \mathrm{Id} + tX = \begin{pmatrix} 1 & t & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

De même,

$$\exp tY = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \exp tZ = \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

— 3. $g_{a,b,c} = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$.

$$\exp aX \exp bY = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & ab \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix},$$

d'où $\exp aX \exp bY = g_{a,b,ab}$.

On a $\exp(aX + bY + cZ) = g_{a,b,c+\frac{ab}{2}}$, d'où

$$g_{a,b,c} = \exp(aX + bY + (c - \frac{ab}{2})Z).$$

— 4. D'après ce qui précède, le sous-groupe de $\mathbf{GL}(3,\mathbb{R})$ engendré par $\exp \mathfrak{h}$ est

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

Il est clair que l'application exponentielle est injective et surjective.

— 5. Toutes les droites vectorielles dans $\mathfrak{h}$ sont bien sûr des sous-algèbres de Lie. Cherchons maintenant les sous-algèbres de dimension 2. Soient A et B deux éléments engendrant une telle sous-algèbre $\mathfrak{a}$. Le crochet de deux éléments de $\mathfrak{h}$ est toujours dans la droite engendrée par Z. Supposons $[A,B] \neq 0$. Alors A, B et Z sont liés. On peut alors remplacer soit A, soit B par Z pour obtenir une base de $\mathfrak{a}$. Mais on voit alors que le crochet est toujours nul : contradiction. Donc $[A,B] = 0$. Si Z n'est pas dans $\mathfrak{a}$, on voit qu'alors $\mathfrak{h}$ est engendré par A, B et Z : contradiction car $\mathfrak{h}$ serait abélienne. Donc $\mathfrak{a}$ contient Z. Réciproquement, tout espace de dimension 2 qui contient Z est une sous-algèbre abélienne de $\mathfrak{h}$.

— 6. Soit v un vecteur propre non nul pour la valeur propre λ de $\phi(Z)$. On a, pour tout $A \in \mathfrak{h}$, $[Z,A] = 0$, donc

$$0 = \phi([Z,A])\cdot v = \phi(Z)\phi(A)\cdot v - \phi(X)\phi(A)\cdot v = \phi(Z)\phi(A)\cdot v - \lambda\phi(A)\cdot v.$$

Ceci montre que $\phi(A)\cdot v \in V_\lambda$.

— 7. Comme ϕ est irréductible, $V = V_\lambda$ et donc $\phi(Z)$ est l'opérateur $\lambda \mathrm{Id}_V$. Or $\mathrm{Tr}\, \lambda \mathrm{Id}_V = \lambda \dim V$ et

$$\mathrm{Tr}\, \phi(Z) = \mathrm{Tr}\,(\phi([X,Y])) = \mathrm{Tr}\,([\phi(X),\phi(Y)])$$
$$= \mathrm{Tr}\,(\phi(X)\phi(Y)) - \mathrm{Tr}\,(\phi(Y)\phi(X)) = 0.$$

Ceci montre que $\lambda = 0$.

— 8. On a donc $\phi(Z) = 0$ et

$$\phi(Z) = \phi([X,Y]) = [\phi(X),\phi(Y)] = \phi(X)\phi(Y) - \phi(Y)\phi(X) = 0$$

donc les opérateurs $\phi(X)$ et $\phi(Y)$ commutent. Soit v un vecteur propre non nul simultané de $\phi(X)$ et $\phi(Y)$. Il est clair que le sous-espace engendré par ce vecteur est stable par ϕ, et comme ϕ est irréductible, c'est l'espace V tout entier. Donc V est de dimension 1.

— 9. Réciproquement, si α, β sont dans $\mathbb{C}$, on pose $\phi(X) = \alpha$, $\phi(Y) = \beta$, $\phi(Z) = 0$. Il est clair que ceci définit une représentation de dimension 1 de $\mathfrak{h}$. On la note $\phi_{\alpha,\beta}$. Des représentation de dimension 1 sont équivalentes si et seulement si elles sont égales. On cherche maintenant des représentations $\pi_{\alpha,\beta}$ de H telles que $(d\pi_{\alpha,\beta})_{|\mathrm{Id}} = \phi_{\alpha,\beta}$. On doit avoir

$$\pi_{\alpha,\beta}(\exp tZ) = \exp(t\phi_{\alpha,\beta}(Z)) = \exp 0 = \mathrm{Id}$$

$$\pi_{\alpha,\beta}(\exp tX) = \exp(t\phi_{\alpha,\beta}(X)) = \exp t\alpha$$

$$\pi_{\alpha,\beta}(\exp tY) = \exp(t\phi_{\alpha,\beta}(X)) = \exp t\beta$$

D'où $\pi_{\alpha,\beta}(g_{a,b,c}) = \exp(a\alpha)\exp(b\beta)$.

Comme $g_{a,b,c}g_{a',b',c'} = g_{a+a',b+b',c+c'+ab'}$ on voit que, réciproquement,

$$\pi_{\alpha,\beta}(g_{a,b,c}) = \exp(a\alpha)\exp(b\beta)$$

définit une représentation de H, dont la différentielle est $\phi_{\alpha,\beta}$.

Toute représentation π de H définit par différentiation une représentation ϕ de $\mathfrak{h}$. Si π est irréductible, alors ϕ aussi (cours). Les seules représentations irréductibles de H sont donc les $\pi_{\alpha,\beta}$. Elles sont unitaires si et seulement si $\alpha \in i\mathbb{R}$, $\beta \in i\mathbb{R}$.

Deuxième partie.

— 1. On calcule à l'aide d'une intégration par partie :

$$\begin{aligned}
(af_1, f_2) &= \int_{\mathbb{R}} \frac{1}{\sqrt{2}} \left(tf_1(t) + f_1'(t)\right) \overline{f_2(t)}\, dt \\
&= \int_{\mathbb{R}} \frac{1}{\sqrt{2}} f_1(t)\overline{tf_2(t)}\, dt + \int_{\mathbb{R}} \frac{1}{\sqrt{2}} f_1'(t)\overline{f_2(t)}\, dt \\
&= \int_{\mathbb{R}} \frac{1}{\sqrt{2}} f_1(t)\overline{tf_2(t)}\, dt - \int_{\mathbb{R}} \frac{1}{\sqrt{2}} f_1(t)\overline{f_2'(t)}\, dt \\
&= \int_{\mathbb{R}} \frac{1}{\sqrt{2}} f_1(t) \left(\overline{tf_2(t) - f_2'(t)}\right) dt = (f_1, a^* f_2)
\end{aligned}$$

— 2.

$$((aa^* - a^*a)(f))(t) = \frac{1}{2}\left((t + \frac{d}{dt})(t - \frac{d}{dt})f(t) - (t - \frac{d}{dt})(t + \frac{d}{dt})f(t)\right)$$

$$= \frac{1}{2}(t^2 f(t) - t\frac{d}{dt}f(t) + \frac{d}{dt}tf(t) - \frac{d^2}{dt^2}f(t))$$

$$- \frac{1}{2}(t^2 f(t) + t\frac{d}{dt}f(t) - \frac{d}{dt}tf(t) - \frac{d^2}{dt^2}f(t))$$

$$= \frac{d}{dt}tf(t) - t\frac{d}{dt}f(t) = f(t) + tf'(t) - tf'(t) = f(t)$$

On a $\phi([X,Y]) = \phi(Z) = \mathrm{Id}_{\mathcal{S}(\mathbb{R})}$ et $[\phi(X), \phi(Y)] = [a, a^*] = \mathrm{Id}_{\mathcal{S}(\mathbb{R})}$. De même, pour tout $A \in \mathfrak{h}$, $\phi([A,Z]) = \phi(0) = 0$ et $[\phi(A), \phi(Z)] = [\phi(A), \mathrm{Id}_{\mathcal{S}(\mathbb{R})}] = 0$ car $\mathrm{Id}_{\mathcal{S}(\mathbb{R})}$ commute avec tout les opérateurs sur $\mathcal{S}(\mathbb{R})$. Par linéarité, on en déduit que

$$\phi([A,B]) = [\phi(A), \phi(B)]$$

pour tous $A, B \in \mathfrak{h}$, ce qui signifie que ϕ est une représentation de $\mathfrak{h}$ dans $\mathcal{S}(\mathbb{R})$.

— 3. Comme $aa^* = a^*a + 1$

$$[E,a] = (aa^* + a^*a)a - a(aa^* + a^*a) = (2a^*a + 1)a - a(2a^*a + 1)$$

$$= 2a^*a^2 - 2aa^*a = 2a^*a^2 - 2(a^*a + 1)a = -2a$$

De même $[E, a^*] = 2a^*$. Comme $N = \frac{1}{2}(E - [a, a^*]) = \frac{1}{2}(E - \mathrm{Id}_{\mathcal{S}(\mathbb{R})})$, on en déduit

$$[N,a] = -a, \quad [N,a^*] = a^*.$$

— 4. L'équation $N \cdot f = 0$ est l'équation différentielle linéaire du second ordre, homogène

$$\frac{1}{2}((t^2 - 1)f(t) - f''(t)) = 0$$

dont l'espace des solutions est de dimension 2.

Cherchons les solutions sous la forme $t \mapsto e^{\alpha t^2}$. On trouve $\alpha = -\frac{1}{2}$. On cherche une autre solution par la méthode de variation de la constante : $K(t)e^{-\frac{1}{2}t^2}$. On trouve $K''(t) = 2tK'(t)$, soit $K'(t) = Ce^{t^2}$ et l'on obtient une solution linéairement indépendante de la première qui n'est pas à décroissance rapide, donc pas dans $\mathcal{S}(\mathbb{R})$.

Les seules solutions dans $\mathcal{S}(\mathbb{R})$ sont de la forme

$$t \mapsto K_1 e^{-\frac{t^2}{2}}.$$

Si l'on impose de plus la condition $(v_0, v_0) = 1$, ceci fixe la constante K_1.

— 5. On a, pour $v \in \mathcal{S}(\mathbb{R})$ telle que $N \cdot v = \lambda v$

$$-a \cdot v = [N, a] \cdot v = Na \cdot v - aN \cdot v = Na \cdot v - \lambda a \cdot v$$

d'où $Na \cdot v = (\lambda - 1) a \cdot v$. Ceci montre que $a \cdot v$ dans le sous-espace propre de N pour la valeur propre $\lambda - 1$. Le calcul pour $Na^* \cdot v$ est similaire.

— 6. D'après ce qui précède, v_k est vecteur propre de N pour la valeur propre k. Comme $N = a^* a$ est autoadjoint, ses sous-espaces propres sont donc orthogonaux. Pour montrer que $(v_k, v_k) = 1$, on raisonne par récurrence. On a

$$(v_{k+1}, v_{k+1}) = \frac{1}{k+1}(a^* v_k, a^* v_k) = \frac{1}{k+1}(aa^* v_k, v_k)$$

Or $aa^* = N + 1$ d'où

$$(v_{k+1}, v_{k+1}) = \frac{1}{k+1}((N+1) v_k, v_k) = (v_k, v_k).$$

On montre v_k est de la forme voulue par récurrence sur k, sans difficulté. Les H_k sont les polynômes d'Hermitte.

— 8. On a :

$$(e^{isq} \cdot f)(t) = (Id_{\mathcal{S}(\mathbb{R})} \cdot f + isq \cdot f + \frac{(isq)^2}{2!} \cdot f + \frac{(isq)^3}{3!} \cdot f + ...)(t)$$
$$= f(t) + istf(t) + \frac{(ist)^2}{2!} f(t) + \frac{(ist)^3}{3!} f(t) + ... = e^{ist} f(t)$$

Pour calculer $(e^{isp} \cdot f)(t)$, on peut envisager deux méthodes. La première est que $s \mapsto e^{isp}$ est l'unique solution de $a'(s) = ipa(s)$, telle que $a(0) = \mathrm{Id}_{\mathcal{S}(\mathbb{R})}$. Or si l'on pose

$$(a(s) \cdot f)(t) = f(t+s)$$

alors

$$(a'(s) \cdot f)(t) = \frac{d}{ds}(a(s) \cdot f)(t) = \frac{d}{ds} f(t+s) = f'(t+s) = (ipa(s) \cdot f)(t)$$

et bien sûr $a(0) = \mathrm{Id}_{\mathcal{S}(\mathbb{R})}$.

Une autre méthode est de calculer formellement

$$(e^{isp}\cdot f)(t) = (Id_{\mathcal{S}(\mathbb{R})}\cdot f + isp\cdot f + \frac{(isp)^2}{2!}\cdot f + \frac{(isp)^3}{3!}\cdot f + ...)(t)$$
$$= (f + sf' + \frac{s^2 f''}{2!} + \frac{s^3 f^{(3)}}{3!} + ...)(t)$$

On reconnaît le développement de Taylor de $f(t+s)$.

— 8. On veut montrer que

$$\pi_\lambda(g_{a,b,c}) = e^{2i\pi\lambda c}u(\lambda b)v(a)$$

définit bien un morphisme de groupes de H dans $GL(\mathcal{S}(\mathbb{R}))$. Pour cela, il s'agit de vérifier que

$$\pi_\lambda(g_{a,b,c}g_{a',b',c'}) = \pi_\lambda(g_{a,b,c})\pi_\lambda(g_{a',b',c'}).$$

Or $g_{a,b,c}g_{a',b',c'} = g_{a+a',b+b',c+c'+ab'}$ donc

$$\pi_\lambda(g_{a,b,c}g_{a',b',c'}) = \pi_\lambda(g_{a+a',b+b',c+c'+ab'}) = e^{2i\pi\lambda(c+c'+ab')}u(\lambda(b+b'))v(a+a').$$

D'autre part

$$\pi_\lambda(g_{a,b,c})\pi_\lambda(g_{a',b',c'}) = e^{2i\pi\lambda c}u(\lambda b)v(a)e^{2i\pi\lambda c'}u(\lambda b')v(a')$$
$$= e^{2i\pi\lambda(c+c')}u(\lambda b)v(a)u(\lambda b')v(a').$$

Il s'agit de faire commuter $v(a)$ et $u(\lambda b')$. Or

$$(v(a)u(\lambda b')\cdot f)(t) = e^{i\lambda b'(t+a)}f(t+a)$$

et

$$(u(\lambda b')v(a)\cdot f)(t) = e^{i\lambda b' t}f(t+a)$$

D'où

$$\pi_\lambda(g_{a,b,c})\pi_\lambda(g_{a',b',c'}) = e^{2i\pi\lambda(c+c'+ab')}u(\lambda b)u(\lambda b')v(a)v(a')$$
$$= e^{2i\pi\lambda(c+c'+ab')}u(\lambda(b+b'))v(a+a').$$

Montrons maintenant que π_λ est unitaire. Il s'agit de montrer que pour tout $g_{a,b,c}\in H$ et pour toutes fonctions $f_1, f_2 \in \mathcal{S}(\mathbb{R})$, on a

$$(\pi_\lambda(g_{a,b,c})\cdot f_1, \pi_\lambda(g_{a,b,c})\cdot f_2) = (f_1, f_2).$$

Or

$$
\begin{aligned}
&(\pi_\lambda(g_{a,b,c}) \cdot f_1, \pi_\lambda(g_{a,b,c}) \cdot f_2)\\
&= \int_{\mathbb{R}} e^{i\lambda bt} f_1(t+a)\, \overline{e^{i\lambda bt} f_2(t+a)} dt\\
&= \int_{\mathbb{R}} f_1(t+a)\overline{f_2(t+a)} dt = \int_{\mathbb{R}} f_1(t)\overline{f_2(t)} dt \qquad = (f_1, f_2))
\end{aligned}
$$

On a utilisé l'invariance de la mesure de Lebesgue par translation.

Pour la continuité : il s'agit de montrer que

$$H \times \mathcal{S}(\mathbb{R}) \to \mathcal{S}(\mathbb{R}), \quad (g_{a,b,c}, f) \mapsto \pi_\lambda(g_{a,b,c}) \cdot f$$

est continue. Soient $g_{a,b,c}, g_{a',b',c'} \in H$ et $f_1, f_2 \in \mathcal{S}(\mathbb{R})$. On a

$$
\begin{aligned}
&||\pi_\lambda(g_{a,b,c}) \cdot f_1 - \pi_\lambda(g_{a',b',c'}) \cdot f_2||_2\\
&= \left(\int_{\mathbb{R}} |e^{2i\pi\lambda c} e^{i\lambda bt} f_1(t+a) - e^{2i\pi\lambda c'} e^{i\lambda b' t} f_2(t+a')|^2 \, dt \right)^{1/2}\\
&= \left(\int_{\mathbb{R}} |e^{2i\pi\lambda(c-c')} e^{i\lambda(b-b')(t-a')} f_1(t+a-a')) - f_2(t)|^2 \, dt \right)^{1/2}\\
&= ||e^{2i\pi\lambda(c-c')} e^{i\lambda(b-b')(t-a')} f_1(t+a-a')) - f_2(t)||_2\\
&\leq ||e^{2i\pi\lambda(c-c')} e^{i\lambda(b-b')(t-a')} f_1(t+(a-a')) - f_1(t+(a-a'))||_2\\
&+ ||f_1(t+(a-a')) - f_1(t)||_2 + ||f_1(t) - f_2(t)||_2
\end{aligned}
$$

Or

$$
\begin{aligned}
&||e^{2i\pi\lambda(c-c')} e^{i\lambda(b-b')(t-a')} f_1(t+(a-a')) - f_1(t+(a-a'))||_2\\
&= ||(e^{2i\pi\lambda(c-c')} e^{i\lambda(b-b')(t-a)} - 1) f_1(t)||_2
\end{aligned}
$$

Fixons $\epsilon > 0$. Comme f_1 est de carré intégrable, il existe un réel $R > 0$ tel que

$$\int_{\mathbb{R}\setminus[-R,R]} |f_1(t)|^2 \, dt \leq \frac{\epsilon^2}{4}$$

et comme

$$|(e^{2i\pi\lambda(c-c')} e^{i\lambda(b-b')(t-a)} - 1)| \leq 2$$

On obtient

$$\int_{\mathbb{R}\setminus[-R,R]} |(e^{2i\pi\lambda(c-c')}e^{i(a-a')(t-\lambda(b-b')} - 1)f_1(t)|^2\, dt \leq \epsilon^2$$

D'autre part, on si $|c-c'|$ et $|b-b'|$ sont suffisamment petits, on a par continuité uniforme sur le compact $[-R,R]$:

$$\int_{[-R,R]} |(e^{2i\pi\lambda(c-c')}e^{i\lambda(b-b')(t-a)} - 1)f_1(t)|^2\, dt \leq \epsilon^2||f_1||_2^2,$$

d'où :

$$||(e^{2i\pi\lambda(c-c')}e^{i\lambda(b-b')(t-a)} - 1)f_1(t)||_2 \leq \epsilon(1+||f_1||_2^2)^{1/2}.$$

La majoration de $||f_1(t+(a-a'))-f_1(t)||_2$ est similaire. On coupe l'intégrale en deux : sur $\mathbb{R}\setminus[-R,R]$ et sur $[R,R]$, où l'on utilise la continuité uniforme de f_1 et $|a-a'|$ petit. On obtient ainsi

$$||f_1(t+(a-a')) - f_1(t)||_2 \leq \epsilon$$

Au final, on voit que l'on peut rendre

$$||\pi_\lambda((g_{a,b,c})\cdot f_1 - \pi_\lambda((g_{a',b',c'})\cdot f_2||_2$$

aussi petit que l'on veut en prenant $|c-c'|$, $|a-a'|$, $|b-b'|$ et $||f_1-f_2||_2$ suffisamment petits. Ceci montre la continuité.

— 9. Soit A un opérateur d'entrelacement de π_λ avec elle-même. Alors A commute avec les translations et les multiplications par e^{ist}. On a donc pour toute fonction $f \in \mathcal{S}(\mathbb{R})$, pour tout réel s :

$$e^{ist}(A\cdot f)(t) = A(e^{ist}f)$$

et en dérivant par rapport à s, puis en évaluant en $s=0$

$$it(A\cdot f)(t) = A(itf).$$

Donc A commute avec la multiplication par t : on en déduit que A est un opérateur scalaire.

Supposons que π_λ ne soit pas irréductible. Alors il existe un sous-espace W fermé de $L^2(\mathbb{R})$ stable par H, qui n'est ni trivial ni $L^2(\mathbb{R})$ tout entier. Comme π_λ est unitaire, on a $L^2(\mathbb{R}) = W\oplus W^\perp$. Mais alors, les projections sur W et $W^\perp$ sont des opérateurs d'entrelacement de π_λ qui ne sont pas des opérateurs scalaires : contradiction.

Remarque : Il est connu que les $(v_k)_{k\in\mathbb{N}}$ forment une base hilbertienne de $L^2(\mathbb{R})$. On peut utiliser ceci pour montrer qu'un opérateur qui commute avec les translations et les multiplications par t est scalaire.

Examen du 10 décembre 2007

Le but du problème est d'étudier la notion de *paire de Gelfand* et de fonction sphérique relativement à une telle paire. Une paire de Gelfand (G, K) est constituée d'un groupe G et d'un sous-groupe K, tels que pour toute représentation irréductible V de G, l'espace des points fixes de K soit de dimension 0 ou 1. Une caractérisation des paires de Gelfand est que l'algèbre de convolution des fonctions sur G bi-invariantes par K est commutative. La première partie concerne le cas des groupes finis. La seconde partie concerne la paire $(\mathrm{SO}(3), \mathrm{SO}(2))$. On voit sur cet exemple que certains résultats de la première partie se généralisent aux groupes compacts. *Les deux parties sont indépendantes*, sinon dans l'esprit, au moins dans la forme.

Un certains nombres de faits évidents ou venant du cours sont rappelés dans l'énoncé. Il n'est pas demandé de les redémontrer.

Première partie : groupes finis

Soit G un groupe fini. On note 1 son élément neutre, la notation e étant réservée à autre chose. On note $A = \mathcal{F}(G)$ l'algèbre de convolution des fonctions sur G à valeurs complexes.

Soit K un sous-groupe fini de G. On note $\mathbf{1}_K$ la fonction caractéristique de K dans G :

$$\mathbf{1}_K(g) = 1 \text{ si } g \in K, \ 0 \text{ sinon.}$$

I.1. Calculer $\mathbf{1}_K * \mathbf{1}_K$. En déduire une constante c telle que $e = c\mathbf{1}_K$ soit un idempotent de A (c'est-à-dire $e * e = e$).

II.2 Considérons le projecteur $p : \ A \to A, \ f \mapsto f * e$ et notons Ae son image. Déduire la dimension de Ae en calculant la trace de p.

I.3. Montrer que pour tout $k \in K$, $\delta_k * e = e * \delta_k = e$. Soit $g_1, \ldots, g_p$ un système de représentants des classes dans G/K.

Montrer que $(\delta_{g_i} * e)_{i=1,\ldots,p}$ forme une base de Ae.

I.4. Montrer que

$$Ae = \{f \in A |\, f(gk) = f(g),\ (\forall g \in g, \forall k \in K)\}.$$

De même, on pose $q\,:\, A \to A,\ f \mapsto e * f$. On a les résultats (et les notations) analogues à ceux ci-dessus en échangeant gauche et droite. Ainsi

$$eA = \{f \in A |\, f(kg) = f(g),\ (\forall g \in g, \forall k \in K)\} = \{e * h,\ h \in A\}.$$

Remarquons que $f \mapsto \check{f}$, où $\check{f}(g) = f(g^{-1})$ permet d'échanger gauche et droite. Par exemple, $(f * h)\check{} = \check{h} * \check{f}$. On a aussi que $f \mapsto \check{f}$ est un G-isomorphisme entre Ae et eA. Par ailleurs, $eA = \mathrm{Ind}_K^G(1)$, où 1 est la représentation triviale de K. D'après ce qui vient d'être dit, $Ae \simeq \mathrm{Ind}_K^G(1)$ par $f \mapsto \check{f}$.

II.1. Posons $eAe = \{e * f * e, f \in A\} = eAe = Ae \cap eA$. Montrer que eAe est une sous-algèbre de A dont l'unité est e.

II.2. Le groupe G agit sur A par la représentation régulière gauche L. On rappelle que quels que soient $h, f \in A$,

$$L(h) \cdot f = h * f.$$

Montrer que Ae est un sous-espace stable sous l'action de G. On note (L, Ae) cette sous-représentation.

II.3. Considérons l'espace $\mathrm{End}_G(Ae) = \mathrm{Hom}_G(Ae, Ae)$ l'espace des opérateurs d'auto-entrelacement de la représentation (L, Ae). Montrer que

$$\Psi\,:\ \mathrm{End}_G(Ae) \to Ae, \quad \phi \mapsto \phi(e)$$

est à valeurs dans eAe et réalise un isomorphisme entre $\mathrm{End}_G(Ae)$ et eAe. Montrer que $\Psi(\phi_1 \circ \phi_2) = \Psi(\phi_2) * \Psi(\phi_1)$.

II.4. Montrer que les conditions suivantes sont équivalentes :

(i) eAe est commutative.

(ii) $\mathrm{Ind}_K^G(1)$ est sans multiplicité, c'est-à-dire que toute représentation irréductible de G intervient dans la décomposition en irréductibles de $\mathrm{Ind}_K^G(1)$ avec multiplicité 0 ou 1.

(On pourra montrer que si une représentation irréductible apparait avec une multiplicité au moins 2 dans $\mathrm{Ind}_K^G(1)$, alors

$$\mathrm{End}_G(Ae) \simeq \mathrm{End}_G(\mathrm{Ind}_K^G(1))$$

contient une sous-algèbre isomorphe à $M_2(\mathbb{C})$).

Lorsque ces conditions sont réalisées, on dit que (G, K) est une paire de Gelfand. Dans la suite, on suppose que (G, K) est une paire de Gelfand. Ecrivons $Ae = \sum_{i=1}^{s} V_i$, où les V_i sont des représentations irréductibles de G, deux à deux non isomorphes, et l'on note Θ_i le caractère de la représentation de G dans V_i.

III.1. On pose $d_i = \dim V_i$ et $\omega_i = \overline{\Theta_i} * e$. Montrer que

$$\omega_i(1) = 1, \quad w_i(x^{-1}) = \overline{\omega_i(x)}.$$

(On pourra montrer que $\omega_i(1) = (\Theta_{i|K}, \mathbf{1}_K)_K$ où $(.,.)_K$ est le produit hermitien habituel de $\mathbb{C}[K]$ et le fait que $\mathbf{1}_K$ est le caractère de la représentation triviale de K.)

III.2. Montrer que $\omega_i \in eAe \cap V_i$ puis que $eAe \cap V_i = V_i^K$, où V_i^K est l'ensemble des vecteurs de V_i fixés par tous les éléments de K. Pourquoi la dimension de V_i^Kest-elle 1 ?

III.3. Montrer que $\omega_i * \omega_j = \delta_{ij} \frac{1}{d_i} \omega_i$ (δ_{ij} étant ici le symbole de Kronecker), puis que $(\omega_i, \omega_j)_G = \delta_{ij} \frac{1}{d_i}$, $(.,.)_G$ étant le produit hermitien habituel de A. En déduire que les ω_i, $i = 1, \ldots s$ forment une base orthogonale de eAe.

III.4. Montrer que les morphismes d'algèbres (unitaires) de eAe dans $\mathbb{C}$ sont donnés par

$$f \mapsto \omega_i * f(1), \quad (f \in eAe)$$

On appelle les fonctions ω_i les fonctions sphériques de la paire de Gelfand (G, K).

IV.1. Montrer que si pour tout $x \in G$, $Kx^{-1}K = KxK$, alors (G, K) est une paire de Gelfand.

IV.2. Soit G un groupe fini et σ un automorphisme de G tel que $\sigma^2 = \mathrm{Id}_G$. Posons

$$K = \{g \in G |\, \sigma(g) = g\}, \quad P = \{g \in G |\, \sigma(g) = g^{-1}\}.$$

Si $G = KP$ (c'est-à-dire si tout $g \in G$ se décompose en $g = kp$, $k \in K$, $p \in P$), montrer que (G, K) est une paire de Gelfand.

V. Soit ω une fonction à valeurs complexe sur G. Montrer que les conditions suivantes sont équivalentes :

(i) ω est une fonction sphérique de la paire de Gelfand (G, K).

(ii) $\omega(1) = 1, \quad \omega \in eAe$ et pour tout $f \in eAe$, $f * \omega = \lambda_f\, \omega$ pour une certaine constante λ_f.

(iii) $\omega \neq 0$ et

$$\omega(x)\omega(y) = \frac{1}{|K|} \sum_{k \in K} \omega(xky).$$

(Remarque : $(ii) \Rightarrow (iii)$ est un peu plus difficile que le reste : on introduira la fonction

$$\omega_y :\ x \mapsto \frac{1}{|K|} \sum_{k \in K} \omega(xky).$$

et l'on montrera que

$$\lambda_f \omega(y) = f * \omega_y(1) \quad .)$$

Deuxième partie : $(\mathrm{SO}(3), \mathrm{SO}(2))$

Notons $G = \mathrm{SO}(3)$ le groupe des rotations de $\mathbb{R}^3$. L'action d'un élément $g \in G$ sur un vecteur $v \in \mathbb{R}^3$ est notée $g \cdot v$. De même, si f est une fonction sur $\mathbb{R}^3$ à valeurs complexes, on note :

$$g \cdot f \ : v \mapsto f(g^{-1} \cdot v).$$

Soit K le sous-groupe de G des rotations d'axe e_1, (e_1, e_2, e_3) étant la base canonique de $\mathbb{R}^3$.

On munit G et K de mesure de Haar μ_G et μ_K normalisées par $\mu_G(G) = 1$ et $\mu_K(K) = 1$.

— 1. Posons $J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. Notons $\sigma = \mathrm{Ad}(J)$: c'est un automorphisme intérieur de G, et $\sigma^2 = 1$. Quel est le groupe des points fixes de σ ? Décrire ses composantes connexes.

— 2. Notons $P = \{g \in G |\, \sigma(g) = g^{-1}\}$. Montrer que tout élément de G est produit d'une rotation d'axe e_1 (donc d'un élément de K) et d'une rotation dont l'axe est orthogonal à e_1. En déduire que tout élément g de G s'écrit $g = kp$ avec $k \in K$ et $p \in P$. Déterminer $K \cap P$.

— 3. Soit $A = \mathcal{C}(G)$ l'algèbre de convolution des fonctions continues sur G. Posons

$$p(f)(g) = \int_K \int_K f(kgk')\, d\mu_K(k) d\mu_K(k'), \quad (g \in G).$$

Montrer que l'image de p est exactement l'espace des fonctions $f \in A$ bi-invariantes par K, c'est-à-dire vérifiant

$$f(kgk') = f(g), \quad (\forall g \in G, k, k' \in K).$$

Notons A_K l'image de p. Vérifier que A_K est une sous-algèbre (pour la convolution) de A. Possède-t-elle une unité ?

— 4. Si $f \in A$, notons f^σ la fonction $g \mapsto f(\sigma(g))$. Montrer que si $f \in A_K$, alors $f^\sigma = \check{f}$. (On rappelle que $\check{f}$ est la fonction $g \mapsto f(g^{-1})$). En déduire que A_K est commutative (pour la convolution).

Soit Δ le Laplacien de $\mathbb{R}^3$:

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}.$$

Cet opérateur différentiel est invariant sous l'action de G, c'est-à-dire que pour toute fonction f de classe $\mathcal{C}^2$ sur $\mathbb{R}^3$,

$$\Delta(g \cdot f) = g \cdot (\Delta(f)), \quad (\forall g \in G)$$

Notons $\mathcal{P}_l$ l'espace des polynômes homogènes de degré l sur $\mathbb{R}^3$ et $\mathcal{H}_l$ le sous-espace de $\mathcal{P}_l$ des polynômes vérifiant $\Delta(f) = 0$.

—5. Montrer que Δ envoie surjectivement $\mathcal{P}_{l+2}$ dans $\mathcal{P}_l$. Quelle est la dimension de $\mathcal{P}_l$? En déduire la dimension de H_l. Montrer que $\mathcal{H}_l$ est stable sous l'action de G. On note $(\rho_l, \mathcal{H}_l)$ cette représentation de SO(3).

On rappelle que l'algèbre de Lie $\mathfrak{so}(3)$ est l'espace des matrices de la forme :

$$M(x,y,z) = \begin{pmatrix} 0 & -2z & 2y \\ 2z & 0 & -2x \\ -2y & 2x & 0 \end{pmatrix}$$

et que $\mathcal{I} = M(1,0,0)$, $\mathcal{J} = M(0,1,0)$, $\mathcal{K} = M(0,0,1)$ est une base de $\mathfrak{so}(3)$ vérifiant

$$[\mathcal{I}, \mathcal{J}] = 2\mathcal{K}, \quad [\mathcal{J}, \mathcal{K}] = 2\mathcal{I}, \quad [\mathcal{K}, \mathcal{I}] = 2\mathcal{J}.$$

Rappelons que $\mathfrak{so}(3)$ est isomorphe à $\mathfrak{su}(2)$ par

$$M(x,y,z) \mapsto N(x,y,z) = \begin{pmatrix} iz & -y+ix \\ y+ix & -iz \end{pmatrix}.$$

On pose $I = N(1,0,0)$, $J = N(0,1,0)$, $K = N(0,0,1)$.

— 6. Calculer $d\rho(M(x,y,z))$. (On pourra considérer une courbe $t \mapsto c(t) = (c_{ij}(t))_{1 \leq i,j \leq 3}$ dans SO(3) telle que $c(0) = \mathrm{Id}$ et $c'(0) = M(x,y,z)$.)

Nous voulons maintenant montrer que les représentations $(\rho_l, \mathcal{H}_l)$, $l \in \mathbb{N}$, sont irréductibles, et donc (d'après le cours) décrivent à équivalence près toutes les représentations irréductibles de SO(3).

Il suffit de montrer que $(\rho_l, \mathcal{H}_l)$ est isomorphe à la représentation irréductible (π_{2l}, V_{2l}) du cours. (On rappelle que les représentations (π_n, V_n)

de dimension $n+1$ sont les représentations irréductibles de SU(2) construites dans le cours, et que si n est pair, elles se factorisent par la projection de SU(2) sur SO(3)).

— 7. Soit (ϕ, W) une représentation (dans un espace vectoriel complexe W) de $\mathfrak{su}(2)$ de dimension $n+1$ et supposons que $\phi(K)$ admette un vecteur propre dans W de valeur propre in. Montrer que (ϕ, W) est irréductible, et plus précisement qu'elle est isomorphe à la différentielle de la représentation (π_n, V_n).

— 8. Montrer que le polynôme $P(X, Y, Z) = (iX + Y)^l$ est dans $\mathcal{H}_l$ et qu'il est vecteur propre pour $d\rho_l(K)$ pour la valeur propre $2il$. Conclure.

— 9. Montrer que le sous-espace des vecteurs fixés par tout $k \in K$ dans une représentation irréductible de $G = \mathrm{SO}(3)$ est toujours de dimension 1.

Corrigé de l'examen du 10 décembre 2007

Exercice 1

I.1. Calculons, en utilisant que $\mathbf{1}_K(kg) = \mathbf{1}_K(g)$ pour tout $k \in K$:

$$\mathbf{1}_K * \mathbf{1}_K(g) = \frac{1}{|G|} \sum_{t \in G} \mathbf{1}_K(t)\mathbf{1}_K(t^{-1}g) = \frac{1}{|G|} \sum_{t \in K} \mathbf{1}_K(t^{-1}g)$$
$$= \frac{1}{|G|} \sum_{t \in K} \mathbf{1}_K(g) = \frac{|K|}{|G|} \mathbf{1}_K(g).$$

On a utilisé $\mathbf{1}_K(kg) = \mathbf{1}_K(g)$, pour tout $k \in K$ et tout $g \in G$. Ceci resservira souvent.

On prendra donc $c = \frac{|G|}{|K|}$.

I.2. On a (propriété des projecteurs) $\dim \operatorname{Im} p = \operatorname{Tr} p$. Calculons cette trace dans la base des δ_g. On a $p(\delta_g) = \delta_g * e$, et

$$\delta_g * e(y) = \frac{1}{|G|} \sum_{t \in G} \delta_g(t) e(t^{-1}y) = e(g^{-1}y) = \frac{1}{|K|} \sum_{x \in gK} \delta_x(y).$$

Chaque élément δ_g de la base contribue donc de $\frac{1}{|K|}$, et ainsi $\operatorname{Tr} p = \frac{|G|}{|K|}$.

I.3. On a

$$\delta_k * e(g) = \frac{1}{|G|} \sum_{t \in G} \delta_k(t) e(t^{-1}g) = c\mathbf{1}_K(k^{-1}g) = c\mathbf{1}_K(g) = e(g).$$

idem pour l'autre.

$Ae = \operatorname{Im} p$ est l'espace engendré par les $\delta_g * e$. Or pour tout $k \in K$,

$$\delta_{gk} * e = \delta_g * \delta_k * e = \delta_g * e$$

donc Ae est engendré par les $\delta_{g_i} * e$. Comme on a montré que $\dim Ae = \frac{|G|}{|K|}$, ce système de générateurs est minimal, et forme donc une base de Ae.

I.4. Si $f \in Ae$, on a pour tout $g \in G$ et tout $k \in K$,

$$f(gk) = (R(k) \cdot f)(g) = f * \delta_{k^{-1}}(g) = f * e * \delta_{k^{-1}}(g) = f * e = f(g).$$

Réciproquement, si $f(gk) = f(g)$ pour tout $g \in G$, et tout $k \in K$, on a

$$\begin{aligned} f * e(g) &= \frac{1}{|G|}\sum_{t\in G} f(t)e(t^{-1}g) = \frac{1}{|G|}\sum_{t\in G} f(gt)e(t^{-1}) \\ &= \frac{1}{|G|}\sum_{k\in G} f(gk)e(k^{-1}) = \frac{1}{|G|}\sum_{k\in G} f(gk)\frac{|G|}{|K|} = f(g), \end{aligned}$$

et donc $f \in Ae$.

II.1. Si $e*f_1*e$ et $e*f_2*e$ sont dans eAe, on a $(e*f_1*e)*(e*f_2*e) = e*f_1*e*f_2*e \in eAe$, et donc eAe est une sous-algèbre. Comme pour tout $f \in eAe = eA \cap Ae$, $e*f = f*e = f$, e est l'unité de cette algèbre.

II.2. Soit $f \in Ae$. On a pour tout $k \in K$:

$$(L(y)\cdot f)(gk) = f(y^{-1}gk) = f(y^{-1}g) = (L(y)\cdot f)(g)$$

et donc $L(y)\cdot f \in Ae$.

II.3 . Soit $\phi \in \mathrm{End}_G(Ae)$. Alors

$$e*\phi(e) = L(e)\cdot\phi(e) = \phi(L(e)\cdot e) = \phi(e*e) = \phi(e)$$

Donc $\phi(e) \in eAe$.

Montrons que Ψ est injective. Comme cette application est linéaire, il suffit de voir que si $\phi(e) = 0$, alors $\phi = 0$. Or dans cette hypothèse, on a pour tout $f \in Ae$,

$$\phi(f) = \phi(f*e) = f*\phi(e) = 0,$$

ce qui montre le résultat voulu.

Montrons que Ψ est surjective. Si $f \in eAe$, définissons $\phi \in \mathrm{End}_G(Ae)$ par

$$\phi : h \mapsto h*f$$

Il est clair que $h*f$ est bien dans Ae, et que pour tout $g \in G$,

$$\phi(L(g)\cdot h) = \phi(\delta_g * h) = \delta_g * h * f = L(g)\cdot(\phi(h)),$$

ce qui montre que ϕ est bien un opérateur d'entrelacement. De plus $\phi(e) = e*f = f$, ce qui montre que Ψ est surjective.

Enfin, $(\phi_1\circ\phi_2))(e) = \phi_1(\phi_2(e)) = \phi_1(\phi_2(e)*e) = \phi_1(L(\phi_2(e))\cdot e) = L(\phi_2(e))\cdot\phi_1(e) = \phi_2(e)*\phi_1(e)$.

II.4 . Remarquons que comme $Ae \simeq \mathrm{Ind}_K^G 1$ en tant que représentation de G, (ii) est équivalent à : Ae est sans multiplicité. Décomposons Ae en somme directe de sous-représentations irréductibles de G :

$$Ae = \bigoplus_{i=1}^{s} V_i.$$

Et donc

$$eAe \simeq \mathrm{End}_G(Ae) \simeq \mathrm{Hom}_G(\oplus_i V_i, \oplus_j V_j).$$

Cet isomorphisme étant un antiautomorphisme d'algèbres, eAe est commutative si et seulement si $\mathrm{End}_G(Ae)$ l'est.

Or un G-endomorphisme préserve les composantes isotypiques. Donc si les multiplicités sont ≤ 1, on a

$$\mathrm{Hom}_G(\bigoplus_i V_i, \bigoplus_j V_j) = \bigoplus_i \mathrm{Hom}_G(V_i, V_i) = \bigoplus_i \mathbb{C}$$

la dernière égalité étant le lemme de Schur. Remarquons au passage que $\dim eAe = s$. Réciproquement, si une sous-représentation irréductible apparait dans Ae avec multiplicité au moins 2, disons $V_1 \simeq V_2$ par exemple. Alors

$$\mathrm{Hom}_G(\bigoplus_i V_i, \bigoplus_j V_j)$$

contient une sous-algèbre isomorphe à $M_2(\mathbb{C})$ et n'est donc pas commutative : en effet, soit ϕ_1 l'identité de V_1 prolongée par 0 à tous les autres V_i, ϕ_2 l'identité de V_2 prolongée par 0 à tous les autres V_i, ϕ_3 un G-isomorphisme entre V_1 et V_2, prolongé par 0 sur les autres V_i et ϕ_4 l'inverse de ϕ_3 entre V_2 et V_1, prolongé par 0 sur les autres V_i. On vérifie que

$$\phi_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \phi_2 \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad \phi_3 \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \phi_4 \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

donne l'isomorphisme voulu.

III.1. Calculons

$$\omega_i(1) = \overline{\Theta_i} * e(1) = \frac{1}{|G|} \sum_{t \in G} \overline{\Theta_i}(t) e(t^{-1}) = \frac{1}{|K|} \sum_{t \in K} \overline{\Theta_i}(t) = (\Theta_{i|K}, \mathbf{1}_K)_K.$$

Donc par réciprocité de Frobénius

$$\omega_i(1) = (\Theta_{i|K}, \mathbf{1}_K)_K = (\Theta_i, \mathrm{Ind}_K^G(1))_G = 1$$

car V_i apparait avec multiplicité 1 dans $\mathrm{Ind}_K^G(1)$.

Calculons

$$\check{\omega}_i = (\overline{\Theta}_i * e)\check{} = \check{e} * \check{\overline{\Theta_i}} = e * \Theta_i = \Theta_i * e = \overline{\omega_i}.$$

— III.2 . Comme $\omega_i = \overline{\Theta}_i * e = e * \overline{\Theta}_i$, il est clair que $\omega_i \in eAe = Ae \cap eA$. On sait (cours) que la composante isotypique de Ae de type V_i (c'est-à-dire V_i elle-même à cause de la multiplicité 1) est

$$L(\overline{\Theta_i}) \cdot Ae = \overline{\Theta_i} * A * e = A * \overline{\Theta_i} * e = A * \omega_i.$$

Donc $\omega_i \in V_i$.

Soit $f \in eAe \cap V_i$. Alors pour tout $k \in K$,

$$L(k) \cdot f = \delta_k * f = \delta_k * e * f = e * f = f$$

donc $f \in V_i^K$. Réciproquement, si $f \in V_i^K \subset Ae$, alors $e * f = L(e) \cdot f = f$. Ainsi f est dans eA, donc dans eAe.

Comme la dimension de V_i^K est la multiplicité de la représentation triviale de K dans V_i, d'après la réciprocité de Frobénius on a

$$\dim V_i^K = (\Theta_{iK}, \mathbf{1}_K)_K = (\Theta_i, \Theta_{\mathrm{ind}_K^G(1)})_G = 1.$$

— III.3. Les idempotents $e_i = d_i \overline{\Theta_i}$ vérifient (*cf.* cours)

$$e_i * e_j = \delta_{ij} e_i$$

On en déduit que

$$\omega_i * \omega_j = (e * \overline{\Theta_i}) * (\overline{\Theta_j} * e) = \frac{\delta_{ij}}{d_i} e * \omega_i * e = \frac{\delta_{ij}}{d_i} \omega_i$$

D'où

$$(\omega_i, \omega_j)_G = \omega_i * \omega_j(1) = \frac{\delta_{ij}}{d_i} \omega_i(1) = \frac{\delta_{ij}}{d_i}.$$

Les ω_i, $i = 1, \ldots, s$ forment un système orthogonal de eAe. Il suffit de montrer que $\dim(eAe) = s$ pour conclure que c'est une base. Or ceci a été déjà établi dans la preuve de 9.

— III.4. Dans l'exercice II.8.10 du poly, nous avons vu que les morphismes d'algèbres de A^G dans $\mathbb{C}^\times$ sont donnés par les

$$\chi_\delta : \; f \mapsto d_\delta^{-1}(\Theta_\delta, f), \quad (\delta \in \hat{G})$$

L'idée est la même ici, eAe remplaçant $A^G = \mathcal{F}(G)^G$ et les ω_i jouant le rôle des χ_δ.

Soit donc $\chi : eAe \to \mathbb{C}$ un morphisme d'algèbres. On a

$$\chi(\omega_i)\chi(\omega_j) = \chi(\omega_i * \omega_j) = \frac{\delta_{ij}}{d_i}\chi(\omega_i).$$

Ceci montre, comme χ n'est pas identiquement nul et que les ω_i forment une base de eAe, qu'il existe un i tel que $\chi(\omega_i) = (d_i)^{-1}$ et que $\chi(\omega_j) = \frac{\delta_{ij}}{d_i} = w_i * w_j(1)$. Par linéarité

$$\chi(f) = w_i * f(1), \quad (f \in eAe).$$

La réciproque est claire, car par linéarité, il suffit de vérifier que

$$\omega_i * (\omega_j * \omega_k)(1) = \omega_i * \omega_j(1)\ \omega_i * \omega_k(1),$$

ce qui est immédiat avec les formules ci-dessus.

IV.1. Si $Kx^{-1}K = KxK$ pour tout $x \in G$, alors $\check{f}(x) = f(x^{-1}) = f(x)$ pour tout $f \in eAe$. On a alors, pour $f, h \in eAe$:

$$f * h(g) = \frac{1}{|G|}\sum_{t\in G} f(t)h(t^{-1}g) = \frac{1}{|G|}\sum_{t\in G} f(t^{-1})h(g^{-1}t)$$
$$= \frac{1}{|G|}\sum_{t\in G} h(t)f(t^{-1}g^{-1}) = h * f(g^{-1}) = h * f(g).$$

Plus conceptuellement $f * h = (f * h)\check{} = \check{h} * \check{f} = h * f$.

IV.2 Si $x = kp$, alors $\sigma(x) = kp^{-1} = kx^{-1}k$, et donc

$$K\sigma(x)K = Kx^{-1}K, (\forall x \in G).$$

L'argument est alors le même que ci-dessus, en introduisant les σ à l'endroit voulu :

$$f * h(g) = \frac{1}{|G|}\sum_{t\in G} f(t)h(t^{-1}g) = \sum_{t\in G} f(\sigma(t)^{-1})h(\sigma(g^{-1}t))$$
$$= \sum_{t\in G} h(t)f(t^{-1}\sigma(g)^{-1}) = h * f(\sigma(g^{-1})) = h * f(g)$$

V. $(i) \Rightarrow (ii)$. On a vu dans les questions précédentes que si ω est une fonction sphérique, alors $\omega(1) = 1$ et $\omega \in eAe$. D'autre part, si $f \in eAe$, on voit en le décomposant dans la base des ω_i

$$f = \sum_i a_i \omega_i,$$

que $f * \omega_j = a_j (d_j)^{-1} \omega_j$.

$(ii) \Rightarrow (iii)$. On a bien sûr $\omega \neq 0$ puisque $\omega(1) = 1$. Posons, pour $y \in G$,

$$\omega_y(x) = \frac{1}{|K|} \sum_{k \in K} \omega(xky).$$

Comme on suppose ω bi-invariante par K, on voit que ω_y est aussi bi-invariante par K, c'est-à-dire $\omega_y \in eAe$. Pour tout $f \in eAe$ et tout $k \in K$, on a

$$\lambda_f \omega(y) = \lambda_f \omega(ky) = f * \omega(ky) = \frac{1}{|G|} \sum_{x \in G} f(x^{-1}) \omega(xky).$$

En en moyennant sur k, on obtient

$$\lambda_f \omega(y) = \frac{1}{|G|} \sum_{x \in G} \frac{1}{|K|} \sum_{k \in K} f(x^{-1}) \omega(xky) = \frac{1}{|G|} \sum_{x \in G} f(x^{-1}) \omega_y(x) = f * \omega_y(1).$$

D'autre part,

$$\lambda_f = \lambda_f \omega(1) = f * \omega(1)$$

et donc

$$(f * \omega)(1) \omega(y) = (f * \omega_y)(1),$$

ce que l'on réécrit

$$(f * (\omega(y)\omega - \omega_y))(1) = 0.$$

En prenant $f = e$, on obtient $\omega_y = \omega(y)\omega$, c'est-à-dire

$$\omega(y)\omega(x) = \frac{1}{|K|} \sum_{k \in K} \omega(xky).$$

$(iii) \Rightarrow (i)$. Si $f, h \in eAe$, on a

$$\omega * f * h(1) = \sum_{x,y \in G} \omega(xy) f(y^{-1}) h(x^{-1}) = \sum_{x,y \in G} \omega(xky) f(y^{-1}) h(x^{-1}),$$

pour tout $k \in K$. En moyennant sur K, on obtient

$$\omega * f * h(1) = \sum_{x,y \in G} \omega(x)\omega(y) f(y^{-1}) h(x^{-1}) = (\omega * f)(1)\,(\omega * h)(1).$$

Ceci montre que $f \mapsto \omega * f(1)$ est un morphisme d'algèbres de eAe dans $\mathbb{C}$, et donc ω est une fonction sphérique d'après 13.

Exercice 2

Remarque : $J^{-1} = J$.

— 1. Un calcul direct montre que le groupe des points fixes de σ est l'ensemble des matrices de la forme

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -\cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \end{pmatrix}$$

et donc $G^\sigma = K \coprod BK$ où B est la matrice $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Le groupe K est la composante connexe de l'identité de G^σ, la seule autre composante connexe étant BK.

— 2. Tout élément g de SO(3) est une rotation admettant un axe. Si cet axe est la droite engendré par e_1, $g \in K$ et l'assertion est claire. Sinon, on prend une rotation $y \in \mathrm{SO}(3)$ d'axe u perpendiculaire à $g(e_1) \neq e_1$ et e_1 amenant $g(e_1)$ sur e_1 (en particulier u est dans le plan (e_2, e_3) . On a alors $yg(e_1) = e_1$, donc $yg = k \in K$, ou encore $g = ky^{-1}$. Il reste à montrer que y^{-1} est dans P. Regardons l'effet de JyJ sur la base $(e_1, y(e_1), u)$ de $\mathbb{R}^3$. Tout d'abord, comme u est dans le plan (e_2, e_3), $Ju = -u$, d'où

$$Jy^{-1}J(u) = u = y(u).$$

D'autre part, J laisse stable le plan orthogonal à u, c'est-à-dire le plan $(e_1, y(e_1))$. Ses valeurs propres dans ce plan sont 1 et -1, et $J(e_1) = 1$. La restriction de J au plan $(e_1, y(e_1))$ est donc une symétrie par rapport à la droite engendrée par e_1. On en déduit que la restriction de $Jy^{-1}J$ au plan $(e_1, y(e_1))$ est l'inverse de la restriction de y^{-1} à ce plan. Donc $Jy^{-1}J = y$.

$K \cap P$ est constitué des éléments de K égaux à leurs inverses, c'est-à-dire l'identité et J.

— 3. Pour tous $k_1, k_2 \in K$ et tout $g \in G$,

$$\begin{aligned} p(f)(k_1 g k_2) &= \int_K \int_K f(k k_1 g k_2 k')\, d\mu_K(k) d\mu_K(k') \\ &= \int_K \int_K f(k g k')\, d\mu_K(k) d\mu_K(k') = p(f)(g) \end{aligned}$$

On utilise l'invariance par translation à gauche et à droite de la mesure de Haar μ_K. La fonction $p(f)$ est donc bi-invariante par K.

Il est immédiat si f est bi-invariante par K que $p(f) = f$. L'application linéaire p est le projecteur sur le sous-espace A_K des fonctions bi-invariantes par K.

Si f et h sont dans A_K, k, k' dans K et g dans G, on a

$$\begin{aligned} f * h(kgk') &= \int_G f(t) h(t^{-1} k g k')\, d\mu_G = \int_G f(t) h(t^{-1} k g)\, d\mu_G \\ &= \int_G f(kt) h(t^{-1} g)\, d\mu_G = \int_G f(t) h(t^{-1} g)\, d\mu_G = f * h(g) \end{aligned}$$

L'algèbre A_K n'a pas d'unité.

— 4. Ecrivons $g = kp$, $k \in K$, $p \in P$. On a alors

$$f^\sigma(g) = f(\sigma(g)) = f(\sigma(kp)) = f(kp^{-1}) = f(kg^{-1}k) = (g^{-1}) = \check{f}(g).$$

L'idée est que σ est un automorphisme, alors que $f \mapsto \check{f}$ est un anti-automorphisme. S'il sont égaux, c'est que A_K est commutative :

$$\check{h} * \check{f} = (f * h)\check{} = (f * h)^\sigma = f^\sigma * h^\sigma = \check{f} * \check{h}.$$

Mais $f \mapsto f^\sigma$ est-il bien un automorphisme de l'algèbre A_K ?

On a pour $f, h \in A_K$,

$$(f * h)^\sigma(g) = (f * h)(\sigma(g)) = \int_G f(t) h(t^{-1} \sigma(g))\, d\mu_G$$

On a envie de faire le changement de variable $t \mapsto \sigma(t)$, ce qui donne

$$(f * h)^\sigma(g) = \int_G f(\sigma(t)) h(\sigma(t^{-1} g))\, d\mu_G = \int_G f^\sigma(t) h^\sigma(t^{-1} g))\, d\mu_G = (f^\sigma * h^\sigma)(g).$$

Mais on a utilisé le fait que la mesure μ_G est invariante par σ, c'est-à-dire que si l'on définit la mesure μ_G^σ par

$$\int_G f(g)\, d\mu_G^\sigma(g) := \int_G f^\sigma(g)\, d\mu_G(g),$$

on a $\mu_G^\sigma = \mu_G$. On montre ceci comme dans le cours, pour montrer que la mesure de Haar à gauche sur un groupe compact est aussi une mesure de Haar à droite.

On voit que facilement μ_G^σ est encore une mesure de Haar à gauche. On en déduit que $\mu_G^\sigma = c\mu_G$ pour une certaine constante réelle positive c. On voit que $c = 1$ en évaluant sur la fonction constante égale à 1.

— 5. Montrons la surjectivité de $\Delta : \ \mathcal{P}_{l+2} \to \mathcal{P}_l$. Remarquons que pour tout $q \in \mathbb{N}$, les polynômes Z^q, XZ^q et YZ^q sont dans l'image de Δ :

$$\Delta(Z^{q+2}) = (q+2)(q+1)Z^q, \quad \Delta(XZ^{q+2}) = (q+2)(q+1)XZ^q,$$

$$\Delta(YZ^{q+2}) = (q+2)(q+1)YZ^q.$$

Comme pour tous $k, m, q \in \mathbb{N}$,

$$\Delta(X^kY^mZ^q) = k(k-1)X^{k-2}Y^mZ^q + m(m-1)X^kY^{m-2}Z^q + q(q-1)X^kY^mZ^{q-2},$$

si $X^kY^mZ^q \in \operatorname{Im}\Delta$ pour $k+m = n-2$ et tout $q \in \mathbb{N}$, alors $X^kY^mZ^q \in \operatorname{Im}\Delta$ pour tout $k+m = n$ et tout $q \in \mathbb{N}$. Comme elle est vraie pour $n = 0, 1$, elle est démontrée par récurrence.

Comme $\dim \mathcal{P}_l = \sum_{i=0}^{l} i + 1 = \frac{(l+1)(l+2)}{2}$ (on fixe le degré en Z égal à $l - i$, la dimension des polynômes en X et Y homogènes de degré i est $i+1$, on somme sur i), on obtient :

$$\dim \mathcal{H}_l = \dim \ker[\Delta : \mathcal{P}_l \to \mathcal{P}_{l-2}] = \dim \mathcal{P}_l - \dim \mathcal{P}_{l-2} = 2l + 1.$$

L'action de G préserve évidemment les polynômes homogènes et leurs degrés, donc stabilise $\mathcal{P}_l$. Si $P \in \mathcal{H}_l$, c'est-à-dire si $\Delta P = 0$, alors $\Delta(g \cdot P) = g \cdot \Delta(P) = 0$, pour tout $g \in G$. On voit donc que l'action de G stabilise $\mathcal{H}_l$.

— 6. Considérerons une courbe $t \mapsto c(t) = (c_{ij}(t))_{1\leq i,j\leq 3}$ dans SO(3) telle que $c(0) = \mathrm{Id}$ et $c'(0) = M(x, y, z)$.)

Soit $P = P(X,Y,Z)$ un polynôme dans $\mathcal{H}_l$. On a

$$c(t)\cdot P(X,Y,Z) = P(c(t)^{-1}\cdot(X,Y,Z)) = P({}^t c(t)\cdot(X,Y,Z))$$
$$= P(c_{11}(t)X + c_{21}(t)Y + c_{31}(t)Z, c_{12}(t)X + c_{22}(t)Y + c_{32}(t)Z, c_{13}(t)X + c_{23}(t)Y + c_{33}(t)Z)$$

En dérivant par rapport à t et en prenant la valeur en $t = 0$, on obtient :

$$d\rho(M(x,y,z)\cdot P(X,Y,Z)) = (2zY - 2yZ)\partial_1 P(X,Y,Z)$$
$$+(-2zX + 2xZ)\partial_2 P(X,Y,Z) + (2yX - 2xY)\partial_3 P(X,Y,Z)$$

— 7. La représentation de $\mathfrak{su}(2)$ dans W se prolonge par linéarité en une représentation de $\mathfrak{sl}(2,\mathbb{C})$ dans W. Avec les notations du cours $K = ih$, donc l'hypothèse est que $\phi(h)$ admette la valeur propre n. On décompose W en somme directe de représentations irréductibles de $\mathfrak{sl}(2,\mathbb{C})$:

$$W \simeq \bigoplus_{j\in\mathbb{N}} m_j V_j.$$

Puisque n est valeur propre de $\phi(h)$, il existe $j \in n$ tel que $j \geq n$. Donc $\dim W \geq j+1 \geq n+1$. Or $\dim W = n+1$ par hypothèse, donc $j = n$ et $m_i = 0$, $i \neq j$.

— 8. Il est clair que $P = (iX+Y)^l$ est dans $\mathcal{P}_l$ et que $\Delta(P) = 0$. D'autre part

$$d\rho_l(\mathcal{K})\cdot P(X,Y,Z) = 2Y\partial_1 P(X,Y,Z) - 2X\partial_2 P(X,Y,Z)$$
$$=2Yli(iX+Y)^{l-1} - 2lX(iX+Y)^{l-1} = 2ilP(X,Y,Z).$$

D'après la question précédente, $(\rho_l, \mathcal{H}_l) \simeq (\pi_{2l}, V_{2l})$.

— 9. L'algèbre de Lie de K est la sous-algèbre des éléments $M(x,0,0)$ de $\mathfrak{so}(3)$. Elle est engendré par l'élément $\mathcal{I}$. Le sous-espace des vecteurs fixés par l'action du groupe K dans $\mathcal{H}_l$ est le sous-espace propre de $d\rho_l(\mathcal{I})$ pour la valeur propre 0.

On sait que la multiplicité de la valeur propre 0 de $\phi(h)$ dans une représentation irréductible (ϕ, W) de $\mathfrak{sl}(2,\mathbb{C})$ est 0 si $\dim W$ est paire, 1 si $\dim W$ est impaire. Donc la multiplicité de la valeur propre 0 de $d\rho_l(\mathcal{K})$ dans $\mathcal{H}_l$ est 1.

Or $\mathcal{I}$,$\mathcal{J}$ et $\mathcal{K}$ sont indicernables du point de vue de la structure d'algèbre de Lie de $\mathfrak{so}(3)$, donc ce qui est vrai pour $\mathcal{K}$ doit être vrai pour $\mathcal{I}$.

Un peu plus rigoureusement :

$$\theta : \mathcal{I} \mapsto \mathcal{K}, \quad \mathcal{J} \mapsto \mathcal{I}, \quad \mathcal{K} \mapsto \mathcal{J}$$

est un isomorphisme d'algèbre de Lie, la représentation $(d\rho_l \circ \theta, \mathcal{H}_l)$ est irréductible de dimension $l+1$, donc isomorphe à ρ_l, et $d\rho_l \circ \theta(\mathcal{I})$ admet un sous-espace propre pour la valeur propre 0 de dimension 1. Il en est donc de même de $d\rho_l(\mathcal{I})$.

On peut aussi faire un calcul direct...

Examen du 10 décembre 2008

Exercice I. Groupes finis

On donne, à toute fin utile, les formules suivantes : pour $k \in \mathbb{N}^*$,

$$\sum_{x=0}^{k-1} \cos^2\left(\frac{\pi\alpha x}{k}\right) = \begin{cases} k \text{ si } \alpha = 0 \text{ ou } \alpha = k \\ \frac{k}{2} \text{ si } \alpha = 1, \ldots, k-1. \end{cases}$$

$$\sum_{x=0}^{k} \cos^2\left(\frac{2\pi\alpha x}{2k+1}\right) = \begin{cases} k+1 \text{ si } \alpha = 0 \\ \frac{2k+3}{4} \text{ si } \alpha = 1, \ldots, k-1. \end{cases}$$

Soit $G = \mathbb{Z}/n\mathbb{Z} \times \{\pm 1\}$ muni de la loi de groupe

$$(x, \epsilon)(y, \epsilon') = (x + \epsilon y, \epsilon\epsilon'),$$

et soit H le sous-groupe $\mathbb{Z}/n\mathbb{Z} \times \{1\} \simeq \mathbb{Z}/n\mathbb{Z}$ de G.

— 1. Rappeler quelles sont les représentations irréductibles de H.

— 2. Montrer que si n est pair, $n = 2k$, il y a $k+3$ classes de conjugaison dans G, et si n est impair, $n = 2k+1$, il y en a $k+2$. Donner un représentant de chacune de ces classes, et leur nombre d'éléments.

—3. Soit χ une représentation irréductible de H, et $\pi_\chi = \mathrm{Ind}_H^G \chi$. Quelle est la dimension de π_χ. Calculer le caractère de π_χ (on pourra par exemple utiliser la formule pour le caractère des représentations induites de l'exercice III.4.1). Etablir pour quels χ la représentation π_χ est irréductible, et parmi celles-ci, lesquelles sont équivalentes.

—4. Notons χ_0 la représentation triviale de H et $\pi_0 = \mathrm{Ind}_H^G \chi_0$. Montrer que la représentation triviale de G apparait avec multiplicité 1 dans π_0 et que π_0 est somme de la représentation triviale de G et d'une autre représentation ρ_1 dont on calculera le caractère.

—5. Montrer que G possède (à équivalence près) $k-1$ représentations irréductibles de dimension 2 et 4 représentations de dimension 1 dans le cas $n = 2k$. Dans le cas $n = 2k + 1$, montrer qu'il y a k représentations irréductibles de dimension 2 et 2 de dimension 1.

—6. Montrer que si $n = 2k$, la formule $\rho_2((x, \epsilon)) = (-1)^x$ définit une représentation de dimension 1 de G qui apparait avec multiplicité 1 dans une des représentations réductibles π_χ déterminée au 3. En déduire que π_χ est somme de ρ_2 et de ρ_3 où ρ_3 est une représentation irréductible de G dont on donnera le caractère.

—7. Conclure en donnant (à équivalence près) la liste des représentations irréductibles de G.

Exercice II. Groupes linéaires

—1. Soit G un groupe linéaire connexe et $\mathfrak{g}$ son algèbre de Lie. Soit $Z(G)$ le centre de G, et $\mathfrak{z}$ le centre de $\mathfrak{g}$, c'est-à-dire

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

Montrer que $\mathfrak{z}$ est l'algèbre de Lie de $Z(G)$.

—2. Supposons de plus G compact. Soit

$$\mathfrak{g} = \bigoplus_{i=1}^{k} V_i$$

une décomposition de la représentation adjointe de G dans $\mathfrak{g}$ en somme de représentations irréductibles. Montrer que chaque V_i est un idéal de $\mathfrak{g}$ qui ne contient aucun autre idéal propre.

—3. Soit $[\mathfrak{g}, \mathfrak{g}]$ le sous-espace de $\mathfrak{g}$ engendré par les éléments de la forme $[X, Y]$, $X, Y \in \mathfrak{g}$. Montrer que $[\mathfrak{g}, \mathfrak{g}]$ est un idéal de $\mathfrak{g}$ ainsi que chacun des $[V_i, V_i]$.

—4. Montrer que si $\dim V_i = 1$, alors $V_i \subset \mathfrak{z}$, et que si $\dim V_i > 1$, alors $[V_i, V_i] = V_i$. En déduire que

$$\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}] \oplus \mathfrak{z},$$

où $\mathfrak{z}$ est la somme des V_i de dimension 1 et $[\mathfrak{g}, \mathfrak{g}]$ la somme des autres V_i.

—5. On abandonne (provisoirement) l'hypothèse que G est compact (G est un groupe linéaire connexe). On note (G, G) le sous-groupe de G

engendré par les éléments de la forme $xyx^{-1}y^{-1}$, $x, y \in G$. Montrer que (G, G) est un sous-groupe distingué connexe de G.

—6. Montrer que $[\mathfrak{g}, \mathfrak{g}] \subset \mathrm{Lie}((G, G))$. On pourra pour cela considérer

$$\exp tX \exp sY \exp -tX \exp -sY, \quad s, t \in \mathbb{R}, \quad X, Y \in \mathfrak{g}.$$

On suppose de nouveau G compact, disons $G \subset \mathbf{GL}(W)$, où W est un espace vectoriel complexe de dimension finie. En particulier W est l'espace d'une représentation (fidèle) de G, notée π, que l'on décompose en une somme directe de sous-représentations irréductibles :

$$W = \bigoplus_{j=1}^{l} W_j.$$

Pour tout $g \in G$, notons $\pi_j(g)$ la restriction de $\pi(g)$ à W_j, définissons

$$\chi_j : G \mapsto \mathbb{C}^\times, \quad g \mapsto \det(\pi_j(g)),$$
$$\phi : G \mapsto (\mathbb{C}^\times)^l, \quad g \mapsto (\det(\pi_j(g)))_{j=1,\ldots,l},$$

et posons $H = \ker \phi$, et $\mathfrak{h} = \mathrm{Lie}(H)$.

—7. Soit $Z \in \mathfrak{z}$ et soit $t \in \mathbb{R}$. Montrer que $\pi_j(\exp tZ)$ est de la forme $c_j(t)\mathrm{Id}_{W_j}$, où $c_j(t) \in \mathbb{C}^\times$, $c_j(0) = 1$. En déduire que

$$d\pi_{\mathrm{Id}}(Z) = \oplus_{j=1,\ldots,n}(d\pi_j)_{\mathrm{Id}}(Z) = \oplus_{j=1,\ldots,n} c'(0)\,\mathrm{Id}_{W_j}.$$

et que $d\phi_{\mathrm{Id}}(Z) = 0$ si et seulement $Z = 0$.

—8. Montrer que $[\mathfrak{g}, \mathfrak{g}] \subset \ker d\phi_{\mathrm{Id}}$.

(On rappelle que la différentielle du déterminant en l'identité est la trace :

$$(d\det)_{\mathrm{Id}}(X) = \frac{d}{dt}_{|t=0} \det(\mathrm{Id} + tX) = \mathrm{Tr}\,(X),$$

car $\mathrm{Tr}\,(X)$ est le coefficient du terme de degré $n - 1$ dans le polynôme caractéristique de $-X$.)

En déduire que $[\mathfrak{g}, \mathfrak{g}] = \ker d\phi_{\mathrm{Id}}$, puis que $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{h}$.

—9. Montrer que $(G, G) \subset H$. En déduire que $\mathrm{Lie}(G, G) = \mathfrak{h} = [\mathfrak{g}, \mathfrak{g}]$.

Corrigé de l'examen du 10 décembre 2008

Exercice I. Groupes finis

—1. Les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ sont de dimension 1 et sont données par

$$\chi_\alpha(x) = e^{\frac{2i\pi\alpha x}{n}}, \quad (x \in \mathbb{Z}/n\mathbb{Z}),$$

avec $\alpha = 0, \ldots, n-1$.

—2. Calculons

$$\begin{aligned}
&(x,\epsilon)(y,\epsilon')(x,\epsilon)^{-1} = (x,\epsilon)(y,\epsilon')(-\epsilon x,\epsilon)\\
=&(x+\epsilon y,\epsilon\epsilon')(-\epsilon x,\epsilon) = (x+\epsilon y-\epsilon\epsilon'\epsilon x,\epsilon\epsilon'\epsilon)\\
=&(x+\epsilon y-\epsilon' x,\epsilon')
\end{aligned}$$

La classe de conjugaison de $(y,1)$ est donc l'ensemble des éléments de la forme $(\epsilon y,1)$. Si $n=2k$ est pair $(k,1)=(-k,1)$ et $(0,1)=(-0,1)$, les classes de conjugaison de $(k,1)$ et $(0,1)$ sont donc des singletons. Pour $y \in \mathbb{Z}/n\mathbb{Z}$, $y \neq 0, k$, la classe de conjugaison de $(y,1)$ est $\{(y,1),(-y,1)\}$. Si $n=2k+1$ est impair, pour $y \in \mathbb{Z}/n\mathbb{Z}$, $y \neq 0$, la classe de conjugaison de $(y,1)$ est $\{(y,1),(-y,1)\}$.

La classe de conjugaison de $(y,-1)$ est l'ensemble des éléments de la forme $(\epsilon y+2x,-1)$. Si $n=2k$, la parité d'un élément de $\mathbb{Z}/n\mathbb{Z}$ est bien définie car la parité d'un représentant ne dépend pas du choix de celuici. La parité de $\epsilon y+2x$ est celle de y, et tous les éléments de la forme $(y',-1)$ avec y' de même parité que y sont dans la classe de $(y,-1)$. On a donc dans ce cas deux classes de conjugaison : $\{(y',-1),\ y'\text{pair}\}$ et $\{(y',-1),\ y'\text{impair}\}$ toute deux de cardinal k. Si $n=2k+1$, tous les éléments de la forme $(y',-1)$ sont dans la classe de $(y,-1)$. On a dans ce cas une seule classe de cardinal $n=2k+1$.

Résumons, en donnant un représentant de chaque classe de conjugaison, et le cardinal de la classe :

Cas n=2k : $(0,1)$, 1 élément ; $(k,1)$, 1 élément ; $\{(y,1)\}$, 2 éléments, $y=1,\ldots,k-1$; $(0,-1)$, k éléments ; $(1,-1)$, k éléments.

Soit en tout $k+3$ classes de conjugaison.

Cas n=2k+1 : $(0,1)$, 1 élément ; $(y,1)$, 2 éléments, $y=1,\ldots,k$; $(0,-1)$, $2k+1$ éléments.

Soit en tout $k+2$ classes de conjugaison.

—3. On induit une représentation de dimension 1 d'un sous-groupe d'indice 2, donc la dimension de $\mathrm{Ind}_H^G(\chi)$ est 2. Pour $\chi=\chi_\alpha$, posons $\pi_\chi=\pi_\alpha$ et notons Θ_α le caractère de cette représentation. On calcule Θ_α sur chaque représentant des classes de conjugaison par la formule de l'exercice II.4.1.

Cas n=2k : $\Theta_\alpha((0,1))=2$; $\Theta_\alpha((k,1))=2(e^{i\pi\alpha})=2(-1)^\alpha$;
$\Theta_\alpha((x,1))=(e^{\frac{2i\pi\alpha x}{n}}+e^{\frac{2i\pi\alpha x}{n}})=2\cos\frac{2\pi\alpha x}{n}$, $x=1,\ldots,k-1$;
$\Theta_\alpha((x,-1))=0$.

Cas n=2k+1 : $\Theta_\alpha((0,1))=2$;
$\Theta_\alpha((x,1))=(e^{\frac{2i\pi\alpha x}{n}}+e^{\frac{2i\pi\alpha x}{n}})=2\cos\frac{2\pi\alpha x}{n}$, $x=1,\ldots,k$;
$\Theta_\alpha((x,-1))=0$.

On remarque qu'en fait la formule est toujours

$$\Theta_\alpha((x,1))=2\cos(\frac{2\pi\alpha x}{n}),\quad \Theta_\alpha((x,-1))=0,\quad x=0,\ldots,n-1.$$

On a $\Theta_\alpha=\Theta_{n-\alpha}$, donc les représentations π_α et $\pi_{n-\alpha}$ sont équivalentes.

On calcule maintenant $(\Theta_\alpha,\Theta_\alpha)$, $\alpha=0,\ldots,n$:

Cas n=2k :

$$\begin{aligned}(\Theta_\alpha,\Theta_\alpha)&=\frac{1}{2n}\left(2^2+2^2+\sum_{x=1}^{k-1}2\left(2\cos(\frac{2\pi\alpha x}{n})\right)^2\right)\\&=\frac{2}{k}\sum_{x=0}^{k-1}\cos^2(\frac{2\pi\alpha x}{n})\\&=\begin{cases}2 \text{ si } \alpha=0 \text{ ou } \alpha=k\\ 1 \text{ sinon}\end{cases}\end{aligned}$$

Cas n=2k+1 :

$$\begin{aligned}(\Theta_\alpha, \Theta_\alpha) &= \frac{1}{2n}\left(2^2 + \sum_{x=1}^{k} 2\left(2\cos(\frac{2\pi\alpha x}{n})\right)^2\right) \\ &= \frac{4}{n}\left(\left(\sum_{x=0}^{k}\cos^2(\frac{2\pi\alpha x}{n})\right) - \frac{1}{2}\right) \\ &= \begin{cases} 2 \text{ si } \alpha = 0 \\ 1 \text{ sinon}\end{cases}\end{aligned}$$

Ainsi, si $n = 2k$, les représentations π_α, $\alpha = 1, \dots k-1$ sont irréductibles, et inéquivalentes puisque leur caractères sont différents. De même pour les représentations π_α, $\alpha = 1, \dots k$ si $n = 2k+1$.

—4. On a d'après la réciprocité de Frobenius :

$$\mathrm{Hom}_G(\mathrm{Triv}_{\mathrm{G}}, \pi_0) \simeq \mathrm{Hom}_H(\mathrm{Res}_H^G(\mathrm{Triv}_{\mathrm{G}}), \chi_0) = \mathrm{Hom}_H(\chi_0, \chi_0) \simeq \mathbb{C}.$$

Ainsi, la multiplicité de la représentation triviale de G dans π_0 est 1. Comme π_0 est réductible de dimension deux, on a

$$\pi_0 = \mathrm{Triv}_G \oplus \rho_1$$

où ρ_1 est une représentation de dimension 1 dont le caractère est donné par

$$\Theta_{\rho_1}(x, \epsilon) = \Theta_0(x, \epsilon) - \Theta_{\mathrm{Triv}_G}(x, \epsilon) = \begin{cases} 2 - 1 = 1 \text{ si } \epsilon = 1 \\ 0 - 1 = -1 \text{ si } \epsilon = -1\end{cases}$$

—5. Pour $n = 2k$, on doit avoir $k+3$ représentations irréductibles, et l'on en a obtenu $(k-1)+2 = k+1$. Il en manque donc 2. D'autre part, leurs dimensions d_1, d_2 vérifient

$$2n = 4k = (k-1)2^2 + 1 + 1 + d_1^2 + d_2^2,$$

d'où $d_i = 1$, $i = 1, 2$. Il nous manque donc 2 représentations de dimension 1.

Pour $n = 2k+1$, on doit avoir $k+2$ représentations irréductibles, et l'on en a obtenu $k+2$.

—6. $(-1)^x$ est bien défini pour $x \in \mathbb{Z}/n\mathbb{Z}$ car la parité d'un représentant de x ne dépend pas du choix de celui-ci (deux représentants diffèrent d'un multipliple de $n = 2k$). De plus

$$\rho_2((x,\epsilon)(y,\epsilon')) = \rho_2(x+\epsilon y, \epsilon\epsilon') = (-1)^{x+\epsilon y} = (-1)^{x+y} = \rho_2((x,\epsilon))\rho_2((y,\epsilon')).$$

et donc ρ_2 est bien une représentation de dimension 1 de G.

On remarque que $\mathrm{Res}_{\mathrm{H}}^{\mathrm{G}}\rho_2 = \chi_k$, et donc par réciprocité de Frobenius

$$\mathrm{Hom}_G(\rho_2, \pi_k) \simeq \mathrm{Hom}_H(\chi_k, \chi_k) \simeq \mathbb{C}.$$

Ainsi, la multiplicité de ρ_2 dans π_k est 1. Comme π_k est réductible de dimension deux, on a

$$\pi_k = \rho_2 \oplus \rho_3$$

où ρ_3 est une représentation de dimension 1 dont le caractère est donné par

$$\Theta_{\rho_3}(x,\epsilon) = \Theta_k(x,\epsilon) - \Theta_{\rho_2}(x,\epsilon) = \begin{cases} 2(-1)^x - (-1)^x = (-1)^x \text{ si } \epsilon = 1 \\ 0 - (-1)^x = -(-1)^x \text{ si } \epsilon = -1. \end{cases}$$

—7. Résumons : pour $n = 2k$, on a $k-1$ représentations de dimension 2, π_α, $1 \leq \alpha \leq k-1$ et 4 representations de dimension 1, Triv_G, ρ_1, ρ_2, ρ_3.

Pour $n = 2k+1$, on a k représentations de dimension 2, π_α, $1 \leq \alpha \leq k$ et 2 représentations de dimension 1, Triv_G et ρ_1.

Exercice II. Groupes linéaires

—1. Soit $Z \in \mathrm{Lie}(Z(G))$, c'est-à-dire que pour tout $t \in \mathbb{R}$, $\exp tZ \in Z(G)$. On a donc pour tout $t \in \mathbb{R}$, pour tout $g \in G$,

$$\exp(tgZg^{-1}) = g \exp tZg^{-1} = \exp tZ.$$

Pour t assez petit, on se trouve dans le domaine où l'exponentielle est injective, et donc on en déduit $\mathrm{Ad}(g)\cdot Z = gZg^{-1} = Z$, pour tout $g \in G$. En prenant g de la forme $\exp sX$, on obtient

$$\mathrm{Ad}(\exp sX) \cdot Z = \exp s\mathrm{ad}(X) \cdot Z = Z, \quad (\forall X \in \mathfrak{g}, \forall s \in \mathbb{R}).$$

En dérivant par rapport à s et en évaluant en $s = 0$, on obtient

$$\mathrm{ad}(X) \cdot Z = 0, \quad (\forall X \in \mathfrak{g}).$$

Ainsi, $\mathrm{Lie}(Z(G)) \subset \mathfrak{z}$. Réciproquement, prenons $Z \in \mathfrak{z}$: pour tout $t \in \mathbb{R}$ et tout $X \in \mathfrak{g}$,

$$\mathrm{Ad}(\exp tZ)\cdot \exp X = \exp(\mathrm{Ad}(\exp(tZ))\cdot X) = \exp(\exp(t\,\mathrm{ad}(Z))\cdot X) = \exp X.$$

Ainsi, $\exp tZ$ commute avec les $\exp X$, qui engendrent G, et est donc dans $Z(G)$, ceci pour tout $t \in \mathbb{R}$. Ainsi $\mathfrak{z} \subset \mathrm{Lie}(Z(G))$.

—2. Pour tout $t \in \mathbb{R}$, pour tout $X \in X$, pour tout $Y \in V_i$,

$$\mathrm{Ad}(\exp tX) \cdot Y = \exp(t\,\mathrm{ad}(X)) \cdot Y \in V_i,$$

ce qui donne en différentiant et en évaluant en $t = 0$,

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

Ceci montre que V_i est un idéal de $\mathfrak{g}$. Soit J un idéal de $\mathfrak{g}$ contenu dans V_i. Alors $\mathrm{ad}(X) \cdot Y \in J$ pour tout $X \in \mathfrak{g}$, pour tout $Y \in J$, d'où

$$\mathrm{Ad}(\exp X) \cdot Y = \exp(\mathrm{ad}(X)) \cdot Y = \sum_{i=0}^{\infty} \frac{\mathrm{ad}(X)^n}{n!} \cdot Y \in J.$$

Comme G est engendré par les $\exp X$, on voit que J est une sous-représentation de G. Comme V_i est supposée irréductible, on a donc $J = \{0\}$ ou bien $J = V_i$.

—3. Il est clair que $[[\mathfrak{g}, \mathfrak{g}], \mathfrak{g}] \subset [\mathfrak{g}, \mathfrak{g}]$. Quels que soient $X, Y \in V_i$ et $Z \in \mathfrak{g}$,

$$[[X, Y], Z] = -[[Y, Z], X] - [[Z, X], Y] \in [V_i, V_i],$$

donc $[V_i, V_i]$ est un idéal de $\mathfrak{g}$.

—4. Comme pour tout $i \neq j$, $[V_i, V_j] \subset V_i \cap V_j = \{0\}$, on a $[V_i, \mathfrak{g}] = [V_i, V_i]$. Si $\dim V_i = 1$, alors bien sûr $[V_i, V_i] = 0$ et $V_i \subset \mathfrak{z}$. Si $\dim V_i > 1$, $[V_i, V_i]$ est un idéal de $\mathfrak{g}$ contenu dans V_i, et par 2, $[V_i, V_i] = 0$ ou $[V_i, V_i] = V_i$. La première possibilité est exclue, car ce qui précède montre qu'on a alors $V_i \subset \mathfrak{z}$, c'est-à-dire que G agit trivialement sur V_i. Tout sous-espace est alors une sous-représentation, et ceci contredit l'irréductibilité de V_i. Ainsi $[V_i, V_i] = V_i$. Ceci montre que $\mathfrak{z}$ est la somme des V_i de dimension 1 et que $[\mathfrak{g}, \mathfrak{g}]$ est la somme des V_i de dimension > 1, d'où

$$\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}] \oplus \mathfrak{z}.$$

—5. Soient $x, y \in G$. Comme G est connexe, x et y sont reliés à l'élément neutre, disons respectivement par des chemins $a(t)$ et $b(t)$, $t \in$

$[0,1]$, $a(0) = \mathrm{Id} = b(0)$, $a(1) = x$, $b(1) = y$. Le commutateur $xyx^{-1}y^{-1}$ est alors relié à Id par le chemin $a(t)b(t)a(t)^{-1}b(t)^{-1}$. Tout produit de commutateur est donc relié à Id, et (G, G) est connexe.

L'égalité

$$gxyx^{-1}y^{-1}g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1}$$

montre que le conjugué d'un commutateur est un commutateur, et donc que (G, G) est distingué.

—6. Quels que soient $t, s \in \mathbb{R}$, $X, Y \in \mathfrak{g}$,

$$\exp tX \exp sY \exp -tX \exp -sY \in (G, G)$$

et donc, en dérivant en t et en évaluant en $t = 0$, on obtient que pour tout $s \in \mathbb{R}$,

$$\mathrm{Id} - (\exp sY)X(\exp -sY) \in \mathrm{Lie}(G, G).$$

Comme $\mathrm{Lie}(G, G)$ est un espace vectoriel, en dérivant en s et en évaluant en $s = 0$, on voit que

$$YX - XY = [Y, X] \in \mathrm{Lie}(G, G).$$

Ainsi $[\mathfrak{g}, \mathfrak{g}] \subset \mathrm{Lie}(G, G)$.

—7. Pour tout $Z \in \mathfrak{z}$, pour tout $t \in \mathbb{R}$, $\exp tZ \in Z(G)$, et donc, comme W_j est irréductible, le lemme de Schur nous dit que $\pi_j(\exp tZ) = c_j(t)\mathrm{Id}_{W_j}$, où $c_j(t) \in \mathbb{C}^\times$. Bien sur $c_j(0) = 1$. Par définition

$$\begin{aligned} d\pi_{\mathrm{Id}}(Z) &= \frac{d}{dt}_{|t=0} \pi(\exp tZ) = \frac{d}{dt}_{|t=0} \oplus_{j=1,\dots,l} \pi_j(\exp tZ) \\ &= \frac{d}{dt}_{|t=0} \oplus_{j=1,\dots,l} c_j(t)\,\mathrm{Id}_{W_j} = \oplus_{j=1,\dots,l} c_j'(0)\,\mathrm{Id}_{W_j}. \end{aligned}$$

On a aussi

$$\begin{aligned} d\phi_{\mathrm{Id}}(Z) &= \frac{d}{dt}_{|t=0} \phi(\exp tZ) = \frac{d}{dt}_{|t=0} (\det(\pi_j(\exp tZ)))_{j=1,\dots,l} \\ &= \frac{d}{dt}_{|t=0} (\det(c_j(t)\mathrm{Id}_{W_j})_{j=1,\dots,l} = \frac{d}{dt}_{|t=0} (c_j(t)^{\dim W_j})_{j=1,\dots,l} \\ &= (c_j'(0)c_j(0)^{\dim W_j - 1}))_{j=1,\dots,l} = (c_j'(0))_{j=1,\dots,l} \end{aligned}$$

On voit que $d\phi_{\mathrm{Id}}(Z)$ est nul si et seulement si $d\pi_{\mathrm{Id}}(Z)$ est nul. or π est fidèle, c'est-à-dire injective, et il en est donc de même de $d\pi_{\mathrm{Id}}$. Ainsi $d\phi_{\mathrm{Id}}(Z)$ est nul si et seulement si Z est nul.

—8. On a

$$\begin{aligned} d\phi_{\mathrm{Id}}([X,Y]) = \frac{d}{dt}_{|t=0}\phi(\exp t[X,Y]) &= \frac{d}{dt}_{|t=0}(\det(\pi_j(\exp t[X,Y])))_{j=1,\dots,l} \\ (d\ \det)_{Id}((d\pi_j)_{\mathrm{Id}}([X,Y])) &= \mathrm{Tr}\,((d\pi_j)_{\mathrm{Id}}([X,Y])) \\ &= \mathrm{Tr}\,([(d\pi_j)_{\mathrm{Id}}(X),(d\pi_j)_{\mathrm{Id}}(Y)]) = 0. \end{aligned}$$

Ceci montre que $[\mathfrak{g},\mathfrak{g}] \subset \ker d\phi_{\mathrm{Id}}$.

Comme on a vu précédemment que $\mathfrak{g} = [\mathfrak{g},\mathfrak{g}] \oplus \mathfrak{z}$, et que $d\phi$ est injective sur $\mathfrak{z}$, on en déduit $\ker d\phi_{\mathrm{Id}} = [\mathfrak{g},\mathfrak{g}]$. D'autre part, on sait d'après le cours que $\ker d\phi_{\mathrm{Id}} = \mathrm{Lie}(\ker\phi) = \mathrm{Lie}(H) = \mathfrak{h}$, d'où $[\mathfrak{g},\mathfrak{g}] = \mathfrak{h}$.

—9. Le déterminant d'un commutateur est 1, donc $(G,G) \subset H$ et l'on en déduit $\mathrm{Lie}((G,G)) \subset \mathfrak{h} = [\mathfrak{g},\mathfrak{g}]$. Finalement, avec 6, ceci montre que $\mathrm{Lie}((G,G)) = [\mathfrak{g},\mathfrak{g}]$.

BIBLIOGRAPHIE

[1] A. Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[2] D. Bump. *Automorphic forms and representations*, volume 55 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[3] A. Robert. *Introduction to the representation theory of compact and locally compact groups*, volume 80 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.

[4] J.-P. Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, revised edition, 1978.

[5] S. Sternberg. *Group theory and physics*. Cambridge University Press, Cambridge, 1994.